PLAN ESTRATÉGICO DE SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

HOSPITAL DE COLLADO-VILLALBA

DIRECCIÓN SISTEMAS Y TIC

diciembre 2012

INDICE

1. INTRODUCCIÓN

El Plan Estratégico de Sistemas de Información y Comunicaciones establece el marco tecnológico, funcional y organizativo que se implantará en el Hospital de Collado-Villalba y que ha de dar respuesta al desarrollo de la función TIC en el Hospital.

El nuevo Hospital se concibe como una organización totalmente digitalizada, con tecnología avanzada tanto para el diagnóstico como para el tratamiento, que centra su gestión en torno a las necesidades de sus ciudadanos y pacientes.

El Hospital es de nueva constitución, por lo que el Plan de Sistemas ha de ir enfocado a diseñar la dotación inicial de todos los sistemas de información y las infraestructuras que han de darles soporte desde el momento de su apertura, definir cuál es el punto de partida y su evolución tecnológica en los próximos años.

Para la elaboración del Plan se ha conformado un equipo de especialistas en distintas áreas de trabajo que han trabajado de forma coordinada junto con la Dirección del Proyecto. Este equipo ha estado conformado por personal técnico del área de Sistemas y TIC.

Existen una serie de elementos condicionantes que determinan el Plan de Sistemas:

- Los objetivos estratégicos a corto y medio plazo de la organización.
- Requerimientos funcionales de la organización y de la relación con terceros, especialmente con la Consejería de Sanidad de la Comunidad de Madrid y los centros de ella dependientes.
- Las necesidades y requerimientos de los usuarios, en base a los procesos de negocio.
- Los escenarios tecnológicos existentes que aporten el menor riesgo, la mayor protección de las inversiones y los máximos beneficios para pacientes y profesionales.
- Los sistemas de información permitirán una informatización integral del Hospital y dar respuesta a las prescripciones recibidas de la Consejería de Sanidad de la Comunidad de Madrid (CSCM).

El presente Plan de Sistemas de Información deberá constituir una herramienta en evolución continua, de mejora en los procesos de negocio, optimizando la función informática y estableciendo las líneas estratégicas para los sistemas, con objeto de dar un soporte ágil y eficiente a las necesidades presentes y futuras de la organización.

Las áreas definidas en el Plan son las siguientes:

- La definición de las características técnicas de la dotación de infraestructuras de ubicación, físicas y lógicas que darán soporte a los sistemas de información y comunicaciones del Hospital, y la elaboración de la normativa e instrucciones para su utilización por los usuarios propios y externos.
- La definición de los sistemas de información a implantar en el Hospital, así como su integración con los sistemas de información de la CSCM.
- Los sistemas y servicios a habilitar orientados al ciudadano.

- El desarrollo y mantenimiento de sistemas y aplicaciones informáticas del Hospital y la formación de su personal en la utilización de los productos y/o equipos instalados, así como los servicios de soporte a usuarios.

- Adecuación para el cumplimiento con la LOPD y normativa de la AGPDM, en cuanto al tratamiento de la información mecanizada que contenga datos de carácter personal y/o confidencial.

- Definición de la función TIC en el Hospital para la materialización del Plan de Sistemas y la dotación y estructura del equipo a formar.

- Definición del plan de despliegue de todas las acciones e hitos necesarios para garantizar los requerimientos del Plan y la apertura del Hospital.

Capio garantiza la evolución tecnológica del Hospital, tanto en el marco de su relación e integración con los sistemas de la CSCM como en el de los propios sistemas de Capio, implantados en todos sus Hospitales y que proporcionan un importante valor añadido a la actividad hospitalaria. El Plan de Sistemas supone la materialización de este compromiso y de su evolución en el tiempo.

2. INFRAESTRUCTURA DE UBICACIONES

En este capítulo se describen las especificaciones técnicas de la infraestructura de locales técnicos que alojen todas las infraestructuras técnicas y de comunicaciones del Hospital, así como el espacio asignado a la función TIC dentro del mismo.

Las referencias seguidas para el diseño han sido las siguientes:

- EIA/TIA-942: "The Telecommunications Infrastructure Standard for Data Centers"
- EN 50173-5: Data Centre Cabling Overview
- Anexo IX Informática.pdf - Anexo relativo a los sistemas de Información y Comunicaciones del proceso
- Especificación de estándares de la Consejería de Sanidad de la CSCM.

El diseño de CPD y estructuras asociadas responde a la necesidad de dar respuesta a los siguientes requisitos básicos, que han de garantizar la normalidad en la actividad del Hospital.

- *Disponibilidad y Fiabilidad "24x7"*. El centro de datos debe estar diseñado para estar disponible y accesible la 24 horas del día, todos los días del año con una alta fiabilidad.
- *Seguridad***.** La seguridad afecta a todos los entornos del CPD. Seguridad sobre la información que se maneja, seguridad en los accesos físicos, seguridad en el estado ambiental de la sala, seguridad de los elementos de almacenamiento, etc.
- *Comunicaciones***.** Los centros de datos deben disponer de sistemas de comunicaciones altamente eficientes y redundantes, tanto para el interior como con el exterior.
- *Capacidad de evolución y ampliación.* Un CPD es un elemento vivo, por tanto, tiene que ser capaz de adaptarse a las nuevas necesidades que vayan surgiendo, así como a las futuras ampliaciones necesarias.
- *Gestión, Control y Monitorización***.** Todos los elementos, dispositivos y sistemas que incluye un CPD deberán permitir su gestión y monitorización.
- *Niveles de Servicio y recuperación***.** El CPD no debe ser susceptible a pérdidas de tiempo causadas por actividades no asociadas con su funcionamiento. Para ello se han determinado distintos niveles de disponibilidad.

Ubicaciones de infraestructuras

La arquitectura de servidores, sistemas de almacenamiento, elementos de comunicaciones y otros servicios del Hospital de Collado-Villalba está distribuida en tres ubicaciones físicas diferentes: CPD principal, CPD de backup y CPD corporativo de Capio, donde se alojan aplicaciones y servicios que se utilizarán en el Hospital.

El objeto de esta arquitectura es asegurar la disponibilidad de los servicios de manera acorde a la criticidad de cada uno de ellos, habilitando servidores en clúster, y la replicación de servicios/datos para minimizar los tiempos de parada y los tiempos objetivos de pérdida.

El CPD principal estará ubicado en el propio Hospital, dimensionado adecuadamente para la operativa diaria. Junto con el entorno de contingencia asegurará los niveles de servicio SLA y continuidad (TIERs) de cada servicio identificado.

Dicho CPD estará ubicado en la PLANTA BAJA del Hospital, por encima del sótano. Estará ubicado en espacios interiores, sin paredes adjuntas a los exteriores del edifico.

La ubicación del CPD de backup será EXTERNA al propio hospital. En este entorno se habilitarán aquellos servicios que permitan replicar/sustituir los servicios principales del Hospital en caso de caída/rotura de los servicios principales. Dentro de este entorno de mantendrán servicios replicados, en ocasiones de forma degradada respecto al servicio primario.

Las alternativas de localización para el CPD de BACKUP serán las siguientes:

- Edificio TELVENT (Avda. Valgrand,6 Alcobendas, Madrid), proveedor actual de Capio de servicios de hosting y Datacenter.
- CPD de otro Hospital de la red de CAPIO, interconectado por la red WAN de CAPIO.

Capio comunicará su decisión definitiva a la CSCM para validar conjuntamente las condiciones del CPD.

CPD corporativo de Capio: ubicado en edificio de Telvent (Avda. Valgrand,6 Alcobendas, Madrid), aloja una serie de aplicaciones y servicios compartidos por todos los Hospitales gestionados por Capio, entre ellos: servicio de correo electrónico y acceso a Internet, Gestión de RH y Nómina, DW, etc.).

Indicadores de Continuidad

Con las ubicaciones identificadas, se plantea a continuación una arquitectura lógica y física de servidores para cubrir los principales indicadores que se definen para cada servicio:

- TIER. Identificación del TIER recomendado para el servicio, acorde con el estándar TIA-942.
- Criticidad del servicio. Se definen cuatro niveles, usualmente coinciden con el TIER del punto anterior:
    - *No Críticos* – Sus funciones se pueden interrumpir durante un período relativamente largo, con poco o ningún costo.
    - *Sensitivos* – Sus funciones pueden ser ejecutadas manualmente durante un período relativamente largo, con coste de personal adicional. El coste de la interrupción es medio.
    - *Vitales* – Sus funciones pueden ser ejecutadas manualmente durante un período corto. Cierta tolerancia a interrupciones. El coste de interrupción es medio si la caída es inferior a 3 días.
    - *Críticos* – Sus funciones no pueden ser ejecutadas a menos que sean reemplazadas por recursos funcionalmente idénticos. No permiten métodos manuales y el coste de interrupción es muy alto.
- Disponibilidad del servicio. Contabilizada como un índice porcentual, se estimará como el tiempo que el servicio está disponible para los usuarios del total previsto, salvo paradas programadas. Por ejemplo: un 99,999% (cinco nueves) indica que el servicio estará indisponible (salvo paradas programadas) un máximo total de 5 minutos al año (total de todas las paradas no programadas)

- Punto objetivo de Recuperación (PR). Identificación el grado de actualización que requiere la información tras una pérdida del servicio. Por ejemplo: se debe tener una copia de los datos de cómo máximo de 12 h. de antigüedad
- Tiempo objetivo de recuperación (TR). Tiempo máximo de parada establecido. Por ejemplo, si se estiman 2 hr. de TR, el tiempo de indisponibilidad no debería superar las 2 horas

Independientemente, y de forma paralela, el plan de Calidad del Hospital elaborará y gestionará una serie de procedimientos de contingencia para realizar las tareas usuales del Hospital en caso de indisponibilidad completa de los sistemas de información afectados.

Dicho plan contemplará tanto las actuaciones en caso de parada programada de los servicios (actualizaciones, mantenimientos, etc.) como las interrupciones no planificadas (incidencias).

Distribución física CPD

La arquitectura de servicios y servidores que se describe en el capítulo *Equipamiento técnico* identifica los siguientes armarios del CPD y del entorno de CONTINGENCIA. Los armarios aquí dimensionados son susceptibles en variar en número para ajustarse al dimensionamiento detallado de servicios que lo requieran.

CPD HOSPITAL:

- RACK 1 – Armarios de servidores gama media y alta (en clúster con servidores de RACK 2) y la unidad de almacenamiento tipo SAN
- RACK 2 – Armario de servidores gama media y alta (en clúster con servidores de RACK 1) y la unidad de cintas para BACKUP
- RACK 3 – Armario de servidores gama baja

  Se habilitará espacio para al menos dos armarios adicionales con el objeto de permitir el crecimiento futuro de servicios del Hospital. En el capítulo *Requisitos técnicos* se describen los servidores y servicios dimensionados.
- RACK BackBone 1 – Electrónica de red de CPD (en réplica física con Rack BackBone 2). Incluirá un FIREWALL en clúster con el existente en el Rack Backbone 2 (contingencia). También contendrá Routers y Equipos Terminal de Cliente de las operadoras, para conexiones exteriores.

NOTA: El dimensionamiento de las plantas para la electrónica de red en armarios repartidores se comenta en el capítulo *Comunicaciones*.

CPD CONTINGENCIA:

- RACK 4 – Armario de servidores en contingencia y unidad de almacenamiento secundaria tipo SAN.
- Se habilitará espacio para al menos un RACK adicional si se requiriera para crecimientos futuros
- RACK BackBone 3 – En el entorno de contingencia existirán habilitados RACKS específicos para BACKBONE de comunicaciones
- RACK ComExt 2 – Existirá en el entorno de contingencia con interconexión con el Hospital, con CSCM, salida redundante a INTERNET, etc.

Diseño del CPD

Para atender los criterios requeridos para el CPD se detallan a continuación los parámetros seleccionados, de acuerdo con la recomendación para los entornos implicados en el diseño de un CPD. El EIA/TIA-942 los clasifica como Arquitectónico, Comunicaciones, Eléctrico y Mecánico.

1. Entorno arquitectónico

Localización

El CPD se ubicará en una de las salas habilitadas para el Dpto. de Informática. Se habilitará una sala entre 35 y 50 m2 para el CPD, junto a una sala de menores dimensiones que se habilitará para el sistema anti-incendios. Para la construcción del CPD se contemplarán las siguientes premisas de factores a evitar:

- Proximidad a maquinaria pesada, almacenes de productos inflamables, equipos de alta tensión (en un radio mínimo de 15 m.).
- Separado de ubicaciones próximas a paredes exteriores, salas de espera (vandalismo, sabotaje) (en un radio de 10 m).
- Ubicación en sótanos: riesgo de inundaciones, dificultad de acceso.
- Ubicación en última planta: accidentes aéreos, fuego, dificultad de acceso.
- Interferencias electromagnéticas: (estaciones de radio y TV, parques de alta tensión, etc.) → Se situará el CPD a más de 50 m. de distancia de la fuente de irradiación más cercana.
- Seguridad del entorno (vandalismo, sabotaje, etc.)

Espacios

El CPD tendrá suficiente espacio para alojar todos los equipos de comunicaciones necesarios y espacio extra para poder realizar la mayoría de las ampliaciones sin interrumpir el funcionamiento normal.

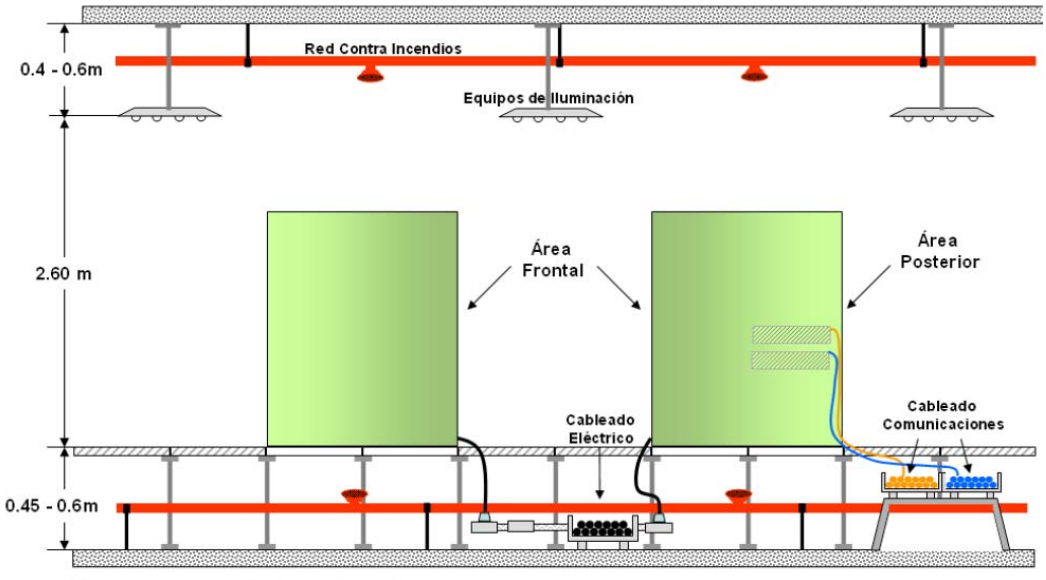
La separación en áreas se aprovechará para el control de acceso, reducción de los riesgos de incendio y control ambiental. Se habilitará la entrada al CPD sólo desde el entorno del personal de Sistemas de Información.

Se minimizarán las rutas entre las salas que permitan la propagación del fuego, humo, agua, gases o de explosiones (las rutas del cable se sellarán con materiales cortafuegos: masillas o espumas de silicona).

Los recintos también necesitarán alimentación eléctrica, HVAC (sistemas de calefacción, ventilación y aire acondicionado), protección contra incendios y rutas de acceso independientes.

- La altura mínima de la sala de suelo a techo será de 3 m. El piso tendrá un falso suelo de 300 milímetros (mínimo) y proporcionará el suficiente espacio libre para los equipos y racks.
- Las puertas de acceso tendrán un mínimo de 1 m. de ancho y 2,13 m. de alto.
- Se asegurará un espacio libre de al menos 1 m. alrededor de los equipos.

El siguiente croquis muestra los requerimientos de altura que deberá cumplir el CPD:



Tratamiento acústico

Los equipos ruidosos tales como equipos de aire acondicionado o equipos sujetos a gran vibración, estarán en una de las habitaciones anexas a la sala de servidores, de forma que tanto el ruido como las vibraciones se encuentren atenuados.

Suelo técnico

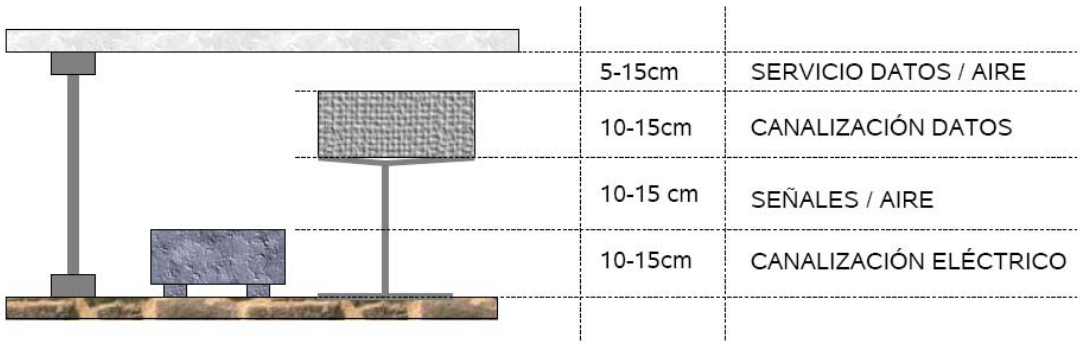
El espacio destinado al CPD dispondrá de suelo técnico, realizando si fuera necesario una rampa de acceso a la sala elevando toda la zona aproximadamente un mínimo de 30 cm. con la instalación del suelo técnico.

El suelo técnico está compuesto por baldosas y la estructura que las sustenta. Sus múltiples usos se basan en que por debajo de él puede transitar todo lo que comporta una instalación en general (cables de alimentación, cables de datos, fibras ópticas, cañerías de cualquier tipo, aire acondicionado, etc.).

El diseño del suelo técnico tendrá en cuenta las siguientes consideraciones:

- Sellado hermético.
- Modularidad precisa de las baldosas.
- Nivelado topográfico.
- Posibilidad de realizar cambios en la situación de las unidades.
- Debe cubrir los cables de comunicación entre la unidad central de proceso y los dispositivos periféricos, cajas de conexiones y cables de alimentación eléctrica.
- Deberá proporcionar seguridad al personal.
- Deberá permitir que el espacio entre los dos suelos actúe como una cámara llena de aire, que facilite el reparto de las cargas.

- La altura prevista será de 30 cm. (Recomendable para un área del CPD de menos de 100 m²). En caso extremo, la altura mínima podría ser de 25 cm. , a fin de que el aire acondicionado pueda fluir adecuadamente.
- Será de acero, de aluminio o madera resistente al fuego.
- Deberá estar soportado por pedestales con travesaños.



Baldosas

Según la norma para suelos deberán proporcionar una protección M2 o más favorable. Las condiciones de reacción al fuego a elementos constructivos se justificarán mediante la clase que figura en cada caso, conforme a la nueva clasificación europea.

Panel modular aglomerado de madera y resinas de alta densidad (700 Kg/m²), de 600x600 mm de lado con un espesor de 35mm.

Acabado interior en hoja de aluminio o acero y acabado superior en PVC, estratificado, linóleo, etc. "canteado" y autoextinguible.

La carga uniforme repartida será de hasta 1700 Kg. /m²

Control de accesos en la Sala

Se habilitará un sistema de control de acceso a la sala que permita:

- Evitar el acceso de personas no autorizadas
- Permitir la evacuación de las personas en caso de ser necesario
- Permitir trazabilidad de las personas del CPD

Se proveerá de un sistema de acceso mixto mediante tecleo de código de accesos y lectura de tarjeta (magnética o de proximidad). Se podrá optar el tecleo de código por un lector de huella digital.

El servicio tendrá las siguientes características:

- Lector de Huella/tarjeta operativo incluso sin alimentación eléctrica
- Conectado por red IP, con un servidor central para la generación de un repositorio del registro electrónico de presencia

- Acceso remoto al aplicativo del servidor para gestionar los permisos de acceso y acceder al registro electrónico. El acceso se realizará a través de un navegador web o de un aplicativo cliente específico

Paredes y techos

Las paredes del CPD tendrán un grado mínimo de resistencia al fuego de una hora (RF-60), proporcionando barrera contra el humo. Todos los materiales usados en la construcción de la sala de ordenadores serán incombustibles. Para controlar los daños por agua, todas las entradas del piso, de la pared y del techo estarán selladas.

Sala de operaciones

El CPD dispondrá de un lugar de trabajo destinado al personal informático que eventualmente puede ser usado, este lugar estará orientado de para maximizar la visión global del perímetro de la sala.

Estará dotado de lo indispensable para el trabajo para el personal informático, es decir, teléfono, ordenador, impresora, etc.

Se entiende como lugar de trabajo el conjunto de tomas de voz, datos y enchufes de SAI que se requieran según las necesidades.

Se deberá realizar un cerramiento de esta área teniendo en cuenta que no se debe perder de la visibilidad del interior del CPD. Se habilitará mediante mamparas de cristal y una climatización y ventilación independiente del la del CPD.

La sala de operaciones estará anexa al CPD, y tendrá visibilidad del CPD a través de una mampara de cristal de alta resistencia. Se habilitarán al menos 45 m2 para la sala de operaciones.

Sistema de vídeo vigilancia

Se habilitará un sistema de video-vigilancia CCTV con cámaras IP, integrado con un servidor, accesible desde uno o varios puestos de control de seguridad a través de un navegador web.

El servicio tendrá las siguientes características:

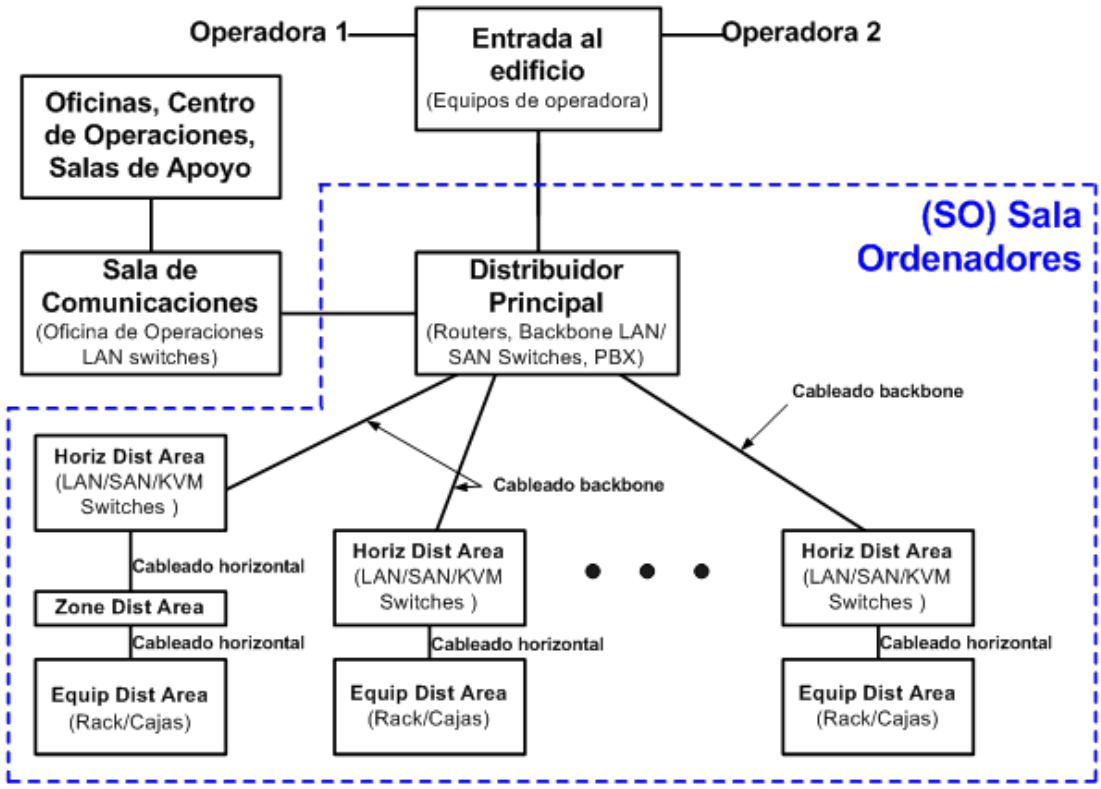
- Dos cámaras tipo minidomo interior, situadas una en la entrada al CPD, y otra panorámica del CPD
- Servidor central de recolección de grabaciones, con capacidad para grabar en modo “sensor de presencia”
- Acceso remoto al aplicativo del servidor y visualizador de imágenes a través de navegador web o aplicativo cliente.

2. Comunicaciones del CPD

NOTA: Ver Capítulo *Comunicaciones* para más detalle.

Distribución

El EIA/TIA-942 establece la topología típica de un CPD la del siguiente esquema:



Se definen las siguientes áreas y zonas:

- Entrada al edificio "Entrance Room" (ER): Es el espacio donde llegan las líneas y los equipos de la/s operadora/s. La ER (RITI) se habilitará en el sótano del edificio, y los equipos de operadora y cableado se establecerán en un RACK, a una altura elevada de al menos 1,5 m. sobre el nivel del suelo. En el caso de Collado-Villalba, se habilitará la entrada de (al menos) los siguientes elementos de operadora:
    - 2 conexiones de datos (redundantes) para la interconexión a Ethernet Gigabit con la CSCM
    - 2 conexiones de datos (redundantes) con la red central del licitador, para la gestión remota y comunicación con el CPD de Contingencia (si procede)
    - 3 conexiones de primario de voz (hasta 90 canales de voz)

- 1 conexión de primario de móviles
- Tantas líneas analógicas como se identifiquen requeridas por sistemas instalados de alarmas, ascensores, etc. (ver capítulo específico de Obra y Construcción).
- Adicionalmente, se habilitará otro RITS, para comunicaciones aéreas (satélite, TV, móviles) en la última planta (planta cubierta) del edificio-

- Sala de ordenadores "Computer Room" (CR)
- Distribuidor principal "Main Distribution Area" (MDA): Es el centro de distribución del sistema de cableado estructurado. El CPD dispondrá al menos de un MDA. Incluye los routers y switchs de backbone. Se habilitará dentro del CPD, en RACKS separados de los RACKS para los servidores.
- Sala de comunicaciones "Telecomunications Room" (TR): Es la zona desde donde se distribuye el cableado a las áreas externas al CPD. En Collado-Villalba, se combinará con el MDA, unificando una única área.
- "Horizontal Distribution Area" (HDA): Enumerados como Cajas repartidoras en el capítulo "Comunicaciones". Se habilitarán cuatro HDA en las planta BAJA, 1ª y 2ª del Hospital, y 2 HDA en la planta técnica (entre 2ª y 3ª) y otros dos HDAs (uno por torre), uno en la planta 7ª de una de las torres y otro en la planta 4ª de la otra torre. La distribución de las HDA se ha evaluado para asegurar la comunicación a menos de 90 m de distancia de cualquier punto de conexión del Hospital.
- "Equipment Distribution Area" (EDA): Es el espacio definido por los equipos finales como servidores, ordenadores, impresoras, etc.
- "Zone Distribution Area" (ZDA): Punto de consolidación. En la primera aproximación del CPD, se ha descartado este elemento, aunque es susceptible de incorporarse con la evolución futura del CPD

Firewall

Se habilitarán dos firewall habilitados en modo CLUSTER, y situados en racks separados de comunicaciones troncales (Backbone).

Cableado estructurado

El Sistema de Cableado Estructurado se define en el entorno de un CPD como el conjunto de elementos, incluido paneles de terminación, módulos, conectores, cable y cables de asignación, instalados y configurados para proporcionar conectividad principalmente de datos desde los repartidores hasta las rosetas o puntos de planta que dan servicio al equipamiento situado en el CPD (Host, servidores, dispositivos de almacenamiento, electrónica de red, etc.).

En la tabla siguiente podemos ver las distintas aplicaciones de red que podríamos encontrar en un CPD y los distintos medios que las transportan. Se indica con fondo azul las soluciones que se han preseleccionado para el CPD de Collado-Villalba, aunque se admitirán las otras opciones aceptables.

Aplicación	Medio	ANSI Cat.	ISO Class	Distancia	Apli CPD
Cable Cobre					
10Gbase-T	Par trenzado	Cat.6A	E_A	100m.	Seleccionado
Fibra					
10Gbase-S	F.O. OM3 MM	850nm	50/125 µm	300m.-550m.	Seleccionado
Soporte PoE					
PoE plus	Par trenzado	Cat. 6A		30W a 55W	Seleccionado

La instalación cubrirá las recomendaciones del EIA/TIA-942 de los siguientes medios:

- Cobre 4 pares trenzados 100Ω Cat.6
- Fibra óptica multimodo 50/125 a 850nm láser optimizado
- Utilización de "trunk" multifibra preconectorizados entre racks.

Debido al uso de la red IP para los sistemas de control (cámaras de vigilancia, sensores, controles de acceso), se asumirán tomas de cableado (EO) para estos elementos que no están asociados a puestos de trabajo. Dentro de la definición de la red se habilitarán redes virtuales y sistemas de gestión independientes sobre dichas redes virtuales (VLAN).

Se implantarán sistemas con paneles de cableado "inteligentes" para disponer de un sistema preciso de administración de la red de cableado, que permitan gestionar estos entornos de forma separada y ágil.

Espacio para la ubicación de las entradas de líneas directas de operadores

El CPD dispondrá de un espacio específico dedicado para la ubicación de las líneas directas de los operadores "Entrance Room" (ER), tanto para voz como para datos, el espacio estará situado en una zona interconectada a los racks de comunicaciones, para el enlace con los mismos y se cumplirán los siguientes requerimientos:

Introducción y normativa ICT

Se establecen los requisitos que, desde un punto de vista técnico, cumplirán las canalizaciones, recintos y elementos complementarios que alberguen la infraestructura común de telecomunicaciones (ICT) para facilitar su despliegue, mantenimiento y reparación, contribuyendo de esta manera a posibilitar que los usuarios finales accedan a los servicios de telefonía disponible al público y servicios de comunicaciones de banda ancha, acceso sin hilos (SAFI) que se requieren para la realización de su labor profesional.

Las redes de alimentación de los distintos operadores se introducen en la ICT, a través de la arqueta de entrada y de las canalizaciones externas de enlace, atravesando el punto de entrada general del inmueble y por su banda superior a través del pasamuros y de la canalización de enlace, hasta los registros principales situados en los recintos de instalaciones de telecomunicaciones, donde se produce la interconexión con la red de distribución de la ICT.

Desde el punto de vista del dominio en el cual están situados los distintos elementos que componen la ICT, se establece la siguiente división:

a) *Zona exterior del inmueble:* en ella se encuentran la arqueta de entrada y la canalización externa.

b) *Zona común del inmueble:* donde se sitúan todos los elementos de la ICT comprendidos entre el punto de entrada general del inmueble y los puntos de acceso del usuario (ER)

c) *Zona privada del inmueble:* la cual comprende los elementos de la ICT que conforman la red interior de los usuarios.

Canales, bandejas y sus accesorios:

Los sistemas de conducción de cables tendrán como características mínimas, para aplicaciones generales, las indicadas a continuación:

*Características Canales/Bandejas. L*os canales cumplirán la norma UNEIX EN 50085 y las bandejas la norma UNEIX EN 61537.

Registros de terminación de red. Las mediciones mínimas serán en mm, provisto de tapa. Estos registros se instalarán a más de 200 mm y menos de 2300 mm del suelo.

Canalización interior de usuario. Donde se realice mediante canales, estas serán de material plástico, en montaje superficial o enrasado, uniendo los registros de terminación de red con los distintos registros de toma. Dispondrán, como mínimo, de 3 espacios independientes que alojarán únicamente servicios de telecomunicación, uno para TB+RDSI, otro para TLCA+SAFI y otro para RTV.

El dimensionamiento de la canalización se realizará con canal de material plástico de 100x500 con tres tabiques separadores.

Requisitos de seguridad entre instalaciones. Se procurará la máxima independencia entre las instalaciones de tele-comunicaciones y el resto de servicios. Los cruces con otros servicios se realizarán preferiblemente pasando las canalizaciones de tele-comunicaciones por encima de las de otro tipo.

Los requisitos mínimos serán los siguientes:

a) La separación entre una canalización de telecomunicaciones y las de otros servicios será, como mínimo, de 100mm para trazados paralelos y de 30 mm para cruces.

b) Si las canalizaciones interiores se realizan con canales para la distribución conjunta con otros servicios que no sean telecomunicaciones, cada uno de ellos se alojará en compartimentos diferentes. La rigidez dieléctrica de los tabiques de separación de estas canalizaciones conjuntas deberá tener un valor mínimo de 15KV/mm (según norma UNEIX EN 60243). Si son metálicas, se les dará tierra.

Canalizaciones

Para el soporte y protección mecánica del cableado, se usará en las zonas visibles, canaleta tanto para la pared como para el suelo según el tramo correspondiente. Consideraciones técnicas sobre las canalizaciones:

- La canalización se realizará por debajo del suelo técnico.
- La distribución por el suelo técnico se realizará teniendo en cuenta el criterio de pasillos fríos y calientes. La canalización de los cables de potencia por el pasillo frío y en la parte baja del espacio del suelo técnico y los cables de comunicaciones por el pasillo caliente y en la parte alta del espacio del suelo técnico.
- Las canalizaciones se sobredimensionarán como mínimo un 30% para futuras ampliaciones.
- El recorrido de la canalización se realizará para minimizar la longitud del cable.
- En la instalación de canaleta y tubo se usarán los elementos accesorios tales como codos, tapas, uniones, que el fabricante de cada elemento recomienda.
- La canalización se realizará de manera que el cable no sea visible en ninguna parte del trazado.
- Los productos situados en el interior de falsos techos o suelos elevados, como es el caso que nos ocupa, deberán serán mínimo de clase M1.

Las canalizaciones deben de ser adecuadas para asegurar que el cable sea instalado sin afectar a sus prestaciones. La separación de las líneas eléctricas seguirá las especificaciones que se detallan a continuación:

- La separación entre los cables de diferentes sistemas debe ser tan grande como sea posible, pero el espacio disponible siempre tiene limitaciones.
- Los sistemas especialmente sensibles o sistemas que emitan interferencias deben ser identificados y diseñados con los requisitos adecuados a las normas del fabricante. En el caso de que el cableado cercano a la zona de Radiología (o cualquier otra zona con emisiones electromagnéticas) no supere los umbrales mínimos definidos, se optará por cablear con cable APANTALLADO de las mismas características de transmisión esitmadas
- Todos los cabes deben ser fácilmente identificables, para el mantenimiento y futuras modificaciones.
- La separación con cableado eléctrico será de suficiente separación (>1,5m) o se habilitarán las adecuadas barreras protectoras.
- La distribución por el suelo técnico se realizará teniendo en cuenta el criterio de pasillos fríos y calientes.

Electrónica de red

La electrónica de backbone a implementar en el CPD se definirá para cumplir los siguientes requisitos básicos: Altas prestaciones, alta disponibilidad, gestionable, redundante, escalable, flexible.

Se habilitará electrónica de red con PoE (Power over Ethernet) no sólo para la telefonía IP sino también para cámaras de videovigilancia, sensores y controles de acceso. Para los elementos alimentados por POE con funciones mecánicas se habilitará electrónica de red con POE Plus.

Ver descripción de la electrónica de red en el capítulo *Comunicaciones*.

Racks

Los racks de comunicaciones cumplirán las siguientes especificaciones:

- Medidas exteriores: 2.000 x 800 x 1000 (alto, ancho, fondo) y 42 U de altura.
- Materiales: Construido en chapa de acero los laterales y puerta posterior.
- El techo, base y las cuatro columnas exteriores en chapa de acero laminado en frío.
- Soporte de equipos de 19".
- Puertas laterales de fácil manejo a la hora de montar y desmontar.
- Acceso de cables por la parte superior e inferior.
- Techo provisto para ser elevado para ventilación.
- Bastidor robusto y ligero de montaje en suelo diseñado para cubrir todos los requisitos necesarios para la gestión del Sistema de Cableado Estructurado.
- Armadura inferior que tiene forma de aspa para ofrecer máxima flexibilidad para el encaminamiento de cables desde la base o la parte superior del rack.
- El diseño debe permitir montar el armario después de tender el cable, al contrario que los rack de base rectangular, donde todos los cables deben atravesar la armadura inferior, con este diseño se puede maniobrar más fácilmente sobre el bastidor y manejar e instalar el cable de una manera sencilla.
- Opcionalmente dispondrá de bandejas verticales de gestión de cables en el interior de rack (en uno o ambos laterales) para facilitar el encaminamiento de los mismos, para reducir el tiempo de instalación y mejorar la calidad de la misma.
- Soporta de hasta 250 Kg. El diseño del bastidor minimizará el riesgo de dañar el cableado de entrada del rack.
- Todos los productos se fabricarán de acuerdo con la norma ISO-9002 y estarán diseñados y desarrollados según la norma ISO-9001.
- Los bastidores cumplirán las normas internacionales para equipos electrónicos de 19" DIN 41494 IEC297.
- Unidades de ventilación adicionales de 1U que no ocupen espacio libre en rack.
- Sistema pivotante incorporado para la nivelación del rack en las 4 columnas.
- Bandejas adicionales desplazables en profundidad (con disponibilidad de ranuras para ventilación) para soporte de equipos de hasta 35 Kg que no cumplan los estándares de 19" i ETSI.
- Dispondrán de base de enchufes tipo shucko. (5 o 9 enchufes)

3. Entorno Mecánico

Climatización

Las unidades de climatización se calculan para un funcionamiento continuo de 24h/día y 365 días/año y su potencia frigorífica para un temperatura inferior de 24º será capaz de mantener las características de las salas para las variaciones de temperatura ambiental medias actuales y para el 120% de la carga total de los locales (carga eléctrica + aportaciones de los locales + iluminación + presencia no continua de personas en sala).

Se proveerá un sistema de ventilación y aire acondicionado separado que se dedique al CPD de forma exclusiva, que permitan mantener que los valores de temperatura y humedad, en condiciones normales de trabajo, estén lo más próximas a las siguientes:

Temperatura: 22ºC (+/- 2ºC)

Humedad relativa: 45 a 55%.

Eficiencia de filtrado: 5 micras

Se habilitará un dispositivo de alarma que se active cuando la temperatura y humedad registradas en la sala del CPD estén fuera de los límites señalados, éste se deberá de conectar al sistema general de alarma del edificio.

Para la climatización del CPD se habilitarán dos unidades de climatización en redundancia.

Capacidad del equipo de aire acondicionado

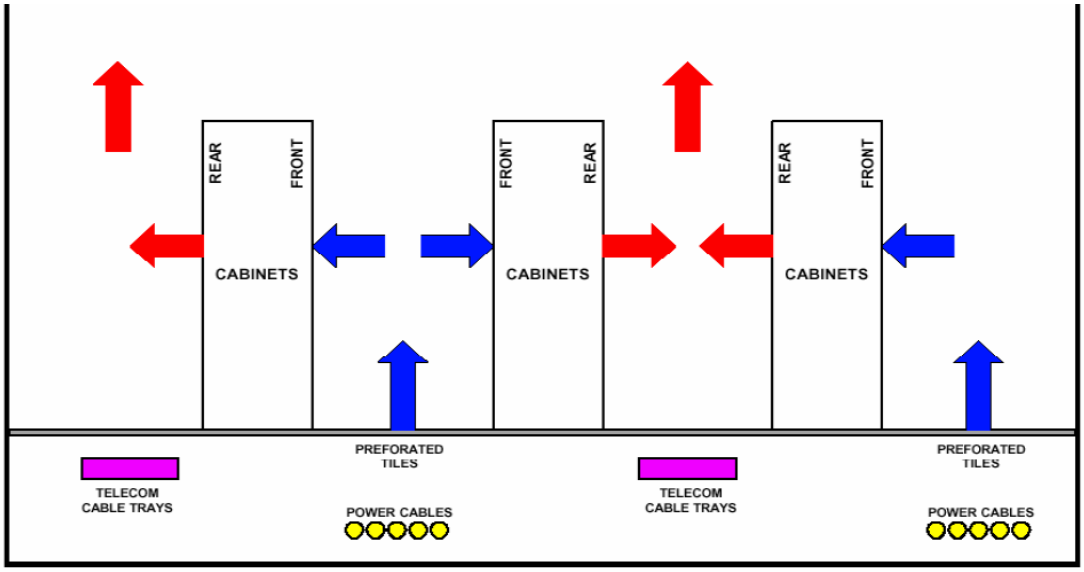
Se consideran estos aspectos para dimensionar el sistema de aire acondicionado:

- Disipación térmica de las maquinas
- Cargas latentes, aire de renovación
- Perdidas por puertas y ventanas
- Transmisión de paredes, techos y suelo
- Disipación de otros aparatos
- El aire acondicionado para la sala CPD debe ser independiente del aire general del edificio
- El calor disipado por los diferentes elementos del CPD obliga a necesitar aire frío todo el año

Distribución por suelo técnico

El espacio entre el suelo del edificio y el suelo técnico se utiliza como una cámara plena de aire. Todo el aire se descarga en la sala a través de registros en el suelo. El aire retorna a la unidad acondicionadora por rejillas en el techo.

La distribución del equipamiento y los racks se realizará de formando pasillos FRIOS y CALIENTES sobre el suelo técnico, como se muestra en la figura de abajo. Esto permite, además, diferenciar los tendidos de cable según su función y voltaje: los cables de potencia coincidiendo con los pasillos fríos y los cables de comunicaciones y control coincidiendo con los pasillos calientes.



Se incluirá el siguiente equipamiento:

Instalación de dos equipos de aire acondicionado redundantes de aprox. 18 KW. Cada equipo debe ser suficiente para mantener la sala a 20ºC:

- Ambos equipos conmutarán entre sí de forma automática en caso de fallo.
- Los equipos deben tener entrada de aire por parte superior y salida por parte delantera inferior.
- Se habilitará sistema de monitorización a través de conexión LAN Ethernet
- El sistema de Aire acondicionado se conectará a un sistema de SAI para asegurar alimentación continuada en caso de caída eléctrica específico
- El sistema de refrigeración dispondrá de su propio cuadro eléctrico
- Equipos propuestos: Se proponen dos equipos cen redundancia con sistema automático de balanceo, similares en características a los siguientes: LIEBERT HPM S20DA

Contaminantes

La concentración de partículas en el aire es una medida útil para determinar la calidad en el ambiente del CPD. En el Hospital de Collado-Villalba de respetarán los límites sugeridos por la TIA/EIA 942-2005 para los contaminantes más comunes de un CPD y se adecuará su control a la política que defina la CSCM.

Sistema contra incendios

El CPD dispondrá de un sistema propio de detección de incendios y de extinción.

Dentro del CPD, los riesgos se reducirán al mínimo colocando las impresoras, u otros elementos susceptibles de generar ignición, lejos de otros equipos y servidores. En la medida de lo posible, todos los elementos de estas características quedarán fuera de la sala de servidores.

Las paredes del CPD tendrán un grado mínimo de resistencia al fuego de una hora (RF-60), y deberán proporcionar barrera contra el humo.

Todas las puertas de acceso tendrán una ventana con cerramiento propio. Los materiales usados en la construcción de la sala de ordenadores deberán ser incombustibles.

Para controlar el daño por agua, todas las entradas del piso, de la pared y del techo deben estar selladas.

No habrá componentes químicos de extinción por polvo seco en el área de los ordenadores.

Extintores de incendio

Los extintores manuales contra el fuego serán de dióxido de carbono u otros gases con agentes de extinción. Se colocaran en lugares visibles y accesibles, próximos a los puntos donde se estime mayor probabilidad de iniciarse el incendio y en las salidas de evacuación. Estarán colocados sobre soportes fijados a paramentos verticales, de manera que la parte superior del extintor quede, como máximo a 1,70 sobre el suelo.

Se colocarán al menos dos extintores de incendios en la sala de ordenadores, uno cercano a la puerta y otro cercano a los elementos del Backbone de comunicaciones.

Puerta ignífuga con barra antipánico

El CPD dispondrá de una única puerta de entrada/salida, con las siguientes especificaciones:

- Material ignífugo, cortafuegos RF-60-90.
- Barra antipánico y ojo de buey.
- Marco tres lados de acero galvanizado de 1,5mm. Acabado con imprimaciones + protector.
- Junta termoexpandible en marco.
- Garra de fijación (6 uds).
- 1 o 2 hojas de acero de 62mm de espesor acabada con imprimaciones + film protector.
- 2 bisagras, una de ellas con muelle resorte de cerramiento semiautomático.
- 1 punto antipalanca.

Armario ignífugo para el material de alta importancia

Las copias de back-up y los servidores de respaldo, también contarán con protección ante eventuales riesgos que puedan afectar el servicio que deben proporcionar. Se habilitarán armarios ignífugos para datos, rack y equipos, para proporcionar protección ante agentes externos como incendios, explosiones, acceso, gases, radiaciones y daños criminales.

Se habilitará una sala/armario con combinación de acero, células de hormigón y materiales especiales que absorben el calor, aseguran el mayor nivel de seguridad. Se asegurará el nivel de seguridad S120 DIS. El armario ignífugo estará equipado con un tipo de cerramiento hermético de auto sellado ante agentes agresivos externos (gas, fuego, agua, etc.).

La sala de seguridad con armario ignífugo no estará anexa al CPD, pero sí al área de operaciones del personal de TI. Contará con acceso diferenciado desde el área de operaciones.

Control de inundaciones

Se habilitará un detector de inundación con alarma en el CPD, ya que la ausencia de estos lectores supone la existencia de un riesgo muy elevado de pérdida de equipos en caso de producirse una inundación.

Se evitará la construcción del CPD en el sótano para reducir riesgo de inundaciones.

Monitorización del entorno

Como medida de seguridad de la infraestructura instalada, se dispondrá de un gestor centralizado de las variables ambientales del CPD. Dicho elemento medirá al menos las siguientes variables ambientales: temperatura, humedad.

También se habilitará un sistema detector de caídas capaz de detectar y reportar averías eléctricas como caídas de circuitos y ausencia de tensión eléctrica de compañía.

Se incluirá sistema de monitorización de red basado en Cisco Works (ver apartado *Suministro y puesta en marcha de plataformas y sistemas de monitorización y gestión* en capítulo *Comunicaciones*) y servidores basado en CISCO Works.

Los servidores incluirán el software de administración HP Insight Management WBEM Providers for Windows Server 2003/2008.

Además, se incluirá el sistema de monitorización de Sistemas para los servidores NAGIOS versión 3.x (o de mismas funcionalidades). Se integrará con el sistema de gestión de red anterior. Se integrará con los sistemas de monitorización de SAIs, Climatización.

4. Sistema Eléctrico

Instalación eléctrica

El CPD es el mayor consumidor de alimentación y fuente de calor, por lo que la provisión de sistemas de respaldo como grupos electrógenos, sistemas de alimentación ininterrumpida (SAI), tienen gran importancia.

Para el suministro eléctrico al CPD, se utilizará una línea independiente del resto de la instalación para evitar interferencias, con elementos de protección y seguridad específicos, siempre a través de SAI, y en combinación con grupos electrógenos.

La instalación debe contar con un cuadro específico para los Servicios de Información. Se certificará la calidad de la toma de tierra, y estará dimensionado para futuros crecimientos, con espacio libre del 30%. Además se habilitará cuadro específico para el sistema climatizador del CPD.

Acometida

La acometida se realizará con multiconductor concéntrico que permite reducir la emisión de campo magnético respecto al uso de conductores monopolares. Se utilizarán canalizaciones metálicas de aluminio sobre hierro u otros materiales. Se prefiere que las acometidas eléctricas de alimentación a los cuadros se ejecuten por los bordes exteriores de las salas.

Cuadros

Se instalará un doble armario eléctrico dedicado para el CPD del que colgarán todos los elementos críticos, seccionados con protecciones de altas prestaciones como bloques diferenciales súper inmunizados. Los materiales (interruptores, magnetotérmicos, diferenciales, etc.) se instalarán con las últimas tecnologías para la conexión en caliente.

Se habilitará un segundo cuadro eléctrico, independiente del de SAI, para los sistemas y equipos que no requieran alimentación de SAI. Cada SAI habilitado tendrá su propio cuadro eléctrico separado.

Distribución

Las líneas desde el cuadro de distribución se realizarán por canalizaciones de cable, por la zona baja del falso suelo, se llevarán hasta tres líneas, una de cada fase, a los equipos críticos y a los racks de servidores y como mínimo una línea para cada equipo o grupo homogéneo de equipos.

Como en el resto del Hospital, se dotará al CPD de enchufes de corriente eléctrica de SAI y no SAI para los diferentes equipos que se puedan conectar a la red eléctrica temporal o provisionalmente.

Las tomas de enchufes de No SAI estarán diferenciadas de las de SAI por su color, y su uso estará dedicado a posibles herramientas eléctricas.

Toda la instalación cumplirá, tanto los materiales como su ejecución, con el Reglamento Electrotécnico para la Baja Tensión (REBT).

Iluminación

El alumbrado general proporciona una iluminación uniforme sobre el área iluminada, distribuyendo las luminarias de forma regular por todo el techo de la sala.

- La iluminación tendrá la alimentación diferenciada de los equipos instalados en el CPD.
- Del 100% de la iluminación se deberá destinar el 25% para la iluminación de emergencia y se conectará al sistema de alimentación ininterrumpida o al grupo electrógeno si lo hubiese.

Niveles de iluminación

Se aplicarán lo siguientes niveles medidos a 1m sobre la superficie acabada del falso suelo en la mitad de dos filas de equipos.

Sistema de alimentación ininterrumpida

El SAI es un elemento imprescindible en un CPD para evitar las caídas intempestivas de la alimentación eléctrica en los equipos y sistemas del CPD.

El SAI se dimensionará para permitir un funcionamiento normal del equipamiento del CPD (backbone, electrónica de red, servidores, equipamiento Hardware) de mínimo 15 minutos desde la caída de la alimentación eléctrica. Se dimensionará para dar soporte hasta un 30% más de la potencia estimada consumida por el CPD, y cumplirá las siguientes características:

- Tipo ON-LINE, onda de salida sinusoidal
- Esquema: "Doble conversión" o "Conversión Delta". También pueden ser rotativos.
- Alto rendimiento
- Baja re-inyección armónica con distorsión de corriente de entrada inferior al 5%.
- Transformador con aislamiento galvánico.
- By-Pass estático automático.
- Elevada capacidad de sobrecarga: En funcionamiento normal y en by-pass.
- Capacidad de añadir equipos en paralelo.
- Capacidad de redundancia.
- Autonomía: Entre 20 minutos y 1 hora
- Gestionable SNMP.
- Posibilidad de conexión a paneles remotos de diagnóstico.
- Diseñado y fabricado de conformidad con las normas de protección y seguridad. (IEC950/ EN50091-1, UL1778, CE) de compatibilidad electromagnética (EN55022-B, VDE0160, EN50082-1) norma de calidad ISO 9001.

Para el entorno propuesto se habilitarán dos equipos SAI de características similares (o superiores) a los siguientes: Emerson Liebert serie NX de 20 KVA TRI/TRI, con baterías de plomo hermético con una autonomía de 30 minutos, con tarjeta de comunicación OC WebCard para monitorización remota vía protocolo SNMP y HTTP. La monitorización de los SAIs se integrará con el sistema NAGIOS de monitorización.

Toma de tierra

Todo el equipamiento de servidores, racks, cajas eléctricas y cableado eléctrico del CPD sea adaptará a la normativa vigente y seguirá las mismas recomendaciones generales del Hospital en lo relativo a las tomas de tierra.

3. EQUIPAMIENTO TÉCNICO

En este capítulo se describe el esquema de arquitecturas técnicas y de servidores y sistemas de almacenamiento para los Servicios Tecnológicos y de Sistemas de Información asociados a la gestión y soporte del Hospital.

Las referencias seguidas para el diseño han sido las siguientes:

- ITIL v3 - ITIL V3 Foundation Handbook
- EIA/TIA-942: "The Telecommunications Infrastructure Standard for Data Centers"
- Anexo IX Informática.pdf - Anexo relativo a los sistemas de Información y Comunicaciones del proceso
- Especificación de estándares de la Consejería de Sanidad de la CSCM.

Descripción de Servicios

A continuación se enumeran los servicios que se establecerán en la provisión de Sistemas de Información, y que se describen y detallan más adelante. Otros servicios que puedan surgir se adaptarán a infraestructuras similares a las propuestas.

Sistemas de Información Hospitalarios

Servicios Generales

- Telefonía y servicios de voz
- Servicios de colaboración e Intranet corporativa
- Repositorio documental / de archivos
- Servicio de acceso a Internet
- Correo electrónico corporativo
- Web pública del Hospital
- Servicios FTP
- Extranet
- Gestión de Identidad Corporativa / Usuarios
- Cuadro de Mando / DSS / EIS
- Gestión de Seguridad LOPD

Servicios específicos técnicos

- Servicios básicos Internet (TCP/IP) – DHCP / Directorio Activo / DNS / Gateway
- Servicios de Seguridad y gestión de Usuarios y Dominios
- Servicios de BACKUP e Imágenes
- Servicio de Actualizaciones
- Servicio Antivirus
- Monitorización (Cisco Works + HP Insight + NAGIOS)
- Gestión del Servicio: HelpDesk, Incidencias/Problemas, Gestión del Cambio, Inventario
- Servicio gestión de Red
- Despliegue del servicio: Gestión de la capacidad, continuidad, disponibilidad
- Servicios de virtualización de servidores.

Servicios de Seguridad

Sistema de videovigilancia

Se habilitará un sistema de video-vigilancia CCTV mediante dispositivos cámaras IP, integrado con un servidor único, accesible desde uno o varios puestos de control de seguridad a través de un navegador web.

El servicio tendrá las siguientes características:

- Cámaras tipo minidomo, interiores, situadas en los puntos de control que se definan, y en todos los puntos que requieran control de acceso
- Cámaras de exterior, fijas, situadas en los exteriores del Hospital y zonas abiertas (parking, etc.)
- Cámaras móviles, con motor de direccionamiento, situados en los puntos críticos que lo requieran
- Servidor central de recolección de grabaciones, con capacidad para grabar en modo "sensor de presencia"
- Acceso remoto al aplicativo del servidor y visualizador de imágenes a través de navegador web o aplicativo cliente. Posibilidad para configurar el servicio para rotar secuencialmente por imágenes, bajo demanda del usuario o en caso de detección de movimiento
- Gestión segura de usuarios y acceso al aplicativo, con protocolos seguros (https). A ser posible, integrado con seguridad de Directorio Activo

Sistema de Control de Acceso/Presencia

Se habilitará un sistema de control de accesos integrado que permita gestionar los puntos de acceso críticos (CPD, Farmacia, Laboratorio, etc.) mediante el uso de dispositivos lectores de tarjeta/lectores de huella.

El servicio tendrá las siguientes características:

- Lectores de Huella/tarjeta operativo incluso sin alimentación eléctrica
- Conectado por red IP, con un servidor central para la generación de un repositorio del registro electrónico de presencia
- Acceso remoto al aplicativo del servidor para gestionar los permisos de acceso y acceder al registro electrónico. El acceso se realizará a través de un navegador web o de un aplicativo cliente específico
- Gestión segura de usuarios y acceso al aplicativo, con protocolos seguros (https). A ser posible, integrado con seguridad de Directorio Activo

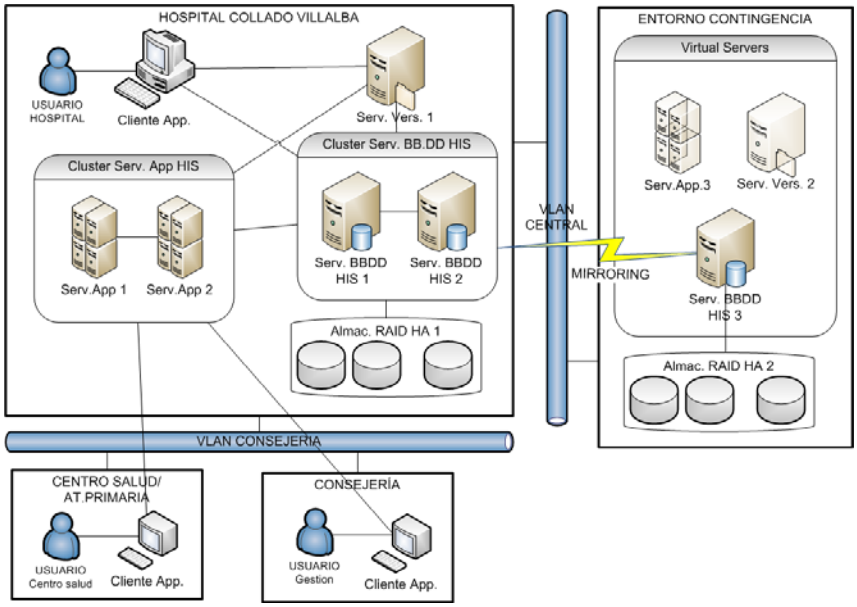
Infraestructura básica

A continuación se describen los principales servicios y la infraestructura propuesta para cada uno de ellos. Para cada servicio se han incluido los indicadores estimados de continuidad, de acuerdo a lo establecido en el capítulo *Infraestructura de Ubicaciones*.

Todas las infraestructuras básicas aquí descritas son propuestas validadas en entornos productivos actuales similares del licitador. En todo caso, se requerirá un análisis más detallado que permita ajustarse a los requerimientos específicos del Hospital en tiempo y forma.

Sistema de Información Hospitalario (HIS)

El diseño lógico establecido para este servicio es la siguiente:



Para cubrir esta arquitectura los servidores propuestos son los siguientes:

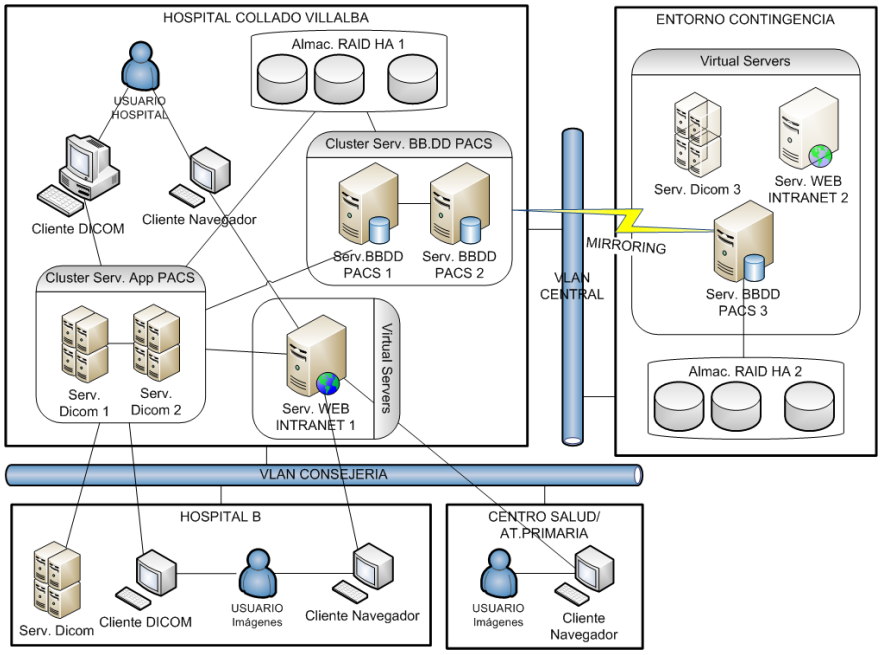
- Serv. Versiones 1 – Despliegue de actualizaciones y configuración del HIS → Servidor gama baja
- Serv. App.1 / Serv. App. 2 – Servidor de Aplicaciones → 2 Servidores gama media en CLUSTER
- Serv.BBDD HIS 1 / Serv. BBDD HIS 2 – Servidores de Bases de datos → 2 servidores gama alta en CLUSTER
- SERVIDORES VIRTUALIZADOS:
    - Serv. App 3 – Imagen detenida (iniciar bajo demanda) de aplicaciones. Gama media
    - Serv. Vers. 2 – Imagen detenida del servidor de actualizaciones y configuración del HIS. Gama baja.
    - Serv. BBDD HIS 3 – Imagen iniciada (ejecuta en paralelo) del servidor de BBDD → Replicación mediante MIRRORING o LOG SHIPPING con el clúster principal. Gama media

Los indicadores de continuidad para este servicio son los siguientes (se considera disponibilidad salvo paradas controladas/programadas):

INDICADOR	VALOR	COMENTARIOS
TIER	3	
Criticidad	Vital	
Disponibilidad	99,9%	Anual (8:40 h. /año)
Máximo número de paradas	4	Anuales
Máximo tiempo por parada	1 hr.	
Máximo tiempo parada acumulado	8 hr.	Anual
Punto Recuperación (PR)	1 hr.	
Tiempo Recuperación (TR)	1 hr.	

Servicio de Transmisión de Imagen Digital (PACS)

La arquitectura de servidores establecida para este servicio es la siguiente:



El servidor WEB se extiende con la funcionalidad relativa a Visor de Imágenes avanzado por WEB. Para cubrir esta arquitectura los servidores propuestos son los siguientes:

- Serv. Dicom 1 / Serv. Dicom 2 – Servidor de Aplicaciones DICOM. → 2 Servidores gama media en CLUSTER
- Serv.BBDD PACS 1 / Serv. BBDD PACS 2 – Servidores de Bases de datos → 2 servidores gama media en CLUSTER
- SERVIDORES VIRTUALIZADOS:

- Serv. Web Intranet 1 – Imagen iniciada. Servidor WEB, habilita interfaz Web del PACS → Servidor virtual gama baja
- Serv. Web Intranet 2 – Imagen detenida. Servidor WEB de respaldo. Servidor virtual gama baja
- Serv. Dicom 3– Imagen detenida del servidor de aplicaciones DICOM. Gama baja
- Serv. BBDD PACS 3 – Imagen iniciada (ejecuta en paralelo) del servidor de BBDD. Replica en modo WARM mediante réplica espejo o LOG SHIPPING de SQL SERVER 2005 con el cluster principal. Gama baja

Los indicadores de continuidad para este servicio son los siguientes (se considera disponibilidad salvo paradas controladas/programadas):

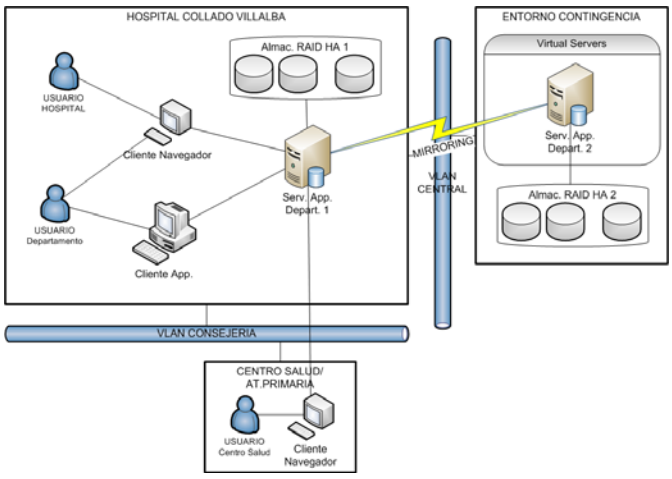
INDICADOR	VALOR	COMENTARIOS
TIER	3	
Criticidad	Vital	
Disponibilidad	99,9%	Parada/Año: 8:40 hr.
Máximo número de paradas	4	Anuales
Máximo tiempo por parada	2 h.	
Máximo tiempo parada acumulado	8 h.	Anual
Punto Recuperación (PR)	2 h.	
Tiempo Recuperación (TR)	2 h.	

Sistemas Departamentales

Dentro de esto servicios se engloban todos aquellos aplicativos o servicios de carácter departamental, que tendrán una infraestructura similar a la presentada.

Dentro de esta categoría se pueden englobar los siguientes servicios: Laboratorio, Banco de Sangre, Anatomía Patológica, y en general aquellos servicios que se requieran similares funciones.

La arquitectura de servidores establecida para estos servicios es la siguiente:



Para cubrir esta arquitectura los servidores propuestos son los siguientes:

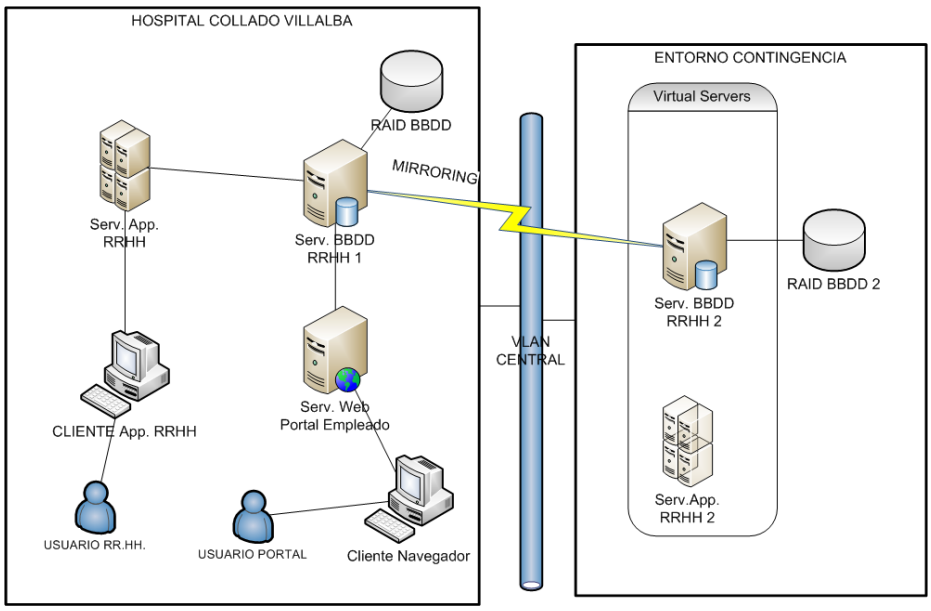
- Serv. App Depart. 1 – Servidores de Bases de datos y Aplicación → 1 servidor Gama media
- SERVIDORES VIRTUALIZADOS:
  - Serv. App Depart. 2 – Imagen iniciada (ejecuta en paralelo) del servidor anterior. Replica en modo WARM mediante réplica espejo o LOG SHIPPING con el servidor principal. Gama baja.

Los indicadores de continuidad usuales para estos servicios serán los siguientes (se considera disponibilidad salvo paradas controladas/programadas):

INDICADOR	VALOR	COMENTARIOS
TIER	3	
Criticidad	Vital	
Disponibilidad	99,9%	Parada/Año: 8:40 h.
Máximo número de paradas	4	Anuales
Máximo tiempo por parada	2 h.	
Máximo tiempo parada acumulado	8 h.	Anual
Punto Recuperación (PR)	4 h.	
Tiempo Recuperación (TR)	2 h.	

Servicio RR.HH. y Nóminas

La arquitectura de servidores establecida para este servicio es la siguiente:



Este servicio se ofrecerá en modo centralizado, como servicio compartido. Para cubrir esta arquitectura los servidores propuestos son los siguientes:

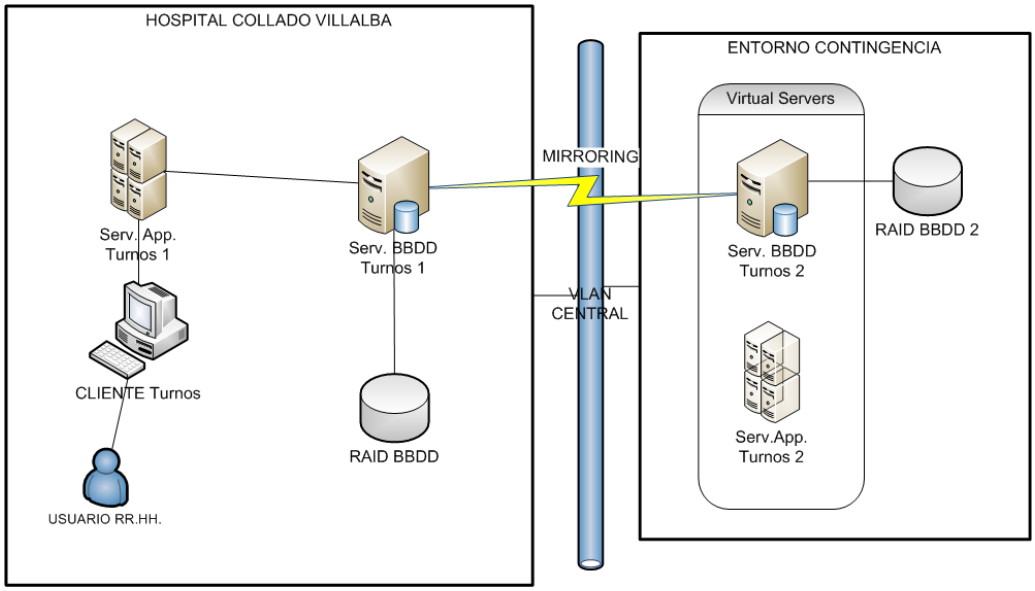
- Serv. App RRHH – Servidores de Aplicaciones → Gama media
- Serv. BBDD RRHH 1 – Servidor de BBDD → Gama media
- Serv. Web Portal Empleado – Servidor capa acceso Web. Gama Baja
- SERVIDORES VIRTUALIZADOS:
    - Serv. App. RRHH 2 – Imagen detenida. Servidor de respaldo. Gama baja
    - Serv. BBDD RRHH 2 – Imagen iniciada (ejecuta en paralelo) del servidor de BBDD. Replica en modo WARM mediante réplica LOG SHIPPING con el servidor principal. Gama baja

Los indicadores de continuidad para este servicio son los siguientes (se considera disponibilidad salvo paradas controladas/programadas):

INDICADOR	VALOR	COMENTARIOS
TIER	2	
Criticidad	Sensitivo	
Disponibilidad	99,45%	Parada/Año: 2 Días
Máximo número de paradas	8	Anuales
Máximo tiempo por parada	8 hr.	
Máximo tiempo parada acumulado	48 hr.	Anual
Punto Recuperación (PR)	6 hr.	
Tiempo Recuperación (TR)	8 hr.	

Servicio Gestión Turnos Enfermería

La arquitectura de servidores establecida para este servicio es la siguiente:



Este servicio se ofrecerá en modo centralizado, como servicio compartido. Para cubrir esta arquitectura los servidores propuestos son los siguientes:

- Serv. App. Turnos 1 – Servidores de aplicación → Gama alta
- Serv. BBDD Turnos 1 – Servidor de BBDD → Gama media
- SERVIDORES VIRTUALIZADOS:
  - Serv. App. Turnos 2 – Imagen detenida. Servidor de respaldo. Gama media
  - Serv. BBDD Turnos 2 – Imagen iniciada (ejecuta en paralelo) del servidor de BBDD. Replica en modo WARM mediante réplica espejo o LOG SHIPPING con el servidor principal. Gama baja

Los indicadores de continuidad para este servicio son los siguientes (se considera disponibilidad salvo paradas controladas/programadas):

INDICADOR	VALOR	COMENTARIOS
TIER	2	
Criticidad	Sensitivo	
Disponibilidad	99,45%	Parada/Año: 2 Días
Máximo número de paradas	8	Anuales
Máximo tiempo por parada	8 hr.	
Máximo tiempo parada acumulado	48 hr.	Anual
Punto Recuperación (PR)	24 hr.	
Tiempo Recuperación (TR)	8 hr.	

Servicios Comunes Correo / Acceso a Internet

Se habilitarán los servicios de correo electrónico y acceso a Internet que se requiera para la ejecución normal de las labores profesionales de los empleados del Hospital.

Los indicadores de continuidad para estos servicios serán los siguientes (NOTA: se considera disponibilidad salvo paradas controladas/programadas):

INDICADOR	VALOR	COMENTARIOS
TIER	3	
Criticidad	Crítico	
Disponibilidad	99,85%	Parada/Año: 13 hr.
Máximo número de paradas	6	Anuales
Máximo tiempo por parada	2,5 hr.	
Máximo tiempo parada acumulado	13 hr.	Anual

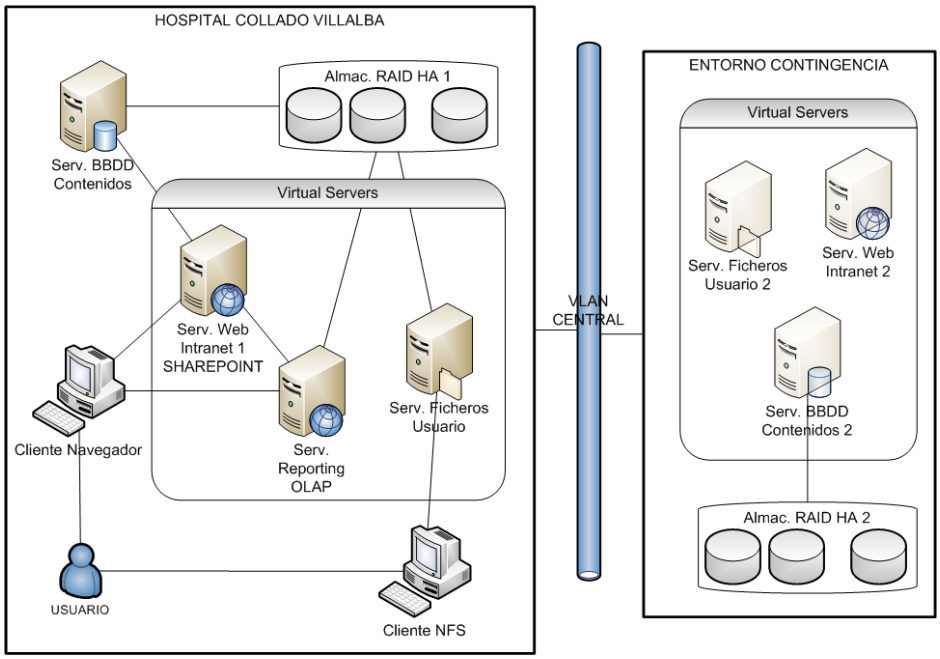
Punto Recuperación (PR)	4 hr.	
Tiempo Recuperación (TR)	2,5 hr.	

Servicios INTRANET / Gestión Contenidos / Colaboración

Dentro de este grupo se engloban los siguientes servicios:

- Servicio INTRANET
- Servicio Colaboración/gestión documental (sobre Sharepoint Portal Services v.3)
- Servicio de Almacenamiento de Ficheros de Usuarios (sobre Network File System)

La arquitectura de servidores para este servicio es la siguiente



Para cubrir esta arquitectura los servidores propuestos son los siguientes:

- Serv. BBDD Contenidos → Servidor de Base de Datos, proporciona almacenamiento para los contenidos del servidor Sharepoint de INTRANET, y otras aplicaciones internas web. Gama media
- SERVIDORES VIRTUALIZADOS:
  - Serv. Web INTRANET 1 → Ofrece servicio de INTRANET (Web) y herramientas de colaboración mediante Servicios Sharepoint Services v.3. Ofrece también capa WEB para el servidor de reporting OLAP. Gama media
  - Serv. Reporting OLAP → Servidor de Informes y análisis OLAP. Ofrece servicios analíticos de información y toma de decisiones. Gama media
  - Serv. Ficheros Usuario → Servidor virtual de unidades compartidas de ficheros de usuarios/grupos. Ofrecerá almacenamiento para los usuarios del hospital. Las carpetas

compartidas por grupos permite trabajo colaborativo, de forma complementaria a los servicios colaborativos Sharepoint. Gama baja

- Serv. Ficheros Usuario 2 → Imagen detenida. Servidor de contingencia para el servicio de ficheros. Gama baja
- Serv. Web INTRANET 2 → Imagen detenida. Servidor virtual de contingencia para el servicio de Intranet (Web) y Contenidos. Gama baja
- Serv. BBDD Contenidos 2 → Imagen detenida, Servidor virtual de contingencia para el servidor BBDD de contenidos. Gama baja

Los indicadores de continuidad para los servicios Serv. Web INTRANET Sharepoint son los siguientes (se considera disponibidad salvo paradas controladas/programadas):

INDICADOR	VALOR	COMENTARIOS
TIER	2	
Criticidad	Sensitivo	
Disponibilidad	99,45%	Parada/Año: 2 Días
Máximo número de paradas	8	Anuales
Máximo tiempo por parada	8 hr.	
Máximo tiempo parada acumulado	48 hr.	Anual
Punto Recuperación (PR)	24 hr.	
Tiempo Recuperación (TR)	8 hr.	

Los indicadores de continuidad para los servicios de Reporting y Análisis OLAP son los siguientes (se considera disponibidad salvo paradas controladas/programadas):

INDICADOR	VALOR	COMENTARIOS
TIER	1	
Criticidad	No Crítico	
Disponibilidad	98%	Parada/Año: 7 días
Máximo número de paradas	10	Anuales
Máximo tiempo por parada	24 hr.	
Máximo tiempo parada acumulado	7 días	Anual
Punto Recuperación (PR)	24 hr.	
Tiempo Recuperación (TR)	24 hr.	

Servicios EXTRANET / Integración WS

Estos servicios son conceptualmente similares a los anteriores, pero se separan y definen en servidores diferentes y específicos porque:

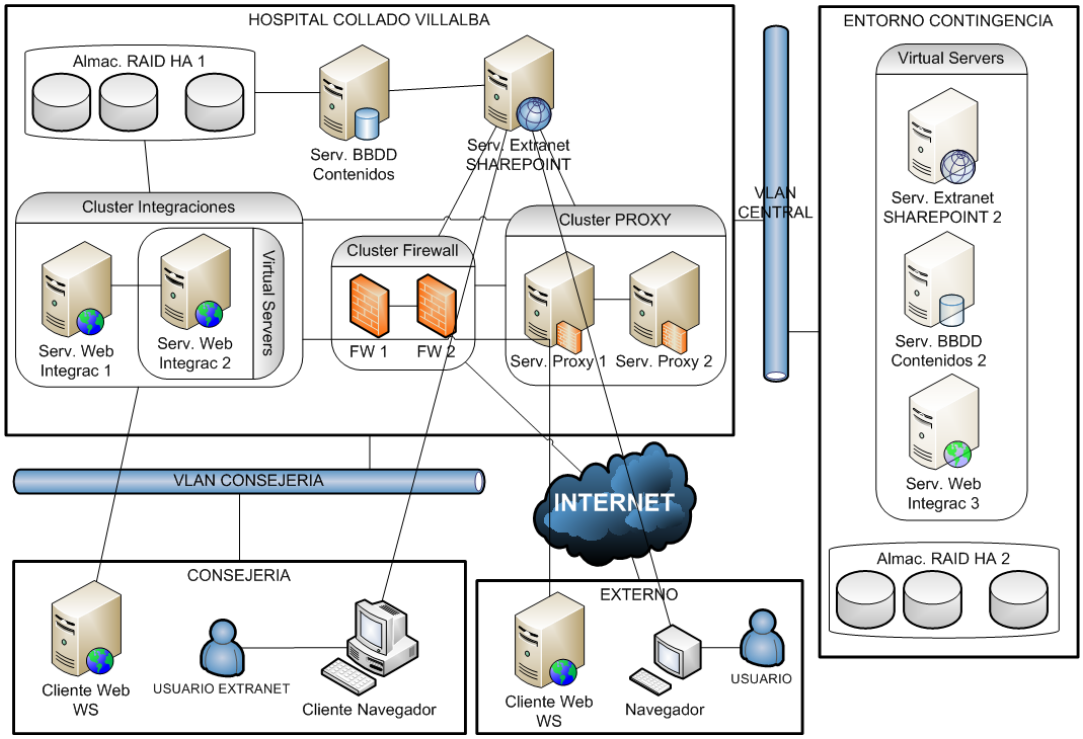
a) Suponen servicios de comunicación/integración con terceros, por lo que su criticidad es distinta (usualmente, mayor)

b) Mayoritariamente a través de redes públicas (internet), por lo que requieren incluir protocolos y mecanismos de seguridad más estrictos, tales como certificados públicos, y es recomendable separarlos de entornos de acceso interno

c) En el caso de comunicaciones externas con terceros, todas las comunicaciones externas con estos servicios irán a través del clúster de Firewalls y PROXY habilitado al efecto en la DMZ

d) En el caso de comunicaciones a través de VLAN específicas (p.e. con la CSCM, se habilitará a través del clúster de Firewalls

La arquitectura lógica de estos servicios se muestra a continuación:



Los servidores identificados para proporcionar estos servicios son:

- Serv. BBDD Contenidos → Servidor de Base de Datos SQL SERVER 2005, proporciona almacenamiento para el servidor Sharepoint de EXTRANET (compartido con el servidor BBDD de contenidos de INTRANET). Gama media
- Serv. Extranet Sharepoint → Servidor de servicios Sharepoint Portal Services, incluye gestión de certificados. Servicios de tipo web para terceros externos. Gama baja

- Serv. Web Integrac 1 → En cluster con el servidor virtual Serv. Web Integrac 2. Cluster de Servicios WEB e integraciones. La implementación de los servicios web se adatará a los protocolos HL7 (principalmente), SNOMED y CIE. En caso de evolucionar hacia una plataforma middleware de integración específica (p.e. Biztalk) se implementaría sobre este cluster de servidores. Gama media
- NOTA: Estos servidores crecerán horizontal y verticalmente para asegurar los servicios de integración que se definan y aquellos nuevos que se requieran.
- SERVIDORES VIRTUALIZADOS:
    - Serv. Web Integrac 2 → Imagen en ejecución. En cluster con el servidor Serv. Web Integrac 1. Cluster de Servicios WEB e integraciones. Gama media
    - Serv. Web Integrac. 3 → Imagen detenida. Imagen de servidor de contengencia para el servicio de integraciones. Gama media
    - Serv. Extranet Sharepoint 2 → Imagen detenida. Servidor virtual de contingencia para el servicio de Extranet (Web) y Sharepoint. Gama baja
    - Serv. BBDD Contenidos 2 → Imagen detenida, Servidor virtual de contingencia para el servidor BBDD de contenidos. Gama baja

Los indicadores de continuidad para los servicios Serv. Web Extranet Sharepoint son los siguientes (se considera disponibidad salvo paradas controladas/programadas):

INDICADOR	VALOR	COMENTARIOS
TIER	2	
Criticidad	Sensitivo	
Disponibilidad	99,45%	Parada/Año: 2 días
Máximo número de paradas	8	Anuales
Máximo tiempo por parada	8 hr.	
Máximo tiempo parada acumulado	2 días	Anual
Punto Recuperación (PR)	24 hr.	
Tiempo Recuperación (TR)	8 hr.	

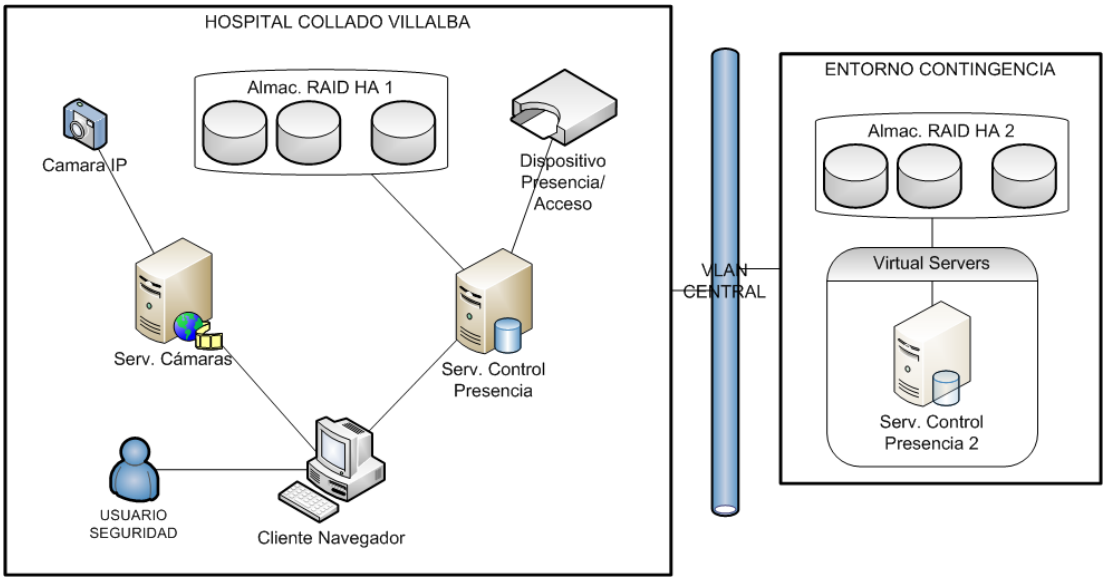
Los indicadores de continuidad para los servicios Serv. Integraciones son los siguientes:

INDICADOR	VALOR	COMENTARIOS
TIER	3	
Criticidad	Vital	
Disponibilidad	99,85%	Anual (13 hr. /año)

Máximo número de paradas	6	Anuales
Máximo tiempo por parada	2,5 hr.	
Máximo tiempo parada acumulado	13 hr.	Anual
Punto Recuperación (PR)	1 hr.	
Tiempo Recuperación (TR)	2,5 hr.	

Servicios de Seguridad

Entendiéndose seguridad los elementos de control de acceso/presencia y videovigilancia, la arquitectura que se propone es la siguiente:



Los servidores que se habilitarán para ofertar este servicio son los siguientes:

- Serv. Cámaras → Servidor web y de almacenamiento de imágenes/vídeo, centralizará la recolección de grabaciones de las cámaras IP desplegadas en el Hospital. Gama media
- Serv. Control Presencia → Servidor de BBDD asociado al registro del control de presencia/acceso y réplica centralizada de la información de identificaciones de acceso y gestión de seguridad de los dispositivos implantados, integrados por IP. El servicio de seguridad de accesos podrá estar integrado con el Directorio activo. Gama baja
- SERVIDORES VIRTUALIZADOS:
    - Serv. Control Presencia → Imagen detenida. Imagen de contingencia para el servidor de control de acceso/presencia. Gama baja

NOTA: Dado el volumen previsible de vídeo/imágenes a almacenar, el servidor de cámaras contará con su propio almacenamiento independiente del almacenamiento RAID HA del Hospital.

NOTA 2: Los dispositivos de control de presencia deberán poder gestionarse centralizadamente a través del servidor controlador, pero deberán poder funcionar de forma independiente y autónoma en caso de pérdida de conexión con el servidor.

Los indicadores de continuidad para los servicios Serv. Cámaras son los siguientes (se considera disponibilidad salvo paradas controladas/programadas):

INDICADOR	VALOR	COMENTARIOS
TIER	2	
Criticidad	Sensitivo	
Disponibilidad	99,45%	Parada/Año: 2 Días
Máximo número de paradas	8	Anuales
Máximo tiempo por parada	8 hr.	
Máximo tiempo parada acumulado	48 hr.	Anual
Punto Recuperación (PR)	24 hr.	
Tiempo Recuperación (TR)	8 hr.	

Los indicadores de continuidad para los servicios Serv. Control Presencia son los siguientes (se considera disponibilidad salvo paradas controladas/programadas):

INDICADOR	VALOR	COMENTARIOS
TIER	2	
Criticidad	Sensitivo	
Disponibilidad	99,45%	Parada/Año: 2 Días
Máximo número de paradas	8	Anuales
Máximo tiempo por parada	8 hr.	
Máximo tiempo parada acumulado	48 hr.	Anual
Punto Recuperación (PR)	24 hr.	
Tiempo Recuperación (TR)	8 hr.	

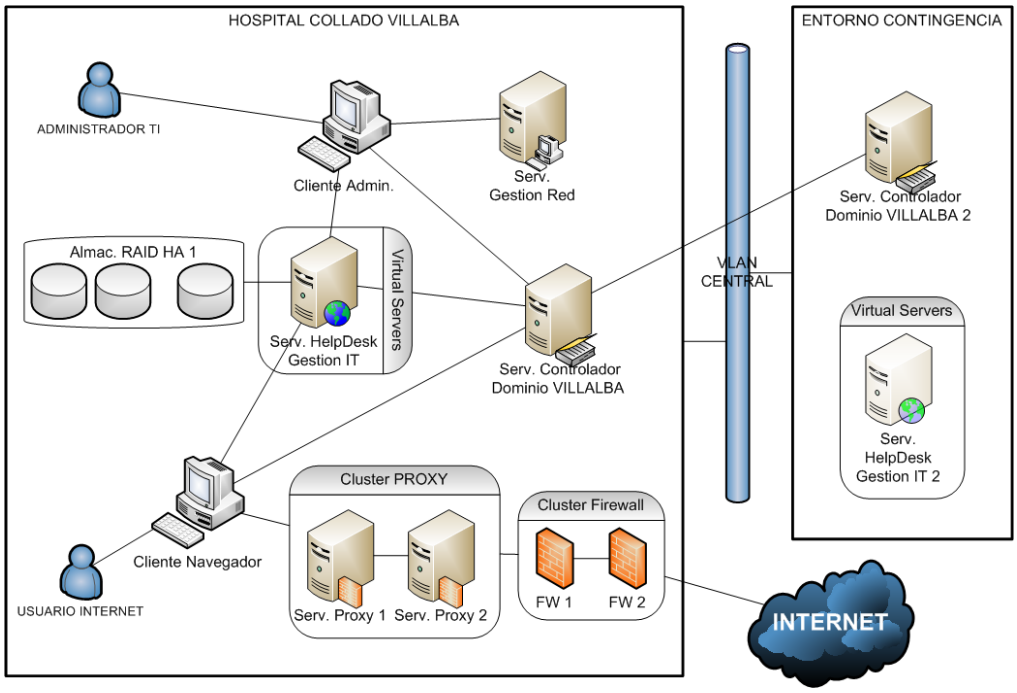
Servicios Comunes

Dentro de los servicios comunes se enumeran aquellos servicios de bajo nivel TCP/IP, o globales de servicios de TI. Se incluyen los siguientes:

- Servidores de administración de paneles/rack, tanto para el Hospital como para el de Contingencia (no presentados en la infraestructura)

- Servidores de Herramientas de Gestión de Red y Monitorización (Cisco Works, Nagios o similares)
- Controlador de Dominio / DNS / DHCP
- Servidor de HelpDesk / Incidencias / Gestión del servicio → (Herramienta SysAID o similar)

El siguiente cuadro muestra la arquitectura de servidores para estos servicios:



Los servidores que se habilitarán para ofertar estos servicios son los siguientes:

- Serv. Admin Racks/Paneles → Servidor(es) de administración. Gama baja
- Serv. Gestión Red → Servicios de monitorización de red LAN, gestión de WIFI, servicios de soporte y alertas NAGIOS, etc. Gama baja
- Serv. Controlador Dominio COLLADO → Controlador de Dominio, DNS, DHCP, servidor de licencias. Será un controlador secundario, sincronizado con el servidor primario de la red completa. Gama baja
- Serv. Controlador Dominio COLLADO 2 → Servidor de contingencia para los servicios anteriores. Gama baja
- SERVIDORES VIRTUALIZADOS:
    - Serv. HelpDesk Gestión IT 1 → Imagen ejecutada. Servicios de gestión del servicio (HelpDesk, Incidencias, Gestión del cambio, etc.). Gama baja
    - Serv. HelpDesk Gestión IT 2 → Imagen detenida. Imagen de contingencia para el servidor de HelpDesk. Gama baja

Los indicadores de continuidad para los servicios Serv. Gestión Red son los siguientes (se considera disponibilidad salvo paradas controladas/programadas):

INDICADOR	VALOR	COMENTARIOS
TIER	2	
Criticidad	Sensitivo	
Disponibilidad	99%	Parada/Año: 3 Días
Máximo número de paradas	10	Anuales
Máximo tiempo por parada	12 hr.	
Máximo tiempo parada acumulado	72 hr.	Anual
Punto Recuperación (PR)	24 hr.	
Tiempo Recuperación (TR)	12 hr.	

Los indicadores de continuidad para los servicios Controlador Dominio son los siguientes:

INDICADOR	VALOR	COMENTARIOS
TIER	3	
Criticidad	Crítico	
Disponibilidad	99,9%	Parada/Año: 8 hr.
Máximo número de paradas	4	Anuales
Máximo tiempo por parada	2 hr.	
Máximo tiempo parada acumulado	8 hr.	Anual
Punto Recuperación (PR)	1 hr.	
Tiempo Recuperación (TR)	2 hr.	

Los indicadores de continuidad para los servicios Help Desk/Gestión IT son los siguientes:

INDICADOR	VALOR	COMENTARIOS
TIER	2	
Criticidad	Sensitivo	
Disponibilidad	99%	Parada/Año: 3 Días
Máximo número de paradas	10	Anuales
Máximo tiempo por parada	12 hr.	
Máximo tiempo parada acumulado	72 hr.	Anual
Punto Recuperación (PR)	24 hr.	
Tiempo Recuperación (TR)	12 hr.	

Servicios BACKUP

Se habilitará un servicio de BACKUP para el Hospital de los datos que corresponda, identificándose los niveles de criticidad y necesidad de copias que se estimen oportunos, además de asegurar el cumplimiento de la legislación pertinente en lo relativo a Protección de datos de carácter personal.

En este apartado se contemplan los siguientes servicios:

- Servicio de BACKUP (a cinta mediante unidades robóticas / a disco / dispositivos externos) mediante Symantec BACKUPEXEC o software de similar funcionalidad. El BACKUP es vital para aquellos servicios donde no se aplican otros mecanismos de réplica por contingencia, tales como MIRRORING para Bases de datos, etc.)
- Servicio de IMÁGENES de servidores, mediante Symantec Recovery o software de similar funcionalidad
- Servicio de Actualización de versiones y despliegue de aplicaciones, mediante WSUS o software de similar funcionalidad, a nivel de:
    - Parches y actualizaciones de sistema operativo (Servidores, Desktop)
    - Parches de Servidores (Servidores)
    - Despliegue de aplicaciones (Servidores, Desktop)
- Servicio de Antivirus y actualización de antivirus, mediante McAfee Viruscan Enterprise 8.5.0i y distribución/despliegue mediante ePolicy Orchestrator 4.0 o software de similar funcionalidad

Los indicadores de continuidad para los servicios de BACKUP son:

INDICADOR	VALOR	COMENTARIOS
TIER	2	
Criticidad	Sensitivo	
Disponibilidad	99,45%	Parada/Año: 2 Días
Máximo número de paradas	8	Anuales
Máximo tiempo por parada	8 hr.	
Máximo tiempo parada acumulado	48 hr.	Anual
Punto Recuperación (PR)	24 hr.	
Tiempo Recuperación (TR)	8 hr.	

Los indicadores de continuidad para los servicios de Recovery / Despliegue Parches / Antivirus son:

INDICADOR	VALOR	COMENTARIOS
TIER	1	
Criticidad	No crítico	
Disponibilidad	98 %	Parada/Año: 7 Días

Máximo número de paradas	12	Anuales
Máximo tiempo por parada	18 hr.	
Máximo tiempo parada acumulado	7 días	Anual
Punto Recuperación (PR)	48 hr.	
Tiempo Recuperación (TR)	18 hr.	

Servidores Virtualización

Se dimensionarán todos los servicios no críticos tratando de llevar la ejecución a entornos virtualizados que permiten optimizar la gestión de la capacidad de los sistemas y la inversión en hardware y servidores. Además, permite tener imágenes de servidores "paradas" (sin consumo de recursos máquina) hasta que requieran ser iniciadas bajo demanda, cubriendo los siguientes procesos:

- Gestión de contingencia → Ejecución de planes de contingencia para dar soporte a servicios ofrecidos por servidores caídos o sin conexión: levantamiento de máquinas bajo demanda
- Gestión de la capacidad →
  - Vertical : Ampliación/reducción de las capacidades de las máquinas virtuales, asignando o quitando memoria, CPU o disco de forma dinámica
  - Horizontal : Levantamiento de nuevas máquinas virtuales para añadirse a CLUSTERS existentes de servicios
- Entornos de preproducción → Copias y levantamiento de máquinas virtuales para habilitar entornos de preproducción adecuados

Los dos entornos de virtualización que se comentan en este apartado son los siguientes:

- Hospital Collado-Villalba: Dentro del CPD del propio Hospital
- Entorno Contingencia: Separado del CPD del Hospital. Se situará en una localización física separada, unida con el Hospital a través de una línea dedicada de alta capacidad

En ambos entornos, se dimensionarán los servidores de virtualización mediante CLUSTERS de servidores con capacidad suficiente para dar soporte a todas las máquinas virtuales que requieran estar operativas a la vez (iniciadas), y al menos el 50% de las máquinas que no requieran estar iniciadas (paradas).

Dichos servidores de virtualización ofrecerán los niveles de servicio adecuados para cubrir los niveles que los servidores virtuales requieran.

Equipamiento de acceso

A continuación se detallan las características del equipamiento de los usuarios del Hospital. Se han distinguido varias configuraciones, que se asignarán a sus usuarios por sus requerimientos específicos.

Equipamiento sobremesa

- PC sobremesa, plataforma INTEL y/o AMD con las siguientes características (o superiores): 4 Gb Memoria RAM, Procesador Dual CORE a 3GHz (o superior), Disco duro 200 Gb, Pantalla TFT de

17" o 19", Conectores externos de USB / lectores de tarjeta, tarjeta de conexión Ethernet a 100 Mbps, Teclado 102 teclas y ratón.

En aquellos puestos con acceso a imagen digital, se asegurará la incorporación de tarjetas de vídeo adecuadas (resolución hasta 2048x1536, 32 bits).

Plataforma: se habilitará la plataforma corporativa del licitador en el equipamiento, que según la evolución del mercado podrá ser: Windows XP Pro, Windows Vista Pro o Windows 7 Pro.

- Impresora local (opcionalmente, en algunos puestos): Equipo láser blanco y negro.

- Equipo portátil. Según la necesidad del usuario para la realización de su labor profesional, se le podrá dotar con equipos tipo Tablet PC o portátiles, que permitan acceder por red inalámbrica a los sistemas de información del Hospital o realizar su labor remotamente. Las características de estos dispositivos serán similares a las siguientes:

  Procesador Dual CORE a 2,4 GHz, 4 Gb Memoria RAM, Disco duro 200 Gb, Pantalla de 15" o 17", en aquellos equipos con acceso a imagen digital, se asegurará la incorporación de tarjetas de vídeo adecuadas (resolución hasta 1280x800, 32 bits) , Conector de acceso WIFI integrado, Conectores externos de USB / lectores de tarjeta, Tarjeta de conexión Ethernet a 100 Mbps.

La dotación inicialmente prevista es la siguiente:

- 350 PCs sobremesa, cubriendo todos los puestos de trabajo hospitalarios. De ellos, 100 serán dotados de monitores clínicos mejorados para visualización de imagen digital.
- 20 portátiles, para profesionales de Dirección y diferentes áreas que exigen movilidad.

Telefonía fija

Se habilitará telefonía IP integrada con el sistema de gestión de telefonía IP (CISCO Call Manager o de similares funcionalidades), en todos los puestos que lo requieran. Se determinará la gama de dispositivo a instalar según las siguientes consideraciones:

- Administración de Centralita / Admisiones / Att. Cliente → Gama Alta (10 unid.)
- Secretarías / Administración / Gerencia → Gama media (30 unid.)
- Resto → Gama Baja (300 unid.)

Telefonía móvil

En aquellos casos que se requiera, se habilitará a los usuarios con un dispositivo móvil que le permita realizar sus funciones fuera del Hospital. Para estas funciones, se definen dos tipos de perfiles:

- Perfil MOVIL – Requiere estar accesible a través del móvil tanto en el Hospital como fuera de él, y además requiere acceso de datos para Internet (20 unid.)

- Perfil INALAMBRICO– Requiere móvil interno, sólo dentro del hospital, con fines de localización (40-60 unid.)

Recursos compartidos

Habrá una serie de recursos habilitados por red, compartidos por varios usuarios del mismo departamento o interdepartamentales:

- Impresora en red. Equipo a color láser
- Multifunción en red (fotocopiadora / impresora / scanner / fax) a color láser

Estaciones Diagnósticas

Bajo este epígrafe enmarcamos los equipos que serán usados por los servicios de Radiodiagnóstico para realizar los informes de las pruebas que se realicen. También serán usados por el personal del Telediagnostic Capio Center. En función de su uso encontramos varias tipologías:

Radiología Convencional

En este caso hablamos de estaciones con 2 monitores en blanco y negro de alta resolución y un monitor color de apoyo en desde el que se tendrá acceso al RIS-HIS del hospital, así como al resto de aplicativos. Las características mínimas de estos monitores serán:

- Resolución: 2048/1536, 3 Megapixel
- Panel: 20,8'', TFT niveles grises
- Contraste: 900:1
- Luminancia: 1000cd/m2
- Ángulo de Visión: 170º vertical y horizontal
- Niveles de grises: 11.9bit (3826)
- Control de calibración: Luminancia, Gamma, temperatura de color
- Monitores con certificación médica UL y CE y conforme Dicom Part 14.

TAC, Resonancia, ultrasonidos

Estaciones con 2 monitores color de alta resolución y un monitor de apoyo. Las características mínimas de los monitores diagnósticos serán:

- Resolución: 1200/1600, 2 Megapixel
- Panel: 21,3'', TFT
- Contraste: 450:1
- Luminancia: 450cd/m2
- Ángulo de Visión: 170º vertical y horizontal
- Niveles de grises: 8bit
- Control de calibración: Luminancia, Gamma, temperatura de color
- Monitores con certificación médica UL y CE y conforme Dicom Part 14.

Mamografía

Estaciones con 2 monitores Blanco y negro de alta resolución y un monitor de apoyo. Las características mínimas de los monitores diagnósticos serán:

- Resolución: 2048/2560, 5 Megapixel
- Panel: 21,3'', TFT
- Contraste: 800:1
- Luminancia: 750cd/m2

- Ángulo de Visión: 170º vertical y horizontal
- Niveles de grises: 11.9 bit
- Control de calibración: Luminancia, Gamma, temperatura de color
- Monitores con certificación médica UL y CE y conforme Dicom Part 14.

Todas las estaciones estarán dotadas de las tarjetas gráficas adecuadas a cada tipo de monitor y al trabajo que deban realizar.

Monitores clínicos

Se habilitarán monitores clínicos de alta resolución para desplegar en las áreas asistenciales asociadas al Hospital que permitan la correcta visualización de imagen clínica.

Arquitectura y estándares

Plataforma y sistemas operativos

Toda la plataforma base de servidores y equipamiento de acceso se basa mayoritariamente en tecnologías MICROSOFT, distribuida según el siguiente esquema funcional:

Servidores

A continuación se enumera el catálogo de sistemas asociados a los servidores:

- Sistemas operativos (podría variar la versión específica en curso):
  - Microsoft Windows Server 2003 Standard y Enterprise Edition 64 bits
  - Microsoft Windows Server 2008 Standard y Enterprise Edition 64 bits

  (NOTA: circunstancialmente, y si existe algún software o tecnología que lo requiera, se instalarán sistemas operativos de servidor con plataformas de 32 bits)
- Directorio Activo: Microsoft Active Directory
- Proxy / Acceso Internet / VPN: Microsoft ISA Server 2006 (versión en curso) o software de similares funciones.
- Bases de Datos (o versiones en curso):
  - Microsoft SQL Server 2005 Standard y Enterprise Edition 64 bits
  - Microsoft SQL Server 2008 Standard y Enterprise Edition 64 bits
  - Oracle 10g/11g Standard Edition

  (NOTA: circunstancialmente, y si existe algún software o tecnología que lo requiera, se instalarán servidores de BBDD sobre plataformas de 32 bits)
- Servidores de Aplicaciones:
  - .NET Framework 3.5 (o superior)

  - Internet Information Server 6 / 7 (versión en curso)
  - En caso necesario, se habilitarán otros servidores de aplicaciones de acuerdo a las necesidades previstas por la CSCM, según sus entornos y recomendaciones
- Virtualización: VMWARE ESX Server 3.5 / 4.x (versión en curso) o similar
- Correo electrónico: Microsoft Exchange Server 2007 (o versión en curso) con Outlook Web Access (o similar) para acceso a correo a través de Web
- Antivirus (o software de similares características):
  - McAfee Viruscan Enterprise 8.5.x (versión en curso)
  - Distribución mediante ePolicy Orchestrator (versión en curso)
- Distribución de parches, Service Packs, despliegues: Microsoft WSUS 3 (versión en curso) o herramienta similar
- Backup e Imágenes: Symantec BackupExec 12.x (o versión en curso) o similar y Symantec Recovery 8.x (o versión en curso) o similar
- AntiSpam: (Appliance) BARRACUDA 400 o equipamiento de similares características. Montado por duplicado en clúster balanceado
- Entorno de colaboración / Gestión de contenidos:Sharepoint Portal Services v.3 (versión en curso) o entorno colaborativo de similares funciones.

Equipos clientes (desktop)

- Sistemas Operativos (se mantendrán las plataformas a versiones soportadas por Microsoft):
  - Microsoft Windows XP Proffesional Edition 32 bits
  - Microsoft Windows 7 Proffesional Edition 32 bits y 64 bits
- Ofimática:
  - Microsoft Office Professional Edition 2007 (o versión en curso) → Equipos usuarios que lo requieran para su labor profesional
  - OpenOffice.org 3.1 (o versión en curso) → Equipos usuarios estándar
  - Microsoft Outlook 2007 (versión en curso) o software cliente de similares características → Equipos usuarios que lo requieran para su labor profesional
- Navegador Web:
  - Microsoft Internet Explorer 7 y 8

  (NOTA: circunstancialmente se dará soporte a otros navegadores de amplia distribución: Mozilla Firefox o Google Chrome, para aquellos usuarios que lo requieran para su labor profesional)
- Antivirus: McAfee Viruscan Enterprise 8.5.0i (versión en curso) o software antivirus corporativo de similares características

Categorías de servidores

A continuación se describen los 3 tipos básicos de servidores que se han catalogado. Estas tipologías son susceptibles de revisarse y actualizarse hasta la apertura del Hospital, en base a la evolución tecnológica y a los cambios de requerimientos de las aplicaciones.

Estas configuraciones estándar pueden ser posteriormente adaptadas (aumento de memoria, CPU, disco) para ajustarse a los requisitos específicos del servicio o servicios que la máquina ofrezca.

Servidor gama baja

Servicios no críticos o de consumo reducido. Poca carga de procesos. Efectos sobre la disponibilidad de servicios o la percepción de los usuarios bajos o nulos. Características básicas del equipo propuesto:

- 4GB / 8GB RAM
- 1/2 procesador(es) (4 core)
- Doble Fuente de alimentación
- 2 Discos Duros en RAID 1
- 1 tarjeta FC HBA para conexión a almacenamiento EVA
- COMBO DRV 24X Lector CD/DVD
- Referencia: HP Proliant DL 360 G6 (1 U) o similares características

Servidor gama media

Servicios sensitivos o vitales, con carga media de procesos. Asumibles servicios que en momentos puntuales (pico) ofrezcan un rendimiento degradado. Características básicas del equipo propuesto:

- 8GB / 12GB / 16GB RAM
- 2 procesadores (4 core)
- Doble fuente alimentación
- 2 Discos en RAID 1
- 2 tarjeta FC HBA para conexión a almacenamiento SAN
- Referencias (o similares caracterísitcas):
    - HP Proliant BL 460c G6 E5540
    - HP Proliant DL380 G6 X5560

Servidor gama alta

Servicios vitales o críticos, con elevada carga de procesos. Es crítico ofrecer un rendimiento continuo, sin degradaciones. Características del equipo propuesto:

- 32GB / 64GB RAM
- 4/8 procesadores (4 core)
- Fuentes de alimentación de alta redundancia

- 2 Discos de sistema en RAID 1
- 2 Tarjeta FC HBA para conexión a almacenamiento SAN con redundancia
- Referencia: HP ProLiant BL680c G5 E7440 8G (o similares características)

Servidores virtuales

Gran parte de los servicios del Hospital, tanto de Producción, como de contingencia como de preproducción se implementarán a través de servidores virtuales sobre plataforma VMWARE ESX server versión 4 (o versión en curso), o software de virtualización de las mismas capacidades.

Para dichos servidores se aplicará una categorización similar que para los servidores físicos, en gama baja, media, alta. En este caso, las características de CPU, Memoria y disco serán similares a las detalladas en dichas gamas.

Almacenamiento

Todos los servidores incorporarán discos en RAID 1 de al menos 36GB para mantener el disco de sistema y SWAP de memoria. Para el almacenamiento de datos se proponen dos entornos de almacenamiento de alta capacidad:

- Entorno de PRODUCCIÓN – Almacenamiento Primario RAID HA 1
  - Almacenamiento tipo SAN compartido
  - Al menos 4 HBAs de conexión por fibra de 8 GB/sg
  - Espacio desde 3,2 TB → Crecimiento viable hasta 96 TB
  - Montaje de volúmenes en RAID 5
  - Referencia: HP StorageWorks EVA4400 para BLADE Systems (o similares características)
- Entorno de CONTINGENCIA – Almacenamiento Secundario RAID HA 2
  - Almacenamiento tipo SAN compartido
  - Al menos 2 HBAs de conexión por fibra a 4 GB/s
  - Espacio desde 1,8 TB → Crecimiento hasta 6 TB
  - Montaje de volúmenes en RAID 5
  - Referencia: Sistema de almacenamiento HP StorageWorks MSA2312fc (o similar)

Entorno pre-producción

Para habilitar los correspondientes entornos de preproducción, se propone la siguiente actividad: Todos los entornos tendrán una imagen virtual (en el caso de imágenes virtuales para contingencia, será la misma), cuya copia que se habilitará bajo demanda como entorno de preproducción que se requiera.

Una vez correctamente testado, y validado, el entorno de preproducción pasará a convertirse en imagen de contingencia, y mediante Gestión del Cambio, todos los procesos realizados sobre el entorno de Preproducción pasarán a realizarse sobre el entorno de producción.

En caso de alta criticidad, temporalmente los entornos de preproducción darán servicio como entorno de producción durante la actualización del entorno de producción.

Sistemas de Monitorización

Se incluirá sistema de monitorización de red basado en Cisco Works (ver apartado *Suministro y puesta en marcha de plataformas y sistemas de monitorización y gestión* en capítulo *Comunicaciones*) y servidores basado en CISCO Works (o software de control de similares características).

Además, se incluirá el sistema de monitorización de Sistemas para los servidores NAGIOS versión 3.x (o software de similares características). Se integrará con el sistema de gestión de red anterior. Se integrará con los sistemas de monitorización de SAIs, Climatización.

Soporte / mantenimiento

Para todos los servidores y equipamiento anexo requeridos, se habilitará siempre el siguiente soporte de fabricante:

- Servidores críticos y vitales – Paquete soporte y mantenimiento 24x7, con tiempo de sustitución de 4 Horas
- Servidores sensibles y no críticos – Paquete soporte y mantenimiento 13x5, con tiempo de sustitución 1 día laborable
- Equipos de cliente (DESKTOP) y otro hardware – Soporte estándar del proveedor durante la garantía (objetivo reparación/ sustitución menor a 5 días hábiles). Resto del tiempo, sustitución por equipo similar.
- Disponibilidad de equipamiento en almacén para sustitución inmediata → Disponibilidad según al siguiente tabla:

DISPOSITIVOS / EQUIPOS	%ALMACEN	CANTIDAD ALMACEN
1-10	20%	1-2
11-30	12%	2-3
31-50	8%	3-4
51-100	5%	4-5
101-500	2%	6-7
501-2000	1%	10-14

Para estos dispositivos, se aplicarán los protocolos de configuración adecuados que permitan minimizar su instalación y puesta en marcha para sustituir a un equipo defectuoso.

4. COMUNICACIONES

En el presente punto se describe la solución de comunicaciones de la Red IP Multiservicio del Hospital de Collado-Villalba.

DISEÑO DE LA RED

Descripción de la solución – nivel físico.

La arquitectura de comunicaciones se ha diseñado de acuerdo a dos criterios:

- Alta disponibilidad: Dada la criticidad de los servicios de explotación que operan, con objeto de evitar puntos únicos de fallo, todos los equipos de la red de comunicaciones disponen de un camino principal y otro camino secundario el cual se utilizará en caso de caída del principal.

- Multiservicio: La red de comunicaciones se ha diseñado para que sea capaz de albergar servicios de diferente índole como son los servicios de datos, voz sobre IP o inalámbricos.

El diseño se divide en dos niveles:

- Capa troncal.
- Capa de acceso.

Capa Troncal.

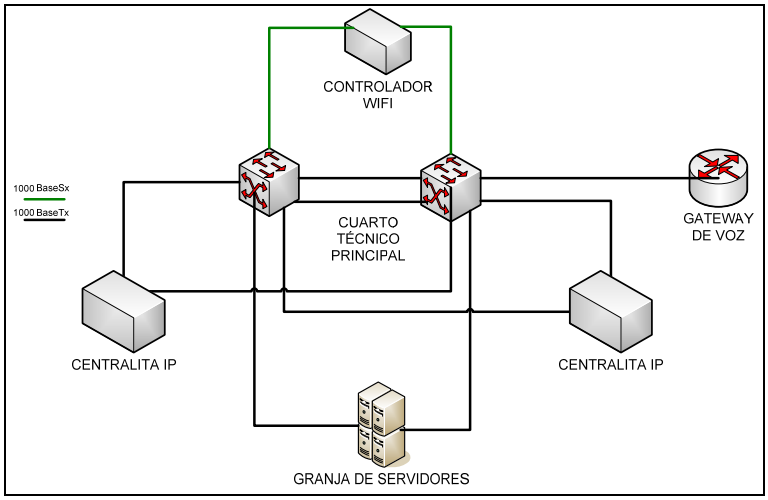
Será la encargada de albergar los servidores y recursos centrales del Hospital, los cuales se ubicarán en el cuarto técnico RP.

Dada su criticidad se dotará de redundancia a nivel de equipamiento de comunicaciones como de fuentes de alimentación.

En cuanto a hardware se dotará a la capa troncal de dos conmutadores de alta disponibilidad tipo Cisco Catalyst 6500 series o similar con doble fuente de alimentación funcionando en redundancia. Este equipo podrá albergar hasta 9 bandejas la cuales incluirán puertos ethernet UTP 10/100/1000 para la conexión de los servidores y recursos centrales así como de puertos gigabit ethernet por fibra óptica multimodo para la interconexión con los equipos de comunicaciones ubicados en los cuartos técnicos RS.

La interconexión entre los dos nodos troncales se realizará vía fibra óptica multimodo utilizando dos enlaces consiguiendo así una velocidad de 2 Gbps.

La capa troncal será la encargada de la interconexión con Internet y las redes y recursos externos mediante un router/gateway.



Capa troncal de la Red de Comunicaciones:

Capa de acceso.

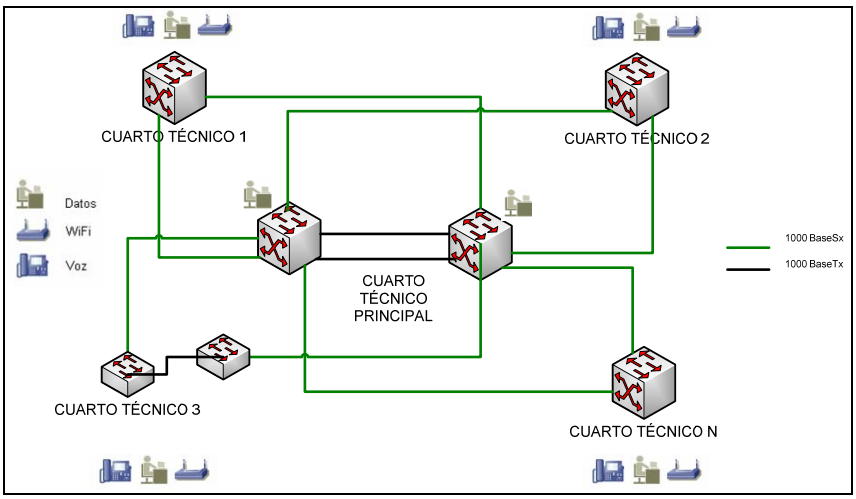
La red de acceso permitirá a los dispositivos finales ubicados a lo largo de todo el Hospital la conexión a la Red de Comunicaciones IP, para lo cual se dotará al resto de cuartos técnicos RS de la electrónica de red necesaria para cada ubicación.

Los nodos de la red de acceso dispondrán de bocas ethernet autonegociables 10/100/1000 Mbps para la interconexión de los dispositivos finales, algunos de ellos poseerán la capacidad Power overEthernet (PoE), la cual permite la transmisión de los datos y la alimentación eléctrica por el mismo cable de red y que se utilizará para los teléfonos IP, puntos de acceso Wi-Fi, megafonía IP o cámaras IP.

Todos los cuartos RP dispondrán de conexiones redundantes vía fibra óptica multimodo a velocidades de 1000 Mbps con la capa troncal.

Topología física de la red de comunicaciones IP.

A continuación se detalla la topología física estimada, ya que en esta fase se desconoce el número de cuartos técnicos y número de conexiones LAN que se asignará a cada uno:



Descripción de la solución – Nivel lógico.

El diseño lógico se ha llevado a cabo para dotar a la red de la funcionalidad multiservicio, proporcionando una inteligencia que dote a la comunicación de los distintos servicios de explotación de una manera eficiente, fiable y segura.

Segmentación del tráfico por servicio - Redes virtuales.

Con objeto de independizar datos de distinta naturaleza, el tráfico se ha segmentado atendiendo al servicio de explotación.

La ventaja principal radica en que un problema que pueda ocurrir en un servicio de explotación no repercuta en el resto, reduciendo el impacto de una posible incidencia.

Por cada tipo de servicio se creará una red virtual (VLAN) que permitirá aplicar a cada una de ellas distintas políticas de seguridad y/o priorización de tráfico.

En el nivel de acceso se crearán VLANes extendidas a todos los nodos de éste nivel y en el caso del nivel de troncal serán VLANes locales al cuarto técnico RP. Un ejemplo de este tipo de configuración podría ser el que se detalla a continuación:

CAPA TRONCAL		
Descripción	**Nº VLAN**	**Nombre**
Gestión de red y seguridad (ACS, Ciscoworks, WLC service port)	2	GESTSEG
Red administración WiFi	3	WIFIMGMT
Recursos VoIP	4	TLFMGMT
Granja servidores Red 1	5	CPD1
Granja servidores Red 2	6	CPD2
Red Wi-Fi Datos	10	WIFIDATAUSR1
Red Wi-Fi Voz	12	WIFITLFUSR1
Reservado futuros usos	14-31	---

CAPA DE ACCESO		
Descripción	**Nº VLAN**	**Nombre**
Gestión de la electrónica de red	32	NETADMIN
Red gestión Wi-Fi	33	LWAP
Telefonía fija VoIP	34	VOIP
Red ofimática (impresoras,..)	36	OFIMATICA
Sistema de información hospitalaria (SIA)	38	SIA
Centralización de video	39	CCTV
Reservado para futuros usos	40-149	---
Distribución e intercambio de imágenes y laboratorio (PACS)	150	PACS
Reservado para futuros usos	151-255	---

La asignación de la vlan de servicio se hará de forma estática a cada puerto según las necesidades de cada emplazamiento.

Protocolos de redundancia de nivel 2.

Atendiendo al criterio de diseño en el nivel físico anteriormente expuesto, cada cuarto técnico RS de la capa de acceso ofrece caminos redundantes ante la caída de algún enlace. De la misma manera, el diseño redundante en el cuarto técnico RP proporciona enlaces alternativos ante un fallo del mismo.

El protocolo de redundancia de nivel 2 propuesto es el estándar Rapid Spanning Tree 802.1w, el cual permitirá gestionar automáticamente los enlaces redundantes de nivel 2 con una velocidad de conmutación del tráfico no superior a 10sg en caso de caída de uno de los enlaces.

Por cada servicio/VLAN existirá un árbol de Spanning-Tree. La arquitectura propuesta consigue reducir el tamaño de los árboles y la probabilidad de que se produzcan bucles de red y por tanto el impacto sobre la misma.

Se propone la centralización y balanceo de los “root” de spanning-tree en los dos nodos troncales del cuarto técnico RP de tal forma que las VLANes pares poseerán el “root” en el primer Catalyst o similar y las VLANes impares en el segundo Catalyst o similar.

Protocolo de enrutamiento de datos.

Los nodos de los cuartos técnicos RS se configurarán para su funcionamiento en modo nivel 2 por lo que no correrán ningún proceso de routing. El enrutamiento entre servicios/VLANes se realizará en los dos nodos Catalyst 6500 o similares del cuarto técnico RP.

Los nodos troncales poseerán todas las redes directamente conectadas por lo que la comunicación entre ellas será automática sin necesidad de utilizar ningún protocolo de enrutamiento de datos.

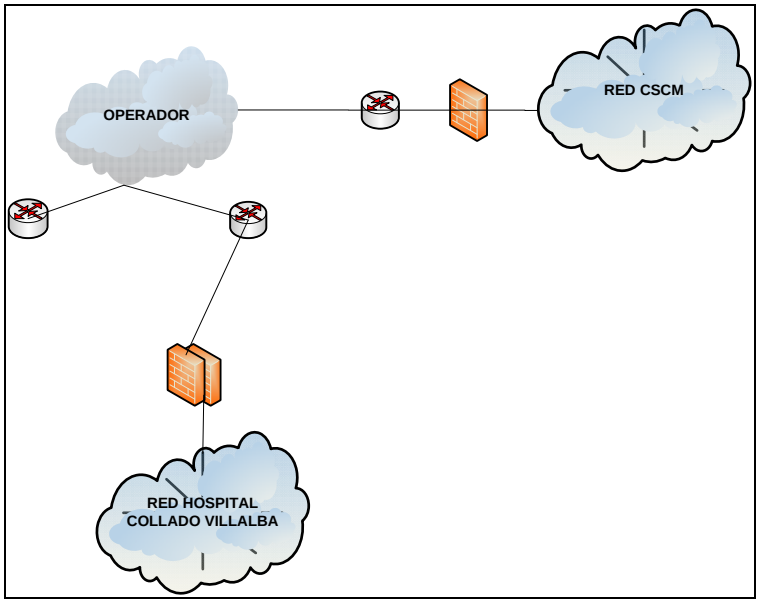
Interconexión con la Red de datos de la CSCM.

Se plantea establecer inicialmente la conexión con la Red de la CSCM a través de dos enlaces redundantes de 100 Mb, cumpliendo la normativa, estándares, requisitos de conectividad, direccionamiento y seguridad establecidos por la CSCM. Cuando la demanda progresiva de ancho de banda así lo requiera, se ampliará hasta Gigabit redundante.

Esta línea de comunicaciones dispondrá de sistemas de seguridad en el extremo (Firewall) y encriptado de la información, configurado de forma que garantice el acceso seguro y exclusivo a los sistemas, aplicaciones y datos necesarios para el normal desarrollo de la actividad del Hospital y su comunicación con la CSCM, garantizando la mejor calidad de servicio y tiempos de respuesta en las comunicaciones.

El dimensionamiento y configuración de las líneas de comunicaciones cumplirán con los requisitos que en esta materia establece la CSCM.

A continuación se detalla la topología estimada:



INFRAESTRUCTURA DE RED INALÁMBRICA WIFI.

Controladores de puntos de acceso.

Como plataforma de centralización del control de los Puntos de Acceso se empleará el Cisco 4404 Wireless LAN Controller o similar. Se trata de un dispositivo capaz de proporcionar funciones esenciales dentro de un despliegue de infraestructura inalámbrica, como son:

- Propagación de las políticas de seguridad.
- Funciones IPS (Intrusion Prevention Services).
- Gestión del medio radio.
- Propagación de las políticas de calidad de servicio (QoS – Quality of Service).
- Gestión de la movilidad de los clientes (roaming entre puntos de acceso).

Cada controlador dispone de hasta 4 interfaces Gigabit Ethernet (formato SFP) para su interconexión con la electrónica de red.

Para realizar la gestión del medio radio, los controladores disponen de una algoritmia específica (RRM – Radio Resource Management), la cual permite realizar cálculos que se traducirán potencialmente en modificaciones de las configuraciones de los puntos de acceso, que se enviarán encapsuladas vía LWAPP. Entre los parámetros del medio gestionados por los controladores, se encuentran los siguientes:

- Asignación dinámica de canales: Se asignarán canales a los AP's para optimizar la cobertura, en función de las variaciones que se produzcan en las condiciones de propagación.
- Detección de interferencias: Reajuste del entorno radio ante la detección de interferencias, para conseguir una mínima afección.
- Balanceo de carga: En caso de coexistencia de muchos clientes móviles en un área asignada a un único punto de acceso, el controlador es capaz de repartir el tráfico entre AP's cercanos, para

conseguir con ello un rendimiento óptimo de la red. Para esto, el despliegue radio se realizará teniendo en cuenta un área de solape entre AP's adyacentes.

- Detección y corrección de "zonas de sombra" de cobertura. Reajuste automático de la potencia de salida de los puntos de acceso para evitar la existencia de sombras de cobertura.
- Control de ganancia automático. El sistema ajusta de forma automática la potencia de salida adaptándose a las condiciones de la red, consiguiendo así el aseguramiento de la disponibilidad y el rendimiento inalámbricos.

Los controladores permiten asimismo propagar la configuración de seguridad que se haya estimado más conveniente, a los efectos de autenticar clientes móviles y securizar las transmisiones que tienen lugar a través del medio radio.

A través de los controladores de WLAN, se soportan múltiples funcionalidades que constituyen mecanismos de protección del entorno radio, y que constituyen por tanto barreras ante posibles intrusos. Algunas de estas funcionalidades se citan a continuación:

- Seguridad RF: Detección y control de interferencia.

- Detección y Protección contra intrusos (Intrusion Detection / Protection), en el medio radio: Detección y localización de AP's "maliciosos", así como de posibles invulnerabilidades asociadas a la configuración "lógica" de la red.

- Creación y propagación de políticas de seguridad individualizadas, por perfil, entre otras:
  - Seguridad en capa 2 (IEEE 802.1x, IEEE 802.11i, WPA).
  - Seguridad en capa 3 (IPsec, autenticación basada en Web).
  - Mapeo VLAN a SSID.
  - Soporte de ACL's (Access Control Lists), con restricción de dirección IP, tipo de protocolo, nº de puerto y valor del campo DSCP de la cabecera IP.
  - QoS (distintos niveles de servicio, asignación de ancho de banda, marcado de tráfico, grado de utilización de medio radio, etc.)
  - AAA (Authentication, Authorisation and Accounting) vía RADIUS/TACACS+.

- Control del acceso a la red (NAC – Network Access Control): Posibilidad de establecer políticas de seguridad con un elevado nivel de granularidad, lo cual permite limitar el acceso a los recursos de red.

- Movilidad segura: Los controladores incorporan funcionalidades para garantizar los mayores niveles de seguridad cuando los clientes se mueven a lo largo de la zona de cobertura. Entre otras, permite el establecimiento de VPN's (Virtual Private Networks), de forma que, cuando se produzca el salto de un AP a otro (roaming), el cliente no tenga que reestablecer de nuevo un túnel seguro. Además, incorpora una extensión al estándar 802.11i (Proactive Key Caching) que facilita el roaming seguro, empleando algoritmos de encriptación AES (Advanced Encryption Standard) y un Servidor RADIUS.

Los controladores se encargan en todos los casos de gestionar el proceso de traspaso de un AP al adyacente, garantizando que éste se produzca de forma completamente transparente a protocolos y aplicaciones de niveles superiores. El control que ejercen los WLAN controllers permite incluso

recomponer la cobertura cuando se producen fallos en dispositivos de la infraestructura Wifi. Los escenarios degradados previstos son:

- Fallo de un AP: Una vez que se detecta el fallo de un AP, los AP's vecinos automáticamente reajustan el nivel de potencia transmitida para intentar proporcionar cobertura en la zona afectada.
- Fallo de un Controlador. En escenarios dotados de redundancia, como el previsto (1+1), si se produce un fallo en un controlador, los AP's pasan inmediatamente a ser gestionado por su par activo, garantizando que no haya interrupciones en los servicios inalámbricos.

Puntos de acceso WIFI.

Para proporcionar cobertura inalámbrica en el interior del hospital se emplearán puntos de acceso compatibles como mínimo con los siguientes estándares:

- IEEE 802.11a
- IEEE 802.11b
- IEEE 802.11g
- IEEE 802.11n

Son AP's preparados para proporcionar cobertura en entornos de interiores, disponiendo de antena integrada. Permite realizar despliegues inalámbricos altamente seguros, gracias a su compatibilidad total con el estándar IEEE 802.11I (WPA2), y gracias a soportar múltiples mecanismos de autenticación EAP. Para acelerar los procesos de encriptación de los datos, previo a su transmisión al medio radio, incorpora algoritmos AES implantados en el hardware, de manera que, por más complejo que sea el esquema de encriptación, nunca se produzca una merma en su rendimiento.

Se llevará a cabo el correspondiente análisis de cobertura del Hospital para asegurar la cobertura WIFI al 99,99% de todas las localizaciones (se evitan, por causas obvias, zonas con aislamiento electromagnético, tales como Radiología), con un número adecuado de puntos de acceso. Se estima, a priori, cubrir el Hospital con un número de entre 120 y 150 puntos de acceso (APs) WIFI.

INFRAESTRUCTURA DEL SISTEMA DE VOZ SOBRE IP.

Dentro de la solución telefonía IP, se plantea la utilización de la centralita modelo Cisco Call Manager o similar. Dicha plataforma se configurará en cluster para dotar a la solución de voz sobre IP del suficiente grado de redundancia y disponibilidad.

En lo que respecta a las funcionalidades del sistema como centralita, cumple las siguientes:

- Funcionalidades generales:
  - Soporte SIP, H.323, SCCP y MGCP.
  - Atenuación y ganancia de ajuste por dispositivos (teléfono y gateway).
  - Selección automática de ancho de banda.
  - Soporte codificación- decoficación para selección automática de ancho de banda.
  - Soporte codecs G711 mu-law y a-law, G723.1 y G729a/b.
  - Análisis de dígitos y tratamiento de llamadas (inserción, borrado, quita y traducción de dígitos.

- Soporta de un nº elevado de teléfonos IP (>2.000).
- Fax sobre IP-G711.
- Interfases H.323 para dispositivos seleccionados.
- Servicio de Hotline.
- Soporta múltiples protocolos RDSI.
- Monitorización SNMP.
- Seguimiento de llamadas.
- Bloqueo de llamadas salientes.
- Tolerancia a fallos en la red telefónica normal en caso de no disponibilidad de ruta de salida de llamada.
- Supresión de silencio y detección de actividad de voz.
- Plan de numeración y rutas unificado o particionado por grupos.
- Preparado para la integración de servicios convergentes (mensajería unificada, vídeo y voz).
- Software de gestión de Call Center, en el que se pueden establecer menús de entrada, priorización de colas, gestión de flujos de llamadas, estadísticas, etc.
- Software de gestión de operadora automática, creación de menús de atención, enrutamiento de llamadas por destino, estadísticas, etc.

- Funcionalidades entregadas al usuario final:
  - Desvío de llamada (incondicional, ocupado, no contesta).
  - Rellamada directa en caso de ocupado.
  - Grupos de atención, captura de llamada.
  - Identificación de nombre y número llamante.
  - Restricción de llamada por identificación de línea.
  - Discado directo entrante y saliente.
  - Almacenamiento de directorios de llamadas perdidas, recibidas, atendidas por
  - teléfono IP.
  - Diferencia de timbre de llamada externa e interna.
  - Tono de llamada diferenciado por teléfono llamante.
  - Sistema de seguimiento/ movilidad.
  - Manos libres.
  - Rellamada del último número marcado.
  - Aplicación de gestión de llamadas (filtro, desvío, etc.).
  - Música en espera.
  - Silencio para auricular y manos libres.
  - Discado sin descolgar.
  - Consola de operadora por software.
  - Estadísticas de calidad de servicio en tiempo real vía web al teléfono.
  - Lista de llamadas recientes, llamadas al y desde el teléfono.
  - Múltiples velocidades de marcado por teléfono.
  - Control de volumen de la estación.
  - Transferencia de llamadas.
  - Acceso de servicios de web a través del teléfono.
  - Buzones de voz a modo de contestadores automáticos a las extensiones correspondientes.

- Administración de la plataforma:
  - Aplicación de descubrimiento y registro a un gestor SNMP.
  - CDR (Registro de llamada).
  - Notificación cambios automatizados de la base de datos.
  - Formato configurable de fecha y hora por teléfono.
  - Información de trazas a un fichero común de syslog.
  - Agregado de dispositivos a través de asistentes.
  - Bloqueo de asignación de IPs a teléfonos y gateways.
  - Tabla de traducción de números llamados.
  - Servicio de identificación de número llamado (DNIS).
  - Interfaces H.323 compatible con clientes H.323, gateways y gatekeepers (interoperable con otras plataformas de VoIP).
  - Actualización remota de dispositivos (teléfonos IP, gateways, etc).
  - Soporta señalización y control de protocolo MGCP para gateways VoIP seleccionados.
  - Soporta servicios suplementarios para gateways H.323.
  - Ejecución-seguimiento de estadísticas SNMP desde aplicaciones al gestor SNMP.
  - Estadísticas registradas de calidad de servicio (QoS) por llamada.
  - Único punto de configuración de dispositivos y sistema.
  - Zona horaria configurable por teléfono.
  - Módulo de control de facturación, según parámetros de la llamada.

La centralita se complementa con un módulo de tarificación de voz, soportado por el aplicativo cHar uTile, que aporta las siguientes funcionalidades:

- Tarificación e imputación de costes de llamadas.
- Análisis de enrutamiento saliente óptimo por coste.
- Fecha, hora, usuarios, centros de coste y ubicaciones.
- Control de los datos de las llamadas: orígenes, destinos, números, duración, llamadas atendidas, no atendidas, tiempo de respuesta, etc.

Gateway de voz para interfaz con operador.

Para este fin se empleará una plataforma basada en un Cisco ISR (Integrated Services Routers) o similar. Este dispositivo dispone de una serie de características y funcionalidades que lo hacen apto para aplicaciones de todo tipo, incluyendo voz y vídeo sobre IP.

PLAN DE DESPLIEGUE Y PUESTA EN SERVICIO.

El despliegue de las líneas de comunicación, equipos de comunicaciones, equipos de seguridad, y su posterior puesta en servicio comenzará a la entrega de la obra y finalizará antes de la apertura del Hospital. Durante este periodo, en el que se realizará el despliegue de la electrónica de red, líneas de comunicaciones y toda la configuración de red, se incluye el plan de pruebas.

SUMINISTRO DE LÍNEAS Y EQUIPAMIENTO.

Todas las líneas de comunicaciones, junto con su equipamiento, serán suministradas y configuradas antes de la apertura del Hospital. Se dispondrá de una conexión con la red de Capio y otra conexión con la red de la CSCM. En ésta última se asegura la conexión con al menos dos enlaces redundantes Gigabit Ethernet. Todas las líneas de comunicaciones estarán dimensionadas para garantizar una comunicación sin retardos ni tiempos de espera elevados.

DESPLIEGUE DE RED.

Se procederá al despliegue de la red por las conducciones de comunicación habilitadas para tal efecto.
El cableado de datos estructurado será del tipo UTP categoría 6 o 6A debidamente certificado.

Los armarios de comunicaciones del CPD tendrán comunicación directa mediante fibra óptica con el RITI.

Todos los raks del CPD tendrán conexión directa con el armario distribuidor de cableado mediante conexiones de cobre.

El CPD tendrá comunicación con el resto de cuartos técnicos mediante un enlace de fibra óptica redundado.

Cada armario contará con las regletas de 24 tomas RJ45 hembra necesarias para dar servicio a todos los racks (14 regletas x 24 UTP). Cada uno de los bastidores (racks) de la sala, dispondrá de una regleta de 24 tomas RJ45 hembra, cajeada de forma que las conexiones posteriores de roseta queden protegidas (de forma que puedan ubicarse y moverse bajo el falso suelo sin dañarse). Este cajeado podrá ser retirado, para que la regleta se pueda colocar dentro del bastidor de máquinas a las guías de 19 pulgadas. Las 12 primeras rosetas estarán conectadas a un panel de conexiones situado cerca de uno de los conmutadores, las 12 restantes terminaran en otro panel situado cerca del conmutador de respaldo.
Se intentará respetar la distancia mínima entre el cableado de red y cableado eléctrico. En los tramos que no sea posible, se utilizará mangueras de cables de tensión apantalladas.

El cableado estructurado se entregará a las regletas de los armarios con una holgura mínima de 2 metros.

Se seguirán las especificaciones de la CSCM referentes al cableado, rotulado y documentación de la red de comunicaciones.

En cuanto al despliegue de puntos de red del Hospital, se ha estimado entre 2400 y 2500 puntos de red en pared, de los cuales se patchearán a la red de comunicaciones inicialmente entre 2000 y 2100. Con este despliegue, se cubrirán las necesidades de conexión del equipamiento hospitalario, PCs, portátiles, impresoras en red, teléfonos IP, puntos de acceso WIFI, televisiones con necesidades interactivas, kioskos y cartelería digital de todo el Hospital.

PLAN DE PRUEBAS.

Se establecerá un plan de pruebas dividido en equipamiento de comunicaciones internas, equipamiento de comunicaciones externas y equipamiento de seguridad.

En las pruebas de equipamiento interno se verificará la redundancia de la alimentación eléctrica a nivel hardware. En los casos que el equipamiento interno se encuentre redundado, se verificará que la operación de failover y rollback funcionan correctamente. En la fase de failover se garantiza que el hardware que queda activo es capaz de soportar toda la carga y no existe una degradación del servicio.

Existirá una verificación de la comunicación por todos los caminos redundantes entre el cuarto técnico principal y el resto de cuartos técnicos.

En las pruebas de comunicaciones externas se verificará que la configuración, enrutamiento y calidad de la línea es correcta. Se verificará el correcto dimensionamiento de las líneas de comunicaciones y que éstas no tengan ningún error del tipo CRC o similar. Por otro lado, donde exista redundancia, se verificará que el protocolo HSRP está funcionando correctamente y en caso de caída de la línea principal es capaz de enrutar la comunicación por la línea de backup.

En las pruebas del equipamiento de seguridad se verificarán los servicios de enrutamiento, los servicios de seguridad, servicio de balanceo y la calidad de servicio, en el caso que se requiera.

En todos los casos se verificará el correcto funcionamiento de los sistemas de alimentación ininterrumpida en caso de caída de la línea eléctrica, y se garantizará el 100% de disponibilidad.

Todo el cableado del centro estará debidamente certificado.

PUESTA EN SERVICIO.

El licitador realizará un seguimiento continuo de los trabajos de ingeniería y dotación al Hospital de toda la infraestructura de red. Se procederá a verificar que todos los cuartos técnicos son aptos y cumplen las normas establecidas antes de realizar la instalación de los equipos hardware. La configuración y puesta en marcha inicial de la red y sus servicios se realizarán bajo la supervisión del licitador. La configuración de los dispositivos de red se basará en el diseño de red propuesta por el licitador.

Se implantarán los sistemas de monitorización, administración y gestión de la red necesarios para proporcionar al Hospital una red de comunicaciones que garantice un servicio óptimo. Los sistemas de monitorización se dividirán tres niveles, que serán leves, importantes y críticos, haciendo un tratamiento de los mismos acordes a su severidad. Se garantiza en este sentido un soporte de monitorización de la red 7x24x365 días. En el apartado 'SERVICIOS DE SOPORTE Y MANTENIMIENTO DE LÍNEAS Y EQUIPOS' se detallan los niveles de escalado de incidencias detectadas en la red de comunicaciones. Por otro lado, existirá un servicio que permitirá realizar modificaciones en la configuración de red en horario de 24x7x365 días.

Se garantiza la implantación de una red de comunicaciones capaz de crecer tanto en horizontal como en vertical, capaz de interactuar con diversos componentes de la red de datos que puedan surgir a futuro.

El licitador se compromete a realizar el seguimiento del proyecto garantizando que todo el equipamiento relativo a la red de comunicaciones y su configuración corresponde con el acordado. El licitador realizará el seguimiento de proyecto bajo el control y supervisión de la CSCM.

SUMINISTRO Y PUESTA EN MARCHA DE PLATAFORMAS Y SISTEMAS DE MONITORIZACIÓN Y GESTIÓN.

El sistema de gestión de Red estará compuesto por un servidor CiscoWorks-LMS o similar. El equipo recogerá todas las alarmas que generen los equipos de comunicaciones centralizando la visualización de las mismas en una única consola, y monitorizando el estado de cada equipo de comunicaciones para detectar posibles incidencias.

A continuación se detallan algunas funcionalidades del software de gestión CiscoWorks, pudiendo ser ésta la solución final u otra que cubra las exigencias mínimas de monitorización.

Características:

- Ofrece descubrimiento inteligente automático de equipos Cisco para crear así vistas de la topología de la red.
- Aporta indicaciones del estado de la topología.
- Configura, gestiona y monitoriza Virtual LANs (VLANs), asociadas de forma lógica a servicios y/o aplicaciones.
- Descubre estaciones finales y terminales conectados a los puertos del conmutador e identifica las ubicaciones de usuarios basadas en user ID (identificador de usuario).
- Traza conectividad de Nivel 2 y Nivel 3 entre dos puntos de la red (dispositivos, servidores, teléfonos....).
- Analiza de forma inteligente las condiciones de fallos diseñadas para detectar los problemas antes de que generen distorsiones en la red.
- Interpreta las condiciones de fallo en los niveles de dispositivo y VLAN.
- Recoge estadísticas RMON/RMON2 de los switches LAN, y dispositivos de electrónica tradicionales.
- Facilita las tareas de resolución de problemas en la Red.
- Ofrece software detallado e informes del inventario del hardware.
- Facilita herramientas de actualización para el software de dispositivos y para los cambios de configuración.
- Facilita el registro (logging) de cambios centralizado.
- Ofrece gestión gráfica de los equipos.
- Proporciona seguridad en el acceso a las aplicaciones.

Las anteriores características habilitan la realización de las siguientes tareas de gestión de una forma centralizada (desde una única consola de gestión):

- Inventario detallado tanto software como hardware de todo el equipamiento Cisco (IOS instaladas, módulos, tarjetas, configuraciones, etc).
- Captura mensajes generados en la consola de cada nodo de una forma remota y desatendida (Syslog Analysis).
- Actualización de IOS (Sistema Operativo) desatendidamente y de una forma planificada.
- Monitorización de la accesibilidad y el tiempo de respuesta de los dispositivos de red.
- Control de cada cambio hardware de cada dispositivo Cisco.
- Control del histórico de Configuraciones de cada dispositivo Cisco, permitiendo comparar distintas versiones.
- Modificación, borrado e incorporación de nuevos configuraciones de una forma desatendida y programada.

- Diseño de un mapa de todos los nodos instalados permitiendo filtrar por VLAN, dominios VTP, etc.
- Creación, modificación y borrado de VLANs de varios de equipos de la red a la vez.
- Control de todos los equipos conectados a cada puerto del equipamiento de red. (Dirección MAC, Dirección IP, Nombre del equipo, Usuario Conectado, etc.).
- Visualización gráfica de cada dispositivo Cisco (CiscoView o similar). Esta característica es muy útil por cuanto permite tener una representación gráfica en pantalla de un dispositivo dado, mostrando una representación de los puertos o interfaces del mismo completamente sensible al estado real de los mismos.

La aplicación CiscoWorks LMS (como referente) es un Software complejo, formado a su vez por varios módulos componentes, cada uno de los cuales abarca un subconjunto de las funciones. A continuación se incluye una descripción de los mismos, así como de las tareas más relevantes encomendadas a cada uno de ellos:

RME (Resource Manager Essentials)

Este módulo permite el inventariado y la gestión de los cambios en la configuración de todos los equipos Cisco de la red. Constituye un punto central para la gestión, mantenimiento y distribución de las versiones de software y ficheros de configuración de los equipamientos. Dispone de una interfaz rápida e intuitiva, basada en Web.

CiscoView

El CiscoView permite a los operadores de red observar la configuración física, monitorizar el estado, obtener estadísticas de la red y modificar configuraciones de los equipos Cisco. Se basa en la presentación en pantalla de un sinóptico del equipo completo, incluido chasis, tarjetas de medios, etc. lo cual facilita la interacciójn con la aplicación. Como en el caso anterior, se trata de un módulo con interfaz Web, que permite realizar lo siguiente:

- Monitorización en tiempo real del rendimiento, tráfico y utilización de los equipos, permitiendo el análisis de diferentes parámetros, tales como: porcentaje de utilización, paquetes transmitidos y recibidos, tasa de errores, etc.
- Modificación de configuraciones en remoto.
- Acceso al soporte online que ofrece Cisco para la resolución de problemas en sus equipos.

Campus Manager

Campus Manager representa un subconjunto de aplicaciones basadas en Web; desde las cuales se puede realizar la gestión de redes de nivel 2 (layer 2) de equipos Cisco. Entre las funcionalidades que ofrece destacan: descubrimiento automático de conectividad y de equipos, la gestión y descubrimiento de servidores de workflow, vistas detalladas de las topologías de red, configuración de VLAN y ATM, detección de estaciones terminales, herramientas de análisis de trayectos de capa 2 y 4, etc.

DFM (Device Fault Manager)

Permite realizar el análisis en tiempo real, de fallos detectados en los equipos de red. Genera “intelligent Cisco traps” (alarmas) a través de una variedad de técnicas de análisis y recogida de datos.

Las alarmas pueden visualizarse localmente, pueden ser enviadas por e-mail o pueden ser transmitidas a otros sistemas de gestión de eventos.

El Device Fault Manager posee las siguientes características:

- Análisis de fallos enfocados en problemas.
- Integración con sistemas de Gestión empresarial.
- Soporte para equipos Cisco de Layer 2 y Layer 3.

RMON (Real-Time Monitoring)

Es una herramienta Web, basada en el tratamiento de las estadísticas RMON, que permite la monitorización de patrones de tráfico y troubleshooting, manteniendo la disponibilidad de la red. Permite a los administradores de la red una anticipada percepción de potenciales problemas de la red, evitando así una posible degradación de la misma.

Esta herramienta aporta una monitorización del desempeño y utilización de los links, resolución y aislamiento de problemas de red, generación de estadísticas, gráficos e informes de la capacidad de la red en tiempo real, para una correcta planificación del crecimiento de la misma.

La red Wi-Fi contará con su propio sistema de gestión, Wireless Control System o de similares prestaciones, residente en un servidor de la red. Desde esta plataforma se realizará la planificación, configuración y mantenimiento de las redes inalámbricas.

De forma resumida, las características más relevantes del Cisco WCS son las siguientes, desde un punto de vista de administrador de red:

- Monitorización de red y resolución de problemas:
  - Visualización del esquema global de red.
  - Obtención de los parámetros que determinan el rendimiento del sistema radio.
  - Visualización de mapas de cobertura dinámicos, con curvas de nivel de señal constante.
  - Ventana de configuración centralizada, para modificar la forma en que los controladores WLAN regulan la asignación de canales, los niveles de señal de salida / AP, etc.
- Acceso seguro a invitados: Permite establecer un entorno radio controlado (con acceso limitado a recursos) para permitir a usuarios invitados acceder a recursos, de forma controlada. La regulación de este acceso puede realizarse de diversas formas: mediante dupla user/password y token de acceso (con validez por un periodo de tiempo), etc.

- Protección del entorno radio. Además de permitir la centralización de la configuración de seguridad del entorno inalámbrico, y la propagación de los parámetros de configuración al resto de los equipos de la infraestructura inalámbrica, el WCS permite a los administradores de red crear ficheros de firmas que identifiquen ataques comunes en el entorno radio: DoS (Denial of Service), Nestumbler, FakeAP. El WCS puede programarse para activar automáticamente una alarma cuando se verifique una de las firmas. Además, a través de la capa de acceso y control, el WCS permite la supervisión constante del medio radio, en busca de posibles AP's maliciosos. En caso de que un dispositivo

malicioso (AP o cliente) intente acceder a la red, el WCS recopilará los datos del mismo, e incluso podrá realizar un seguimiento y localizar, sobre el plano, la posición aproximada del intruso.

- Por último, como se comentaba anteriormente, el WCS dispone de un interfaz sencillo para la centralización de las políticas de QoS y seguridad en el entorno inalámbrico. Así, el entorno inalámbrico puede acomodar servicios sensibles a retardos y latencias en la transmisión (por ejemplo VoIP – Voz sobre IP) sin que ello suponga un incremento en la dificultad de la gestión (basta con establecer las políticas adecuadas de seguridad y el nivel de priorización de tráfico de voz). Podrán además crearse listas de exclusión específicas, para identificar unívocamente a los dispositivos intrusos. Además ofrece las siguientes posibilidades de cara a una gestión global de entorno inalámbrico:

    - Configuración escalable. Se podrán fijar configuraciones por grupo de controladores o AP's, permitiendo la telecarga de dicha configuración en los grupos, a través de la red y de forma centralizada y automatizada.

    - Resolución de errores. El WCS actúa como elemento consolidador de los datos de "campo", convirtiéndolos en metadatos. Los administradores podrán tener acceso, de forma visual, a parámetros tales como la relación señal a ruido, el nivel de interferencia, el nivel de señal y la topología de red, todo ello en tiempo real.

    - Actualizaciones de SW. Las actualizaciones de firmware se podrán realizar de forma controlada, automatizada y centralizada, desde una única consola de gestión, lo cual redunda en una más óptima gestión de la infraestructura inalámbrica, reduciendo en el coste total de la propiedad.

    - Descubrimiento automático de nuevos equipos. En el momento en que aparezcan nuevos componentes en la capa de acceso o de control, éstos serán descubiertos por el WCS, y automáticamente dados de alta en el sistema, sin necesidad de tener que mantener actualizadas de forma manual bases de datos complejas.

    - Informes personalizados. Los administradores de red podrán emplear el WCS para convertir los datos recolectados en informes que documentan la actividad de red, por ejemplo: estadísticas de clientes, utilización del medio radio, contadores 802.11, historial de configuración del entorno radio y alarmas detectadas.

    - Acceso seguro. La comunicación entre el WCS y los controladores tiene lugar a través de SNMP v3, lo cual garantiza que los datos estén encriptados, y por tanto securizados. El acceso a la consola de gestión del WCS puede realizarse a través de navegador Web, vía HTTP(S).

5. SISTEMAS DE INFORMACIÓN HOSPITALARIOS

El Hospital de Collado-Villalba dispondrá de Sistemas de Información integrados que den soporte a toda la actividad desarrollada en el Hospital y cubran todas las áreas funcionales englobadas en la cartera de servicios hospitalaria, alineados con el compromiso de la sanidad madrileña en el desarrollo de un sistema sanitario más cercano, accesible, de mayor capacidad de respuesta y en el menor tiempo a las necesidades de los ciudadanos y profesionales sanitarios.

Los objetivos específicos a cubrir con el sistema de información son:

- Situar al ciudadano en el núcleo de la actividad asistencial, permitiéndole disponer de su propia información.
- Facilitar al ciudadano el acceso a los recursos sanitarios y a la asistencia sanitaria mediante la identificación unívoca del mismo a través de su tarjeta sanitaria.
- Incrementar la eficiencia del Sistema Sanitario a través de optimizar los mecanismos de gestión.
- Disponer de sistemas de información flexibles que permitan su adaptación al entorno hospitalario y sanitario madrileño actual y futuro.
- Permitir una gestión Uniproceso / Multiproceso orientada a la calidad.
- Ayudar a la toma de decisiones, mediante la implantación de mecanismos que permitan monitorizar la calidad de los servicios que se presta y los niveles de eficacia y eficiencia de los mismos.

El Hospital de Collado-Villalba se construye bajo el paradigma de “Hospital Digital”, con disponibilidad de un sistema integrado, con el centro del mismo enfocado en el paciente, y cuyos pilares básicos sean:

- Identificación única del paciente, manteniendo la separación entre información clínica y la información administrativa.
- Integración de la información en la Historia Clínica Única en una plataforma común, capturando la información en el lugar en donde se origina.
- Garantizar los mecanismos de intercambio e integración de información.
- Accesibilidad a la historia por parte de los profesionales y los usuarios con las medidas de seguridad necesarias.

Más ampliamente, la Historia Clínica Digital debe:

- Ser única para cada paciente.
- Debe disponer de una interfaz que muestre la información completa y homogénea. Siendo capaz de alimentarse de los diferentes sistemas existentes, los cuales no disponen de un sistema homogéneo de generación de información.
- Accesible por los profesionales y usuarios en función de sus permisos y desde cualquier punto del sistema dónde se necesite.

MODELO CAPIO DE SISTEMAS PARA HOSPITALES DE LA COMUNIDAD DE MADRID

Capio cuenta con un modelo de sistemas, que ha implantado en los hospitales que gestiona en colaboración con la Comunidad de Madrid y que extenderá al Hospital de Collado-Villalba.

Este modelo, además de ajustarse a los principios básicos comentados hasta ahora, se caracteriza por contar con:

- Catalogo corporativo de soluciones integradas y de amplia cobertura funcional.
- Apoyo de socios tecnológicos de reconocido prestigio y solvencia en el sector de la sanidad.
- Área interna de desarrollo que permite complementar las soluciones de mercado con aportaciones de valor añadido, funcionales y tecnológicas.
- Constante evolución y adaptación a los nuevos retos en los que las TIC están obligadas a dar respuesta en un entorno sanitario cambiante.
- Sinergias de grupo :
    - Amplio equipo de profesionales de las TIC, con amplia experiencia en el sector hospitalario.
    - Apoyo y experiencia funcional de un amplio equipo de usuarios expertos de otros centros del Grupo.
    - Aprovechamiento de infraestructuras, recursos y estrategias centralizadas.

SISTEMAS DE INFORMACIÓN HOSPITALARIOS

El mapa del sistema de información hospitalario está conformado por un conjunto extenso de aplicaciones y soluciones de mercado y propias de Capio. El núcleo del sistema de información hospitalario es el HIS de Indra (SIA), con el que se integran el resto de soluciones propias y externas que cubren las áreas de actividad hospitalaria no cubiertas por SIA.

El HIS SIA de Indra es un sistema integral de gestión hospitalaria que responde a las necesidades de operación (agendas, citaciones, admisiones, urgencias...), clínicas (Historia Clínica, Enfermería, seguimiento del paciente, terapéutica, prestaciones...), económico-financieras (contratación y compras, logística, facturación, cobros y pagos...) y de control de gestión (actividad, costes, resultados, beneficios...), de cualquier Centro Asistencial.

Contempla los estándares internacionales de información, con facilidades para la conexión y comunicación con otros Centros, susceptible de implantación modular y gradual y de integrarse con otros sistemas existentes. Permite descentralizar la entrada de datos y la obtención de consultas e informes por toda la organización, sometido a un riguroso sistema de seguridad.

La Historia Clínica conforma el núcleo del Sistema. Todas las acciones clínicas, que se realizan desde los Servicios Médicos y de Cirugía y desde Enfermería, tanto en Urgencias, Hospitalización y en Consultas Externas, así como en los Servicios Centrales (Diagnóstico por Imagen, Laboratorios, etc.), quedan actualizadas con sus resultados en tiempo real en la Historia Clínica del Paciente.

La definición de los protocolos de actuación: antecedentes, anamnesis, exploraciones, valoraciones y tratamientos, asociados a Servicios, diagnósticos, problemas o procedimientos, son definibles por cada Hospital y especialidad en función de sus necesidades.

Algunas de las ventajas más significativas del HIS de Indra se derivan de sus propias características y de los beneficios que supone para profesionales, gestores, pacientes y usuarios del Sistema. A continuación se resumen algunos aspectos destacables con los que cuenta dicho Sistema:

- Identificación única del paciente y la posibilidad de localizar y seguir su evolución, disponiendo de datos clínicos del mismo haya o no estado ingresado y disponga o no de Historia Clínica (carpeta física) abierta.
- Orientación a los Procesos. El producto está concebido de acuerdo con los "flujos de trabajo específicos", del Centro Asistencial. Las informaciones fluyen de un Servicio a otro y de una persona a otra, conforme al trabajo a desarrollar por el personal médico y de enfermería y por el personal administrativo, ayudando y guiando la ejecución de los trabajos, siendo el Sistema el que se adapta a la organización del Centro y no viceversa. La información se captura allí donde se genera y todos los procesos operativos de la solución se ejecutan en tiempo real, teniendo disponible online y de manera permanente la información de la situación del Centro.
- Estructura multidimensional. Con dicha Solución se pueden definir libremente la estructura del Centro, configurando los Servicios Generales, Administrativos, Asistenciales y de Soporte Asistencial, las Agendas, Unidades de Enfermería, Prestaciones, áreas de negocio, áreas asistenciales, o cualquier otra estructura que se desee.
- Incorporación de mecanismos de seguridad a nivel de acceso a la información y ejecución de programas, adaptables por el Administrador del Sistema del Centro Asistencial.
- Arquitectura multi nivel. El Sistema está concebido bajo una arquitectura cliente-servidor y posee un interfaz gráfico de usuario amigable y con ayudas en castellano, integrándose fácilmente con el resto de sistemas, Bases de Datos, Correo Electrónico, Herramientas Ofimáticas, etc. ., distribuible a través de Servicios de Terminal (MTS, Citrix Metaframe), Cliente Ligero.

El HIS de Indra está estructurado en diferentes módulos que pueden implantarse de forma integral o parcialmente, integrándose con el resto de sistemas del Hospital.

Los módulos que componen el Sistema de Información Hospitalario de Indra son los siguientes:

- Admisión de Ingresos
- Lista de Espera
- Hospitalización
- Urgencias
- Citaciones y Consultas
- Hospital de Día
- Codificación y archivo de Historias Clínicas
- Estación de Enfermería
- Neonatos
- Estación Servicios Médicos
- Quirófanos
- Radiodiagnóstico
- Gestor de peticiones electrónicas.
- Farmacia y Unidosis.
- Dietética y Nutrición

- Contabilidad Financiera y área Fiscal.
- Tesorería. Cuentas a cobrar y pagar.
- Facturación
- Activos Fijos.
- Logística. Compras y Almacenes.
- Gestión Presupuestaria.
- Portal del Profesional. Gestión de Honorarios Médicos.

SISTEMAS DE INFORMACIÓN PARA LAS ÁREAS FUNCIONALES DEPARTAMENTALES

Además de la solución de Indra, existen otras soluciones departamentales de terceros que se integran con Indra. Las más relevantes son las siguientes:

ÁREA	APLICACIÓN / SISTEMA	PROVEEDOR
Anatomía Patológica	NOVOPATH	VITRO
Banco de Sangre	DELPHYN	EVOLUTION
Laboratorios	SGLAC	DBSOFT
Endoscopias	ENDOTOOLS	PENTAX
Cardiología	TRACE MASTER VIEW	PHILIPS
PACS Imagen Diagnóstica (RX, Hemodinámica, ...).	OKDICOM	IRC MED
Área de Críticos. UCI. Anestesia.	B-ICU.SAMPLE	B-SAMPLE
Obstetricia y Ginecología.	POR DETERMINAR	
Identificación Madre-Hijo	POR DETERMINAR	
Diálisis y Nefrología	NEFROSOFT	VISUAL-LIMES
Sistema de gestión y almacenamiento digital de electrocardiógrafos.	TRACE MASTER VIEW	PHILIPS
Gestión de reclamaciones.	IGR	CAPIO
Historia Clínica Electrónica Web	HCEw	CAPIO
Gestión centralizada Informes Diagnósticos RX.	TCC	CAPIO
Sistema de avisos y redireccionamiento pacientes	NEMOQ	NEMOQ
Recursos Humanos y Nómina.	MILENA	SERESCO
Gestión Tiempos de trabajo y Planning.	AIDA	HEWLETT-PACKARD
Sistema de gestión para la Investigación. Portal del Investigador.	INVESTIGACIÓN	CAPIO
Gestión de Docencia y MIR.	DOCENCIA	CAPIO
Contabilidad Analítica.	IFMS GESCOT	INDRA SAVAC

OTRAS SOLUCIONES INTEGRADAS

Además de las soluciones descritas anteriormente, que conforman el mapa de sistemas de información hospitalario, existen otra serie de soluciones dirigidas a profesionales que complementan el mapa de soluciones y proporcionan herramientas y sistemas de ayuda a la toma de decisiones y a la gestión de actividad diaria.

DATAWAREHOUSE-BUSSINES INTELLIGENCE

Capio dispone de un sistema completo de cuadro de mandos que sirve de apoyo a la toma de decisiones, control y gestión. El objetivo de este sistema se puede resumir en:

- Dotar a los responsables de gestión de los hospitales, en sus distintos niveles, de un instrumento que permita realizar un seguimiento y control de los objetivos y facilite el proceso de toma de decisiones.
- Obtener un conjunto de indicadores homogéneos para que permitan elaborar un Cuadro de Mando adaptado a cada nivel de responsabilidad en la gestión de los hospitales.

El núcleo central de este sistema se denomina PAI, Punto de Acceso a la Información. Se trata de un portal web que centraliza la información de todas las áreas del centro. Se estructura tanto por áreas asistenciales como por áreas de gestión Económica-Financiera. De esta forma es posible dar acceso a cada profesional al área y nivel de su interés.

INTRANET HOSPITALARIA Y HERRAMIENTAS DE COLABORACIÓN

El Hospital de Collado-Villalba pondrá a disposición de sus profesionales una serie de portales web y entornos colaborativos tanto temáticos como generalistas.

Cómo herramienta para publicar estos portales se usa Microsoft SharePoint lo que proporciona una plataforma para compartir información y trabajar en grupos, comunidades y procesos. De esta forma son los propios usuarios los que tienen la posibilidad de crear y controlar sus propias áreas de trabajo de colaboración.

El acceso a los portales temáticos y áreas de colaboración se realiza mediante la intranet del centro. En esta se encuentra la información relevante para los profesionales del hospital, como pueden ser noticias, anuncios, calendario de eventos, así como link a los portales temáticos creados a petición de los propios profesionales a la medida de sus necesidades.

Estos portales también están pensados con vocación multicentro, de forma que se conviertan no solo en punto de colaboración entre profesionales de un hospital, si no que crezcan hasta convertirse en el punto de encuentro de todos los profesionales de la organización.

TELEDIAGNÓSTICO Y COLABORACION

El Hospital de Collado-Villalba ofrecerá diferentes servicios relacionados con el Telediagnóstico, facilitando la comunicación remota de pacientes y profesionales.

- **Videoconferencia**. Capio dotará al Hospital de Collado-Villalba de sistemas de videoconferencia que permitan la comunicación entre profesionales. El uso de estas tecnologías permitirá:
    - Sistema multi-conferencia, permite la comunicación entre varios centros.
    - Conexión en tiempo real para compartir información.

- Junto con el uso de sistemas de transmisión de imagen médica, discutir diagnósticos.
- Formación de los profesionales.
- Asistencia remota a sesiones clínicas.
- Diagnóstico remoto tanto a otros centros hospitalarios, cómo a centros de salud, cómo inclusive en el hogar del propio paciente.

- **Centro Capio de Tele diagnóstico.** Capio dispone de una solución informática para la gestión remota de informado de pruebas radiológicas. El sistema consiste básicamente en un PACS centralizado que recibe estudios de aquellos hospitales o profesionales que demandan informe, y una vez realizado este se integra en el sistema de información asistencial del Hospital. Este PACS centralizado incorpora un sistema de agendas de especialistas colaboradores, permitiendo asignarles los estudios y remitírselos de forma inmediata.

  El sistema es de aplicación tanto para la derivación de estudios en caso de no ser capaz de asumir la demanda por medios propios y cumplir plazos de entrega rápidos a pacientes como para otras aplicaciones, como segunda opinión

ACCESO WIFI Y SOLUCIONES DE MOVILIDAD

El Hospital de Collado-Villalba ofrecerá desde el inicio, dentro de la cartera de servicios ofertados al ciudadano y al profesional acceso WiFi en todo el Hospital. Esta cobertura permitirá ofrecer los siguientes servicios desde la apertura del Hospital:

- Ofrecer acceso a Internet en Aulas, Biblioteca, Sala Juntas, utilizadas tanto por profesionales propios como externos. Posibilidad de acceso a la red interna para profesionales autorizados.
- Ofrecer conectividad en las áreas hospitalarias para la conexión a los sistemas de equipamiento médico.
- Movilidad: el Hospital de Collado-Villalba dará soluciones de movilidad a sus profesionales utilizando diferentes dispositivos para el acceso a la información. Entre las principales soluciones y utilidades estarán las siguientes:

  - Consulta de HCE de paciente
  - Pase de visita en planta
  - Petición de pruebas (Laboratorio, Radiología, etc.)
  - Listas de pacientes con acceso a su HCE
  - Atención en Urgencias
  - Envío y recepción de mensajería SMS para alertas.
  - Etc.

  El acceso se realizará a través de dispositivos como portátiles, tablet-PC, agendas electrónicas o teléfonos móviles. También se dispondrá de monitores en habitaciones de Hospitalización que además de ofrecer servicios a pacientes como TV y acceso a Internet permitirá la conexión al sistema de información hospitalario para ser utilizado por profesionales médicos y de Enfermería.

6. INTEGRACIÓN CON SISTEMAS CSCM

Es compromiso y política de Capio que todos sus profesionales implicados en la prestación de servicios hagan uso adecuado y extensivo de los sistemas de información, como herramienta de apoyo a la gestión para garantizar la disponibilidad de los datos asistenciales en la Historia Clínica Electrónica y de gestión de los procesos, permitiendo así la explotación de esos datos según los requerimientos de la Administración.

El Hospital de Collado-Villalba estará desde su apertura integrado con los Sistemas de Información de la CSCM, garantizando la evolución de los sistemas de información de acuerdo a las nuevas necesidades de integración que surjan por nuevos sistemas, módulos o proyectos y disponiendo de las infraestructuras necesarias para garantizar los requisitos de disponibilidad que estas integraciones necesitan.

Los sistemas de información a implantar en el Hospital de Collado-Villalba son los mismos que el utilizado en los Hospitales Infanta Elena y Fundación Jiménez Díaz, también gestionados por Capio, lo que garantiza la correcta integración de todos los sistemas desde el inicio de la actividad.

La siguiente tabla muestra todos los sistemas y aplicaciones que serán integrados con las soluciones del Hospital o a las que, sin necesidad de integración, se dará acceso directo a los usuarios:

Sistema	**Integración**	**Acceso**	**Remisión Información**
SSII DE PACIENTES			
ALCOR. Análisis casuística, clasificación y agrupación de pacientes a través de GRDs			X
Clasificación de pacientes en Triaje de Urgencias (Integración con Cuadro Mando)	X		
CESTRAK. Gestión de reclamaciones de Atención al Paciente	X		
CIBELES	X		
ELA. Registro de Esclerosis lateral Amiotrófica.			X
HORUS. Visor de HC unificada.	X		
PALOMA. Detección precoz cáncer de mama. Integración con PACS y RIS.	X		
Petición de órdenes de digitalización			
REMAC. Registro madrileño de agresiones y conflictos.			X
REMER. Registro madrileño de enfermos renales.		X	
RULEQ. Registro unificado de lista espera quirúrgica	X		
SIUL. Registro de trasplantes.			X
TARJETA SANITARIA. Sincronizado con Cibeles.	X		
RULED			X
GESTOR DIGITALIZACIÓN			X

SSII DE CITACIÓN			
ARETEO. Registro de últimas voluntades		X	
MULTICITA. Citación centralizada en Hospitales	X		
SCAE. Solicitud de cita en atención especializada.	X		
SSII INTERNOS DEL HOSPITAL.			
CMBD. Para Hospitalización y ambulantes.			X
SIAE. Sistema de Información de Atención Especializada.			X
SICAR. Sistema de Información Cartera de Servicios		X	
SICYT. Sistema de información de Consultas y Técnicas Diagnósticas.			X
BANCO DE SANGRE.	X		
GESTIÓN AI. Gestión de identidades (altas, bajas usuarios)		X	
GESTIÓN DE CONTENIDOS. Del Hospital en el Portal de Salud		X	
INTRANET SALUD@. Intranet Consejería.		X	
SSII DE FARMACIA			
ASTARE. Gestión de talonarios de recetas.		X	
FARM@DRID. Cuadro mando seguimiento gasto farmacéutico.		X	
REGISTROS SANITARIOS			
HAC. Detección precoz de hipoacusias en recién nacidos		X	
NOSOCOMIALES. Declaración de enfermedad nosocomial en Hospitales de la CAM.		X	
NOTAB. Notificaciones accidentes biológicos producidos en el puesto de trabajo.		X	
VACUNAS. Registro personas vacunadas y gestión vacunas.		X	
OTROS			
SUMMA112. Gestión de traslados programados (no urgentes)	X		
AP MADRID. Integración peticiones y resultados Laboratorio.	X		

Además todas estas integraciones se deben ajustar a los requerimientos y estándares adecuados para la interconexión de la Red Sanitaria con otras redes, establecidos por la DGSIS, considerándose los aspectos arquitectónicos y de seguridad de estas conexiones respecto a:

- Los mecanismos de publicación de aplicaciones y servicios (https, …)
- La autentificación y autorización (AD Microsoft y Certificados)
- La integración de servicios (la pactada, Web Services W3C, …)

SOLUCIONES DE INTEGRACIÓN PARA ATENCIÓN PRIMARIA

PORTAL DEL PROFESIONAL DE ATENCIÓN PRIMARIA

El Hospital de Collado-Villalba habilitará el acceso de todos los profesionales de Atención Primaria de su área de influencia de un portal denominado "Portal del Profesional de Atención Primaria". Al mismo pueden acceder los trabajadores de los Centros de Salud de su área. En este portal encuentran:

- Manuales y documentos
- Listas de contactos
- Noticias y eventos
- Acceso a otros portales
- Información de pacientes

Este último apartado es de un gran valor añadido tanto al profesional asistencial como al administrativo, ya que dispone de acceso a la información online de los pacientes de su centro en el hospital. Más en concreto se ofrece:

- Consulta Historia Clínica de Pacientes, acceso a la Historia Clínica Web de Capio, como se muestra en anexo "Historia Clínica Web"
- Información en formato listado con acceso a informes e historia clínica:
  - Informe de Citas de un Paciente
  - Informe de Anatomía Patológica
  - Informes de Consultas
  - Informes de Enfermería
  - Informes de Laboratorio
  - Informes de Diagnóstico por Imagen
  - Pacientes en Hospitalización
  - Pacientes en Quirófanos
  - Pacientes en Urgencias

Como servicios adicionales a los profesionales de Atención primaria, se habilitarán sistemas electrónicos para la activación de alertas y para la comunicación de altas en Hospitalización y Urgencias.

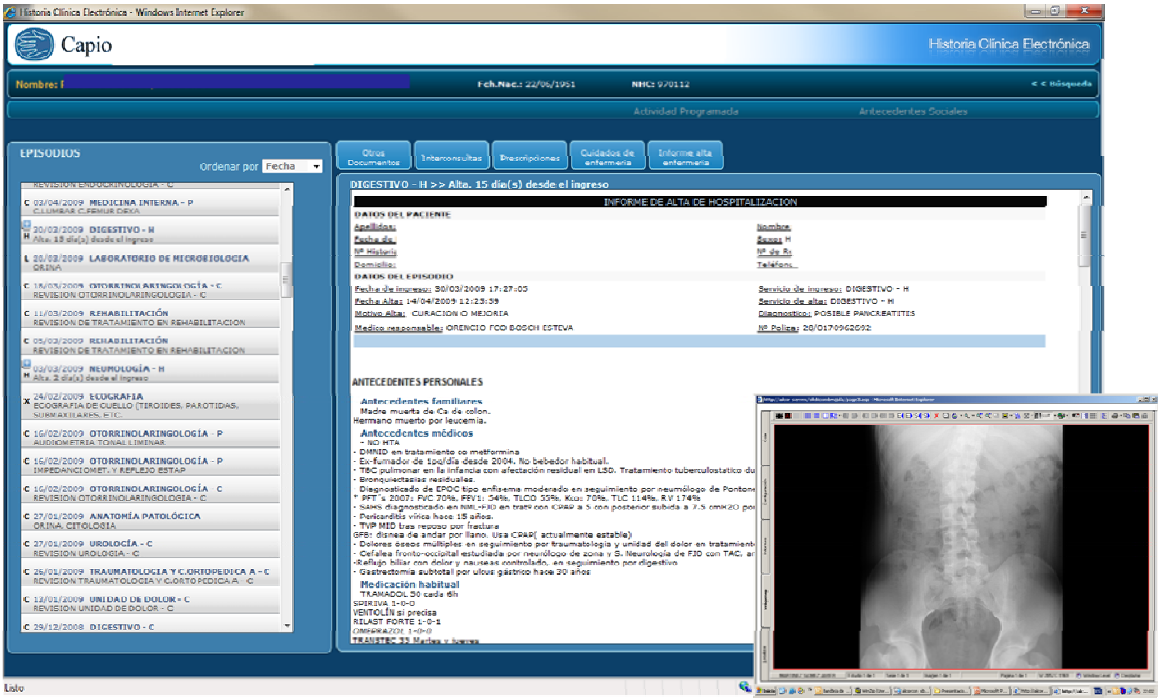
Este portal nace en un contexto previo a la implantación del proyecto de Libre Elección y se viene utilizando desde hace tiempo por los profesionales de Atención Primaria que interactúan con otros hospitales que gestiona Capio Sanidad. Es intención mantener el valor añadido que aportan las funcionalidades aquí reseñadas, así como el factor colaborativo que facilita en la relación entre ambos colectivos de profesionales, pero entendemos también que alguno de los aspectos que contempla están o estarán resueltos con la implantación de otras integraciones que la CSCM ha acometido en el marco de este proyecto, nos referimos a sistemas como el visor HORUS de HC, con el que este hospital nacerá integrado y otras funciones que solapen a las ya existentes en este portal. En este sentido se facilitará el acceso a estas aplicaciones con la incorporación de links específicos en el portal ya existente. También se facilitará el acceso al mismo para otros profesionales que fuera de los centros de salud de referencia se estime deban usar estas herramientas.

VISOR WEB COMPARTIDO HISTORIA CLÍNICA PARA ATENCIÓN PRIMARIA Y ESPECIALIZADA

Dentro de las herramientas con las que cuenta Capio para uso de sus profesionales, se engloba el Visor Web de Historia Clínica. Su objetivo es ofrecer información sobre la actividad realizada sobre un paciente en el entorno de Atención Especializada. Este visor está disponible tanto para los profesionales de Atención Especializada, como también para los profesionales de Atención Primaria, siendo este último punto quizás el más importante, por lo que supone de nexo de unión entre los dos ámbitos de actuación sanitaria.

Este visor muestra la información completa "on line" y se encuentra integrado con OMI en más de 30 centros de salud de la red sanitaria madrileña. También se encuentra integrado con AP Madrid.

Mediante esta integración tiene un acceso directo a la historia del paciente sin necesidad de búsqueda. Además dispondrá de acceso a un buscador a través del Portal del Profesional de Atención Primaria. El acceso a la información se realiza de forma segura mediante acreditación de usuario, pudiendo de esta forma filtrar a que pacientes se tiene acceso.

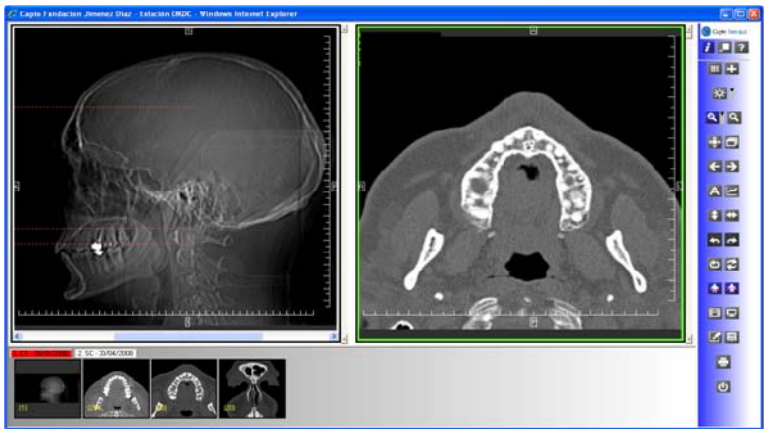


Las características principales de este visor son:

- Vista de todos los episodios del paciente en el centro. Disponible un acceso rápido en la parte de la izquierda a cada uno de ellos. Se pueden ordenar por área, fecha, especialidad o servicio.
- Una vez seleccionado el episodio muestra la información correspondiente en función del carácter de cada uno. Estos datos son:
  - Consentimientos informados
  - Documentación aportada por el paciente

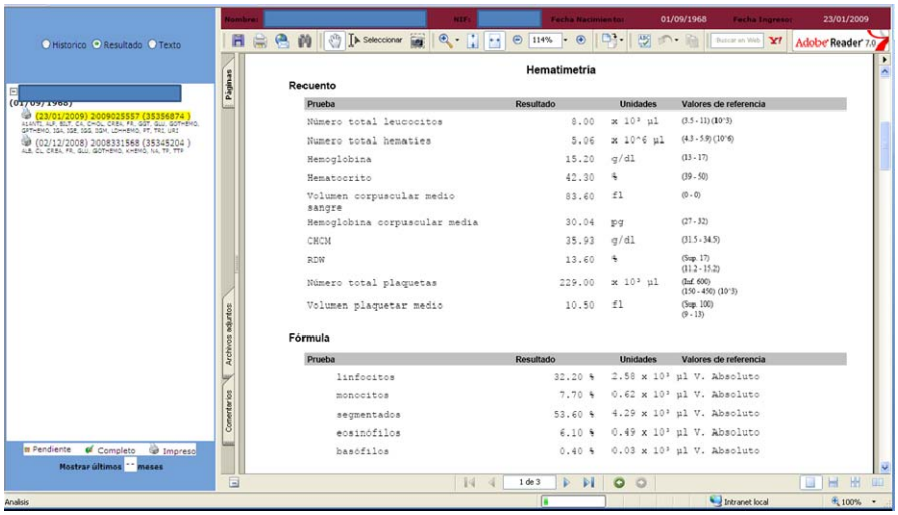
- Informes de alta médicos
- Informes de alta de enfermería
- Informes de seguimiento durante hospitalización
- Medicación suministrada durante hospitalización
- Prescripción al alta.
- Cuidados de enfermería durante hospitalización
- Informes de seguimiento durante urgencias
- Medicación suministrada durante urgencias
- Cuidados de enfermería durante urgencias
- Pruebas de laboratorio
- Informe e imágenes de pruebas de Diagnóstico por Imagen
- Informes de Exploraciones Especiales
- Informes de Interconsultas
- Informes de Consultas
- Informes quirúrgicos
- Informes Preanestésicos

- Acceso a actividad programada
  - Citas de atención especializada
  - Citas de pruebas especiales
  - Intervenciones quirúrgicas
- Acceso a Historia Social del paciente. Si el paciente ha sido atendido por otros profesionales asistenciales, como puede ser trabajo social, se dispone de acceso a su historia y actuaciones efectuadas.
- Visor de estudios de Diagnóstico por imagen. Disposición de un visor en formato Dicom, que cuenta con las siguientes herramientas:



- Elección de número de series e imágenes por serie a mostrar
- Posibilidad de comparación de estudios, incluso de diferentes modalidades
- Zoom y lupa
- Medidas
- Espejo horizontal y vertical
- Líneas de referencia
- Multiframe
- Impresión

- Visor de estudios de laboratorio: Acceso a los resultados de las pruebas de laboratorio. Permite la comparación de históricos.



7. SERVICIOS ORIENTADOS AL CIUDADANO

El Hospital de Collado-Villalba activará una serie de sistemas que aportan accesibilidad, cercanía, información y en general, facilitan la atención del ciudadano en su uso del sistema sanitario, así como fomentan su participación en el mismo. Estas soluciones facilitan el acercamiento del paciente a su Hospital, y en su diseño serán tenidos en cuenta las obligaciones y recomendaciones recogidas en la Ley 30/2002 de servicios de la sociedad de la información y de comercio electrónico.

Algunas de estas soluciones son:

PORTAL WEB DEL CIUDADANO

Espacio web dirigido a ciudadanos y profesionales, ofrecerá las mismas funcionalidades que el resto de Hospitales de la Red Pública Sanitaria de la Comunidad.

Diseño, estructura y contenidos estarán ajustados a los estándares marcados por la CSCM, garantizando su homogeneidad.

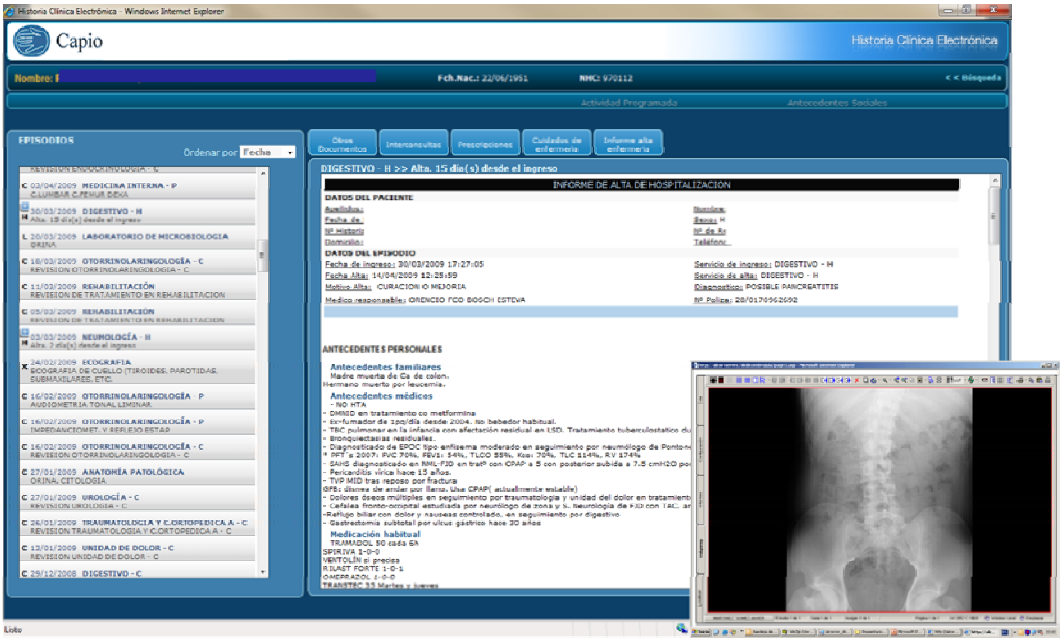
CITACIÓN CENTRALIZADA

Además de la integración del sistema de información hospitalario con sistemas como Multicita, también dispone de una plataforma de citación por internet que puede permitir que sus usuarios gestionen sus propias citas en el centro.

ACCESO DE LOS CIUDADANOS A SU HISTORIA CLÍNICA ELECTRÓNICA A TRAVÉS DE INTERNET

El Hospital de Collado-Villalba activará un sistema de acceso seguro y encriptado de los ciudadanos a su HCE, de esta manera la información está accesible para el ciudadano en cualquier momento. Mediante el uso de los adecuados sistemas de autentificación, y a través del portal del Hospital podrá consultar los siguientes documentos:

- Informes de alta en Urgencias
- Informes de alta de hospitalización
- Informes de Consultas Externas de Especializada
- Pruebas de laboratorio y Radiología (Imagen digital incluida).
- Otros…



LIBRE ELECCIÓN DE ESPECIALISTA

El Hospital de Collado-Villalba garantiza desde su apertura la cobertura de las funcionalidades requeridas para la gestión del derecho de los ciudadanos a escoger al médico especialista y hospital que deseen dentro de toda la oferta.

Cabe comentar que en el momento de redacción de este Plan los hospitales que Capio gestiona en colaboración con la Comunidad de Madrid están implicados en proyectos TIC directamente relacionados con la Libre Elección, como la integración con sistema Multicita y con el Visor de HC Horus.

PUNTOS DE INFORMACIÓN

En diferentes zonas del Hospital se instalaran dispositivos diseñados para comunicar a los ciudadanos información de interés del Hospital y el tipo de información habitual en este tipo de medios.

Adicionalmente, el Hospital de Collado-Villalba utilizara estos puntos de información para ofrecer servicios de autoservicio añadidos a pacientes, como los siguientes:

- Obtener información general sobre el hospital y los servicios sanitarios
- Ubicación de los servicios
- Obtener ticket de autoservicio para las zonas de acceso y espera, integrado con sistemas visuales de aviso y con el sistema de información, de forma que el médico en Consulta conoce la llegada del paciente.
- Autogestión de cita u otra actividad programada.
- Otra información personalizada.

Estos dispositivos dispondrán de interfaces de usuario que permitan una interacción intuitiva, fácil, rápida y exacta al usuario sobre su contenido, utilizando pantallas táctiles y mecanismos de seguridad para aquellas aplicaciones que requieran de la identificación inequívoca del ciudadano.

Teniendo en cuenta la arquitectura del Nuevo Hospital de Collado-Villalba, la ubicación de las zonas de acceso y todas las salas de espera, el número de puntos de información previstos es de 8 unidades de dispensadores o quioscos.

Estos dispensadores estarán provistos de las siguientes características HW:

- Pantalla táctil
- PC en su interior con tarjeta de comunicaciones
- Lector de tarjetas monitorizado
- Impresora térmica expendedora de tickets

SISTEMAS VISUALES DE AVISOS EN ZONAS DE ACCESO Y ESPERA

El Hospital contempla en su oferta la utilización de dispositivos de cartelería electrónica o pantallas visuales para:

- Avance de los turnos de espera en los puntos de admisión o información donde sea necesario.
- Avance de los turnos de espera en las salas de espera de consulta, para lo cual el ciudadano con cita previa habrá tenido que previamente identificarse en un dispensador automático o punto de admisión donde habrá obtenido su ticket de espera.
- Avisos a familiares de pacientes en urgencias o quirófanos, en las salas de espera de estas unidades. Para ello se utilizaran identificadores solo reconocibles por los destinatarios del mensaje.
- Otros puntos donde se requiera mostrar otros mensajes de relevancia

Son requisitos imprescindibles de estos sistemas el cumplimiento de los términos de la LOPD. Estas pantallas, que en general serán dispositivos de tipo LFD, permitirán alternar otro tipo de mensajes informativos específicos sobre el servicio u otros de carácter general sobre el hospital o servicios sanitarios.

De la misma forma, y de acuerdo a la distribución y ubicación de los servicios en el hospital, el número previsto de unidades de estos Sistemas Visuales, es de 30, para dotar al nuevo Hospital de Collado-Villalba.

Las características HW de estas unidades son:

- Monitor LFD profesional (32" o 40") con PC integrado conectado a la red
- Soporte pared o techo, con sistema de bloqueo

PLATAFORMA DE ENVÍO DE SMS

Se dispone de una plataforma de envío de mensajes SMS integrada con el resto de soluciones incluidas. Esta plataforma nos permite actuar en dos ámbitos, usuario y profesional del sistema, facilitando la comunicación. Algunos ejemplos de la utilización de mensajería SMS a usuarios desde Hospital son:

- Generar recordatorios automáticos de citas.
- Anulación de citas.
- Aviso de disponibilidad de resultados de pruebas e informes.
- Información a los familiares de los pacientes en urgencias, quirófanos, hospitalización.
- Etc.

PLATAFORMA DE ENVÍO DE EMAIL

Se dispone de una plataforma de envío de EMail integrada con el resto de soluciones incluidas. Esta plataforma nos permite actuar en dos ámbitos, usuario y profesional del sistema. Algunos ejemplos de uso:

ACCESO WIFI

El Hospital contempla dentro de los servicios ofertados al ciudadano acceso WiFi abierto en todo el Hospital. De esta forma tanto los pacientes como los familiares podrán disponer de una fuente de entretenimiento, información y comunicación con el exterior durante su estancia.

8. SERVICIOS DE MANTENIMIENTO Y SOPORTE A USUARIOS

En este capítulo se incluye la descripción de los servicios de mantenimiento posteriores a la implantación de la infraestructura necesaria para la prestación de los mismos.

El Hospital de Collado-Villalba utilizará como base la Metodología ITIL, de este modo, los procedimientos de gestión y administración aseguran el correcto funcionamiento del hospital y una estandarización y homogeneización de los mismos, así como de los sistemas en entorno de soporte tecnológico y a la implantación de sistemas.

Además el área de T.I. propuesta para el Hospital de Collado-Villalba contempla la interlocución e integración con los sistemas de soporte a usuarios de la CSCM.

Para la correcta administración y mantenimiento, el área T.I. del Hospital se apoyará en los servicios que a continuación se explican en mayor grado de detalle:

- Técnica de Sistemas
- Bases de Datos
- Explotación de Operación
- BRS (Backup&Recovery System)
- Comunicaciones
- Mantenimiento de Aplicaciones
  - Correctivo
  - Evolutivo
- Equipamiento periférico, equipos de usuario
- Soporte a Usuarios y atención de Incidencias
- Gestión de Inventario
- Distribución de SW
- Monitorización
- Mantenimiento de HW en el puesto de trabajo
- Soporte Software a Usuarios
- Gestión del Servicio
- Modelo de Relación Soporte CAPIO-CESUS

El Hospital asegura la disponibilidad de los recursos técnicos apropiados, así como el equipo humano adecuado para llevar a cabo las tareas comprometidas en estos servicios.

La CSCM podrá solicitar en cualquier momento informes sobre las labores de gestión y mantenimiento realizadas. Dichos informes se entregarán en un plazo máximo de cinco días laborables desde su solicitud.

TÉCNICA DE SISTEMAS (Almacenamiento – Sistemas Operativos)

Objetivos

- Mantener la continuidad en el servicio de los recursos disponibles.
- Actualizar los productos instalados: hardware, parches, upgrades, etc.
- Innovar con nuevos servicios: sistemas operativos y aplicaciones, etc.
- Gestionar los recursos de forma preventiva.

Alcance

El Servicio de Técnica de Sistemas tiene como ámbito desarrollar la técnica de sistemas del hardware y software instalados en el Hospital de Collado-Villalba.

Funciones

- Estudiar y responsabilizarse de todas las rutinas que se puedan utilizar para potenciar la capacidad de trabajo de los Sistemas Operativos.
- El tunning del rendimiento de los Sistemas: la configuración y el ajuste de rendimiento de Servidores y Sistemas operativos.
- La gestión de actualizaciones del software de base.
- Cualquier otra tarea de planificación, coordinación y mejora del rendimiento del servicio.
- Analizar y evolucionar las metodologías de trabajo de sistemas.
- Medir y evaluar periódicamente el rendimiento de las máquinas, incluyendo el análisis de la capacidad disponible de espacio en disco.
- Seguir la evolución de los productos e instalar las actualizaciones pertinentes: parches, novedades, utilidades, etc.

Modelo Operativo

Este servicio orienta sus funciones hacia la gestión de los servidores así como los Sistemas Operativos alojados en los mismos.

El modelo aplicar está basado en la Metodología ITIL que aspectos como:

- Gestión de Configuración
  - Instalación y actualización de los sistemas operativos
  - Instalación y configuración de software
  - Administración, instalación y configuración de los servidores,
  - Gestión del cambio en los sistemas (Planificación, Seguimiento, Test de prueba e implementación),
  - Gestión (contacto y seguimiento) con proveedores de soporte a los efectos de la administración y operación diaria

  - Tunning y Capacity Planning.
  - Inicialización del S.O. y sus componentes.
  - Instalación de Racks
- Gestión de Performance
  - Control y análisis de registros de eventos de los sistemas (Mediciones)
  - Planeamiento de capacidad y de actualización
  - Propuesta de soluciones que optimicen la performance
  - Análisis de impacto ante diferentes situaciones
  - Mediciones para administrar el S.O.
- Técnica de Sistemas Correctiva:
  - La gestión del mantenimiento correctivo de los dispositivos hardware y software centrales del cliente
- Técnica de Sistemas Adaptativa:
  - El tunning del rendimiento de los Sistemas: la configuración y el ajuste de rendimiento de Servidores y Sistemas Operativos
  - La gestión de actualizaciones tanto de Hardware y Software Base
  - Gestión del paso a explotación de las nuevas versiones de las aplicaciones.
- Técnica de Sistemas Preventiva:
  - Estudios periódicos del funcionamiento de los sistemas para detectar problemas potenciales: ocupación del espacio en disco, etc.
  - El desarrollo de las mejoras que hayan sido detectadas en los estudios anteriores y que hayan sido aprobadas
  - Así como cualquier otra tarea de planificación, coordinación y mejora del rendimiento del servicio

Procedimientos

- Procedimiento de gestión de configuración.
- Procedimiento de gestión de cambios.
- Procedimientos para el Servicio de Explotación y Operación
- Procedimiento de resolución de incidencias (y el escalado correspondiente que se acuerde)
- Procedimientos para la obtención de las copias de seguridad de los sistemas y de las aplicaciones y de los datos en producción: frecuencia de las copias de seguridad, frecuencia del envío de copias de seguridad a otro centro para prevenir desastres, etc., y los procedimientos para la recuperación de los datos siguiendo los procesos que se establezcan.

BASES DE DATOS

Objetivos

- Gestión integral de las Bases de Datos
- Mantener la continuidad en el servicio de los recursos disponibles.
- Actualizar los productos instalados: hardware, parches, upgrades, etc.
- Gestionar los recursos de las Bases de Datos de forma preventiva.

Alcance

El Servicio de Bases de Datos tiene como ámbito desarrollar aspectos de la técnica de sistemas relativas a las Bases de Datos de los Sistemas instalados en el Hospital de Collado-Villalba.

Funciones

- Instalación y upgrade de nuevas versiones y herramientas de la base de datos.
- Creación de las estructuras de almacenamiento primarias de la base de datos (Tablespaces).
- Creación de los objetos primarios (tablas, vista, índices).
- Creación y modificación de la estructura de base de datos.
- Monitorización y Control de los accesos de los usuarios a la base de datos.
- Monitorización y tunning de la base de datos.
- Backing up y restoring de la Base de Datos.
- Propuesta de soluciones que optimicen la performance
- Análisis de impacto ante diferentes situaciones
- Utilización de recursos
- Definición y mantenimiento del sistema de seguridad.
- Relación con los fabricantes para el soporte técnico de tercer nivel.
- Dimensionamiento del espacio de almacenamiento requerido.
- Estimaciones de los requerimientos de almacenamiento futuros.

Modelo Operativo

Este servicio orienta sus funciones hacia la gestión de las bases de datos.

El modelo aplicar está basado en la Metodología ITIL que cubre aspectos como:

- Gestión de Configuración

- Administración, instalación y configuración nuevas versiones
- Instalación y upgrade de nuevas versiones y herramientas de la base de datos.
- Gestión del cambio en los sistemas (Planificación, Seguimiento, Test de prueba e Implementación)
- Tunning de las Bases de Datos

- Gestión de Performance
  - Control y análisis de registros de eventos de las Bases de Datos (Mediciones)
  - Planeamiento de capacidad y de actualización
  - Propuesta de soluciones que optimicen la performance
  - Análisis de impacto ante diferentes situaciones

Procedimientos

- Procedimiento de recuperación de datos.
- Procedimiento de creación y modificación de la estructura de las bases de datos.
- Procedimiento de tunning de la base de datos.
- Procedimiento de actualización de tablas.

Organización

Responsabilidades y Tareas del Administrador de la Base de Datos:

- Instalación y upgrade de nuevas versiones y herramientas de la base de datos.
- Dimensionamiento del espacio de almacenamiento requerido.
- Creación de las estructuras de almacenamiento primarias de la base de datos .
- Creación de los objetos primarios (tablas, vista, índices).
- Creación y modificación de la estructura de base de datos.
- Definición y mantenimiento del sistema de seguridad.
- Mantenimiento de los perfiles de usuario.
- Mantener la relación con los fabricantes para el soporte técnico de tercer nivel.

EXPLOTACIÓN Y OPERACIÓN

Objetivos

- La gestión de la plataforma de explotación, la obtención de resultados de explotación en relación con el calendario y nivel de servicios previsto y la realización de aquellas operaciones no específicas de usuarios necesarias para el correcto funcionamiento del servicio
- Mantener la continuidad en el servicio de los recursos disponibles.
- Elaborar mecanismos de monitorización proactiva de los elementos críticos de la plataforma de certificación.

- Detectar problemas potenciales/reales.
- Establecer métodos/procedimientos para medir calidad de Servicio
- Lograr la utilización eficaz de los recursos de explotación que configuran la plataforma tecnológica, cumpliendo con los calendarios establecidos y con el nivel de servicio marcado.
- Realizar la operativa diaria del servicio
- Garantizar la seguridad e integridad de los datos

Alcance

El Servicio de Explotación y Operación como ámbito desarrollar aspectos de la técnica de sistemas relativas a la operación del servicio de los Sistemas instalados en el Hospital de Collado-Villalba.

Funciones

- Mantener en estado operativo cada uno de los sistemas de la plataforma tecnológica soporte del servicio, conociendo en cada momento el estado y la carga en cada servidor.
- Identificar origen de alertas como consecuencia de que determinados parámetros del servicio hayan superado los umbrales previstos.
- Gestión de las incidencias del servicio de explotación. Una explotación real es susceptible de tener incidencias por lo que se tendrán previstas medidas para minimizar el impacto de las mismas y reducir el porcentaje de tiempo durante el que los sistemas están o bien fuera de servicio, o bien dando un servicio degradado. Para minimizar este es por lo que se propone un procedimiento de resolución de incidencias que contemple, entre otros:
- Las documentación de las incidencias, analizando las causas y soluciones adoptadas en cada caso, de tal forma que el histórico de incidencias constituya un sistema de conocimiento para facilitar la resolución de las mismas
- Supervisar la recepción y el control de los datos y soportes de entrada a los procesos de explotación.
- Controlar la calidad de resultados de los trabajos y resolver las incidencias dentro de su ámbito de competencia, así como su registro y escalado si procede
- Mantener actualizadas y disponibles las bibliotecas técnicas (manuales técnicos de los equipos y periféricos, de productos del software base y de los manuales de explotación de cada aplicación).
- Control y Seguimiento de los procesos existentes en los distintos planificadores
- Gestión de errores en producción, comprobación y análisis del error producido
- Resolución incidencia o escalado al departamento correspondiente y seguimiento de la misma hasta su resolución.
- Gestión de las alarmas de los diferentes entornos
- Parada y arranque de los sistemas de forma planificada
- Seguimiento de los diferentes servicios del Sistema
- Generación de informes del Sistema

- Gestión, planificación y monitorización de las condiciones físicas de sala: temperatura, suministro eléctrico, acceso, sistema antiincendios, alarmas…

Modelo Operativo

El modelo aplicar está basado en la Metodología ITIL que se describe y cubre aspectos como:

- Gestión de las incidencias del servicio de explotación.
- Una explotación real es susceptible de tener incidencias por lo que se tendrán previstas medidas para minimizar el impacto de las mismas y reducir el porcentaje de tiempo durante el que los sistemas están o bien fuera de servicio, o bien dando un servicio degradado. Para minimizar este es por lo que se propone un procedimiento de resolución de incidencias que contemple, entre otros:
- La tipificación, a priori, de las incidencias: programadas y no programadas y en cada caso una segmentación por criticidad o repercusión.
- Los mecanismos de notificación a los usuarios y a la CSCM por tipo de incidencia, siendo en el caso de incidencias programadas una notificación realizada con la mayor anticipación posible.
- La documentación de las incidencias, analizando las causas y soluciones adoptadas en cada caso, de tal forma que el histórico de incidencias constituya un sistema de conocimiento para facilitar la resolución de las mismas.

Procedimientos

- Procedimiento de recuperación de procesos.
- Procedimiento de instalación de las herramientas de monitorización.
- Procedimiento de parametrización de las herramientas de control.
- Procedimiento de análisis de niveles de rendimiento.
- Procedimiento de Instalación y acceso aplicaciones específica.
- Procedimiento de Resolución de Incidencias
- Procedimiento de documentación de la información del servicio:
- Procedimientos para el Servicio de Explotación y Operación.

Organización

Responsabilidades y Tareas del Administrador de Sistemas.

Confeccionar los calendarios de explotación de los trabajos para cada equipo según la planificación realizada

- Gestionar la cargar y el lanzamiento de los trabajos en cada máquina conforme a las normas de explotación de cada sistema, siguiendo el calendario diario de explotación de cada máquina

- Supervisar la recepción y el control de los datos y soportes de entrada a los procesos de explotación
- Controlar la calidad de resultados de los trabajos
- Mantener en estado operativo cada uno de los sistemas de la plataforma tecnológica soporte del servicio, conociendo en cada momento el estado y la carga en cada servidor
- Planificar las cargas de trabajo previstas en las planificaciones
- Resolver las incidencias dentro de su ámbito de competencia
- Mantener actualizadas y disponibles las bibliotecas técnicas (manuales técnicos de los equipos y periféricos, de productos del software base y de los manuales de explotación de cada aplicación)

Responsabilidades y Tareas del Especialista en Monitorización.

- Instalación y upgrade de nuevas versiones y herramientas de monitorización
- Elaboración de procedimientos de explotación que contemplen la actuación proactiva como medida de anticipación ante la aparición de problemas
- Vigilar los umbrales de calidad del servicio por cada parámetro
- Seguimiento, corrección y documentación de las alertas producidas
- Identificación de oportunidades de mejora en rendimiento de los distintos componentes
- Elaborar estadísticas de comportamiento de los Sistemas

Responsabilidades y Tareas del Operador de Sistemas.

- Mantener la operatividad del Sistema e informar al Supervisor de las incidencias que puedan ocurrir.
- Gestionar en el archivo los soportes magnéticos requeridos por el Sistema
- Gestionar las existencias de material consumible y organizar su almacenamiento

BRS (BACKUP&RECOVERY SYSTEM)

Objetivos

Conseguir la continuidad de los sistemas ante las posibles contingencias que pueden ocurrir y que afecten a la infraestructura técnica del Hospital de Collado-Villalba.

Garantizar la seguridad e integridad de los datos

Alcance

Mantenimiento del Plan de Contingencia diseñado en la fase de implantación.

Funciones

- Mantener en estado operativo cada uno de los sistemas de la plataforma tecnológica soporte del servicio, conociendo en cada momento el estado y la carga en cada servidor.
- Identificar origen de alertas como consecuencia de que determinados parámetros del servicio hayan superado los umbrales previstos.
- Supervisar la recepción y el control de los datos y soportes de entrada a los procesos de explotación.
- Controlar la calidad de resultados de los trabajos y resolver las incidencias dentro de su ámbito de competencia, así como su registro y escalado si procede
- Mantener actualizadas y disponibles las bibliotecas técnicas (manuales técnicos de los equipos y periféricos, de productos del software base y de los manuales de explotación de cada aplicación).
- Backups. Ejecución y Control de los procesos de Backup
- Monitorización réplica de datos.
- Gestión de errores en producción, comprobación y análisis del error producido.
- Resolución incidencia o escalado al departamento correspondiente y seguimiento de la misma hasta su resolución.
- Generación de informes del Sistema.

Modelo Operativo

En cualquier instalación informática existe el riesgo de que a causa de un siniestro inesperado la instalación pierda operatividad, hasta el punto de poder quedar totalmente inoperativa.

Existen medidas proactivas que minimizan el riesgo de estos siniestros, tales como la monitorización de la infraestructura que permite detectar problemas antes de que desencadenen en una pérdida del servicio.

Sin embargo siempre existen incidentes que están fuera del control del explotador de la infraestructura y que desencadenan en una inoperatividad total del sistema.

Las empresas cada vez están más presionadas para ofrecer una continuidad en sus servicios por todos los agentes involucrados con la empresa, por lo que tener un Plan de Continuidad del Negocio es cada vez más una necesidad, algo ya imprescindible en el caso de un hospital.

Componentes de un Plan de Continuidad del Negocio:

- Disaster Recovery Plan: Consiste en recuperar las funcionalidades críticas de la infraestructura técnica en un centro alternativo.
- Business Resumption Plan: Consiste en un plan para continuar con las actividades de negocio mientras se recuperan los sistemas.

- Bussiness Recovery Plan: Consistente en continuar con las actividades del negocio en un centro alternativo, trasladando al personal
- Contingency Plan: Consiste en la gestión de los incidentes externos con gran impacto en el negocio.

La conjunción de estos planes consigue no solo una continuidad de los sistemas sino también una continuidad de todas las funcionalidades críticas de nuestros clientes, obteniendo una auténtica continuidad de su negocio.

Procedimientos

Procedimiento para el mantenimiento del Plan de contingencias:

- Actualizar la Organización de Contingencias, así como las funciones y responsabilidades de cada una de las unidades y equipos que la componen.
- Gestionar la actualización de la Infraestructura HW-SW de Contingencias de manera que el Plan este vigente en todo momento.
- Gestionar los cambios necesarios en el Plan de Contingencias en función de las actualizaciones de HW-SW mencionadas anteriormente.
- Mantener actualizados los procedimientos de actuación incluidos en el Plan de Contingencias.
- Mantener actualizada la información de cada elemento identificado: su definición y ubicación o estado actual, posibles incidencias a las que está expuesto, elementos relacionados a los que pueda repercutir la incidencia, descripción de actividades a realizar para maximizar su seguridad, y elaborar un plan de pruebas y/o controles específicos.
- Confeccionar un Plan de Mantenimiento Preventivo que contemple las instalaciones, equipos y servicios de los edificios de los CPD, que ante una contingencia, puedan afectar al proceso de explotación.

Procedimiento ante desastres:

- Plan de Invocación del Servicio. En este Plan se recogerán los procedimientos logísticos necesarios para activar el Plan de Contingencia. En el mismo estarán determinadas las actividades y tareas necesarias para realizar la recuperación de los sistemas en un Centro de Respaldo, junto con los mecanismos de localización de los responsables (habitualmente teléfonos y direcciones de localización permanente).
- Plan de Recuperación de Sistemas. Estos Planes, de los que existirá un documento específico por cada sistema a recuperar, están enfocados a procedimientos. En ellos se describen en pasos detallados todas las acciones, tareas y comandos necesarios para poner en marcha la infraestructura de los Nuevos Hospitales situada en el centro.
- Plan de retorno: Cuando se recuperen las instalaciones iníciales se procederá a retornar el servicio a los equipos. Para ello se definirá el procedimiento a seguir para la recuperación de los datos alojados en el Centro de Respaldo mediante Backup y su traslado a las instalaciones iníciales.

Contingencia en la Disponibilidad de Recursos:

Organización

El servicio de BRS se organiza de forma coordinada con los Servicios de Contingencias del Negocio.

El responsable del servicio estará claramente identificado y coordinará las actividades con el responsable de contingencias de la CSCM cuando sea necesario.

COMUNICACIONES: SERVICIO INTEGRAL DE RED

Objetivos

- Gestión Integral de Red
- Controlar el funcionamiento de los elementos de comunicación instalados y detectar y resolver incidencias.

Alcance

El Servicio Integral de Red tiene como ámbito desarrollar aspectos de la técnica de sistemas relativas a las comunicaciones).

Funciones

Las funciones a realizar más relevantes serán:

- Gestión (incluyendo monitorización, configuración y operación) de primer y segundo nivel de los elementos de red constitutivos de los servicios de comunicación de datos objeto del servicio
- Mantenimiento de las configuraciones de la red de comunicaciones para adecuarla en cada momento a las necesidades
- Mantener el software de comunicaciones y demás productos afines.
- Supervisar los criterios de seguridad a implantar en la operativa de la red de comunicaciones, según la política de seguridad definida
- Informar e investigar los problemas relativos a seguridad, privacidad de los datos y los posibles intentos de violación al sistema.
- Detectar, recoger y resolver las incidencias relacionadas a la red de comunicaciones y los servicios asociados.
- Obtener medidas de los elementos de la red a fin de vigilar su comportamiento y proponer modificaciones para optimizar el servicio, así como corregir los fallos que se detecten en el servicio y las adaptaciones que sean necesarias para su correcto funcionamiento
- Informar periódicamente sobre el funcionamiento, grado de fiabilidad y servicio prestado por la red de comunicaciones, emitiendo de los informes técnicos preciso para el correcto funcionamiento de la red.

- Prestar el servicio de atención, gestión y mantenimiento bajo una serie de criterios:
- Atención y resolución de cualquier tarea de mantenimiento de la infraestructura física de conexión, equipos, cambios de configuración hardware, etc. que sean precisas.
- Servicio de atención y resolución de incidencias y servicio de mantenimiento dentro de la cobertura horaria prevista para todos los equipos y líneas suministrados.
- Cuando así se requiera, se podrá acordar que las intervenciones se realicen fuera del horario laboral y en festivos.

Modelo Operativo

El modelo aplicar está basado en la Metodología ITIL que cubre aspectos como:

- La gestión de la configuración de elementos de la plataforma de comunicaciones instalada tanto para los elementos hardware, como software como para las líneas de comunicaciones entre el CT, el CR y los Hospitales.
- La gestión de los cambios que sea imprescindible efectuar
- La interlocución con los Operadores de Comunicaciones en el caso de detección de caídas o problemas de funcionamiento en las líneas de comunicación
- La interlocución con los responsables de comunicaciones de la CSCM

Organización

Responsabilidades y Tareas del Especialista en Comunicaciones.

- Detectar y resolver las incidencias en los elementos de los sistemas de comunicaciones.
- Elaborar el Plan de Comunicaciones y actualizarlo según la evolución de las necesidades.
- Mantener el software de comunicaciones y demás productos afines de cada una de las redes.
- Informar periódicamente sobre el funcionamiento, grado de fiabilidad y servicio prestado por las distintas redes de comunicaciones.
- Medir los rendimientos.

Responsabilidades y Tareas del Especialista en Redes.

- Diseñar y modificar las configuraciones de cada red para adecuarlas en cada momento a las necesidades de explotación de los sistemas de información.
- Colaborar en la instalación y conexión física de redes y terminales, supervisando las pruebas a realizar.
- Supervisar los criterios de seguridad a implantar en la operativa de cada red de comunicaciones, en especial la correcta ejecución de los procedimientos de Back-up y Restore de las redes de área local bajo su responsabilidad.
- Controlar los distintos elementos de cada red a través de su monitorización.

- Obtener medidas de los elementos de la red a fin de vigilar su comportamiento y proponer modificaciones para optimizar el servicio.

MANTENIMIENTO DE APLICACIONES

Dentro del Mantenimiento de aplicaciones se consideran los siguientes servicios:

Mantenimiento Correctivo (Gestión de Incidencias). Aquellas actuaciones o modificaciones a realizar sobre los equipos que se encuentran en explotación para corregir mal funcionamiento, o bien, planificar nuevas versiones que mejoren las versiones existentes o pongan parches a las mismas.

Mantenimiento Evolutivo. Actuaciones encaminadas a la mejora y evolución de las aplicaciones existentes, incluyendo nuevas funcionalidades, adaptando las ya existentes y mejorando la calidad global de dichas aplicaciones a las necesidades del usuario o de la normativa.

A continuación se describen en detalle tanto el Mantenimiento Correctivo como el Mantenimiento Evolutivo:

MANTENIMIENTO CORRECTIVO

Objetivos

- Atender las incidencias y peticiones transmitidas por los usuarios o el primer nivel en el menor tiempo y con la máxima calidad posible (mejorando la relación entre la calidad esperada y la recibida y corrigiendo los errores existentes en la aplicación).
- Identificar la posibilidad de que hubiera incidencias ocultas (no siempre los usuarios transmiten los problemas).
- Reducir el número de incidencias recurrentes y no recurrentes proponiendo actuaciones preventivas y planificadas.
- Reparar, mediante traslado a los fabricantes oportunos, de los equipos instalados por defectos en piezas ó componentes, sustituyendo, si es preciso, el componente averiado

Alcance

- Resolución de cualquier avería que se produzca en las aplicaciones instaladas en el Hospital de Collado-Villalba.
- Sustituir aplicaciones cuando no funcionen adecuadamente, así como la realización del seguimiento del correcto funcionamiento de las mismas con posterioridad al cambio realizado

Funciones

- Análisis del mal funcionamiento generado por la operativa del usuario verificando si el origen del mismo es la naturaleza de los datos, la codificación de los programas o aspectos relacionados con la parametrización / configuración de los productos.

- Propuesta de soluciones de contingencia que minimicen el impacto de la incidencia en el Servicio.
- Realización de las actividades del Ciclo de Vida del Desarrollo del Software necesarias para generar, si procede, una nueva versión.

MANTENIMIENTO EVOLUTIVO

Objetivos

Llevar a cabo la mejora y evolución de las aplicaciones existentes, incluyendo nuevas funcionalidades, adaptando las ya existentes y mejorando la calidad global de dichas aplicaciones a las necesidades del usuario o de la normativa.

Funciones

- Realizar las modificaciones en la aplicación o el producto como consecuencia de requisitos externos o internos (cambios de normativa, técnicos, etc.) en la medida de que dichas evoluciones sean necesarias para el funcionamiento futuro de la aplicación o el producto.
- Realizar las modificaciones oportunas para minimizar los problemas que puedan presentarse a corto plazo sin alterar las especificaciones funcionales de la aplicación. Estas intervenciones han de tender a:
- Disminuir el número de errores y el esfuerzo de resolución de los mismos.
- Facilitar el mantenimiento de las aplicaciones, disminuyendo el tiempo y coste de cambios debido al menor impacto de los mismos.
- Corrección proactiva de los componentes de la aplicación o el producto que sean susceptibles de causar un mal funcionamiento del mismo anticipándose a la operativa del usuario dotando a dicha aplicación o producto de una mayor calidad en su explotación.

- Realizar las mejoras de la aplicación, como consecuencia de las evoluciones funcionales de la misma, a petición de los usuarios, así como aquellos cambios necesarios para perfeccionar el funcionamiento y optimizar el rendimiento de la aplicación. Se abordarán en este epígrafe aquellas necesidades funcionales demandadas por el usuario para el desarrollo de su negocio siempre que éstas no supongan un desarrollo de envergadura lo suficientemente amplio como para considerarlo un rediseño total de la aplicación o el producto.
- El desarrollo de este tipo de mantenimientos se adapta al ciclo de vida habitual de todo proyecto de Desarrollo de Aplicaciones.

Modelo Operativo

A continuación se expone el modelo operativo a aplicar tanto para el mantenimiento correctivo como para el mantenimiento evolutivo, que cubre aspecto como:

- Requerimientos de Usuario: Elaborar la lista de Requerimientos completa y recabar del usuario la conformidad a la solución propuesta para cada uno de dichos requerimientos.
- Evaluación: Análisis detallado del impacto de la solicitud de cambio, con el fin de conocer el alcance real de la modificación en función del número, características y relaciones existentes entre los elementos afectados que permita establecer una secuencia y planificación correcta del desarrollo de los cambios, valorando los recursos necesarios para llevarlo a cabo.
- Análisis Funcional: Realizar las especificaciones funcionales derivadas de los requerimientos de usuario y del proceso de Evaluación previo.
- Diseño Técnico: Realizar el diseño técnico como base al equipo de desarrollo para su construcción. Elaborar los planes de pruebas de integración y de usuario. Diseñar los entornos técnicos (herramientas de diseño, pruebas, desarrollo, etc.).
- Desarrollo: Desarrollo de la mejora. Completar los planes de pruebas definidos en la fase anterior.
- Documentación: Realización y/o actualización de la documentación detallada de programas y componentes.
- Pruebas: Pruebas de Sistema: Pruebas de rendimiento y volumen y pruebas de integración de sistema. Plan de Pruebas de Aceptación. Resolución de incidencias surgidas durante las pruebas.
- Instalación: Apoyo al departamento de Explotación en la puesta en producción del nuevo desarrollo.
- Mantenimiento: Durante el período de mantenimiento el área TI del hospital y de Capio, asumirán una completa disponibilidad técnica y funcional para dar soporte a la integración de su sistema con otras aplicaciones corporativas de la CSCM

Procedimientos

Los procedimientos básicos de este servicio serían:

- Procedimiento de identificación/resolución de incidencias
- Procedimiento de escalado de incidencias
- Procedimiento para realizar acciones planificadas y preventivas
- Procedimiento para identificar problemas recurrentes
- Procedimiento para identificar incidencias no comunicadas
- Procedimiento de Sustitución de las aplicaciones
- Procedimiento de cierre de solicitud de instalación
- Procedimiento de Anulación de Solicitud
- Procedimiento para mantener actualizada la base de datos de conocimiento
- Procedimiento de actualización de la base de datos del inventario

DOTACIÓN DEL EQUIPAMIENTO PERIFÉRICO

Objetivos

Instalar en tiempo y calidad los nuevos equipamientos de usuario

Realización de las instalaciones en puesto de usuario de acuerdo a las necesidades, mediante maquetas aceptadas.

Incrementar la productividad y la calidad de la instalación de equipamiento a través de procedimientos y herramientas de racionalización para las instalaciones de equipos

Funciones

- Instalar en tiempo y calidad los nuevos equipamientos de usuario y la actualización de los mismos que procedan de los procesos de Renovación Tecnológica, así como retirar los equipos obsoletos
- Añadir nuevo hardware externo o nuevo software a los equipos de los usuarios
- Reinstalación de equipos motivadas por la adquisición y cambio de hardware, consiste en la desinstalación de una máquina y su posterior instalación en otro usuario

Modelo operativo

La procedencia de las solicitudes, indica el procedimiento de instalación que este servicio ha de seguir en cada caso, con el objetivo de reducir al mínimo posible el impacto en el puesto de trabajo, evitando que repercuta en la productividad del usuario.

Desde que se planifica la instalación hasta que la misma se da por finalizada, se mantiene contacto con el usuario de forma que éste puede conocer en todo momento la situación de su instalación concreta, lo que contribuye a mejorar su predisposición ante cualquier futuro cambio relacionado con tecnologías de la información

La utilización de unos procedimientos y herramientas estándar garantiza la uniformidad en el proceso, facilita las tareas de planificación, disminuye el número de errores, incide en la toma de decisiones más correcta, permite actualizar el parque informático con mayor rapidez y menor número de errores, y proporciona información del equipamiento y su evolución, así como del estado de las instalaciones en todo momento. Permite además racionalizar el tiempo empleado en la realización de las instalaciones del equipamiento.

Procedimientos

- Solicitud de instalación de puesto de trabajo estándar por alta de usuario
- Solicitud de instalación de puesto de trabajo portátil.

- Solicitud de instalación "in situ" (software que no pueda ser distribuido por el sistema de distribución remota de software)
- Solicitud de equipos de Sustitución
- Procedimiento de actualización de equipo retirado (para reutilización)
- Procedimiento de salida de equipo por obsolescencia
- Procedimiento de cierre de solicitud de instalación (coordinado con el CSU)
- Procedimiento de Anulación de Solicitud
- Procedimiento de actualización de la base de datos del inventario

Organización

Responsabilidades y Tareas del Coordinador del Servicio de Dotación de Equipamiento Periférico:

- Recibe las diferentes Solicitudes de Instalación del CSU
- Asigna nivel de criticidad y establece la prioridad de las instalaciones
- Analiza las necesidades de la solicitud y determina si se utilizará un equipo ya utilizado (reutilización), o nuevo (nueva instalación).
- Abre el Parte de Trabajo de la solicitud.
- Notifica la instalación del equipo al tercero correspondiente.
- Sigue el proceso instalación en las dependencias del Servicio de Instalación y Mantenimiento del equipamiento.
- Informa al solicitante de la instalación y planifica la misma con él.
- Verifica la conformidad del usuario una vez realizada la instalación.
- Informa de los cambios al CSU.
- Cierra el Parte de Trabajo Técnico.
- Verifica la actualización de la Documentación del Servicio (Actualización Inventario).
- Cierra la Solicitud.

CENTRO DE SOPORTE A USUARIOS Y GESTIÓN DE INCIDENCIAS (CSU)

Objetivos

- Prestar un mejor servicio al profesional sanitario que proporcione el soporte necesario a los usuarios de las aplicaciones en el Hospital de Collado-Villalba.
- Resolver siempre que sea posible, las incidencias asignadas de acuerdo con los procedimientos establecidos hasta que se produzca su total resolución.
- Proporcionar información sobre las acciones resolutivas tomadas.

- Capturar detalles del cierre de la Incidencia.
- Informar con relación a los compromisos adquiridos en el Acuerdo de Nivel de Servicio.

Alcance

El Centro de Soporte y Gestión de Incidencias atiende las incidencias de los usuarios de los sistemas instalados en el Hospital de Collado-Villalba.

Este servicio cubrirá las necesidades de los usuarios internos y externos de sus sistemas.

Soporte multicanal, telefónico, a través de portal web o fax.

Funciones

- Analizar y estudiar las incidencias en productos o en cuestiones especificas ligadas a un determinado área de conocimiento, así como su resolución.
- Escalar las incidencias a otros Servicios (Soporte local, Mantenimiento, Fabricantes...), manteniéndose como propietario del proceso.
- Mantener el sistema de Base de Incidencias actualizado.
- Proponer actuaciones de Mejora Continua para mejorar el servicio prestado a la comunidad de usuarios en términos de calidad y eficiencia del servicio.
- Cultura basada en el servicio al “Cliente” (usuarios de los Sistemas de Información Sanitarios).
- Capacidad de actuar proactivamente ante errores.
- Control y gestión tanto del soporte de las aplicaciones como de la relación con terceros (proveedores) mediante Acuerdos de Nivel de Servicio.
- Disponibilidad de indicadores e informes para la gestión del servicio proporcionado.
- Integración con el modelo de soporte operativo en la CSCM.
- Automatización de operaciones.
- Gestión del equipamiento distribuido, desde el inventario administrativo hasta la configuración de cada uno de ellos.

Modelo Operativo

El modelo aplicar está basado en la Metodología ITIL que cubre aspectos como:.

- El término Incidencia se utiliza para definir cualquier llamada recibida en el CSU, que requiere que se tomen una serie de acciones para dar una solución.
- A cada Incidencia reportada por un usuario del cliente, se le asigna un nivel de servicio en función del tipo de equipamiento (Prioridad A, Prioridad B, Prioridad C), que indica su gravedad y su tiempo objetivo de resolución. Los niveles de prioridad se han establecido con el cliente y son incluidos en el Acuerdo de Nivel de Servicio (ANS).

- Si nos referimos a las Incidencias que son atendidas en local, hay que destacar las siguientes funciones:
    - Gestión de Incidencias, problemas, peticiones y órdenes a terceros. Esto incluye la recepción de las incidencias de las aplicaciones de los otros lotes del presente concurso y su escalado al servicio de soporte de segundo nivel del adjudicatario correspondiente.
    - Configuración de avisos y notificaciones
    - Registro de seguimiento de resolución de incidencias, peticiones y cambios (tiempos de resolución, responsable, derivación, escalado, etc.)
    - Gestión óptima de cargas de trabajo
    - Gestión según "Acuerdos de Nivel de Servicio"
    - Funcionamiento según flujos de trabajo configurables
    - Integración con el Directorio Activo
    - Compatibilidad con Dispositivos Inalámbricos
    - Integración nativa con el resto de aplicaciones del Centro de Soporte a Usuarios (Distribución, Inventario, monitorización, etc.)
    - Gestión del conocimiento disponible para el soporte y para los usuarios vía web
    - Creación de incidencias automáticas por herramientas externas al módulo de Gestión de Incidencias
    - Plantillas de cumplimentación obligatoria de campos al dar de alta incidencias
    - Interfaz web en castellano para la Gestión de Incidencias
    - Facilidad en la elaboración y personalización de informes
    - Control de cambios (gestión de solicitudes, estado de los cambios)

- Si la incidencia es atendida en remoto, los operadores de este servicio garantizarán:
    - Niveles de control configurables según políticas definidas
    - Registro de sesión (información de sesión, grabación y reproducción de sesiones)
    - Control de accesos según lo exigido por el RD 994/1999 referente a las medidas de seguridad a satisfacer por los Sistemas de Información con datos de Carácter Personal.
    - Múltiples opciones de control remoto (exclusivo, compartido, oculto, seguro)
    - Distribución a múltiples visores simultáneos
    - Conexiones simultáneas a distintos equipos
    - Reinicio Remoto
    - Configuración de permisos de acceso, cifrado y métodos de seguridad
    - Integración con múltiples opciones de directorio
    - Compatibilidad con múltiples protocolos, sistemas y plataformas

  - Integración nativa con el resto de aplicaciones del Centro de Soporte a Usuarios (Gestión de Incidencias, Inventario y Monitorización)
- Proporcionar la información estadística a la CSCM

Procedimientos

Los procedimientos básicos serían:

- Procedimiento para la actualización de la información base:
  - Organización del Hospital
  - Usuarios de los Hospitales
  - Inventario de productos y aplicaciones soportados
  - Inventario de Terceras Partes
- Procedimiento para la actualización de la matriz de prioridades de intervención:
  - Tipos de usuario
  - Tipos de incidencia
- Procedimiento para la revisión de los tiempos de respuesta objetivo
- Procedimiento básico de identificación/resolución de incidencias
- Procedimiento de escalado de incidencias
- Procedimiento para realizar acciones planificadas y preventivas
- Procedimiento para identificar problemas recurrentes
- Procedimiento para identificar incidencias no comunicadas
- Procedimiento para mantener actualizada la base de datos de conocimiento

Herramientas

- Teléfonos de mesa en horario laboral
- Teléfonos de guardia para servicio 7x24.
- Fax
- Herramienta de monitorización y resolución de incidencias
- Herramienta de gestión de incidencias
- Estadísticas. Los responsables realizarán un análisis de las incidencias para detectar posibles acciones preventivas, si es posible tomar alguna acción que evite este problema en el futuro o, al menos, que permita detectarlo y corregirlo rápidamente.

GESTIÓN DEL INVENTARIO

Objetivos

- Contemplará la gestión del inventario de componentes de los Sistemas de Información, ofreciendo un inventario unificado y actualizado que sirva de base efectiva para el soporte a los usuarios.
- Gestionará el ciclo de vida de todos los activos que componen el entorno, incluyendo la gestión de licencias software, el mantenimiento, etc.

Funciones

- Elaboración y aprobación de los procedimientos de inventariado a utilizar en la prestación del servicio.
- Registro de cualquier alta, baja o modificación de equipamiento o software microinformático.
- Es un servicio centralizado que recogerá los contratos que provengan de las Solicitudes de Cambio y/o Incidencias recogidas en el Servicio de Help-Desk
- El inventario se realizará asignando cada elemento a sus respectivos centros de coste sin agrupación de los elementos del inventario por usuario.

DISTRIBUCIÓN DE SOFTWARE

Objetivo

El servicio de distribución de software tiene como objetivo acometer la instalación de distintos tipos de software, tanto aplicaciones como actualizaciones, mediante la distribución masiva de paquetes.

Alcance

La distribución de Software cubre los sistemas instalados en el Hospital y CPD de respaldo

Funciones

- Instalación, configuración y mantenimiento de todo el sistema de distribución (servidores, agentes, BB.DD, etc.)
- Gestión y resolución de incidencias que surgieran con el sistema o cualquiera de sus elementos durante la distribución
- Apoyo en la elaboración de paquetes
- Apoyo en la distribución y seguimiento de los mismos
- Preparación y distribución de paquetes con las aplicaciones que se indiquen para un distribución rápida y centralizada.
- Ejecución de pruebas controladas previas a la distribución masiva
- Obtención periódica de informes de distribución

- Formación y apoyo a los distintos departamentos sobre el sistema de distribución
- Elaboración de documentación: manuales de instalación, explotación y administración.

MONITORIZACIÓN DE SISTEMAS Y PROCESOS

Objetivos

Este servicio contempla la detección y gestión de eventos críticos para los distintos componentes, procesos, elementos y aplicaciones.

Funciones

Monitorización del equipamiento. Es una actividad proactiva de seguimiento y control del estado de los elementos de la infraestructura para detectar incidencias y actuar para resolverlas, además de realizar estudios específicos basados en el procesamiento de históricos, satisfaciendo:

- Gran variedad de entornos soportados
- Facilidad de Instalación / uso
- Alta Capacidad Gráfica
- Multiplataforma
- Representación topológica / geográfica (incorporación de planos, mapas,...)
- Facilidad de customización
- Integración nativa con el resto de aplicaciones del Centro de Soporte a Usuarios (Distribución de Software, Gestión de Incidencias,...)
- Monitorización de BB.DD.
- Monitorización de S.O.
- Monitorización de aplicaciones y procesos
- Creación de Vistas/Mapas configurables por rol, usuarios o grupos
- Creación de Vistas/Mapas de procesos de negocio
- Gestión de históricos
- Gestión de Eventos
    - Soporte de eventos originados en distintas aplicaciones
    - Definición de umbrales de alarma en los elemento monitorizados (Red, CPU, Disco,...)
    - Soporte de lógica de eventos (and, or,...)
    - Opciones de filtrado y enrutamiento de mensajes
    - Centralización del control de eventos
    - Gestión de eventos específicos relativos a todo tipo de dispositivos

  - Correlación de eventos
- Gestión de fallos
  - Anticipación de fallos a partir de alertas
  - Posibilidad de gestión central
  - Integración con alarmas visuales y/o acústicas
  - Determinación de relaciones entre fallos
  - Test periódicos sobre componentes críticos
- Acciones
  - Posibilidad de definir acciones de respuesta ante errores
  - Existencia de acciones predefinidas
  - Compatibilidad con otras herramientas de gestión de red y sistemas
- Recepción de alarmas. Consiste en la solicitud de estado cada media hora a los equipos y la posibilidad de recepción de traps de aquellos elementos críticos que requieran mayores niveles de disponibilidad
- Operación remota. Capacidad de acceder al equipo afectado por una incidencia para intentar recuperar su operatividad habitual.
- Solicitud de intervención al servicio de mantenimiento cuando no es posible la resolución remota

MANTENIMIENTO HARDWARE EN LOS PUESTOS DE TRABAJO

Objetivos

- Minimizar el impacto de averías hardware de usuarios
- Reparar, mediante reparación in-situ o traslado a los fabricantes oportunos, de los equipos instalados por defectos en piezas ó componentes, sustituyendo, si es preciso, el componente averiado

Alcance

El Servicio de Mantenimiento Hardware de equipos atiende las incidencias de los usuarios de los Puestos de Trabajo de Usuarios del Hospital de Collado-Villalba.

Funciones

- Resolución de cualquier avería de hardware que se produzca en los elementos y equipos objeto del contrato
- Sustituir componentes de hardware en los equipos, así como la realización del seguimiento del correcto funcionamiento del equipo con posterioridad al cambio realizado
- Reparación de averías de hardware de los equipos objeto del servicio
- Sustitución de discos duros, placas, fuente de alimentación en los equipos averiados

- Control de stock y almacén de piezas de recambio

Procedimientos

Los procedimientos básicos serían:

- Procedimiento de identificación/resolución de incidencias
- Procedimiento de escalado de incidencias
- Procedimiento para realizar acciones planificadas y preventivas
- Procedimiento para identificar problemas recurrentes
- Procedimiento para identificar incidencias no comunicadas
- Procedimiento de Retirada de Equipo Informático (por sustituciones)
- Procedimiento de cierre de solicitud de instalación (coordinado con el CSU)
- Procedimiento de Anulación de Solicitud
- Procedimiento para mantener actualizada la base de datos de conocimiento
- Procedimiento de actualización de la base de datos del inventario

SOPORTE SOFTWARE A USUARIOS

Objetivos

- Atender las incidencias y peticiones transmitidas por el primer nivel en el menor tiempo y con la máxima calidad posible (mejorando la relación entre la calidad esperada y la recibida).
- Identificar la posibilidad de que hubiera incidencias ocultas (no siempre los usuarios transmiten los problemas).
- Reducir el número de incidencias recurrentes y no recurrentes proponiendo actuaciones preventivas y planificadas.

Funciones

- Soporte avanzado en el uso de los sistemas
- Revisión, resolución y escalado de incidencias (cuando proceda) relativas a los Puestos de
- Detección de la necesidad de soporte presencial para los usuarios afectados por la incidencia.

GESTIÓN DEL SERVICIO

Objetivos

- Ser el máximo responsable en la coordinación de los servicios de mantenimiento prestados
- Coordinar todas las interacciones que puedan producirse entre el Hospital de Collado-Villalba y la CSCM.
- Apoyo al hospital en su función de Dirección de la Función Informática.

Funciones

- Coordinar la prestación del servicio global.
- Elaborar informes y obtener estadísticas del sistema de Base de Incidencias.
- Mantener las reuniones de seguimiento periódicas acordadas
- Velar por el cumplimiento de los acuerdos de nivel de servicio.

- Definir los procedimientos del Servicio.
- Desarrollar actuaciones de Mejora Continua.
- Garantizar y mantener el servicio dentro de sus objetivos y métricas.
- Gestionar y coordinar el equipo de trabajo y el conjunto de recursos tecnológicos asociados al servicio.
- Gestión documental del servicio (procedimientos, manuales, planes de calidad, informes, etc...) y gestión del conocimiento del servicio.

MODELO DE RELACIÓN SOPORTE CAPIO-CESUS

En anexo adjunto , y de acuerdo a la propuesta de la CSCM, se define el modelo de coordinación y los procedimientos de soporte que seguirán tanto CESUS (Centro de Soporte a Usuarios de la Consejería de Sanidad de la Comunidad de Madrid) como los centros de atención a usuarios de los hospitales gestionados por CAPIO Sanidad (en adelante SOPORTE CAPIO) con objeto de llevar a cabo la prestación coordinada del servicio de soporte a los usuarios dependientes de los centros de la Comunidad de Madrid gestionados por la empresa CAPIO Sanidad (Hospitales y Centros de Especialidades).

Se entiende por "usuarios dependientes de los centros de la Comunidad de Madrid gestionados por CAPIO", a los siguientes colectivos:

- Profesionales ubicados en los hospitales y centros de especialidades gestionados por CAPIO: poseen, como Centro de soporte de referencia para el soporte a incidencias TIC, al SOPORTE CAPIO.
- Resto de profesionales que interaccionan con los SSII de los hospitales gestionados por CAPIO ya sea de forma directa, Centros de Salud y Centros de Especialidades dependientes orgánicamente de centros CAPIO o indirecta, siempre que accedan a través de las integraciones de los SSII corporativos: poseen, como Centro de referencia para el soporte a incidencias TIC, a CESUS.

El Modelo de Coordinación propuesto para los Centros de Soporte de la CSCM y los centros CAPIO (CESUS y SOPORTE CAPIO, respectivamente) se fundamenta en los siguientes preceptos:

- La prestación de servicios por uno y otro Centro de Atención Usuarios (CAU) debe ser transparente al usuario final.
- La información relativa a incidencias debe ser única, y la interlocución con el usuario debe proceder de una única fuente.

El alcance de esta coordinación se refiere a las siguientes líneas de actuación:

- Gestión de Incidencias
- Gestión de usuarios
- Coordinación de modificaciones en los servicios existentes

HORARIO DE LOS SERVICIOS

La siguiente tabla representa el horario previsto para cada servicio :

Servicio	Personal IN-SITU	Guardias Permanentes 24x7*
Técnica de Sistemas	8:30 a 19:00 L a V (lab.)	X
Bases de Datos	8:30 a 19:00 L a V (lab.)	X
Explotación de Operación	8:30 a 19:00 L a V (lab.)	X
BRS (Backup&Recovery System)	8:30 a 19:00 L a V (lab.)	X
Comunicaciones	8:30 a 19:00 L a V (lab.)	X
Mantenimiento Correctivo	8:30 a 19:00 L a V (lab.)	X
Mantenimiento Evolutivo	8:30 a 19:00 L a V (lab.)	
Equipamiento periférico, equipos de usuario	8:30 a 19:00 L a V (lab.)	X
Soporte a Usuarios y atención de Incidencias	8:30 a 19:00 L a V (lab.)	X
Gestión de Inventario	8:30 a 19:00 L a V (lab.)	
Distribución de SW	8:30 a 19:00 L a V (lab.)	
Monitorización	8:30 a 19:00 L a V (lab.)	X
Mantenimiento de HW en el puesto de trabajo	8:30 a 19:00 L a V (lab.)	X
Soporte Software a Usuarios	8:30 a 19:00 L a V (lab.)	X
Gestión del Servicio	8:30 a 19:00 L a V (lab.)	

*En caso de ser necesaria resolución in-situ (incidencia crítica), el desplazamiento deberá realizarse en un tiempo inferior a 4 horas, a computar desde el registro de la incidencia.

MONITORIZACIÓN DEL SERVICIO

El Hospital de Collado-Villalba proporcionará a la CSCM de capacidad de monitorización de los equipos informáticos, con el suficiente nivel de autorización para cumplir al menos estos objetivos:

- Comprobar que la instalación se adecua a lo establecido previamente.
- Disponer de información sobre la disponibilidad o indisponibilidad del servicio.
- Obtener garantías de cumplimiento de medidas de seguridad, así como de estándares, políticas y normativas prescritas por la CSCM.

9. SEGURIDAD Y LOPD

El presente capítulo describe las normas de seguridad que se implantarán en el Hospital de Collado-Villalba, en consonancia con la legislación vigente y con los estándares internacionales de Seguridad de la Información a través de la norma ISO 27001 y acordes con los procedimientos de control referenciados en el UNE-ISO/IEC 17799 y en el COBIT (Control Objectives for Information and related Technology).

Las políticas definidas en éste documento han de ser de aplicación por todas aquellas personas que accedan de forma directa o indirecta a los Sistemas de Información.

COPIA Y DEVOLUCIÓN DE LOS DATOS Y DOCUMENTACIÓN CONFIDENCIAL

El Hospital deberá facilitar una copia con la documentación generada y los datos contenidos en sus sistemas de información, en cualquier momento y periodicidad, cuando así sea solicitado por la CSCM. Adicionalmente, será entregada dicha copia, con la documentación e información confidencial generada y datos contenidos en los sistemas de información, al igual que cualquier resultado del tratamiento realizado, y cualquier documento y/o soporte en el que se hallen, por los medios que se determinen por la CSCM, con una antelación mínima de un mes a la fecha de finalización del servicio."

DESCRIPCIÓN DE LAS POLITICAS

ACCESO A LA INFORMACIÓN

Todo el personal que necesita acceder a los Sistemas de Información debe tener acceso sólo a la información necesaria para el desarrollo de sus actividades. En el caso de personas ajenas al Hospital, la Dirección de Sistemas autorizará sólo el acceso indispensable de acuerdo con el trabajo realizado por este personal, previa justificación.

El otorgamiento de acceso a la información está regulado mediante las normas y procedimientos definidos para tal fin, asignando un usuario nominativo del que será responsable la persona a la que se le autorice dicho acceso. Ese usuario dejará de tener acceso valido a los Sistemas de Información inmediatamente después de que la persona responsable de dicho usuario deje de prestar los servicios por los cuales se le autorizó dicho acceso.

Proveedores o terceras personas sólo tendrán el acceso autorizado durante el periodo del tiempo requerido para llevar a cabo las funciones aprobadas.

Mediante el registro de eventos en los diversos recursos informáticos de la plataforma tecnológica se efectuará un seguimiento de los accesos realizados por los usuarios a la información, con el objeto de garantizar la confidencialidad y la integridad de la información. Cuando se presenten eventos que pongan en riesgo la integridad, veracidad y consistencia de la información se deberán documentar y realizar las acciones correctivas que eviten, en la medida de lo posible, que se produzcan situaciones de riesgo.

ADMINISTRACION DE CAMBIOS

Todo cambio (modificación de programas y aplicativos, pantallas, soportes) deberá de contar con la aprobación del Responsable de Sistemas del Hospital quedando constancia por escrito del cambio efectuado.

Esta constancia por escrito ha de ser documentada desde su solicitud hasta su implantación, con el objeto de que se pueda llevar un seguimiento y garantizar el cumplimiento de los procedimientos definidos.

Todo cambio en un recurso informático que afecte al mantenimiento de la plataforma tecnológica, software o modificación de parámetros, deberá de realizarse de tal forma que no provoque una disminución de la seguridad ya existente.

SEGURIDAD DE LA INFORMACION

El Hospital garantizará el cumplimiento de la legislación vigente en materia de prestación de Servicios Sanitarios, así como con todas aquellas normas que hacen referencia a la Protección de Datos de carácter personal que se encuentren en vigor o que puedan estarlo durante la vigencia de la prestación de servicios. Entre todas estas leyes podemos destacar las siguientes:

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD).
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (RDLOPD).
- Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de los derechos y obligaciones en materia de información y documentación clínica.
- Ley 8/2001, de 13 de julio, de Protección de Datos de Carácter Personal de la Comunidad de Madrid.
- Orden 1943/2005, del Consejero de Sanidad y Consumo, por la que se aprueba el Código de Buenas Prácticas para usuarios de Sistemas Informáticos.
- Ley 34/2002, de 11 de julio de los Servicios de la Sociedad de la Información y Comercio electrónico.
- Artículo 4 de la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información, que modifica la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.
- Disposición derogatoria única de la Ley 25/2007, de 18 de octubre, de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones.
- Artículos 197 y 264 de Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.
- Artículos del Código penal (art. 270 y 270) que hacen referencia a las infracciones sobre la propiedad intelectual en referencia a la utilización de software debidamente licenciado.

Toda aquella persona con acceso a los Sistemas de Información será Responsable de la información que maneje debiendo cumplir con las disposiciones legales vigentes en materia de Protección de Datos de

Carácter Personal (LOPD), así como todas aquellas disposiciones que regulan la gestión de la información en el Sector Sanitario.

SEGURIDAD PARA LOS SISTEMAS Y SERVICIOS DE INFORMACIÓN

El sistema de correo electrónico, acceso internet, intranets, Sistema de Gestión Hospitalario y utilidades asociadas de la entidad, deberán de ser usados únicamente para el ejercicio de las funciones competencia de cada usuario y de las actividades contratadas en el caso de personal mercantil o colaborador.

Por otro lado se dispone de una Normativa Interna de utilización de los Sistemas de Información que es de obligado cumplimiento por parte de todos los usuarios con acceso a los SI y que se adjunta en Anexo.

El Responsable de Seguridad informará regularmente a los empleados y colaboradores acerca de sus obligaciones con respecto a la seguridad de los recursos informáticos.

SEGURIDAD EN SISTEMAS DE INFORMACIÓN

Todos los recursos informáticos deben cumplir como mínimo con lo siguiente:

- Administración de usuarios: Establece como deben ser utilizadas las claves de acceso a los recursos informáticos. Se indican además los parámetros de la longitud mínima de las contraseñas, la frecuencia con la que los usuarios deben cambiar su contraseña y los períodos de vigencia de las mismas, entre otras.
- Perfil de Usuario: El sistema de Gestión hospitalario, bases de datos y resto de aplicativos han de contar todos ellos con perfiles de usuarios permiten definir las acciones permitidas por cada uno de estos.
- Auditoria: Hace referencia a los registros de los sucesos relativos a las operaciones realizadas por cada uno de los usuarios que han accedido al los SI.
- Las palabras claves o contraseñas de acceso a los recursos informáticos, son responsabilidad exclusiva del la persona a la que se le asocia el usuario de acceso y no deben ser divulgados ni transferidos a nadie. Los usuarios son responsables de todas las actividades llevadas a cabo con su código de identificación de usuario y sus claves personales.
- Se prohíbe disponer identificaciones de usuario genéricos basados en sus funciones de trabajo. Las identificaciones de usuario deben únicamente identificar individuos específicos.
- El Sistema de Gestión de información dispondrá de perfiles de usuario de acuerdo con la función y cargo de los usuarios que acceden a él.

Todo software utilizado por el Hospital será adquirido de acuerdo con las normas vigentes y siguiendo los procedimientos internos de adquisición.

Existirá un inventario de las licencias de software propiedad del Grupo que permita su adecuada administración y control evitando posibles sanciones por instalación de software no licenciado.

SEGURIDAD EN COMUNICACIONES

Las direcciones internas, topologías de red, configuraciones e información relacionada con el diseño de los sistemas de comunicación de los Centros, deberán ser consideradas y tratadas como información confidencial.

Todas las conexiones a redes externas deberán pasar a través de sistemas de defensa electrónica (firewall) que incluyan servicios de cifrado y verificación de datos, detección de ataques intrusión, administración de permisos de circulación y autenticación de usuarios.

Todo intercambio electrónico de información o interacción entre sistemas de información con entidades externas deberá estar soportado con un acuerdo de confidencialidad o documento de formalización, previa autorización del área de Seguridad.

Toda información secreta y/o confidencial que se transmita por las redes de comunicación de la Entidad e Internet deberá estar cifrada.

SEGURIDAD PARA USUARIOS TERCEROS

Los usuarios externos tendrán acceso a los sistemas informáticos que sean estrictamente necesarios para el cumplimiento de su función, servicios que deben ser aprobados previamente, y deberán firmar el acuerdo de buen uso de los mismos.

La conexión entre sistemas internos de la entidad y otros de terceros debe ser aprobada y certificada por el Área de Seguridad Informática con el fin de no comprometer la seguridad de la información interna de la entidad.

ALMACENAMIENTO Y RESPALDO

Toda la información que forma parte de los Sistemas de Información pertenecientes al Hospital deberá ser almacenada y respaldada de acuerdo con las normas emitidas de tal forma que se garantice su disponibilidad.

Existirá una definición formal de la estrategia de generación, retención y rotación de las copias de respaldo de cada Centro.

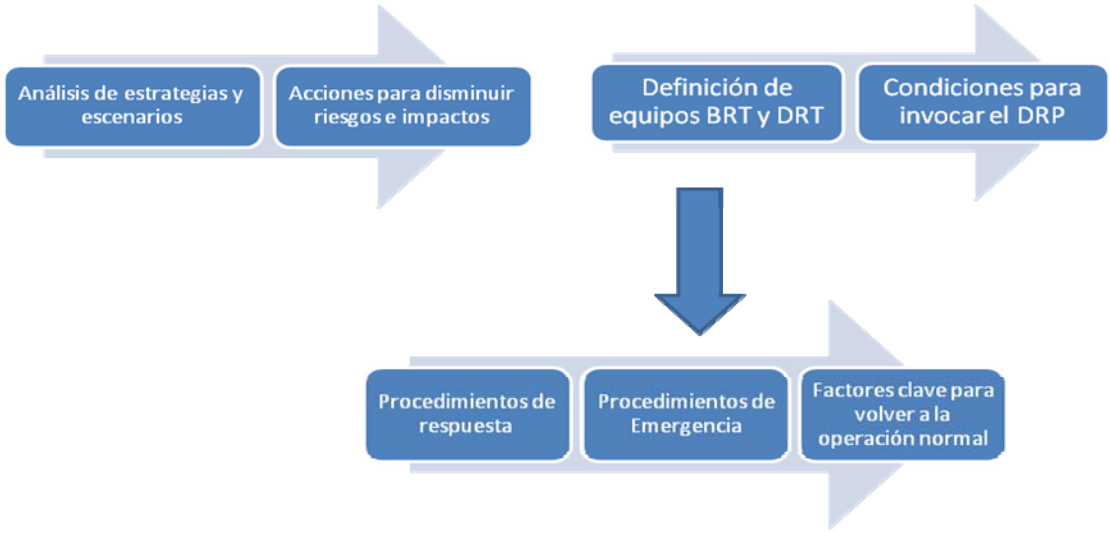
Se prohíbe la utilización de unidades de almacenamiento donde su uso no se encuentre debidamente autorizado por el Responsable de Informática a cargo del área implicada.

CONTINGENCIA

El Responsables de Seguridad del Hospital preparará y actualizará periódicamente un plan de contingencia que permita a las aplicaciones críticas y sistemas de comunicación estar disponibles en el caso de desastre y de cualquier eventualidad que pueda afectar a la disponibilidad e integridad de la información.

Los planes de Contingencia han de cubrir todas las áreas relativas a la continuidad de actividad, definiendo las condiciones necesarias para invocar los planes de recuperación en caso de alerta.

En el siguiente gráfico muestra la evolución del proceso.



* BRT (Business Recovery Task) , DRT (Desaster Recovery Task), DRP (Desaster Recovery Planning).

AUDITORIA

Todos los Sistemas Informáticos que operen y administren información deberán de disponer de un registro de auditoría donde se pueda identificar la modificación, adición o borrado de información.

Todos los archivos de auditorías deberán proporcionar suficiente información para apoyar el monitorización, control y auditorias.

Todos los archivos de auditorías de los diferentes sistemas deberán preservarse por periodos definidos según su criticidad y de acuerdo a las exigencias legales para cada caso.

Todos los archivos de auditorías deberán ser custodiados en forma segura para que no puedan ser modificados y para que puedan ser leídos únicamente por personas autorizadas.

Todos los equipos informáticos computadores de la Entidad deben estar sincronizados y tener la fecha y hora exacta para que el registro en la auditoria sea correcto.

SEGURIDAD FISICA

El Hospital deberá contar con los mecanismos de control de acceso tales como puertas de seguridad, sistemas de control con tarjetas inteligentes, sistema de alarmas y circuitos cerrados de televisión en las dependencias que la Entidad considere críticas.

Los visitantes pertenecientes a terceras empresas que tengan que acceder a áreas restringidas de los Centros Sanitarios, deberán de estar debidamente autorizados existiendo un registro de autorización y acceso. Todo el personal deberá portar su identificación en lugar visible.

ESCRITORIOS LIMPIOS

Todos los escritorios o mesas de trabajo pertenecientes a áreas de uso común deberán permanecer limpios para proteger documentos en papel y dispositivos de almacenamiento como CD',s, usb memory key, disquetes, con fin de reducir los riesgos de acceso no autorizado, perdida y daño de la información durante el horario normal de trabajo y fuera del mismo.

ADMINISTRACION DE LA SEGURIDAD

La evaluación de riesgos de seguridad para los Recursos Informáticos en producción se debe ejecutar al menos una vez cada dos años. Todas las mejoras, actualizaciones, conversiones y cambios relativos asociados con estos recursos deben ser precedidos por una evaluación del riesgo.

Cualquier brecha de seguridad o sospecha en la mala utilización en el Internet, la red corporativa o Intranet, los recursos informáticos de cualquier nivel (local o corporativo) deberá ser comunicada por el usuario que la detecte de forma inmediata al Responsable de Informática del área implicada.

El Responsable de Seguridad del Grupo divulgará, las políticas, estándares y procedimientos en materia de seguridad informática. Efectuará el seguimiento de cumplimiento de las políticas de seguridad y reportara a la Dirección de Sistemas las deficiencias detectadas.

PROCEDIMIENTO DE GESTION DE LA LOPD EN EL GRUPO CAPIO

Describir la metodología que utiliza el Grupo CAPIO y las sociedades que lo forman, para la gestión del cumplimiento de la ley vigente en materia de Protección de Datos.

DOCUMENTACIÓN DE REFERENCIA / LEGISLACIÓN APLICABLE

- Real Decreto 1720/2007 de 21 de diciembre
- LOPD 15/1999 de 13 de diciembre
- Ley básica reguladora de la Autonomía del Paciente 41/2002 de 14 de noviembre
- Ley 34/2002 de 11 de julio de servicios de la sociedad de la información y comercio electrónico.
- Ley 16/2003 de 28 de mayo de cohesión y calidad del Sistema Nacional de Salud.
- Norma UNE-EN-ISO 9001:2.008
- Manual de Calidad de Capio Sanidad.

DESCRIPCIÓN DE PROCESOS

Los procesos que forman parte de la gestión de la LOPD son los siguientes:

1. Identificación y registro de Ficheros de Datos de carácter personal ante la Agencia Protección Datos.
2. Nombramiento del Responsable de Seguridad ó Comité de Seguridad del Centro.
3. Gestión del Documento de Seguridad.
4. Gestión de usuarios que forman parte del personal laboral.
5. Gestión de Terceros con acceso a datos de carácter personal.
6. Gestión de Terceros con acceso a las dependencias, pero sin necesidad de tener acceso a datos de carácter personal.
7. Gestión de derechos ARCO.
8. Registro de incidencias.
9. Registro de Entrada y Salida de Soportes.
10. Registro de control de acceso.
11. Registro de Cesiones de datos
12. Registro de Reuniones en materia de protección de datos
13. Realización de copias de Seguridad de los ficheros registrados.
14. Auditoría bienal (interna ó externa).

1. IDENTIFICACIÓN Y REGISTRO DE FICHEROS DE DATOS DE CARÁCTER PERSONAL ANTE LA AGENCIA DE PROTECCIÓN DE DATOS

   El Responsable de Seguridad del Centro, es el responsable de notificar ante el Responsable de Seguridad y LOPD de Capio, la existencia de un fichero con datos de carácter personal.

   Una vez notificado se realiza un análisis sobre si procede el registro o si dicho fichero contiene un subconjunto de datos de un fichero que ha sido registrado con anterioridad ante la Agencia de Protección de Datos.

El Responsable de Seguridad del Grupo se encargará de efectuar el registro del Fichero que contiene datos de carácter personal ante la Agencia de la Protección de Datos.

La forma de realizar dicha inscripción se hace mediante el formulario "Nota" de titularidad privada, que tiene habilitada la Agencia para tal efecto. La manera en la que se produce la notificación es telemática con certificado digital, obtenido a través de la Fábrica Nacional de Moneda y Timbre.

Realizado el registro, se envía copia de esa notificación al Responsable de Seguridad Centro, que deberá incluir en la Intranet habilitada para la gestión de la Seguridad.

La confirmación de dicho registro por parte de la Agencia, se recibe por correo ordinario 10 días posteriores a la realización de la notificación. Ésta confirmación es escaneada y enviada por correo electrónico al Responsable de Seguridad del Centro para la incorporación del documento en la intranet. Es necesario además, que el Responsable de Seguridad del Centro realice las modificaciones oportunas en el Documento de Seguridad del Centro incorporando los datos de número de registro, nombre registrado, nivel de seguridad aplicable al nuevo fichero registrado.

2. NOMBRAMIENTO DEL RESPONSABLE DE SEGURIDAD Ó COMITÉ DE SEGURIDAD DEL CENTRO

La Dirección del Centro Encargado del tratamiento, se encargará de nombrar el Responsable ó Comité de Seguridad del Centro que se encargará de coordinar todas las tareas correspondientes a la Gestión de la LOPD en el Centro Encargado del tratamiento.

Tal como indica en el Art. 95 del RD 1720/2007 esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciada según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el documento de seguridad.

En ningún caso esta designación supone una exoneración de la responsabilidad que corresponde al responsable del fichero o al encargado del tratamiento de acuerdo con este reglamento.

3. GESTIÓN DEL DOCUMENTO DE SEGURIDAD

El Responsable de Seguridad del Centro será el encargado llevar un control sobre las modificaciones necesarias tanto de índole técnica, como organizativa relacionadas con el Documento de Seguridad de obligado cumplimiento según lo indicado en el Art. 88 RD 1720/2007.

Este documento deberá encontrarse actualizado y publicado en la intranet de Gestión de LOPD del Centro, debiendo de estar impresa la última versión del mismo.

4. GESTIÓN DE USUARIOS CON ACCESO A DATOS DE CARÁCTER PERSONAL QUE FORMAN PARTE DEL PERSONAL LABORAL

El Departamento de Recursos humanos se encargará de entregar a todo el personal que forme parte del personal una cláusula de confidencial que deberá de ser firmada antes de incorporarse el trabajador a la empresa por el personal laboral del centro.

En dicha cláusula están descritas las consideraciones a tener en cuenta a la hora de trabajar con datos de carácter personal así como la Normativa interna de Utilización de los Sistemas de Información.

La custodia de las cláusulas de confidencialidad firmadas se llevará a cabo por el Departamento de Recursos Humanos ya que formará parte de la ficha laboral del trabajador.

El responsable del departamento del nuevo trabajador será el encargado de informar de las aplicaciones y ficheros de carácter personal a las que tendrá acceso en relación a las funciones que va a desempeñar.

Todas las bajas del personal laboral, serán notificadas por el Departamento de Recursos Humanos para que se proceda a la inactivación del usuario con acceso a los recursos.

5. GESTION DE USUARIOS DE TERCEROS CON ACCESO A DATOS DE CARÁCTER PERSONAL

La Dirección del Centro determinará la persona o personas responsables de realizar el control y notificación de Terceros que tendrán que acceder a datos de carácter personal y que será notificado al Responsable de Seguridad para su autorización o negación de acceso.

Todos los Terceros con acceso a datos deberán de haber firmado una cláusula de confidencialidad que incluirá la Normativa interna de utilización de los Sistemas de Información, y que deberá de ser custodiada junto con el contrato firmado de prestación de servicios.

La persona responsable de la Gestión de Terceros del Centro deberá de notificar las altas y bajas de Terceros al Responsable de Seguridad para que éste autorice de carácter temporal el acceso a la información.

6. GESTION DE TERCEROS CON ACCESO A LAS DEPENDENCIAS, PERO SIN ACCESO A DATOS DE CARÁCTER PERSONAL

Según lo descrito en el Art. 91 apartado 5 del RD 1720/2007 es necesario que el personal con acceso a los recursos o a las dependencias del centro esté sometido a las mismas condiciones de control de acceso que el personal laboral, a pesar de que para el desempeño de sus funciones no sea necesario acceder a datos de carácter personal.

De esta manera, la Dirección del Centro nombrará la persona o personas responsables de la gestión de este tipo de terceros en función de las actividades que desempeñen.

Las altas y bajas de éstos Terceros sin acceso a datos, pero con acceso a las dependencias, serán notificadas al Responsable de Seguridad del Centro para que tenga registrado la autorización de acceso a los recursos necesarios para la realización de las funciones contratadas.

7. GESTION DE DERECHOS ARCO

Tal como se indica en el Título III del RD 1720/2007, se publicará en diversos lugares visibles de los Centros encargados del tratamiento, el documento donde los usuarios pueden ejercitar sus derechos de Acceso, Rectificación, Cancelación u Oposición.

En relación a las peticiones efectuadas por los usuarios que ejercitan los derechos sobre los ficheros registrados, será necesario que el Responsable de Seguridad del Centro realice un control sobre el registro de entradas y salidas de las respuestas emitidas en referencia a éstas peticiones.

8. REGISTRO DE INCIDENCIAS

Tal como lo indica el Art. 90 del RD 1720/2007 el Responsable de Seguridad del Centro se encargará de que sean registradas todas las incidencias que afecten a datos de carácter personal de los ficheros registrados.

Los campos que forman parte del registro de incidencias son los siguientes:

- Tipo de incidencia
- Fecha y hora en la que se ha producido
- Fecha y hora en la que se ha detectado
- Nombre del Fichero Registrado al que afecta
- Nombre y apellidos de la persona que lo ha notificado o detectado
- Descripción de la misma
- Nombre y apellidos de la persona encargada de resolverla
- Fecha y hora de la solución
- Descripción de la solución propuesta

9. REGISTRO DE ENTRADA Y SALIDA DE SOPORTES

El Responsable de Seguridad será el encargado de determinar los distintos soportes en los que van a ser gestionados los datos de carácter personal en el Centro.

Una vez identificados se llevará un registro de las entradas de soportes donde se deberán de incorporarse los siguientes campos:

- Nombre y apellidos del Remitente
- Datos de contacto
- Número de inventario
- Fichero registrado al que afecta
- Tipo de soporte
- Fecha de entrada
- Nombre y apellidos del receptor del soporte
- Descripción del contenido
- Observaciones

En el caso de las salidas el registro de información deberá de contener los siguientes campos, y en todos los casos deberá de ser autorizada por el Responsable de Seguridad del Centro:

- Número de inventario
- Nombre y apellidos del solicitante
- Contacto
- Fecha y hora de solicitud

- Tipo de Soporte
- Contenido
- Objetivo
- Destino (Empresa , persona responsable recogida)
- Fichero registrado al que afecta
- Fecha y hora de autorización
- Salida autorizada, pendiente, denegada

10. REGISTRO DE CONTROL DE ACCESO

Según lo dispuesto en el Art. 91 del RD 1720/2007 es de obligado cumplimiento el llevar un control de acceso de los usuarios que acceden a los datos de carácter personal de los ficheros registrados.

En el caso de los Ficheros automatizados, las aplicaciones incorporan las herramientas necesarias para poder efectuar una auditoria de acceso a datos, que serán descritas en el documento de Seguridad.

En el caso de que el acceso se produzca de manera física a lugares como el CPD, el Sistema de Archivo y documentación, o a dependencias del centro donde se encuentren datos de carácter personal, se deberá de llevar a cabo un control manual en el que se registren los siguientes campos:

- Fecha y hora de acceso
- Nombre y Apellidos de persona que accede
- Nombre del Fichero registrado al que afecta el acceso
- Motivo del acceso
- Fecha y hora de salida

En caso de producirse un acceso externo a los Sistemas de Información del Centro, será necesario realizar el mismo registro de control.

11. REGISTRO DE CESIONES DE DATOS

Se entiende por cesión de datos toda revelación de datos realizada por persona distinta al interesado.

Todas las cesiones de datos deberán de ser autorizadas por el Responsable de Seguridad del Centro o por el propio interesado.

El registro de estas cesiones deberá de contener los siguientes campos:

- Fecha y hora de solicitud
- Nombre y apellidos del responsable de la solicitud
- Nombre Fichero registrado al que afecta la cesión de datos
- Entidad a la que se va a realizar la cesión
- Motivo por el que se va a efectuar una cesión de datos.
- Fecha y hora de la autorización
- Quien autoriza la cesión (Responsable de Seguridad, propio interesado)

12. REALIZACIÓN DE COPIAS DE SEGURIDAD DE LOS FICHEROS REGISTRADOS

El Responsable de Seguridad del Centro incorporará en el Documento de Seguridad la política de copia de seguridad que llevará a cabo para garantizar la protección de los Ficheros registrados.

En los casos en los que se disponga de un servicio de externalización de Backups, es necesario que se efectúe un registro que formará parte de la gestión de salida de soportes del centro.

Una vez al trimestre se realizará una prueba de restauración de la copia de seguridad para verificar el correcto estado del mismo. Este resultado quedará registrado en el documento de seguridad junto con los resultados obtenidos.

13. AUDITORIA BIENAL

Según lo dispuesto en el Art. 96 del RD 1720/2007 es de obligado cumplimiento la realización de una auditoría de carácter bienal.

El resultado de esta auditoría será informado al Responsable del Fichero y quedará a disposición de la Agencia de Protección de Datos., donde se pondrán de manifiesto el nivel de cumplimiento y las medidas correctoras necesarias propuestas para una correcta adecuación a la normativa vigente.

14. HERRAMIENTAS

Para la gestión del Documento de Seguridad y los distintos registros de información necesarios para el cumplimiento de la Ley, todos los Centros Encargados de tratamiento disponen de una intranet elaborada con tecnología Share Point con una estructura común inicial pero que puede ser modificable en función de las necesidades de gestión técnica que necesite el centro.

MODELO DOCUMENTO DE SEGURIDAD

CONTENIDO DEL DOCUMENTO

El presente *Documento de Seguridad* (en adelante, el DOCUMENTO) pretende determinar las medidas de Seguridad aplicadas a los Ficheros registrados ante la Agencia de Protección de Datos que contienen Datos de Carácter personal gestionados a través del Hospital de Collado-Villalba, dando así cumplimiento a la obligación establecida en el REAL DECRETO 1720/2007, de 21 de diciembre, por el que se aprueba el *Reglamento de Medidas de Seguridad de los Ficheros que contengan Datos de Carácter Personal*, (en lo sucesivo, el REGLAMENTO) y que desarrolla lo dispuesto en la LOPD 15/1999 de 13 de diciembre.

Dicho DOCUMENTO ha sido elaborado como parte del Plan de Seguridad y de Protección de Datos para dar cumplimiento a las restantes obligaciones fijadas en el REGLAMENTO y garantizar, de esta forma, la seguridad que deben reunir los ficheros automatizados que contienen datos de carácter personal.

El DOCUMENTO resulta de aplicación a todos los Ficheros que contienen datos de carácter personal y que se encontrarán debidamente registrados ante la Agencia de Protección de Datos.

Los documentos de notificación de los Ficheros al Registro de la Agencia de Protección de Datos, así como su descripción se recogerán en el portal *de Seguridad y Protección de Datos-LOPD* del Hospital (en adelante, el PORTAL).

RESPONSABLE DE SEGURIDAD

El Hospital, como Encargado Responsable de Tratamiento de los Ficheros y en virtud de lo previsto en el REGLAMENTO para todos los Ficheros que, como mínimo, exijan la aplicación de las medidas de seguridad de nivel medio determinará el nombramiento de un Responsable ó Comité de Seguridad, con todas las funciones y obligaciones que ello supone, y con sujeción a lo establecido en este DOCUMENTO y en toda la normativa de aplicación.

ÁMBITO DE APLICACIÓN

Este DOCUMENTO es de obligado cumplimiento para todo el personal con acceso a los datos automatizados de carácter personal contenidos en los Ficheros y a los Sistemas de Información.

El DOCUMENTO deberá estar en todo momento actualizado, y deberá ser revisado siempre que se produzcan cambios relevantes en los Sistemas de Información o en la organización del mismo. Así mismo, deberá adecuarse en todo momento a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

Todas las personas con acceso autorizado a los datos de los Ficheros a través de cualquier medio habilitado para este fin, se encuentran obligadas por Ley a cumplir lo establecido en este DOCUMENTO y sujetas a las consecuencias en que pudieran incurrir en caso de incumplimiento.

Por ello, y para garantizar el conocimiento de lo establecido en el DOCUMENTO a todas las personas autorizadas para acceder a los datos contenidos en los Ficheros, una copia del presente estará disponible a todo el personal en el PORTAL.

RECURSOS PROTEGIDOS

La protección de los datos de los Ficheros contra accesos no autorizados se deberá realizar mediante el control, a su vez, de todas las vías por las que se pueda tener acceso a dicha información.

Los recursos que, por servir de medio directo o indirecto para acceder a los Ficheros, deberán ser controlados por esta normativa son:

- Los centros de tratamiento y locales donde se encuentran ubicados los Ficheros, equipos servidores y máquinas auxiliares, donde también se almacenan los soportes.
- Los puestos de trabajo, locales o remotos, desde los que se pueda tener acceso a los Ficheros.
- El entorno del Sistema de Comunicaciones, incluyendo la red corporativa y el entorno del Sistema Operativo del GRUPO.
- Los sistemas informáticos o aplicaciones para acceder a los Ficheros, así como su Estructura Lógica de Datos. Su descripción figura en el PORTAL.

MEDIDAS, NORMAS Y PROCEDIMIENTOS DE SEGURIDAD

MEDIDAS DE SEGURIDAD

El presente DOCUMENTO recoge las medidas, normas, procedimientos, reglas y estándares establecidas por el Hospital para garantizar la confidencialidad, integridad y disponibilidad de la información contenida en los Ficheros con arreglo a los niveles de seguridad aplicables a éstos, exigidos por el Reglamento de Medidas de Seguridad.

Acceso a datos a través de Redes de Comunicaciones. El acceso a los datos a través de redes de comunicaciones debe garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local. Para ello, las aplicaciones que componen los Sistemas de Información deberán implementar la validación de usuarios a través de contraseñas.

Régimen de trabajo fuera de los locales de la ubicación de los Ficheros. El tratamiento de los datos contenidos en los Ficheros se puede llevar a cabo, bien desde los locales donde se encuentran ubicados, bien desde los equipos que se encuentran situados en dichos locales.

En aquellos supuestos en los que se vayan a realizar tratamientos desde equipos situados fuera de los locales de ubicación de los Ficheros, se exige una autorización del Responsable del Fichero, y se debe garantizar el nivel de seguridad correspondiente al tipo de fichero tratado.

La gestión de Solicitudes de Tratamiento Remoto se ajustará a lo establecido en el Protocolo de Gestión Centralizada de Usuarios.

Ficheros temporales. Los ficheros temporales cumplen el nivel de seguridad que les corresponde con arreglo a lo establecido en el REGLAMENTO, siéndoles de aplicación lo establecido en el *Procedimiento para la Gestión de Ficheros Temporales*. Con carácter general, todo fichero temporal será borrado una vez que haya dejado de ser necesario para los fines que motivaron su creación.

Identificación y autentificación. El Responsable de Seguridad mantendrá una relación actualizada de los usuarios que tengan acceso autorizado a los Ficheros (indicando a qué tienen acceso y establecerá los procedimientos de identificación y autenticación para dicho acceso, siéndole de aplicación lo establecido en el Anexo D del DOCUMENTO.

El Responsable de Seguridad o persona designada por aquél será el encargado de asignar los perfiles necesarios para acceder a la información contenida en los Ficheros. Dichos perfiles habilitan para acceder a uno, varios o todos los módulos de la aplicación informática de acceso a los Ficheros, así como a todo o parte de la información, en función de las tareas que se vayan a desarrollar por cada uno de los usuarios autorizados y de su perfil funcional.

Cuando el mecanismo de autenticación se base en la existencia de contraseñas existirá un procedimiento de asignación y distribución que garantice su confidencialidad e integridad. Éste estará disponible en el PORTAL.

El Responsable de Seguridad establecerá un mecanismo que permita la identificación de forma inequívoca y personalizada de todo aquel usuario que intente acceder a los Sistemas de Información y la verificación de que está autorizado. Se limitará la posibilidad de intentar reiteradamente el acceso por parte de personal no autorizado a los Ficheros.

Control del acceso. El sistema informático, la red corporativa y los terminales utilizados por cada usuario autorizado son titularidad del Hospital.

Toda la información, de forma estática o circulando a través de la red corporativa, tiene carácter de confidencial. Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones. El Responsable del Fichero establecerá mecanismos para evitar que un usuario pueda acceder a datos o recursos con derechos distintos de los autorizados.

Exclusivamente, el personal autorizado podrá conceder, alterar o anular el acceso autorizado del personal sobre los datos y recursos, conforme a los criterios establecidos por el Responsable del Fichero.

Auditoría. Los Sistemas de Información e instalaciones de tratamiento de datos se someterán bienalmente a una auditoría interna o externa que verifique el cumplimiento del Reglamento de Medidas de Seguridad, de las obligaciones previstas en LOPD y de los procedimientos e instrucciones vigentes en materia de seguridad de datos que, en su caso, hubiesen sido aprobados o resulten de aplicación.

El Informe de Auditoría deberá dictaminar sobre la adecuación de las medidas, controles y, en general, sobre la Política de Seguridad al Reglamento de Medidas de Seguridad, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias. También incluirá los datos, hechos y observaciones en que se basen los dictámenes alcanzados y recomendaciones propuestas.

Los Informes de Auditoría serán analizados por el Responsable de Seguridad, que elevará las conclusiones al Responsable de los Ficheros para que adopte las medidas correctoras adecuadas y quedará a disposición de la Agencia de Protección de Datos.

Control del acceso físico. Exclusivamente, sólo el Responsable de Seguridad y personal autorizado podrán tener acceso físico a los locales donde se encuentren ubicados los Ficheros con datos de carácter personal. El personal autorizado se encuentra declarado en el PORTAL.

Pruebas con datos reales. Las pruebas que se realicen con anterioridad a la implantación o modificación de los Sistemas de Información que traten los Ficheros declarados no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente.

Utilización del correo electrónico. El uso del correo electrónico queda limitado a fines estrictamente laborales y relacionados con las funciones desarrolladas por el personal del Hospital. Así mismo, se uso deberá ajustarse a la Política de Seguridad y de Protección de Datos del Hospital.

Distribución de soportes. La distribución de soportes que contengan datos de carácter personal procedentes del Fichero PACIENTES que vayan a salir de los Centros de tratamiento, exigirá el cifrado de dichos datos o el empleo de cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulable durante su transporte.

Registro de los accesos. De cada acceso al Fichero PACIENTES se guardará como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el tipo de acceso y si ha sido denegado o autorizado. En cualquier caso, dicha información se conservará durante un mínimo de dos años.

Los mecanismos que permiten el registro de los datos detallados estarán bajo el control directo del Responsable de Seguridad, sin que, en ningún caso, deba permitirse la desactivación de los mismos.

Cifrado de las telecomunicaciones. La transmisión de datos procedentes del Fichero PACIENTES, a través de redes de telecomunicaciones exigirá el cifrado de los datos o el empleo de cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

NORMAS Y PROCEDIMIENTOS DE SEGURIDAD

Asimismo, junto con las medidas de seguridad adoptadas, el presente DOCUMENTO también incorpora las normas y procedimientos de seguridad integrantes de la Política de Seguridad y de Protección de Datos del Hospital, que deberán ser observadas y cumplidas adecuadamente.

Centros de tratamiento y locales. Los locales donde se ubican los equipos que contienen los Ficheros deben ser objeto de especial protección, de forma que se garantice la disponibilidad y confidencialidad de los datos protegidos, de la información en ellos contenida, especialmente en el caso de que los Ficheros estén ubicados en un servidor al que sea posible el acceso a través de una red.

Los locales deberán contar con los medios mínimos de seguridad que eviten los riesgos de indisponibilidad de los Ficheros que pudieran producirse. El acceso a éstos se encuentra limitado únicamente al personal autorizado e identificado en el PORTAL.

Puestos de trabajo. Son todos aquellos dispositivos desde los cuales se puede acceder a los datos contenidos en los Ficheros. Por ejemplo, terminales, ordenadores personales u ordenadores portátiles.
Se consideran también puestos de trabajo aquellos terminales de administración del sistema, como, por ejemplo, las consolas del sistema.

Cada una de las personas autorizadas para acceder a la información contenida en los Ficheros será responsable de su puesto de trabajo y del acceso a los Ficheros que desde los mismos se realice, debiendo garantizar que la información no pueda ser vista por personas no autorizadas.

Tanto las pantallas como las impresoras u otro tipo de dispositivos conectados al puesto de trabajo deberán ubicarse físicamente en lugares que permitan garantizar esa confidencialidad.

Cuando el responsable de un puesto de trabajo lo abandone, bien temporalmente, bien al finalizar su turno de trabajo, deberá dejarlo en un estado que impida la visualización de datos protegidos. Esto podrá realizarse a través de un protector de pantalla que impida la visualización de los datos o mediante el bloqueo de su usuario. La reanudación del trabajo implicará la introducción de la contraseña correspondiente.

Respecto de las impresoras, deberá asegurarse que no queden documentos impresos en la bandeja de salida que contengan datos protegidos. Si las impresoras son compartidas con otros usuarios no autorizados para acceder a los datos de los Ficheros, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos, siendo de su exclusiva responsabilidad el acceso a dicha información impresa por parte de usuarios no autorizados.

Los puestos de trabajo, desde los que se tiene acceso a los Ficheros, tendrán una configuración fija en sus aplicaciones y sistemas operativos que sólo podrá ser cambiada bajo la autorización del Responsable de Seguridad o administradores del sistema autorizados.

Entorno del Sistema Operativo y de Comunicaciones. El acceso a los datos de los Ficheros se realiza a través de diversas aplicaciones, existiendo un administrador responsable de las mismas; Éste deberá estar identificado en el PORTAL.

El Hospital cuenta con una red de área local en cuyos equipos servidores se encuentran instaladas las aplicaciones informáticas, desde las que acceder a los datos de los Ficheros.

El Responsable de Seguridad es el encargado de asegurar que el acceso a los Ficheros, al estar ubicado en equipos a los que se accede a través de la red local del Hospital, no se permite a personas no autorizadas.

Aplicaciones informáticas de acceso a los Ficheros. Las aplicaciones informáticas que permiten el acceso a los Ficheros no podrán ser accesibles a usuarios no autorizados. Su descripción se recoge en el PORTAL.

El acceso a los Ficheros, a través de las aplicaciones informáticas, se realizará de forma restringida, mediante un código de usuario y una contraseña, los cuales deberán ser individuales; cada persona autorizada para acceder a los ficheros deberá tener su propio usuario y una contraseña sólo conocida por él.

Si las aplicaciones informáticas que permiten el acceso a los Ficheros no cuentan con un control de acceso, deberá ser el sistema operativo, donde se ejecuta esa aplicación, el que impida el acceso no autorizado, mediante el control de los citados códigos de usuario y contraseñas.

En cualquier caso se controlarán los intentos de acceso fraudulento a los Ficheros, limitando el número máximo de intentos fallidos y cuando sea técnicamente posible, guardando en un fichero auxiliar la fecha, hora, código y claves erróneas que se han introducido, así como otros datos relevantes que ayuden a descubrir la autoría de esos intentos de acceso fraudulentos.

Salvaguarda y protección de las contraseñas personales. Las contraseñas personales constituyen uno de los componentes básicos de la seguridad de los datos y, por lo tanto, deben estar especialmente protegidas. Como llaves de acceso a los Ficheros, las contraseñas deberán ser estrictamente confidenciales y personales, y cualquier incidencia que comprometa su confidencialidad deberá ser inmediatamente comunicada al Responsable de Seguridad y subsanada en el menor plazo de tiempo posible.

Cada usuario será responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá comunicarlo como incidencia y proceder inmediatamente a su cambio. Cada usuario es absolutamente responsable de todas las actividades que se realicen con su contraseña.

FUNCIONES Y OBLIGACIONES DEL PERSONAL

De conformidad con lo dispuesto en el REGLAMENTO, el DOCUMENTO debe reflejar el conjunto de funciones y obligaciones del personal del CENTRO que tenga acceso a los datos personales contenidos en los Ficheros, siendo de obligado cumplimiento para todos ellos.

El personal del HOSPITAL, que tiene acceso a los Ficheros, afectado por esta normativa se clasifica en dos categorías:

- **Responsables de seguridad y Administradores del Sistema**, todos aquellos encargados de administrar o mantener el entorno operativo y de comunicaciones de los Ficheros y cuya relación se contiene en el PORTAL.
- **Usuarios los Ficheros,** personal del Hospital o externas que utilizan la aplicación informática de acceso a los Ficheros.

Sin perjuicio de las funciones y obligaciones a las que se hace referencia a continuación, el Responsable de Seguridad y administradores, así como los usuarios autorizados también deberán cumplir cualesquiera otras obligaciones que de forma específica aparezcan reflejadas en otros apartados del presente DOCUMENTO.

El Responsable de Seguridad y las personas expresamente autorizadas por él, declaradas en el PORTAL deberán asumir y cumplir las siguientes funciones y obligaciones:

- Controlar, coordinar e implantar las medidas de seguridad establecidas en el presente DOCUMENTO.
- Mantener el contenido del presente DOCUMENTO debidamente actualizado siempre que se produzcan cambios relevantes en las aplicaciones informáticas, Ficheros, organización de los mismos y, en general, en el entorno del sistema informático del GRUPO y del HOSPITAL.
- Adecuar su contenido a las disposiciones vigentes en materia de seguridad de datos que resulten aplicables.

- Mantener una relación actualizada de usuarios que tengan acceso autorizado a los Ficheros.
- Velar por que el acceso a los Ficheros sea restringido mediante un código de usuario y una contraseña, garantizando que ésta sea solamente conocida por la persona responsable.
- Mantener un Registro de Incidencias de conformidad con lo dispuesto en el Apartado 6 del presente DOCUMENTO.
- Establecer mecanismos para evitar que un usuario pueda acceder a datos o recursos distintos de aquellos para los cuales están autorizados.
- Autorizar la salida de soportes informáticos que contengan datos los Ficheros fuera de los locales donde esté ubicado el mismo.
- Mantener un Registro de Entradas y Salidas de Soportes fuera de los locales de ubicación los Ficheros.
- Autorizar expresamente el tratamiento de datos fuera de los locales de ubicación los Ficheros.
- Revisar periódicamente la información de control de accesos registrada y elaborará un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes [(2)].
- Verificar la definición y correcta aplicación de las copias de respaldo y procedimientos de recuperación de los datos [(4)]. Esto se ajustará a lo establecido en el *Procedimiento de Realización y Recuperación de Copias de Respaldo.*
- Analizar los Informes de Auditoría y elevar las conclusiones al GRUPO, como Responsable de los Ficheros.
- Elaborar un informe de las revisiones realizadas y los problemas detectados con la periodicidad mínima indicada en el Apartado 10 del presente DOCUMENTO.

Todos los usuarios expresamente autorizados para acceder a la información contenida en los Ficheros y hacer uso de los SI deberán cumplir las funciones y obligaciones:

- Cumplir el conjunto de disposiciones y obligaciones integrantes del presente DOCUMENTO, así como con las restantes obligaciones previstas en la Política de Seguridad y de Protección de Datos del Hospital.

- Todo usuario deberá utilizar la red corporativa del Hospital y sus datos de forma diligente, sin incurrir en actividades que puedan ser consideradas ilícitas o ilegales, que infrinjan los derechos de terceros o que puedan atentar contra la moral o las normas de buen uso de las redes telemáticas.

- Queda prohibido comunicar a otra persona el identificador de usuario y la clave de acceso. Si el usuario sospecha que otra persona conoce sus datos de identificación y acceso deberá ponerlo en conocimiento del Responsable de Seguridad con el fin de que tome las medidas pertinentes.

- Guardar y garantizar la confidencialidad de la información a la que tengan acceso:

    - No se enviará información al exterior, sin estar debidamente autorizado para ello, mediante soportes materiales o a través de cualquier medio de comunicación, incluyendo la simple visualización o acceso.
    - Los usuarios del Sistema Informático del HOSPITAL deberán guardar, por tiempo indefinido, la máxima reserva y no divulgar ni utilizar directamente ni a través de terceras personas o entidades, los datos, documentos, metodologías, claves, análisis, programas y demás informaciones a las que tengan acceso durante su relación

contractual con el HOSPITAL. Esta obligación queda vigente con carácter definitivo aún extinguido el contrato.

- Ningún colaborador deberá poseer, para fines ajenos a los propios de sus funciones, ningún material o información titularidad del HOSPITAL.
- En el caso de que, por motivos directamente relacionados con el puesto de trabajo, el empleado entre en posesión de información titularidad del GRUPO o de el HOSPITAL contenida en cualquier tipo de soporte, deberá entenderse que dicha posesión es estrictamente temporal, con obligación de secreto y sin que ello le reconozca derecho alguno de posesión, titularidad o copia sobre la referida información.
- El trabajador deberá devolver todos los materiales a los que haya tenido acceso inmediatamente después de la finalización de las tareas que hayan originado el uso temporal de los mismos y, en cualquier caso, a la finalización de la relación contractual.

- Están prohibidas expresamente las siguientes actividades:

  - Compartir o facilitar el identificador de usuario y la clave de acceso. En caso de incumplimiento de esta prohibición, el usuario será el único responsable de los actos realizados por la persona que utilice de forma no autorizada el identificador del usuario.
  - Intentar distorsionar o falsear los registros log del sistema.
  - Intentar descifrar cualquier elemento de seguridad empleado.
  - Destruir, alterar, inutilizar o de cualquier otra forma dañar los datos, programas o documentos electrónicos titularidad del Hospital.
  - Intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios.
  - Intentar aumentar el nivel de privilegios de un usuario en el Sistema.

Es obligación de todo el personal dar cumplimiento al procedimiento de notificación, gestión y respuesta ante las incidencias de las que tuviere conocimiento utilizando el *Procedimiento de Notificación y Gestión de Incidencias* disponible en el PORTAL.

GESTIÓN DE INCIDENCIAS

La Comunicación y Notificación de Incidencias al personal encargado de su resolución, deberá estar sujeta al *Procedimiento de Notificación y Gestión de Incidencias* disponible en el PORTAL. Se establece un Servicio de Resolución de Incidencias, dependiente del Responsable de Seguridad o aquél que este determine, para la gestión y resolución de las incidencias que puedan surgir en el funcionamiento general del Sistema y/o en la aplicación de acceso a los Ficheros.

Así mismo, se establecerá un Registro de Incidencias, cuyo contenido quedará regulado por el *Procedimiento de Notificación y Gestión de Incidencias* disponible en el PORTAL.

El Responsable de Seguridad o aquél que éste determine deberá garantizar que el personal autorizado de respuesta a la incidencia detectadas, y supervisará el trabajo de subsanación de la anomalía.

Así mismo, la comunicación de Incidencias deberá hacerse efectiva en el momento en el que se produzcan, utilizando para ello las vías identificadas en el Procedimiento.

El conocimiento de una incidencia, por parte de un usuario, y su falta de notificación al Servicio de Resolución de Incidencias se considerará como una falta grave contra la seguridad de los Ficheros por parte de dicho usuario.

GESTIÓN Y DISTRIBUCIÓN DE SOPORTES

Los soportes informáticos que contengan datos procedentes los Ficheros deberán permitir identificar el tipo de información que contienen, ser inventariados y etiquetados y almacenarse en un lugar sólo accesible al personal autorizado.

La identificación deberá realizarse mediante un etiquetado apropiado. Se establecerá un Inventario de Soportes en el PORTAL.

La grabación de datos procedentes de los Ficheros en soportes sólo podrá ser realizada por el Responsable de Seguridad o personas autorizadas por aquél. Cualquier otra grabación de datos personales procedentes de los Ficheros, realizada por persona no autorizada a tal efecto será considerada como una infracción de las normas contenidas en el presente DOCUMENTO y la persona que la hubiese llevado a cabo será la única responsable de las consecuencias jurídicas que de ello pudieran derivarse.

Cuando un soporte vaya a ser desechado o reutilizado, se ajustará a lo establecido en el *Procedimiento de Reutilización y Desechado de Soportes*, disponible en el PORTAL.

Se establece un Registro de entrada y salida de soportes informáticos que permite, directa o indirectamente, conocer el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción, que deberá estar debidamente autorizada. La Salida de Soportes deberá ajustarse a lo establecido en el *Procedimiento de Autorización de Salida de Soportes*, disponible en el PORTAL.

Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos.

En cualquier caso, la distribución de soportes que contengan datos procedentes del Fichero PACIENTES exigirá el cifrado de la información que contengan o el empleo de cualquier otro mecanismo que garantice que dicha información no sea inteligible ni pueda ser manipulada durante su transporte.

PROCEDIMIENTOS PARA LA REALIZACIÓN DE COPIAS DE RESPALDO Y RECUPERACIÓN DE DATOS

Para garantizar la integridad y la disponibilidad de los datos contenidos en los Ficheros se establece el *Procedimiento de Realización y Recuperación de Copias de Respaldo*, disponible en el PORTAL, de modo que, frente a fallos, caídas, interrupciones, pérdidas o destrucciones de todo o parte del Sistema de Información, aquéllos garanticen la reconstrucción de éste al estado en el que estaba al tiempo de producirse el fallo.

En los casos en los que haya que proceder a efectuar una recuperación de Datos, ésta deberá de ajustarse al *Procedimiento de Recuperación de Datos*, disponible en el PORTAL, garantizando el cumplimiento de requisitos y autorizaciones.

El Responsable del Fichero o aquél que este determine, se encargará periódicamente de verificar que la realización de Copias de Respaldo es correcta. Para ello se establece el *Procedimiento de Realización de Pruebas y Test*, disponible en el PORTAL.

En todo caso, las Copias de Respaldo deberán almacenarse en una ubicación externalizada físicamente al CPD.

En caso de que las Copias de Respaldo redunden en Cintas Magnéticas o similares, será necesario que estas queden alojadas en una Caja Fuerte de acceso limitado y con llave o clave de acceso. Si estas Cintas son recogidas por un Proveedor Externo para su almacenamiento en ubicaciones seguras externas al Hospital, deberán estar cifradas y seguir el *Procedimiento de Autorización de Salida de Soportes* disponible en el PORTAL.

Si las Copias de Respaldo se almacenan en Unidades de Almacenamiento Masivo dedicadas, estás tendrán que estar ubicadas en un lugar seguro y de acceso limitado.

CONTROLES PERIÓDICOS DE VERIFICACIÓN DEL CUMPLIMIENTO

El Responsable de Seguridad y/o las personas expresamente por aquél designadas son los encargados de velar por el correcto cumplimiento de los términos del presente DOCUMENTO y la aplicación del conjunto de medidas integrantes del Plan de Seguridad y de Protección de Datos del GRUPO, así como los encargados de velar por la veracidad y exactitud de los términos y datos contenidos en los Anexos del presente.

Para la comprobación de todo ello, se procederá a la realización de controles periódicos. Éstos incluyen una evidencia de comprobación, que deberá estar presente para acreditar la aplicación de estas revisiones:

AUDITORÍA: Bienalmente se realizará una auditoria, externa o interna, que dictaminará el correcto cumplimiento y la adecuación de las medidas de seguridad al presente DOCUMENTO y normativa, identificando las deficiencias y proponiendo las medidas correctoras necesarias. Los Informes de Auditoría serán analizados por el Responsable del Fichero o aquél en el que éste determine, quien deberá proponer las medidas correctoras correspondientes.

USUARIOS: El Responsable de Seguridad o aquél que este determine se ajustarán a lo establecido en el *Protocolo de Gestión Centralizada de Usuarios*, así como a otros Protocolos disponibles para el mismo efecto, en cuanto a bajas puntuales de Usuarios.

Así mismo, con una periodicidad trimestral, revisará y procederá a la actualización de la población de usuarios autorizados para acceder a los Ficheros, dando de baja a aquéllos que ya no estén en el Hospital.

La mejor evidencia de estas revisiones será la existencia de la población de Usuarios actualizada a, como máximo, tres meses del día de la revisión.

REGISTROS DE ACCESOS: Con una periodicidad mensual, el Responsable de Seguridad o aquél que este determine activarán el *Procedimiento de Revisión Periódica de Usuarios* disponible en el PORTAL y

emitirá un informe con el contenido que indica el Procedimiento. De este Informe deberá quedar evidencia en el PORTAL.

DOCUMENTO DE SEGURIDAD Y PROCEDIMIENTOS: Cuando resulte necesario modificar los Documentos de Seguridad y/o procedimientos existentes para adaptarlos a la realidad del Hospital y/o a la normativa vigente se dejará evidencia de la revisión con la modificación de la versión documental.

COPIAS DE RESPALDO: Semanalmente se realizará una verificación para comprobar la existencia de Copias de Respaldo recientes. Si se encontrase alguna anomalía sería preciso redactar un Documento indicando de qué trata y las medidas correctivas adoptadas.

Trimestralmente, será necesario ejecutar el *Procedimiento de Realización de Pruebas y Test*, incluido en el PORTAL.

ANEXO 9.A - GLOSARIO. DEFINICIÓN DE LA TERMINOLOGÍA EMPLEADA

- *Accesos Autorizados:* Autorizaciones concedidas a un usuario para la utilización de diversos recursos.
- *Alteración:* Modificación física de las señales representativas de los datos registrados en soportes informatizados por causas accidentales o intencionadas.
- *Autenticación:* Proceso de comprobación de la identidad de un usuario.
- *Cesión o comunicación de datos:* Toda revelación de datos realizada a una persona distinta del interesado.
- *Código de Identificación del Usuario:* Cadena de caracteres utilizados para identificar a un usuario.
- *Confidencialidad:* Propiedad de la información que hace que ésta sólo pueda ser revelada a individuos, personas, entidades o procesos autorizados, en el momento y forma previstos.
- *Contraseña:* Información confidencial, frecuentemente constituida por una cadena de caracteres, que es utilizada en la autenticación de un usuario.
- *Control de Acceso:* Mecanismo que, en función de la identificación ya autenticada permite acceder a determinados datos o recursos.
- *Copia de Respaldo*[)]*:* Copia de los datos de un fichero automatizado en un soporte que posibilite su recuperación.
- *Dato de Carácter Personal:* Comprende cualquier información concerniente a personas físicas identificadas o identificables.
- *Datos especialmente protegidos:* Datos de carácter personal relativos a la ideología, afiliación sindical, religión, creencias, origen racial, salud, vida sexual, comisión de infracciones penales o administrativas y que son objeto de las disposiciones del artículo 7 de la LOPD.
- *Disponibilidad:* Propiedad que requiere que los recursos de un sistema sean accesibles y puedan ser utilizados por un usuario autorizado, en todo momento o dentro de un tiempo razonable.
- *Encargado del tratamiento:* Persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.
- *Entorno:* Conjunto de bienes, muebles e inmuebles, fungibles o no, externos al equipo físico, lógico y datos mediante los cuales son posibles las distintas operaciones que, según el artículo 3 de la LOPD, integran el tratamiento de los datos.
- *Fichero:* Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
- *Fichero Auxiliar:* Fichero de utilidad temporal, usado como almacenamiento auxiliar, que es necesario sólo mientras dure un trabajo o proceso.
- *Identificación:* Procedimiento de reconocimiento de la identidad de un usuario o proceso.
- *Incidencia:* Cualquier anomalía que afecte o pueda afectar a la seguridad de datos, desde el punto de vista de su confidencialidad, integridad y disponibilidad.
- *Integridad:* Propiedad de la información que garantiza que esta es completa, exacta y válida.

- *Pérdida:* Desaparición física de las señales representativas de los datos registrados en soportes informatizados, por causas accidentales o intencionadas.
- *Perfil de acceso de un usuario:* Recursos informáticos y tipos de acceso a los mismos, autorizados para un usuario.
- *Plan de contingencia:* Conjunto documentado de medidas a tomar y de los responsables de las mismas, ante situaciones anómalas o síntomas de estas.
- *Plan de Seguridad:* Documento que describe cómo una Organización gestiona y organiza sus requisitos de seguridad.
- *Red de Telecomunicación:* Conjunto de canales de transmisión, circuitos y, en su caso, dispositivos o centrales de conmutación, que proporcionan conexiones entre dos o más puntos definidos para facilitar la telecomunicación entre ellos.
- *Recurso:* Cualquier parte componente de un sistema de información.
- *Responsable del Fichero o Tratamiento:* Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.
- *Responsable de Seguridad:* Persona o personas a las que el Responsable del Fichero ha asignado formalmente la función de coordinar y controlar las medidas de seguridad aplicables.
- *Salvaguarda:* Proceso de realización de una copia preventiva o de reserva, o la propia copia que resulta del proceso.
- *Sistemas de Información:* Conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.
- *Soporte:* Objeto físico susceptible de ser tratado en un Sistema de Información y sobre el cual se pueden grabar y/o recuperar datos.
- *Usuario:* Sujeto o proceso autorizado para acceder a datos, o recursos.

ANEXO 9.B - CENTROS DE TRATAMIENTO Y LOCALES

Tal y como se indicó en los Documentos de Declaración de Ficheros a la Agencia de Protección de Datos (Ver *Documentos de Declaración* en el PORTAL), los Ficheros se encuentran ubicados en la sede del Hospital, ubicada en **C/ María de Molina 54 6º Planta 28006 Madrid (Madrid).**

Los Ficheros, así como las máquinas en las que se ejecutan las aplicaciones informáticas que hace posible el acceso a los datos contenidos en los Ficheros, entre otros elementos del Sistema de Información del CENTRO, se encuentran ubicados en los mismos locales.

El acceso físico a dichos locales está limitado a aquellas personas expresamente autorizadas a tal efecto, controlándose el acceso mediante el empleo de una llave a la que sólo tienen acceso el Responsable de Seguridad y las personas expresamente autorizadas a tal efecto en el PORTAL.

ANEXO 9.C - GESTIÓN DE FICHEROS TEMPORALES

La gestión de Ficheros temporales seguirá la observancia de lo establecido en el *Procedimiento para la Gestión de Ficheros Temporales disponible en el* PORTAL. En todo caso, cumplirán con los siguientes requisitos:

- Los usuarios deberán garantizar, respecto de los FICHEROS TEMPORALES, el cumplimiento de las medidas integrantes del Documento de Seguridad del Hospital, en particular las relativas al control de acceso mediante el empleo de un nombre de usuario y contraseña que limite y controle el acceso a los mismos.
- El uso de FICHEROS TEMPORALES queda limitado exclusivamente al personal autorizado a acceder y tratar los datos personales.
- La creación de FICHEROS TEMPORALES ha de estar exclusivamente vinculada al desarrollo de las funciones propias de la persona que lleva a cabo su creación, siempre y cuando estos ficheros se conviertan en una herramienta de trabajo.
- Los datos registrados en los FICHEROS TEMPORALES deberán mantenerse actualizados el tiempo que dure su explotación y/o utilidad.
- Desde el momento en el que se tenga constancia de la desactualización de alguno de los datos registrados en los FICHEROS TEMPORALES, la persona que haya procedido a su creación deberá proceder a corregir y actualizar los datos incorrectos.
- Los FICHEROS TEMPORALES deberán ser guardados y almacenados en una carpeta cuyo acceso esté restringido y requiera el empleo de un nombre de usuario y contraseña. En caso contrario, deberá ser el propio FICHERO TEMPORAL el que permita controlar el acceso al mismo mediante el empleo de una contraseña.
- No se mantendrán, bajo ningún concepto, FICHEROS TEMPORALES con datos personales cuando los mismos ya no sean útiles ni necesarios para el fin que justificó su creación, debiéndose proceder a su completo borrado (incluso de la “Papelera de Reciclaje”).
- No se comunicarán, intercambiarán o cederán, en todo o en parte, los FICHEROS TEMPORALES a terceras personas ajenas a la estructura del Hospital o a terceras empresas, salvo que se cumplan las previsiones y obligaciones exigidas por la normativa de protección de datos al respecto.
- Toda persona que utilice FICHEROS TEMPORALES estará obligada a velar por la confidencialidad y privacidad de los datos personales en él registrados. También están obligados a guardar secreto respecto de los mencionados datos.
- La persona que infrinja estas obligaciones asumirá toda la responsabilidad que dicho incumplimiento haya podido generar.

ANEXO 9.D - PERSONAL AUTORIZADO PARA ACCEDER A LOS FICHEROS

El REAL DECRETO establece la necesidad de llevar un registro donde se contenga una relación actualizada de todos los usuarios que tengan acceso autorizado al sistema de información. Además, dicha relación deberá contener los accesos autorizados para cada uno de ellos.

En el caso del HOSPITAL, el número de usuarios autorizados justifica que dicha relación de usuarios, en lugar de mantener un registro periódico, se establezca un procedimiento por el cual obtener la información solicitada de manera inmediata.

El Responsable de Seguridad o aquél que éste determine será el encargado de velar por la actualización periódica, de conformidad con lo dispuesto en el Apartado 10 del presente DOCUMENTO, de dicha relación, autorizando o denegando el acceso a los Ficheros, en función de sus competencias, y creando y deshabilitando usuarios según la validez de éstos.

En cualquier caso, el procedimiento se indicará en el PORTAL, y en todo caso, deberá proporcionar:

- Nombre y apellidos.
- Módulos del Fichero a través de los cuales accede y perfil de acceso.
- Nombre de usuario empleado para acceder al Fichero.
- Fin de validez del Usuario (Si procede).

ANEXO 9.E -PORTAL DE SEGURIDAD Y PROTECCIÓN DE DATOS-LOPD

Con el objetivo de dinamizar el contenido del presente DOCUMENTO, dada la información que ha de contener y para hacerlo llegar a todo el personal del HOSPITAL, se hace recomendable su ampliación en un soporte electrónico constituido por el *Portal de Seguridad y Protección de Datos-LOPD* ubicado en la intranet corporativa.

CONTENIDO DEL PORTAL CENTRALIZADO: Común a todos los Hospitals. DESCENTRALIZADO: Independiente por Hospital.		
FICHEROS DECLARADOS	Contenido de Ficheros declarados al RGPD. Códigos de Inscripción de Ficheros.	DESCENTRALIZADO
LEGISLACIÓN	Legislación aplicable en materia de Seguridad y Protección de Datos.	CENTRALIZADO
GESTIÓN DE INCIDENCIAS	Registro de Incidencias.	DESCENTRALIZADO
INVENTARIO DE SOPORTES	Inventario de soportes físicos que contengan Datos protegidos.	DESCENTRALIZADO
GESTIÓN DE ENTRADA/SALIDA DE SOPORTES	Registro de entrada/salida de soportes que contengan Datos de carácter personal.	DESCENTRALIZADO
RESPONSABILIDADES Y AUTORIZACIONES	Identificación de: Personal con acceso al CPD. Responsable de Seguridad. Administradores del Sistema	DESCENTRALIZADO
SISTEMAS DE INFORMACIÓN	Catálogo de Aplicaciones disponibles en el Grupo Capio. Estructura Lógica de Datos de cada aplicación.	CENTRALIZADO
DOCUMENTOS COMPARTIDOS	Documentos cuyo contenido es de interés general: Documentos de Seguridad. Informes Periódicos. Protocolos de carácter local. Información cuyo conocimiento es básico a todo el personal con acceso a Sistemas de Información.	DESCENTRALIZADO
PROTOCOLOS Y PROCEDIMIENTOS	Protocolos y Procedimientos de aplicación corporativa.	CENTRALIZADO
INFORMES	Informes de revisiones Periódicas.	CENTRALIZADO DESCENTRALIZADO

ANEXO 9.F - CONTROLES PERIÓDICOS

Semestralmente, el Responsable del Fichero o aquél que éste determine, en base a la información que le proporcionen los Responsables de Seguridad y/o personas afectadas al respecto, emitirá un Informe de Revisión con el siguiente contenido.

Además, durante procesos de Auditorias de revisión de cumplimiento, se emitirá un informe con las debilidades detectadas durante el proceso de pre-auditoria. Acabado el proceso de auditoría se emitirá un segundo informe y se cotejarán las debilidades originales.

Las conclusiones detectadas servirán para adoptar medidas correctoras a aplicar. Estos Informes quedarán a disposición de todos los Responsables de Seguridad en el Portal.

1. **Control de la aplicación del Documento de Seguridad**
   - Existencia del documento de seguridad en poder de los responsables de su aplicación.
   - Existencia del documento de seguridad en poder de los usuarios del sistema.
   - Nivel de conocimiento.
   - Nivel de sensibilización.
   - Nivel de aceptación.
   - Nivel de cumplimiento.
   - Ampliación del ámbito del documento de acuerdo con la evolución del HOSPITAL.
   - Ampliación de los recursos protegidos de acuerdo con la evolución del HOSPITAL.
   - Actualización de la estructura de los Ficheros e inclusión de los nuevos ficheros.
   - Detección de irregularidades.
   - Medidas correctoras y disciplinarias.

2. **Control del sistema de identificación y autenticación**
   - Existencia de la lista de usuarios autorizados
   - Nivel de actualización de la lista de usuarios autorizados
   - Nivel de actualización de los privilegios concedidos
   - Correcto funcionamiento del sistema de identificación y autenticación
   - Cambio periódico de contraseñas
   - Almacenamiento cifrado de las contraseñas

3. **Control del sistema de control de acceso**
   - Correcto funcionamiento de los sistemas de control de acceso
   - Pruebas de intrusión
   - Comprobación del contenido de los log
   - Configuración apropiada de los log
   - Almacenamiento seguro de los log
   - Fiabilidad de los controles de acceso físico
   - Respeto de las limitaciones de acceso en función del puesto de trabajo o cargo del usuario
   - Revisar la seguridad de las telecomunicaciones

4. **Control del cumplimiento de las normas de confidencialidad y secreto**
   - Definir el nivel de confidencialidad de cada documento
   - Control de los canales de distribución de documentos
   - Nivel de sensibilización
   - Detección de irregularidades

- Medidas correctoras y disciplinarias
- Comprobación de las normas de cifrado de la información interna y en telecomunicaciones

5. **Control del cumplimiento de las normas internas y las funciones del personal**
   - Existencia de copias de las normas en poder de los responsables de su aplicación
   - Existencia de copias firmadas por los usuarios del sistema
   - Nivel de conocimiento
   - Nivel de sensibilización
   - Nivel de aceptación
   - Nivel de cumplimiento
   - Detección de irregularidades
   - Medidas correctoras y disciplinarias
   - Control de contenidos
   - Monitorización aleatoria del correo electrónico
   - Monitorización aleatoria de los accesos a Internet

6. **Control de los procedimientos de gestión de soportes**
   - Identificación de los soportes
   - Inventario de soportes
   - Almacenamiento seguro de soportes
   - Cumplimiento del procedimiento de autorización de la salida de soportes
   - Medidas a adoptar cuando un soporte vaya a ser desechado o reutilizado
   - Funcionamiento de los registros de entrada y salida
   - Aplicación de medidas a los soportes que salgan de la zona protegida

7. **Control antivirus**
   - Actualización periódica de los programas antivirus
   - Revisión de la automatización del control antivirus
   - Cumplimiento de las obligaciones relativas al control antivirus

8. **Control del cumplimiento de las normas de propiedad intelectual**
   - Revisión de cada terminal mediante programas de auditoría de red o de puesto de trabajo
   - Inventario de licencias de uso
   - Lista de programas homologados
   - Correlación entre las licencias existentes y los programas instalados
   - Control de contenidos y bases de datos
   - Medidas correctoras y disciplinarias

9. **Control del procedimiento de copias de respaldo**
   - Nivel de cumplimiento de las obligaciones relativas a la realización de copias de respaldo
   - Nivel de cumplimiento de la periodicidad establecida
   - Nivel de cumplimiento de las obligaciones relativas al almacenamiento de las copias
   - Nivel de cumplimiento de las obligaciones relativas a las tareas de recuperación

10. **Control del procedimiento de incidencias**
    - Nivel de cumplimiento de la obligación de notificar las incidencias producidas
    - Nivel de cumplimiento de la obligación de dar respuesta a las incidencias producidas
    - Nivel de cumplimiento de la obligación de registrar las incidencias producidas.

ANEXO 9.G - COMUNICACIÓN INTERNA: DEBER DE SECRETO Y CONFIDENCIALIDAD

Los Profesionales (ya sea en virtud de relación laboral, ya sea en virtud de relación mercantil) que en el desempeño de sus funciones profesionales, accedan, usen y/o traten datos personales registrados en cualquiera de los ficheros titularidad del HOSPITAL, quedan obligados al cumplimiento de las siguientes obligaciones:

1. El Profesional sólo tratará y utilizará aquellos datos personales que sean necesarios para el desarrollo de las funciones propias del puesto que ocupa dentro de la estructura del HOSPITAL.

2. El Profesional queda obligado a seguir las instrucciones fijadas por el HOSPITAL, en todo lo que respecta al tratamiento de los datos personales, no pudiendo utilizar y/o tratar los datos para fines distintos de los expresamente indicados.

3. El Profesional queda obligado al cumplimiento del deber de secreto respecto de los datos de carácter personal a los que tenga o haya tenido acceso durante o como consecuencia del desempeño de las funciones profesionales en el HOSPITAL, teniendo dicho deber de secreto una duración indefinida, una vez extinguido el contrato que une al Profesional con el HOSPITAL.

4. El Profesional queda obligado a tratar dichos datos confidencialmente, quedando expresamente prohibida cualquier tipo de comunicación, cesión, transferencia, almacenamiento, envío o entrega, no autorizadas expresamente, de cualesquiera datos personales a los que tenga o haya tenido acceso en el desempeño de sus funciones profesionales, tanto en formato físico como en formato electrónico. Tampoco podrá grabar datos personales en disquetes u otros soportes magnéticos, ni su impresión así como su extracción fuera de las dependencias físicas donde desarrolle sus funciones profesionales.

El incumplimiento, por parte del Profesional, de cualesquiera de los términos, condiciones y obligaciones de la presente Cláusula determinará la responsabilidad de aquel frente a todas las demandas, acciones y/o reclamaciones que contra el HOSPITAL puedan dirigirse o ejercitarse."

ANEXO 9.H - NORMATIVA INTERNA PARA LOS PROFESIONALES ASISTENCIALES Y PERSONAL DE ADMINISTRACIÓN Y DE GESTIÓN DEL HOSPITAL CON RELACIÓN AL CORREO ELECTRÓNICO, INTERNET Y OTROS RECURSOS INFORMÁTICOS

El uso de aplicaciones informáticas, correo electrónico, Internet y otros recursos tanto software como hardware (en adelante, los recursos informáticos), facilitados por el Grupo CAPIO para el desarrollo de las funciones propias de sus profesionales asistenciales así como del personal de administración y de gestión, requerirá la observancia de las siguientes normas de obligado cumplimiento:

- Los recursos informáticos no podrán ser utilizados de forma contraria a los términos contemplados en el Plan de Seguridad y de Protección de Datos del Grupo CAPIO, y en general a la legislación vigente.

- El uso de los recursos informáticos queda limitado a fines estrictamente profesionales y relacionados con las funciones propias desarrolladas tanto por los profesionales asistenciales como por el personal de administración y de gestión del Grupo CAPIO.

- Todo usuario deberá utilizar los recursos informáticos de forma diligente, sin incurrir en actividades que puedan ser consideradas ilícitas o ilegales, que infrinjan los derechos de terceros o que puedan atentar contra la moral o las normas de buen uso de las redes telemáticas.

- Quedan prohibidas las siguientes conductas:

    - Proporcionar a otras personas la clave de acceso (contraseña) a los diferentes recursos informáticos (aplicaciones, acceso a Internet, correo electrónico, etc.). Dejar la clave de forma visible en lugares o documentos en los que pueda ser vista por otras personas.

    - Hacer uso de claves de terceros, independientemente del método utilizado para su obtención.

    - La utilización para fines o usos privados de los recursos informáticos.

    - Obstaculizar voluntariamente el acceso de otros usuarios al Sistema Informático del Grupo CAPIO mediante el consumo masivo de los recursos informáticos, así como realizar acciones que dañen, interrumpan o generen errores en dicho Sistema.

    - Introducir voluntariamente programas, virus, macros, applets o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración en el Sistema Informático del Grupo CAPIO.

    - Descargar de Internet, reproducir, utilizar, ceder, transformar, comunicar públicamente o distribuir documentos o programas informáticos no autorizados expresamente o cualquier otro tipo de obra o material cuyos derechos de propiedad intelectual o industrial pertenezcan a terceros, cuando no se disponga de autorización para ello.

- Instalar copias ilegales de cualquier programa, incluidos los estandarizados.
- Borrar cualquiera de los programas instalados en los servidores para la gestión de la actividad asistencial y no asistencial.
- Utilizar los recursos informáticos, titularidad del Grupo CAPIO, puestos a su disposición, incluida la red Internet, para actividades que no se hallen directamente relacionadas con el puesto de trabajo del usuario.

- Se considera correo electrónico tanto el interno (circulando entre terminales de la red corporativa del Grupo CAPIO), como el externo (dirigido o proveniente de otras redes públicas o privadas, en especial, Internet). Los mensajes de correo electrónico no serán cifrados.
- El Hospital se reserva el derecho de poder revisar los mensajes de correo electrónico y monitorizar cualquier sesión de acceso a Internet con el fin de comprobar el cumplimiento de las normas recogidas en el presente documento, así como el cumplimiento y respeto de las normas del Plan de Seguridad y Protección de Datos, y prevenir actividades que puedan suponer una infracción de las mismas. A tal efecto, los usuarios quedan informados y consienten expresamente que los mensajes de correo electrónico enviados o recibidos puedan ser objeto de monitorización y revisión.
- Todo fichero introducido en la red corporativa o en el terminal del usuario a través de mensajes de correo electrónico que provengan de redes externas deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual e industrial y a control de virus.
- Queda prohibido el acceso a debates en tiempo real, siempre que no sean de temática relacionada con el desempeño de las funciones de los profesionales. (Chat / IRC).
- El acceso a páginas web, grupos de noticias (*newsgroups*) y otras fuentes de información queda limitado a aquellas que contengan información relacionada con la actividad profesional del personal asistencial y no asistencial del Grupo CAPIO y/o con los cometidos del puesto de trabajo del usuario.

10. ORGANIZACIÓN DE LA FUNCIÓN TIC

Se considera de alta criticidad la organización de la función TI, ya que va a gestionar infraestructuras y recursos básicos en un entorno de servicio crítico.

Los recursos asignados a la función TI darán cobertura a los siguientes sistemas y servicios:

- Gestión, administración y operación de la infraestructura tecnológica instalada (equipamiento hardware, de comunicaciones, software de base, puestos de usuario y equipamiento complementario).
- Parametrización, gestión, administración y operación del conjunto de aplicaciones que integran los sistemas de información.
- Implantación, formación a usuarios y puesta en marcha de aplicaciones nuevas o actualizaciones de las existentes.
- Desarrollo de aplicaciones y subsistemas para la gestión interna del Hospital.
- Gestión del mantenimiento correctivo y evolutivo de los sistemas de información.
- Soporte a usuarios para la resolución de las incidencias y para la gestión de la demanda.
- Soporte a usuarios de Atención Primaria en la utilización de sistemas propios del Hospital.
- Explotación de bases de datos y realización de informes a demanda.
- Soporte a la Dirección del Hospital en todo lo referido a las TIC.

EQUIPO DE TRABAJO TIC

Los recursos TIC tendrán diferentes niveles de implicación y formas de vinculación contractual con el Hospital. Los recursos con los que contará el Hospital serán los siguientes:

- Plantilla del Área de Sistemas y TIC del Hospital. Tendrá la siguiente estructura:

  1 Director Sistemas y TIC. Responsable del área, integrado en el equipo directivo del Hospital e interlocutor con la CSCM, Capio y Terceros. Experiencia en entornos hospitalarios.

  1 Administrador de Sistemas y comunicaciones. Responsable de gestionar y administrar los sistemas base y las comunicaciones internas y externas del Hospital. Coordinación y supervisión de proveedores de servicios. 5 años experiencia.

  1 Analista-Programador. Desarrollo de aplicaciones e informes. Explotación de información a demanda. 5 años experiencia.

2 Técnicos de Soporte. Primer nivel de soporte a usuarios en hardware, software, utilidades y aplicaciones. 3 años experiencia.

La distribución de turnos permitirá tener presencia física en el Hospital en horario de 8 a 21 h. Noches, fines de semana y festivos se cubrirán mediante localización de los miembros del equipo, que dispondrán de acceso remoto a los sistemas del Hospital y garantizarán presencia física en caso de necesidad en un plazo inferior a 4 h.

- Otros recursos:

  Sistemas y TIC de Servicios Centrales Capio.

  Capio dispone de un equipo técnico formado por técnicos de los servicios centrales y de otros Hospitales en la Comunidad. Los sistemas de Capio son comunes en todos sus Hospitales y algunos de ellos desarrollados internamente. Servicios de desarrollo, administración de sistemas, gestión de BD, explotación de información y otros son proporcionados directamente por la organización, lo que potencia la capacidad de respuesta y el nivel de soporte a las TIC del Hospital de Collado-Villalba.

  Proveedores de servicios y aplicaciones

  Se contratará la provisión de los siguientes servicios: Mantenimiento preventivo y correctivo hardware, electrónica de red y comunicaciones y soporte (ver sección Mantenimiento).

  La contratación de servicios de mantenimiento con terceros se hará en la modalidad de 24x7x365 para todos los elementos e infraestructuras considerados como críticos, tales como servidores y sistemas de almacenamiento, core de la red local, HIS hospitalario, etc.

  El área de Sistemas y TIC del Hospital de Collado-Villalba coordinará la relación con terceros y el seguimiento de las tareas asignadas a cada uno de ellos.

SEGUIMIENTO DE LOS TRABAJOS

El seguimiento de los trabajos y todos los aspectos relacionados con el Proyecto en sus diferentes fases se hará a través del Responsable de Informática del Hospital, que actuará como Responsable de Proyecto.

En su relación y contactos con la CSCM, estará permanentemente coordinado con los servicios centrales de Capio, que canalizan la coordinación y colaboración con la CSCM en los proyectos y sistemas que afectan al resto de Hospitales en la Comunidad de Madrid (Fundación Jiménez Díaz, Hospital Infanta Elena y Hospital Rey Juan Carlos).

FORMACIÓN

Los recursos en plantilla asignados a Informática dispondrán de La cualificación profesional y nivel académico necesario para garantizar la correcta gestión, administración, uso y explotación de los sistemas de información y del equipamiento tecnológico.

Director Sistemas y TIC	Ingeniero Informático o similar
Administrador de Sistemas y comunicaciones	Ingeniero técnico informático o superior
Analista-Programador	Ingeniero técnico informático o superior
Técnicos de Soporte	FP2 Informática o superior

Los recursos TI del Hospital de Collado-Villalba tendrán acceso a los planes anuales de formación técnica en Capio, a los ofertados por la CSCM y a formación continuada específica relacionada con la práctica diaria y los sistemas de información sanitarios.

11. PLAN DE DESPLIEGUE DE LOS SISTEMAS DE INFORMACIÓN

PLAN DE IMPLANTACIÓN

Todos los aspectos relacionados con la apertura e implantación y despliegue de los sistemas de información en el Hospital de Collado-Villalba serán coordinados por el Comité de Implantación, que estará constituido desde el inicio del proyecto y estará formado por los siguientes miembros:

- Dirección del Hospital (Gerencia, Direcciones Médica, Enfermería, Económica, …).
- Director Sistemas Hospital de Collado-Villalba
- Representante Dirección Sistemas Información Capio.

Entre sus funciones estarán las siguientes:

- Elaboración del Plan de Implantación y cronograma de trabajo.
- Elaboración del Plan de Contingencias para la implantación.
- Realizar el seguimiento del Proyecto y establecer los mecanismos de control para la validación de cada una de las fases y actividades.
- Facilitar los recursos necesarios para el correcto desarrollo de todas las fases del proyecto.
- Establecimiento de los circuitos de coordinación con los SSCC

Del Comité de Implantación dependerán diferentes grupos de trabajo, que reportarán a través del Director de Sistemas del Hospital:

- Equipo Técnico. Participará en las tareas de definición y diseño, instalación, configuración y pruebas de todas las infraestructuras y equipamiento TIC.

- Equipo Funcional. Coordinará todos los aspectos relacionados con las aplicaciones y sistemas de información, parametrizaciones, integraciones, y formación de usuarios. Garantizará la adaptación de los sistemas a los procesos hospitalarios que se implanten.

En ambos grupos de trabajo se incorporará la figura del Comisionado de la CSCM, representante de la Consejería de Sanidad, que supervisará y colaborará en el desarrollo del proceso de implantación., así como los responsables de proyecto de cada una de las empresas suministradoras de aplicaciones y sistemas de información en general.

Las tareas relacionadas con el despliegue se engloban en cada una de estas áreas:

- Comienzo del proyecto. Conformación del comité de implantación.

- Infraestructuras de Locales. CPD.

- Comunicaciones: Dotación, configuración y pruebas de todos los componentes para la provisión de la red de comunicaciones LAN, para su conexión con la Red Sanitaria de la CSCM y de la

electrónica de LAN del CPD del Hospital y para los armarios de distribución situados en las plantas/departamentos del Hospital.

- Instalación: Dotación, instalación y configuración de la infraestructura hardware, software de base y software de aplicaciones.
- Parametrización de los sistemas de información; carga inicial de los datos de partida.
- Pruebas de sistemas e integración: preparación del entorno de pruebas; validación del sistema (ejecución de las pruebas).
- Puesta en Marcha y Pase a Producción.
- Soporte a la Puesta en Marcha: Despliegue del soporte para los primeros días de funcionamiento del sistema; mecanismos y procedimientos especiales para la gestión de incidencias.
- Seguimiento: Fase continua para la verificación del progreso de las actividades y del cumplimiento de los hitos; seguimiento de los acuerdos de niveles de servicio; revisión del plan de contingencia y de seguridad. Establecimiento de medidas correctoras

Al final de este capítulo se incluye cronograma de proyecto con las diferentes fases y actividades a realizar para la implantación de los sistemas, comunicaciones y tecnologías de la Información en el Hospital.

El cronograma estará condicionado por las fechas de adjudicación, comienzo y finalización de obras, y está diseñado de forma que comiencen las actividades con una antelación de 12 meses a la fecha prevista para su apertura.

Se considera asimismo que la puesta en producción del conjunto de las áreas hospitalarias se realizará de forma gradual, en un período de 2 meses, adaptando la formación y soporte a la puesta en marcha a esta ventana temporal.

PLAN DE FORMACIÓN INICIAL

El Hospital contará con Aulas de Informática que estarán operativas desde al menos un mes antes de la apertura, donde se realizarán todas las acciones formativas e informativas a los diferentes colectivos del Hospital. Las aulas estarán dotadas además de ordenadores e impresoras de medios audiovisuales (Proyector, TV, …) para garantizar la mejor calidad de las acciones formativas.

La formación a realizar cubrirá las siguientes áreas:

- Técnica: destinada al equipo técnico de apoyo a la implantación y miembros del área de Sistemas y TIC del Hospital de Collado-Villalba. La formación irá enfocada al conocimiento técnico de las infraestructuras y equipamiento instalados en el Hospital, tanto a nivel de hardware como de software débase y de aplicación. Este personal recibirá también formación

de carácter funcional, para una mejor comprensión de la actividad desarrollada en el Hospital y los circuitos seguidos en cada una de sus áreas.

- Funcional: formación a todos los usuarios del Hospital en el uso, gestión y explotación de información en las aplicaciones a utilizar en sus respectivas áreas de trabajo y niveles de acceso a los sistemas y a la información.

El Comité de Implantación, a través del equipo de trabajo Funcional, realizará el Plan de Formación detallado, y será responsable de la gestión, logística, planificación y coordinación de su ejecución.

Durante el mes previo a la fecha de apertura del Hospital, y al menos durante el proceso de apertura de todas las áreas del mismo más un mes existirá disponibilidad permanente del equipo de formadores para la realización de acciones formativas, tanto colectivas como a nivel individual, en turnos de mañana y tarde, con el objeto de garantizar el acceso a las mismas a todos los profesionales y realizar tantas sesiones como sean necesarias para la formación final de todos los colectivos.

Con carácter general, se trasladará a todos los usuarios, a través de las acciones formativas o en sesiones específicas, de información sobre el Hospital de Collado-Villalba, mapa de aplicaciones e integraciones que conforman el sistema de información hospitalario e integraciones con la CSCM.

Desde la puesta en producción e cada una de las áreas se activará el soporte post-arranque, que tendrá una dotación de recursos humanos superior a la habitual, con objeto de convertir el soporte en acciones formativas in-situ para pequeños grupos de usuarios en los aspectos de las aplicaciones no suficientemente asumidos durante la formación.

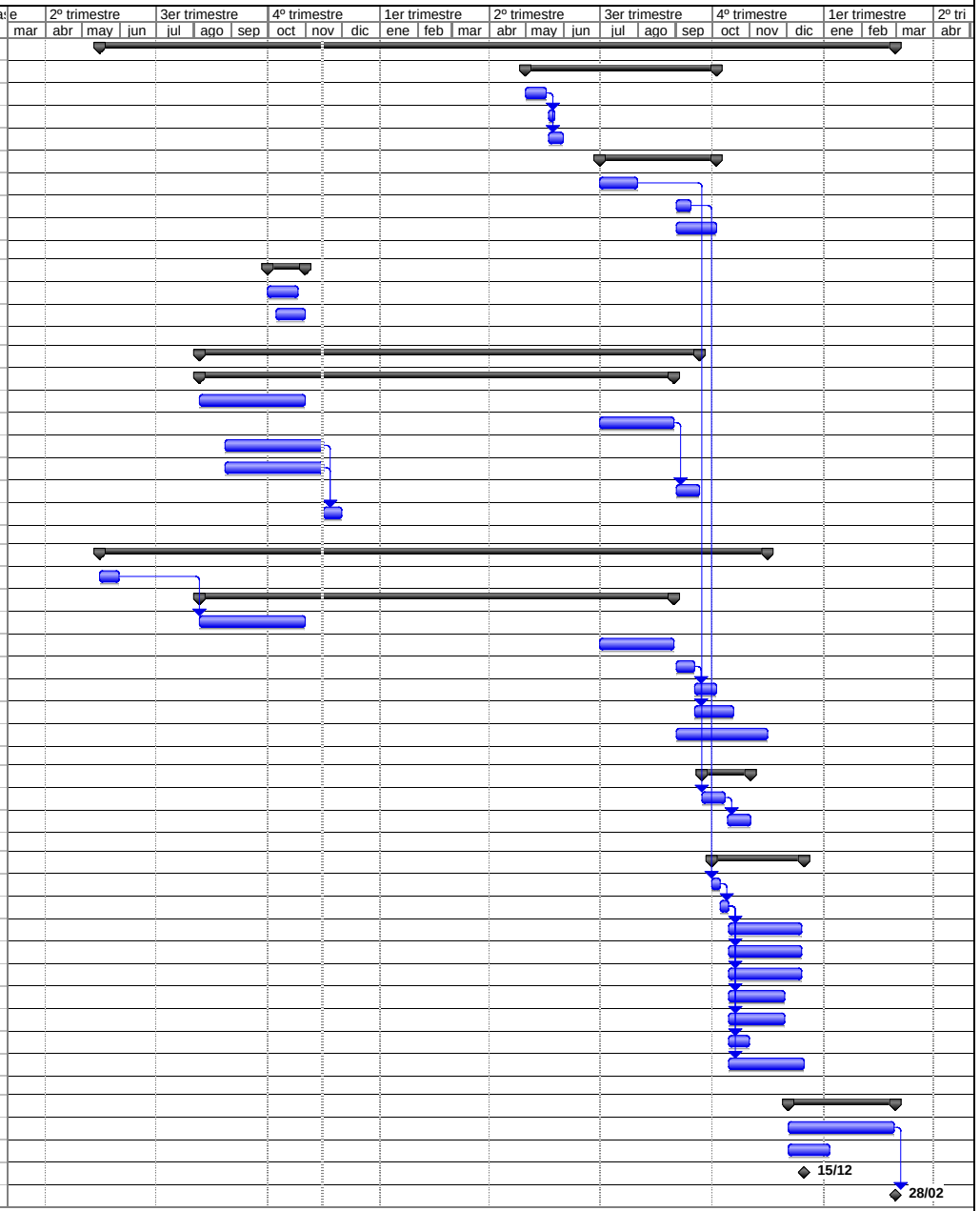
El plan de formación final especificará, para cada colectivo de personas a formar, el número de sesiones estimadas, la duración de las sesiones y el cronograma específico de formación.

PLAN DE CONTINGENCIA

El Comité de Implantación elaborará un Plan de Contingencia, identificando los puntos de riesgo (técnicos y operativos) que puedan convertirse en puntos críticos para el cumplimiento del plan de implantación. Dicho plan de contingencia especificará para cada riesgo las medidas correctoras y de contingencia a aplicar, y se mantendrá actualizado a lo largo de todo el proceso de implantación.

HOSPITAL DE COLLADO VILLALBA
CRONOGRAMA DESPLIEGUE SISTEMAS DE INFORMACIÓN

Id	Nombre de tarea	Comienzo	Fin	Predecesoras
1	**INICIO PROYECTO**	**mié 16/05/12**	**vie 28/02/14**	
2	**ORGANIZACIÓN Y DOCUMENTACIÓN**	**mié 01/05/13**	**vie 04/10/13**	
3	CONSTITUCIÓN COMITÉ IMPLANTACIÓN	mié 01/05/13	vie 17/05/13	
4	CONSTITUCIÓN GRUPOS DE APOYO A LA IMPLANTACIÓN	lun 20/05/13	vie 24/05/13	3
5	PLAN DE IMPLANTACIÓN Y MODELO ORGANIZATIVO	lun 20/05/13	vie 31/05/13	3
6	**DEFINICIÓN PROCEDIMIENTOS Y PLANES**	**lun 01/07/13**	**vie 04/10/13**	
7	ELABORACIÓN DEL PLAN DE PRUEBAS	lun 01/07/13	mié 31/07/13	
8	ELABORACIÓN DEL PLAN DE FORMACIÓN	lun 02/09/13	vie 13/09/13	
9	ELABORACIÓN DEL PLAN DE CONTINGENCIA	lun 02/09/13	vie 04/10/13	
10				
11	**INFRAESTRUCTURAS DE LOCALES**	**lun 01/10/12**	**mié 31/10/12**	
12	ENTREGA CPD Y LOCALES TECNICOS (CAS)	lun 01/10/12	jue 25/10/12	
13	PRUEBAS Y VALIDACIÓN CPD Y LOCALES TÉCNICOS	lun 08/10/12	mié 31/10/12	
14				
15	**COMUNICACIONES**	**lun 06/08/12**	**vie 20/09/13**	
16	**ELECTRÓNICA COMUNICACIONES (VOZ, DATOS, WIFI) Y RFP**	**lun 06/08/12**	**vie 30/08/13**	
17	FASE I	lun 06/08/12	mié 31/10/12	
18	FASE II	lun 01/07/13	vie 30/08/13	
19	CONEXIÓN A RED SANITARIA CSCM	lun 27/08/12	jue 15/11/12	
20	CONEXIÓN A RED CORPORATIVA CAPIO SANIDAD	lun 27/08/12	jue 15/11/12	
21	PRUEBAS Y VALIDACIÓN LAN Y WIFI	lun 02/09/13	vie 20/09/13	18
22	PRUEBAS Y VALIDACIÓN COMUNICACIONES	vie 16/11/12	vie 30/11/12	19;20
23				
24	**HARDWARE Y SOFTWARE**	**mié 16/05/12**	**vie 15/11/13**	
25	DEFINICIÓN ARQUITECTURA A IMPLANTAR Y RFP	mié 16/05/12	jue 31/05/12	
26	**ADQUISICIÓN E INSTALACIÓN SERVIDORES Y ALMACENAMIENTO**	**lun 06/08/12**	**vie 30/08/13**	
27	FASE I	lun 06/08/12	mié 31/10/12	25
28	FASE II	lun 01/07/13	vie 30/08/13	
29	CONFIGURACIÓN Y PARAMETRIZACIÓN HARDWARE Y SOFTWARE DE BASE	lun 02/09/13	lun 16/09/13	
30	INSTALACIÓN Y PARAMETRIZACIÓN SOFTWARE DE APLICACIÓN	mar 17/09/13	vie 04/10/13	29
31	PARAMETRIZACIÓN DE INTEGRACIONES	mar 17/09/13	vie 18/10/13	29
32	ADQUISICIÓN E INSTALACIÓN PUESTOS DE TRABAJO	lun 02/09/13	vie 15/11/13	
33				
34	**PLAN DE PRUEBAS**	**lun 23/09/13**	**vie 01/11/13**	
35	PRUEBAS DE INTEGRACIÓN CON CSCM	lun 23/09/13	vie 11/10/13	7
36	PRUEBAS DE SISTEMA. SOFTWARE DE APLICACIONES E INTEGRACIONES	lun 14/10/13	vie 01/11/13	35
37				
38	**PLAN DE FORMACIÓN INCIAL**	**mar 01/10/13**	**dom 15/12/13**	
39	DOTACIÓN AULAS DE INFORMÁTICA	mar 01/10/13	lun 07/10/13	8
40	FORMACIÓN TÉCNICA Y FUNCIONAL A EQUIPOS DE PROYECTO TIC	mar 08/10/13	lun 14/10/13	39
41	FORMACIÓN FACULTATIVOS (H, U, Q, C, P, …)	mar 15/10/13	vie 13/12/13	40
42	FORMACIÓN ENFERMERÍA (H, U, Q, C, P, …)	mar 15/10/13	vie 13/12/13	40
43	FORMACIÓN ADMISIONES Y ATENCIÓN AL PACIENTE	mar 15/10/13	vie 13/12/13	40
44	FORMACIÓN DEPARTAMENTALES (LAB, A. PAT, B. SANGRE, UCI, …)	mar 15/10/13	vie 29/11/13	40
45	FORMACIÓN IMAGEN DIGITAL-PACS	mar 15/10/13	vie 29/11/13	40
46	FORMACIÓN GESTIÓN ECONÓMICA Y LOGÍSTICA	mar 15/10/13	jue 31/10/13	40
47	OTRAS ACCIONES FORMATIVAS	mar 15/10/13	dom 15/12/13	40
48				
49	**PUESTA EN PRODUCCIÓN**	**mar 03/12/13**	**vie 28/02/14**	
50	SOPORTE PUESTA EN MACRHA	mar 03/12/13	jue 27/02/14	
51	ACTIVACIÓN SISTEMAS DE INFORMACIÓN	mar 03/12/13	dom 05/01/14	
52	APERTURA HOSPITAL	dom 15/12/13	dom 15/12/13	
53	PASO A SOPORTE ESTÁNDAR	vie 28/02/14	vie 28/02/14	50



12. PRESUPUESTO ECONÓMICO DE INVERSIÓN

ÁREA	CONCEPTO	UNID.	IMPORTE
HARDWARE	SERVIDORES	22	370.000,00 €
	UNIDADES DE ALMACENAMIENTO		60.000,00 €
	PUESTOS DE TRABAJO (PCs, PORTÁTILES)	420	354.250,00 €
	IMPRESORAS	175	40.000,00 €
	ESCÁNERES	3	3.600,00 €
	ESTACIONES DE DIAGNÓSTICO	6	150.000,00 €
	GRABADOR CDs IMAGEN DIGITAL	3	21.000,00 €
	SUBTOTAL		998.850,00 €
COMUNICACIONES	CABLEADO VOZ Y DATOS		750.000,00 €
	COBERTURA WIFI		125.000,00 €
	SISTEMA DE TELEFONÍA IP		175.000,00 €
	ELECTRÓNICA DE COMUNICACIONES		600.000,00 €
	FIREWALL		20.000,00 €
	VIDEOVIGILANCIA		30.000,00 €
	TVs		200.000,00 €
	VIDEOCONFERENCIA		44.000,00 €
	SUBTOTAL		1.944.000,00 €
SOFTWARE	LICENCIAS SOFTWARE DE APLICACIÓN		804.500,00 €
	LICENCIAS SISTEMAS OPERATIVOS		88.400,00 €
	LICENCIAS BASES DE DATOS		44.600,00 €
	LICENCIAS MS OFFICE		20.000,00 €
	LICENCIAS CAL		75.400,00 €
	SUBTOTAL		1.032.900,00 €
SERVICIOS	IMPLANTACIONES		567.000,00 €
	SUBTOTAL		567.000,00 €
OTROS SISTEMAS	AUDIOVISUALES-DOCENCIA		20.000,00 €
	CONTROL DE ACCESOS Y PRESENCIA. TARJETA EMPLEADO		90.000,00 €
	SISTEMA RECEPCIÓN DE PACIENTES		75.000,00 €
	DATACENTER CONTINGENCIA		100.000,00 €
	SUBTOTAL		285.000,00 €
	TOTAL		**4.827.750,00 €**

MODELO DE RELACIÓN
Soporte CAPIO - CESUS

Madrid, octubre de 2010

ÍNDICE

Introducción

El objetivo del presente documento es definir el modelo de coordinación y los procedimientos de soporte que seguirán tanto CESUS (Centro de Soporte a Usuarios de la Consejería de Sanidad de la Comunidad de Madrid) como los centros de atención a usuarios de los hospitales gestionados por CAPIO Sanidad (en adelante SOPORTE CAPIO) con objeto de llevar a cabo la **prestación coordinada del servicio de soporte a los usuarios dependientes de los centros de la Comunidad de Madrid gestionados por la empresa CAPIO Sanidad (Hospitales y Centros de Especialidades)**.

Se entiende por "usuarios dependientes de los centros de la Comunidad de Madrid gestionados por CAPIO", a los siguientes colectivos:

- **Profesionales ubicados en los hospitales y centros de especialidades gestionados por CAPIO**: poseen, como Centro de soporte de referencia para el soporte a incidencias TIC, al SOPORTE CAPIO.

- **Resto de profesionales que interaccionan con los SSII de los hospitales gestionados por CAPIO ya sea de forma directa (Centros de Salud y Centros de Especialides dependientes orgánicamente de centros CAPIO) o indirecta** (Resto de centros que accederán a través de las integraciones de los SSII corporativos): poseen, como Centro de referencia para el soporte a incidencias TIC, a CESUS.

El Modelo de Coordinación propuesto para los Centros de Soporte de la CSCM y los centros CAPIO (CESUS y SOPORTE CAPIO, respectivamente) se fundamenta en los siguientes preceptos:

- **La prestación de servicios por uno y otro Centro de Atención Usuarios (CAU) debe ser transparente al usuario final.**

- **La información relativa a incidencias debe ser única, y la interlocución con el usuario debe proceder de una única fuente.**

Ámbitos de actuación coordinada

A continuación enumeran los Sistemas de Información o servicios que conformarán los ámbitos de actuación conjunta CESUS - SOPORTE CAPIO:

I. **Sistemas de Información corporativos**[1]: CIBELES, RULEQ, Telecita,…

II. **Sistemas de Información de hospitales CAPIO**[2]: HIS (IMDH)…

III. **Servicios básicos corporativos**:

- DNS
- Proxy inverso (Publicación de aplicaciones)
- Servicios de acceso remoto – IPSEC.
- Servicios de acceso remoto – SSL.

IV. Red de comunicaciones sanitaria (WAN)

[1] El número y tipología de aplicaciones corporativas accesibles desde el entorno de los hospitales CAPIO o integradas con los SSII de los hospitales CAPIO es susceptible de sufrir modificaciones a lo largo del tiempo.

[2] En este contexto (soporte coordinado entre CAUs), el número y tipología de SSII de los hospitales CAPIO es susceptible de sufrir modificaciones a lo largo del tiempo

Definición del modelo de coordinación entre los Centros de Soporte

El objetivo de este apartado es ilustrar el modelo de coordinación propuesto para el servicio de soporte a usuarios del entorno de los hospitales CAPIO, que tal y como se ha definido en los apartados anteriores se prestará de forma conjunta por CESUS y SOPORTE CAPIO.

A continuación se representa de forma esquemática la propuesta de escenario de trabajo coordinado entre ambas organizaciones:

RED CORPORATIVA DE LA CSCM

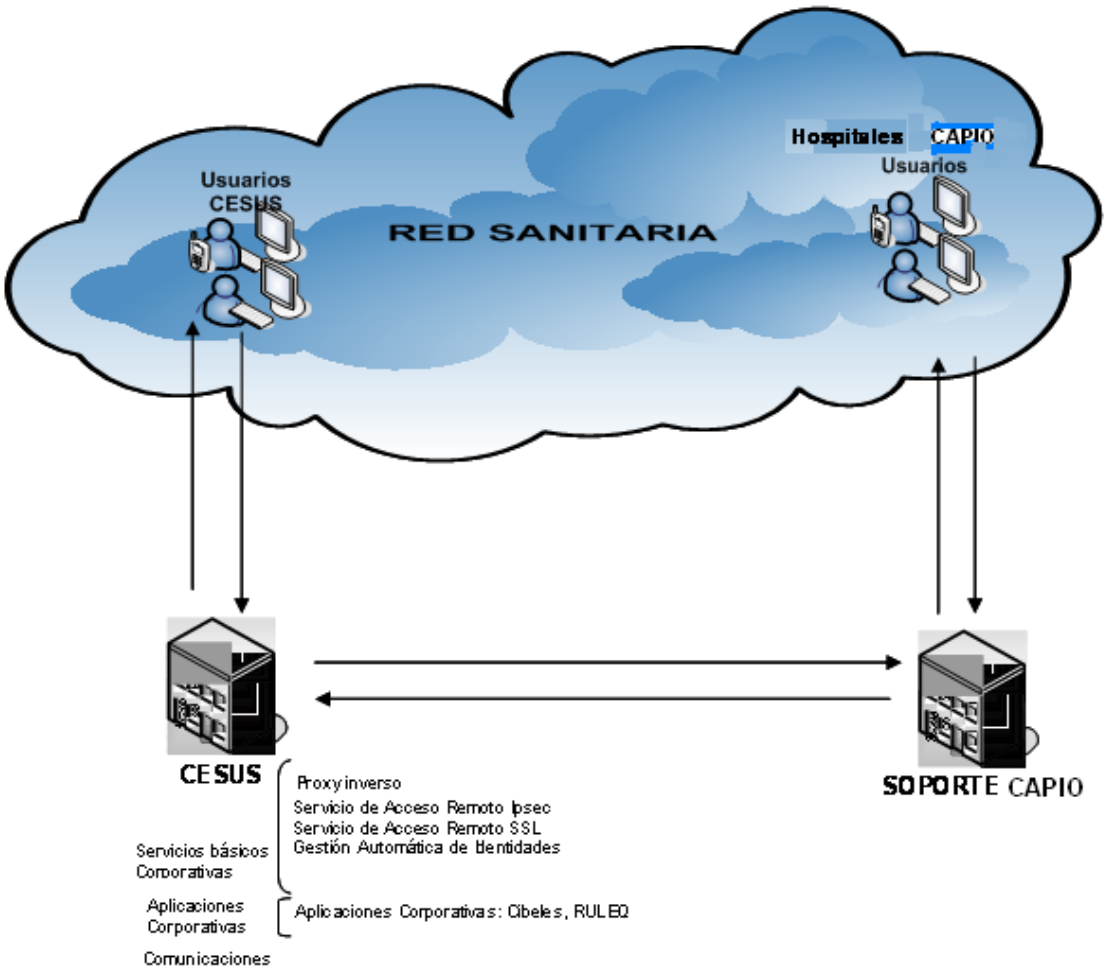


Fig. 1.: Arquitectura y servicios soportados de ámbito común.

Entrando en el detalle de las funciones a realizar por los dos Centros de Soporte, dentro del contexto de coordinación planteado anteriormente, se definen las siguientes líneas de actuación:

- **Gestión de Incidencias**: proceso a seguir en la gestión de los problemas relacionados con las TIC que pudieran afectar a los usuarios del entorno de los centros CAPIO.

- **Gestión de usuarios**: proceso a seguir en la gestión de peticiones de altas, bajas y modificaciones de usuarios dentro del entorno de los centros CAPIO para las aplicaciones, SSII y servicios básicos objeto del alcance del presente documento.

- **Coordinación de modificaciones en los servicios existentes**: procedimientos a seguir para llevar a cabo una modificación en alguno de los servicios prestados a los usuarios del entorno de los centros CAPIO (aplicaciones, SSII y servicios básicos objeto del alcance del presente documento).

Como criterio general, el proceso de soporte seguirá los siguientes pasos:

- Los usuarios contactarán con el soporte de primer nivel de su Centro de Atención al Usuario, que será SOPORTE CAPIO.

- El Centro de Soporte contactado evaluará la información recibida por el usuario, y determinará, a través de un proceso de interacción con el segundo Centro de Soporte (Listado de comprobación o CHKlist), el posible origen del problema.

- Si el problema puede ser resuelto a través de medios propios (resolución in situ o remota), el Centro de Soporte contactado procederá a resolverlo, comunicando al usuario la resolución del mismo al finalizar el proceso.

- En caso negativo, trasladará el problema al segundo Centro de Soporte, tras llevar a cabo las comprobaciones y resoluciones que estén en su mano, y trasladará toda la información que se considere útil para la resolución del problema.

- Una vez resuelta la incidencia, será el Centro de Soporte de referencia del usuario el que comunique el cierre de la misma.

Tomando como punto de partida que, **desde el punto de vista procedimental, las relaciones CESUS – SOPORTE CAPIO y SOPORTE CAPIO – CESUS en los ámbitos de coordinación descritos son simétricas**, en el presente documento sólo se detallarán los procedimientos de relación para la situación -que a priori será más frecuente- en la que un usuario del entorno de los centros CAPIO contacte con su centro de soporte para requerir atención **(Modelo SOPORTE CAPIO → CESUS).**

Bajo este supuesto (Modelo de Coordinación SOPORTE CAPIO → CESUS), las líneas de actuación y entornos de coordinación posibles serían los que se muestran a continuación:

Actuaciones a realizar / Entorno de colaboración	Red de Comunicaciones	Aplicaciones corporativas de la CSCM	Servicios básicos corporativos
Modificación de servicios existentes		X	
Soporte a incidencias	X	X	X
Gestión de usuarios (A/B/M)		X	X

En los próximos apartados se detallan los procedimientos genéricos definidos, dentro del Modelo SOPORTE CAPIO → CESUS, para las distintas líneas de actuación: Coordinación de modificaciones de servicios existentes, Gestión de usuarios y Gestión de Incidencias. **Dichos procedimientos son de aplicación a todos los entornos de coordinación descritos.**

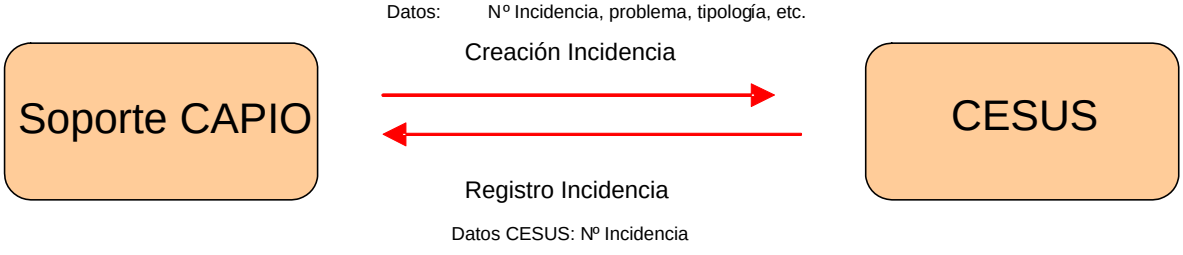
El *Anexo I* recoge, de forma estructurada, las particularidades que entraña, a nivel de procedimientos, la prestación del soporte SOPORTE CAPIO → CESUS en función los entornos de coordinación.

Pese a la simetría procedimental mencionada, la compleción del Modelo de Coordinación requiere la definición, por parte de los responsables del SOPORTE CAPIO, de los métodos concretos de interrelación con CESUS (de forma equivalente a los descritos en el Anexo I). De este modo, y sólo entonces, el Modelo CESUS→ SOPORTE CAPIO quedaría completamente definido.

Gestión de incidencias

1. Creación de una incidencia

Supuesto: SOPORTE CAPIO es el interlocutor (soporte de primer nivel) de los usuarios, transmitiendo a CESUS la incidencia si es necesario. Tal y como se ha comentado anteriormente, el caso contrario (CESUS actúa de soporte de primer nivel) sería equivalente.

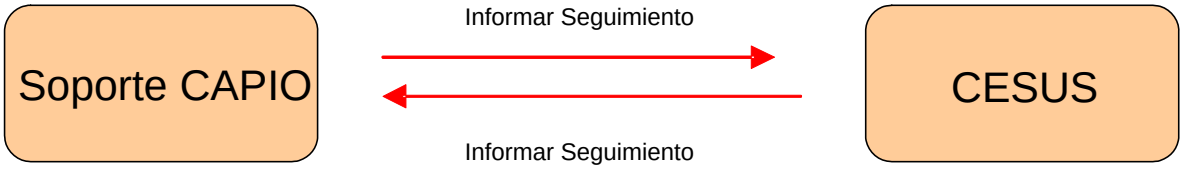


- El SOPORTE CAPIO abrirá una incidencia en su sistema de gestión de incidencias y se la notificará a CESUS cuando determine que la resolución de la misma es competencia de éste último. Esta incidencia deberá ser comunicada con una serie de datos mínimos, imprescindibles para la correcta gestión de la misma (Pendiente de definir: nº incidencia, tipificación, descripción etc.).

- Por su parte, CESUS creará en su sistema de gestión de incidencias (Unicenter ServiceDesk) la incidencia reportada por el SOPORTE CAPIO, indicándole a éste el número de incidencia CESUS.

2. Seguimiento de la incidencia

Supuesto: SOPORTE CAPIO es el interlocutor (soporte de primer nivel) de los usuarios, transmitiendo a CESUS la incidencia si es necesario. El caso contrario (CESUS actúa de soporte de primer nivel) sería equivalente.

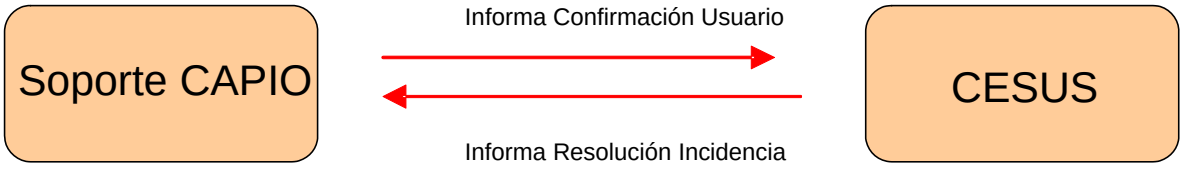


- CESUS realizará seguimientos en las incidencias visibles al usuario con su acceso a la herramienta.

- SOPORTE CAPIO informará a CESUS de actualizaciones en las incidencias reportadas.

3. Cierre de incidencia

Supuesto: SOPORTE CAPIO es el interlocutor (soporte de primer nivel) de los usuarios, transmitiendo a CESUS la incidencia si es necesario. El caso contrario (CESUS actúa de soporte de primer nivel) es equivalente.

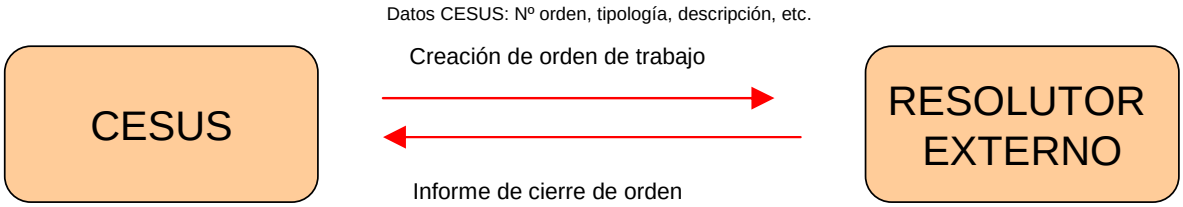


- CESUS notificará la resolución de la incidencia al SOPORTE CAPIO, detallando la solución adoptada, actualizando el estado de la incidencia a “Fijada” a la espera de que el SOPORTE CAPIO le notifique el cierre definitivo de la misma.

- SOPORTE CAPIO validará la solución con el usuario y le notificará el cierre definitivo a CESUS.

4. Dependencia con otros proveedores

Supuesto: CESUS recibe una incidencia del SOPORTE CAPIO y, tras analizarla, detecta la necesidad de asignarla a un proveedor externo. El caso contrario, en el que CESUS actúa de soporte de primer nivel, es equivalente.



- CESUS abrirá una orden de trabajo para el proveedor responsable de la resolución de la incidencia con un conjunto mínimo de datos que aseguren la correcta gestión de las incidencias. Asimismo, CESUS actualizará el estado de la incidencia a "Resolutor externo" a la espera de que el proveedor le notifique el cierre de la orden.

- El proveedor (resolutor externo) registrará la orden de trabajo y, tras adoptar las medidas necesarias para resolver la incidencia, le notificará a CESUS el cierre de la orden.

- Un a vez recibido el cierre de la orden, CESUS procederá a cerrar la orden y posteriormente la incidencia.

Gestión de usuarios.

CESUS será el responsable final de la gestión de peticiones altas/bajas/modificaciones de usuarios de acceso a los sistemas de información y servicios básicos corporativos de la CSCM.

En el modelo simétrico (CESUS-SOPORTE CAPIO), que se omite en este documento por equivalencia al anterior, el centro de soporte CAPIO es el responsable de la gestión de los usuarios de SSII de los hospitales CAPIO.

A continuación se detalla el procedimiento a seguir para la gestión de usuarios:

Supuesto: SOPORTE CAPIO es el interlocutor de los usuarios, transmitiendo a CESUS la incidencia petición recibida relacionada con los SSII o servicios corporativos proporcionados directamente por la CSCM.

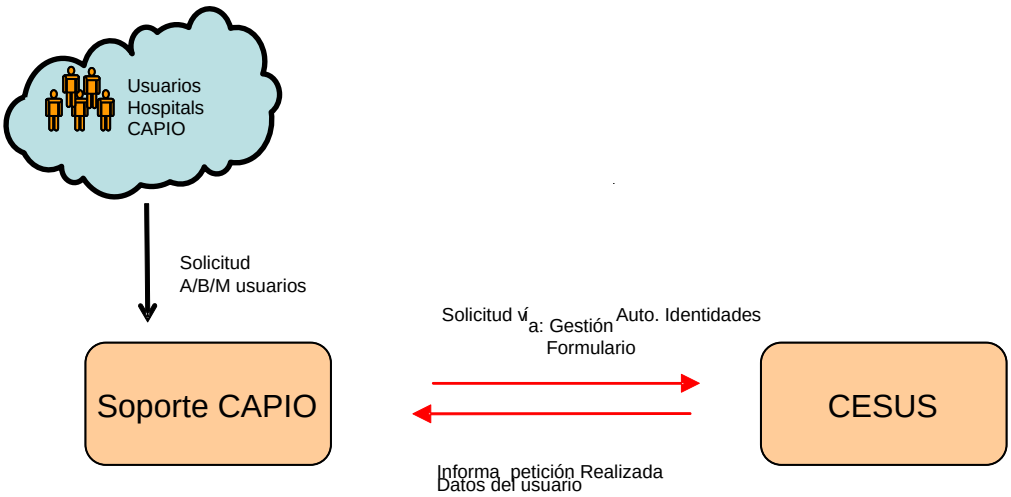
- El usuario contactará con SOPORTE CAPIO para realizar la petición de A/B/M de usuario.
- El SOPORTE CAPIO identificará la petición recibida con una solicitud relacionada con alguno de los servicios básicos corporativos o con una aplicación soportada desde servicios centrales.
- SOPORTE CAPIO gestionará con CESUS la solicitud recibida. Para ello, desde el SOPORTE CAPIO se le solicitarán al usuario los datos necesarios para cumplimentar la petición y posteriormente, se le realizará la petición a CESUS usando una de las dos vías abiertas para tal fin:

    - Aplicación de gestión de identidades

        - https://gestionai.salud.madrid.org/

    - Envío de formularios por correo electrónico

        - cesus@salud.madrid.org



A continuación se detallan las peticiones a realizar directamente desde la aplicación de Gestión Automática de Identidades, y las que se deben realizar -actualmente- por medio del envío de un formulario:

- **Peticiones a realizar desde la aplicación de Gestión Automática de Identidades:**

    i. Directorio activo.
    ii. Carpetas compartidas.
    iii. Sistemas de Información corporativos

- **Peticiones a realizar por formulario[3]:**

i. – IPSEC.	Servicios de acceso remoto
ii. – SSL.	Servicios de acceso remoto

[3] Los formularios actuales -susceptibles de modificación- se incluyen como anexo al final de este documento.

Anexo I: Modelo de coordinación SOPORTE CAPIO → CESUS según entornos de coordinación

(Nota: los métodos de intercambio de información a continuación descritos, sufrirán modificaciones importantes cuando se acometa la integración entre las herramientas de gestión de incidencias de ambos Centros de Soporte -apartado 4 del presente documento-)

Entorno de coordinación	Servicio	Línea de actuación	Tipificación	Formato de recogida de datos	Datos obligatorios	Medio de envío
Servicios básicos corporativos	**DNS**	Gestión de usuarios: Petición A/B/M	Pet.DNS	FORMULARIO DE ALTA EN DNS	Nombre y apellidos NIF Datos de contacto Departamento Centro Descripción de la aplicación URL e IP	**Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org **Fax** : 91 327 40 54 Integración automática entre los sistemas de gestión de incidencias
		Gestión de incidencias	Con.DNS	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org	Nombre y apellidos NIF Datos de contacto Centro/Edificio Aplicación Descripción	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org
			Pro.DNS	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.mad	Nombre y apellidos NIF Datos de contacto Centro/Edificio Aplicación Descripción	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.mad

			rid.org / cesus@salud.madrid.org		rid.org / cesus@salud.madrid.org
Rango de direcciones DHCP	Gestión de usuarios: Petición A/B/M	Pet.DHCP	FORMULARIO DE PETICIÓN DE DIRECCIONAMIENTO IP	Nombre y apellidos NIF Datos de contacto Departamento Centro Direccionamiento IP actual Motivo de la petición Número de IPs a ampliar el rango	**Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org **Fax** : 91 327 40 54 Integración automática entre los sistemas de gestión de incidencias
	Gestión de incidencias	Con.DHCP	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org	Nombre y apellidos NIF Datos de contacto Centro/Edificio Aplicación Descripción	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org
		Pro.DHCP	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org	Nombre y apellidos NIF Datos de contacto Centro/Edificio Aplicación Descripción	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org
DA	Gestión de usuarios: Petición A/B/M	Pet.DA	Gestión Automática de Identidades (https://gestionai.salud.madrid.org)	Nombre y apellidos NIF Datos de contacto Departamento	GestionAI (https://gestionai.salud.madrid.org)

				Puesto usuario y responsable Perfil Datos de la organización Fecha	Integración automática entre los sistemas de gestión de incidencias
	Gestión de incidencias	Con.DA	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org	Nombre y apellidos NIF Datos de contacto Centro/Edificio Aplicación Descripción	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org
		Pro.DA	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org	Nombre y apellidos NIF Datos de contacto Centro/Edificio Aplicación Descripción	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org
Correo electrónico	Gestión de usuarios: Petición A	Pet.STIC.Cor.Alta	Gestión Automática de Identidades. (https://gestionai.salud.madrid.org)	Nombre y apellidos NIF Puesto Departamento Centro Nombre usuario	Gestión Automática de Identidades. (https://gestionai.salud.madrid.org)
	Gestión de usuarios: Petición B	Pet.STIC.Cor.Baja	Gestión Automática de Identidades (https://gestionai.salud.madrid.org)	Nombre y apellidos NIF Puesto Departamento Centro Nombre usuario	Gestión Automática de Identidades (https://gestionai.salud.madrid.org)

		Gestión de usuarios: Petición M	Pet.STIC.Cor.Mod	Gestión Automática de Identidades (https://gestionai.salud.madrid.org)	Nombre y apellidos NIF Puesto Departamento Centro Nombre usuario	Gestión Automática de Identidades (https://gestionai.salud.madrid.org)
		Gestión de incidencias	Con.SW.Corr	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org Gestión Automática de Identidades (https://gestionai.salud.madrid.org)	Nombre y apellidos NIF Datos de contacto Centro/Edificio Aplicación Descripción	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org Gestión Automática de Identidades (https://gestionai.salud.madrid.org)
			Pro.Com.STIC.Cor	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org	Nombre y apellidos NIF Datos de contacto Centro/Edificio Aplicación Descripción	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org
	Carpetas compartidas	Gestión de usuarios: Petición A	Pet.STIC.CarCom.Alta	Gestión Automática de Identidades (https://gestionai.salud.madrid.org)	Nombre y apellidos NIF Puesto Departamento Centro	Gestión Automática de Identidades (https://gestionai.salud.madrid.org)

				Nombre usuario Recurso compartido	
Gestión de usuarios: Petición B	Pet.STIC.CarCom.Baja	Gestión Automática de Identidades (https://gestionai.salud.madrid.org)	Nombre y apellidos NIF Puesto Departamento Centro Nombre usuario Recurso compartido	Gestión Automática de Identidades (https://gestionai.salud.madrid.org)
Gestión de usuarios: Petición M	Pet.STIC.CarCom.Mod	Gestión Automática de Identidades (https://gestionai.salud.madrid.org)	Nombre y apellidos NIF Puesto Departamento Centro Nombre usuario Recurso compartido	Gestión Automática de Identidades (https://gestionai.salud.madrid.org)
Gestión de incidencias	Con.SW.CarCom	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org Gestión Automática de Identidades (https://gestionai.salud.madrid.org)	Nombre y apellidos NIF Datos de contacto Centro/Edificio Recurso compartido Descripción	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org Gestión Automática de Identidades (https://gestionai.salud.madrid.org)
	Pro.Com.STIC.CarCom	WEB (http://incidenciasinf.salud.madrid.org/incidencias/)	Nombre y apellidos NIF Datos de contacto	WEB (http://incidenciasinf.salud.madrid.org/incidencias/)

				Centro/Edificio Recurso compartido Descripción	
Proxy (Navegación por Internet)	Gestión de usuarios: Petición A	Pet.STIC.ProxyInter.Alta	Gestión Automática de Identidades (https://gestionai.salud.madrid.org)	Nombre y apellidos NIF Puesto Departamento Centro Nombre usuario	Gestión Automática de Identidades (https://gestionai.salud.madrid.org)
	Gestión de usuarios: Petición B	Pet.STIC.ProxyInter.Baja	Gestión Automática de Identidades (https://gestionai.salud.madrid.org)	Nombre y apellidos NIF Puesto Departamento Centro Nombre usuario	Gestión Automática de Identidades (https://gestionai.salud.madrid.org)
	Gestión de usuarios: Petición M	Pet.STIC.ProxyInter.Mod	Gestión Automática de Identidades (https://gestionai.salud.madrid.org)	Nombre y apellidos NIF Puesto Departamento Centro Nombre usuario	Gestión Automática de Identidades (https://gestionai.salud.madrid.org)
	Gestión de incidencias	Con.SW	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org	Nombre y apellidos NIF Datos de contacto Centro/Edificio Aplicación Descripción	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org
		Pro.Com.STIC. ProxyInter	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00	Nombre y apellidos NIF Datos de contacto Centro/Edificio Aplicación	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00

				Mail: inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org	Descripción	**Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org
	Proxy inverso	Gestión de usuarios: Petición A proxy inverso	Pet.STIC.ProxyInver.Alta	FORMULARIO DE PETICIÓN DE ACCESO REMOTO	Nombre y apellidos NIF Datos de contacto Empresa/Consejería Motivos del acceso Datos de la conexión Firma solicitante Firma autorizada (Consejería) Fecha	**Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org **Fax** : 91 327 40 54 Integración automática entre los sistemas de gestión de incidencias
		Gestión de usuarios: Petición B proxy inverso	Pet.STIC.ProxyInver.Baja	FORMULARIO DE PETICIÓN DE ACCESO REMOTO	Nombre y apellidos NIF Datos de contacto Empresa/Consejería Motivos del acceso Datos de la conexión Firma solicitante Firma autorizada (Consejería) Fecha	**Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org **Fax** : 91 327 40 54 Integración automática entre los sistemas de gestión de incidencias
		Gestión de usuarios: Petición M proxy inverso	Pet.STIC.ProxyInver.Mod	FORMULARIO DE PETICIÓN DE ACCESO REMOTO	Nombre y apellidos NIF Datos de contacto Empresa/Consejería Motivos del acceso Datos de la conexión Firma solicitante Firma autorizada (Consejería) Fecha	**Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org **Fax** : 91 327 40 54 Integración automática entre los sistemas de gestión de incidencias

		Gestión de incidencias	Con.SW	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org	Nombre y apellidos NIF Datos de contacto Centro/Edificio Aplicación Descripción	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org
			Pro.Com.STIC. ProxyInver	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org	Nombre y apellidos NIF Datos de contacto Centro/Edificio Aplicación Descripción	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org
	Servicios de acceso remoto (IPSEC/SSL)	Gestión de usuarios: Petición A/B/M VPN	Pet.STIC.AccR	FORMULARIO DE PETICIÓN DE ACCESO REMOTO	Nombre y apellidos NIF Datos de contacto Empresa/Consejería Motivos del acceso Datos de la conexión Firma solicitante Firma autorizada (Consejería) Fecha	**Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org **Fax** : 91 327 40 54 Integración automática entre los sistemas de gestión de incidencias
		Gestión de usuarios: Petición A/B/M SSL	Pet.STIC.AccR	FORMULARIO DE PETICIÓN DE ACCESO REMOTO	Nombre y apellidos NIF Datos de contacto Empresa/Consejería Motivos del acceso Datos de la conexión Firma solicitante Firma autorizada (Consejería)	**Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org **Fax** : 91 327 40 54 Integración automática entre los

					Fecha	sistemas de gestión de incidencias
		Gestión de incidencias	Con.SW	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org	Nombre y apellidos NIF Datos de contacto Centro/Edificio Aplicación Descripción	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org
			Pro.Com.STIC. AccR	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org	Nombre y apellidos NIF Datos de contacto Centro/Edificio Aplicación Descripción	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org
ón corporativos	**Aplicaciones: formulario**	Gestión de usuarios: Petición A/B/M usuario	Pet.Apl	FORMULARIO DE PETICIÓN DE ACCESO A APLICACIONES	Nombre y apellidos NIF Datos de contacto Departamento Centro Nombre aplicación Servicio afectado Usuarios autorizados Firma solicitante Firma autorizada (Consejería) Fecha	**Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org **Fax** : 91 327 40 54 Integración automática entre los sistemas de gestión de incidencias

		Gestión de incidencias	Con.Apl	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org	Nombre y apellidos NIF Datos de contacto Centro/Edificio Aplicación Descripción	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org
			Pro.Apl	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org	Nombre y apellidos NIF Datos de contacto Centro/Edificio Aplicación Descripción	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org
	Aplicaciones: gestionai	Gestión de usuarios: Petición A/B/M usuario	Pet.Apl	Gestión Automática de Identidades (https://gestionai.salud.madrid.org)	Nombre y apellidos NIF Datos de contacto Centro (asignación) Cargo usuario y responsable Perfil del usuario Procedencia del usuario Fecha	Gestión Automática de Identidades (https://gestionai.salud.madrid.org)
		Gestión de incidencias	Con.Apl	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org	Nombre y apellidos NIF Datos de contacto Centro/Edificio Aplicación Descripción	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org

			Pro.Apl	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org	Nombre y apellidos NIF Datos de contacto Centro/Edificio Aplicación Descripción	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org
Red de Comunicaciones	**Comunicaciones**	Gestión de incidencias	Con.Apl	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org	Nombre y apellidos NIF Datos de contacto Centro/Edificio Aplicación Descripción	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org
			Pro.Apl	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org	Nombre y apellidos NIF Datos de contacto Centro/Edificio Aplicación Descripción	**Web** (http://incidenciasinf.salud.madrid.org/incidencias/) **Teléfono**: 91 204 35 00 **Mail:** inciprov.cesus@salud.madrid.org / cesus@salud.madrid.org

Anexo II: Formularios de Petición

Formulario de alta en DNS

Nº Orden (A cumplimentar por el administrador):

Datos del solicitante Fecha:

Nombre y Apellidos:

NIF/NIE

Correo electrónico:

Teléfono corporativo:
(Especifique el número completo de teléfono (no sólo la extensión))

Departamento:

Centro:

Descripción de la aplicación/servicio al que se desea dar acceso:

URL (ejemplo www.aplicacion.salud.madrid.org):

IP asociada al servicio:

(*) Todos los campos son obligatorios.

Formulario de petición de Direccionamiento de IP

Nº Orden (A cumplimentar por el administrador):

Datos del solicitante Fecha:

Nombre y Apellidos:

NIF/NIE

Correo electrónico:

Teléfono corporativo:
(Especifique el número completo de teléfono (no sólo la extensión))

Departamento:

Centro:

Direccionamiento IP actual (ejemplo: 10.x.x.x/x):

Motivo de la petición de ampliación de rango de direccionamiento IP:

Número de IPs a ampliar el rango de direccionamiento:

(*) Todos los campos son obligatorios.

Servicio Madrileño de Salud
Dirección General de Sistemas de Información Sanitaria
SaludMadrid

FORMULARIO DE PETICIÓN DE ACCESO REMOTO A RED SANITARIA

Los datos personales recogidos serán incorporados y tratados en el fichero "Gestión de Usuarios", cuya finalidad consiste en: gestionar los usuarios con acceso a los servicios y sistemas de información gestionados por la Dirección General de Sistemas de Información Sanitaria; gestionar y administrar los sistemas y redes de la Consejería; y controlar el acceso a los recursos. Los datos personales recogidos podrán ser cedidos de conformidad a lo previsto en la Ley. El órgano responsable del fichero es la Dirección General de Sistemas de Información Sanitaria de la Consejería de Sanidad de la Comunidad de Madrid, y la dirección donde el interesado podrá ejercer los derechos de acceso, rectificación, cancelación y oposición ante el mismo es: "Calle Aduana, 29, 4a Planta, 28013 Madrid", todo lo cual se informa en cumplimiento del artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Datos personales del solicitante

Nombre (*) _____ Apellido 1 (*) _____ Apellido 2 _____

NIF/ NIE (*) _____ Correo electrónico (*) _____

Teléfono de contacto (*) _____ Móvil de contacto _____ FAX de contacto _____

Procedencia profesional del solicitante

☐ Consejería de Sanidad Dirección General(*) _____

(Ejemplo: D.G de Sistemas de Información Sanitaria, D.G de Hospitales)

Subdirección General / Gerencia (*) _____

(Ejemplo: S.G. de Servicios de Sistemas de Información, Hospital Universitario de Móstoles)

Unidad o servicio del usuario (*) _____

☐ Entidad externa Descripción (**) _____

Dirección (**) _____ Localidad (**) _____

Datos del responsable de la Consejería de Sanidad que autoriza la solicitud

Nombre (*) _____ Apellido 1 (*) _____ Apellido 2 _____

NIF/ NIE (*) _____ Correo electrónico (*) _____

Teléfono de contacto (*) _____ Móvil de contacto _____ FAX de contacto _____

Categoría del responsable de la solicitud (*) _____

Puesto del responsable de la solicitud (*) _____

Dirección General – responsable (*) _____

Subdirección General / Gerencia (*) _____

Unidad o servicio del responsable (*) _____

(*) Los campos marcados deberán rellenarse obligatoriamente.
(**) Los campos marcados deberán rellenarse obligatoriamente, en el caso de que se trate de una empresa externa.

ESTE FORMULARIO DEBE SER ARCHIVADO Y CONSERVADO

(Continua en la siguiente página - 1 de 3)

Servicio Madrileño de Salud
Dirección General de Sistemas de Información Sanitaria
SaludMadrid

FORMULARIO DE PETICIÓN DE ACCESO REMOTO A RED SANITARIA

Datos generales del acceso mediante VPN IPsec usuarios

Fecha inicio: _____ Fecha fin: _____ ☐ Permanente (se deberá renovar cada 12 meses)

Tipo de solicitud: ☑ Alta ☐ Baja ☐ Modificación

NOTA: EL SOLICITANTE SE COMPROMETE A NO ACCEDER A RECURSOS DISTINTOS DE LOS INDICADOS .

Datos técnicos del acceso mediante VPN IPsec usuarios

Servicios (puertos)	SSH	
	SCP	
	HTTPS	
	SFTP	

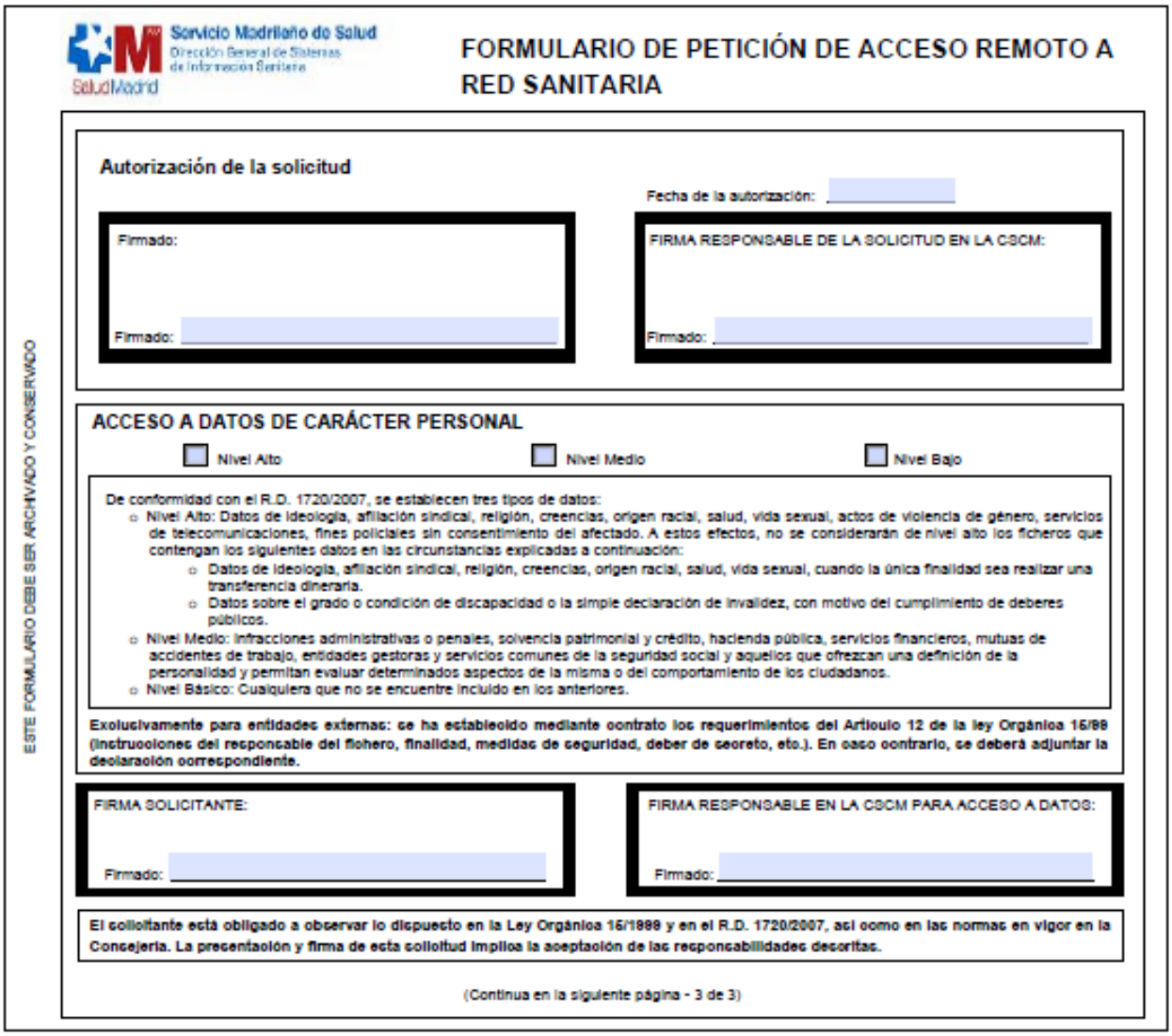
Otros (indicar nombre, puerto, TCP/UDP, IPs destino)

Motivo de la solicitud

Observaciones (En el caso de tratarse de una modificación indicar aquí los campos y justificación de los campos modificados)

ESTE FORMULARIO DEBE SER ARCHIVADO Y CONSERVADO

(Continua en la siguiente página - 2 de 3)



Servicio Madrileño de Salud
Dirección General de Sistemas de Información Sanitaria
SaludMadrid

FORMULARIO DE PETICIÓN DE ACCESO REMOTO A RED SANITARIA

ESTE FORMULARIO DEBE SER ARCHIVADO Y CONSERVADO

Autorización de la solicitud

Fecha de la autorización: _____

Firmado:

Firmado: _____

FIRMA RESPONSABLE DE LA SOLICITUD EN LA CSCM:

Firmado: _____

ACCESO A DATOS DE CARÁCTER PERSONAL

☐ Nivel Alto ☐ Nivel Medio ☐ Nivel Bajo

De conformidad con el R.D. 1720/2007, se establecen tres tipos de datos:

- Nivel Alto: Datos de ideología, afiliación sindical, religión, creencias, origen racial, salud, vida sexual, actos de violencia de género, servicios de telecomunicaciones, fines policiales sin consentimiento del afectado. A estos efectos, no se considerarán de nivel alto los ficheros que contengan los siguientes datos en las circunstancias explicadas a continuación:
  - Datos de ideología, afiliación sindical, religión, creencias, origen racial, salud, vida sexual, cuando la única finalidad sea realizar una transferencia dineraria.
  - Datos sobre el grado o condición de discapacidad o la simple declaración de invalidez, con motivo del cumplimiento de deberes públicos.
- Nivel Medio: Infracciones administrativas o penales, solvencia patrimonial y crédito, hacienda pública, servicios financieros, mutuas de accidentes de trabajo, entidades gestoras y servicios comunes de la seguridad social y aquellos que ofrezcan una definición de la personalidad y permitan evaluar determinados aspectos de la misma o del comportamiento de los ciudadanos.
- Nivel Básico: Cualquiera que no se encuentre incluido en los anteriores.

Exclusivamente para entidades externas: se ha establecido mediante contrato los requerimientos del Artículo 12 de la ley Orgánica 16/99 (instrucciones del responsable del fichero, finalidad, medidas de seguridad, deber de secreto, etc.). En caso contrario, se deberá adjuntar la declaración correspondiente.

FIRMA SOLICITANTE:

Firmado: _____

FIRMA RESPONSABLE EN LA CSCM PARA ACCESO A DATOS:

Firmado: _____

El solicitante está obligado a observar lo dispuesto en la Ley Orgánica 16/1999 y en el R.D. 1720/2007, así como en las normas en vigor en la Consejería. La presentación y firma de esta solicitud implica la aceptación de las responsabilidades descritas.

(Continua en la siguiente página - 3 de 3)

Formulario de Peticiones de Acceso a Aplicaciones

Fecha (obligatorio):

Este formulario debe ser cumplimentado por usuarios en los siguientes casos:

1. El usuario solicita el acceso a una nueva aplicación.
2. El usuario quiere solicitar cambios de permisos sobre aplicaciones existentes que le afecten a él o a un grupo de usuarios que él determine. (Por ejemplo: un jefe de servicio quiere solicitar permisos de acceso a una aplicación existente para un grupo de usuarios).

Datos de la persona de contacto a la que se le dará una confirmación de que el servicio ha sido realizado.
(Datos de cumplimentación obligatoria)

Nombre y Apellidos:

NIF/NIE:

Tlf. Corporativo (completo): Correo electrónico:

Departamento:

Centro:

APLICACIONES

- Nombre de aplicación :

- Dirección General y/o Servicio afectado:

- Especifique el tipo de operación, Nombre y Apellidos (NIF) del usuario y a continuación los permisos olicita.

Tipo: *Autorizo(A), Deniego(D)* **Usuario:** *Nombre y Apellidos (NIF)* **Permisos** : *(Control total (CT), Lectura (L) Escritura (E))*

Para peticiones relacionadas con APLICACIONES son necesarias las firmas del solicitante y el jefe de servicio y remitir el formulario en papel a CESUS, C/ Aduana 29 - MADRID 28013.

Firma del solicitante: *Firma del jefe de servicio:*

(En un plazo breve, se le remitirá por correo una confirmación del servicio realizado incluyendo los datos y cambios efectuados).