Hospital Universitario Rey Juan Carlos

SaludMadrid

Comunidad de Madrid

PLAN DE ACTUACIONES TIC

2015
2018

HOSPITAL UNIVERSITARIO REY JUAN CARLOS

Contenido

1. INTRODUCCIÓN

El Hospital Universitario Rey Juan Carlos (HURJC) de Móstoles, es un centro integrado en la red sanitaria pública, concebido para ofrecer una asistencia universal, cercana y eficaz, a cerca de 180.000 ciudadanos. El Centro está dotado de alta tecnología, ofreciendo una amplia cartera de servicios y con profesionales de prestigio con un alto grado de capacitación en clínica, docencia e investigación.

El Hospital Universitario Rey Juan Carlos, ubicado en la localidad madrileña de Móstoles, inició su actividad asistencial el 22 de Marzo de 2012 con un diseño arquitectónico novedoso (Premio COAM 2012, Premio Mejor Obra Pública Municipal en los Premios Demarcación de Madrid 2014,) que responde a un programa funcional dando especial importancia a la escala humana, el control del soleamiento y la calidad de los espacios destinados a enfermos y familiares.

Los sistemas de información son evaluados periódicamente a través de seguimiento de indicadores, objetivos, auditorías internas y externas y revisión por parte de la Dirección. De dichas evaluaciones surgen las oportunidades de mejora necesarias para abordar el siguiente periodo.

El Hospital Universitario Rey Juan Carlos debe realizar, presentar resultados y desarrollar acciones de mejora, de forma coordinada y siguiendo las directrices del Servicio Madrileño de Salud cumpliendo los objetivos establecidos en el programa marco.

2. PLAN ACTUACIONES

2.1 SITUACION ACTUAL

- ✓ Identificar las actuaciones en marcha y previstas dentro de los planes específicos de actuación del Hospital en materia de las Tecnologías de Información y Comunicaciones, para su alineación con los proyectos estratégicos de la Comunidad de Madrid, como lo son: generalización de la implantación de historia clínica electrónica, factura sanitaria informativa, registros de información (tumores, ictus, infarto, ...), protocolos, trazabilidad oncológica, atención a crónicos, receta electrónica, extensión de la prescripción electrónica en hospitales, carpeta virtual de salud del ciudadano, despliegue del Sistema de Información de Paliativos, Sistema de Compensación Inter-centros, cuadros de mando, indicadores e información de servicios clínicos y quirúrgicos, servicios multicanal a los pacientes, etc.

- ✓ Profundizar en el inventario de activos y contratos existentes en cada uno de los centros, de cara a avanzar en la centralización de las compras en lo que a las infraestructuras y servicios TIC se refiere, en línea con las instrucciones de contratación pública.

- ✓ Identificar sinergias que permitan compartir recursos, reutilizar experiencias y avanzar en la consolidación y centralización de infraestructuras y servicios.

2.2 OBJETIVOS DEL PLAN

Adaptarse a los indicadores propuestos en el contrato programa, dichos puntos han sido definidos por la consejería de sanidad por la OSSI.

Los puntos estratégicos son los siguientes:

- ✓ Cumplimiento plan actuaciones.
- ✓ Realización y pruebas del plan de contingencia.
- ✓ Auditorias de los sistemas y LOPD.
- ✓ Revisión de políticas de Backup y pruebas de restauración.
- ✓ Implementación de mejoras de seguridad.
- ✓ Formación e innovación.
- ✓ Iniciativas de innovación.
- ✓ Reingeniería de procesos.
- ✓ Control y administración de la actividad TIC.
- ✓ Evaluación nivel HIMSS

2.2.1 CUMPLIMIENTO PLAN DE ACTUACIONES

Durante todo el año se realizan los puntos indicados en el plan de actuaciones, todas estas actuaciones se van reflejando a modo de evidencias en la plataforma indicada por la OSSI.

Configurador Cerrado (5.0)

Grupo Indicador
DSI_01: M01 - Política y organización de la seguridad de la información; Nota: 4,333; Valoración: 86,66%

Indicador	Oficina Responsable	Directriz	Realizado	Observaciones	Evidencia	Evidencia Obs	Anexos	
DSI_01.1 Política de Seguridad de la información **Nota: 4,000** (Meta a alcanzar: 5,00) **Cumplimiento: 80%**	OSSI	Respaldada por el responsable de la organización y revisada periódicamente	4	20/07/15. Política de seguridad actualizada en Marzo del 2015. Se modifica la nota de 3 a 4. 17/04/15. El centro ha realizado actualizaciones en la Política de Seguridad. Se solicita evidencia para revisar el nivel de madurez del indicador. (misma Política para todos los centros del grupo)	Sí	Política de seguridad corporativa.	Revisados	400310
DSI_01.2 Aprobada y difundida **Nota: 4,000** (Meta a alcanzar: 5,00) **Cumplimiento: 80%**	OSSI	Difusión periódica de la Política de Seguridad	4	20/07/15. Se anexa evidencia de la publicación de la Política en la intranet y su difusión periódica. Se modifica la nota de 2 a 4. 17/04/15. Se solicita evidencia de la publicación de Política de Seguridad en la intranet así como el acta de aprobación de Política con las ultimas modificaciones.	Sí	La Política de seguridad se ha difundido en la intranet y mediante un comunicado global	Revisados	400284
DSI_01.3 Designar formalmente al responsable/s de seguridad **Nota: 5,000** (Meta a alcanzar: 5,00) **Cumplimiento: 100%**	OSSI	Pertenencia a grupos y/o foros de seguridad.	5	20/07/15. Miembros del Comité pertenecen a grupos de seguridad. Se modifica la nota de 4 a 5. 17/04/15. El responsable de seguridad es representado por el Comité. Se recomienda pertenecer a grupos y/o foros de seguridad para revisar el nivel de madurez.	Sí	Grupo de seguridad de Linkedin: Sistemas de Información Sanidad.	Revisados	400317

En los objetivos del 2014 la puntuación fue superior a la media de los hospitales de la CM del mismo grupo y con un cumplimiento por encima del 99%.

Detalle del informe

Media Global Grupo 3,513
Media del Informe 3,963
Valoración del Informe 99,08%
Observaciones
Actualización OSSI 29/01/15

2.2.2 REALIZACION Y PRUEBAS DEL PLAN DE CONTINGENCIA

Semestralmente se realizan pruebas de contingencia del sistema HIS del hospital, dichas pruebas consisten en mostrar de forma activa al personal del hospital cómo actuar cuando no es posible acceder al sistema, para ello se ha implementado un plan de contingencia según el ámbito (Urgencias, Consultas Externas y Hospitalización) para que se puedan realizar informes, hacer peticiones, etc. Se adjunta ejemplo del plan de contingencia del ámbito de Hospitalización.

MODELO - Plan de contingencia_HRJC

Antes de su realización se comunica a la dirección el día de la actuación a través de un mail para su extensión a todo el personal afectado a través de las diferentes direcciones.

En las pruebas realizadas se realiza un seguimiento de cómo se han desarrollado con el fin de poder extraer las conclusiones para su mejora o mejor difusión al personal.

Adjuntamos ejemplo de una prueba:

Servicio: URGENCIAS	**Criticidad del servicio: ALTA**	**Horario del servicio: 24 HORAS**	**Fecha de prueba: 08/07/2015**
Hora inicio: 5:00H	**Hora fin: 6:27H**		
Resp. Del servicio: Monica Vicente	**Resp. Prueba: Raúl Mesón**		
Participantes: Médicos de urgencia y enfermería de urgencias	**Recursos y/o medios físicos utilizados : Acceso a plantillas para la generación de informes carpeta compartida**		

Descripción de actuación (pasos)

1. Desde de urgencias, antes de la contingencia sabían el nº de teléfono de guardia de informática. Y llaman para indicar el problema, esto se produce a las 5:00h.
2. El técnico de guardia, en este caso Raúl Mesón, analiza el problema, y según su valoración es necesario la aplicación del plan de contingencia.
3. El técnico de informática avisa al responsable de sistemas, sin ningún problema se contacta con él, y a las 5:05 h. se indica a la responsable de hospital, en este caso Maria Jose Venegas, la activación del Plan.
4. Tanto el personal de admisión como el personal sanitario saben cómo acceder a las plantillas para la realización de ingresos, peticiones, altas, etc.
5. Durante la contingencia se registran 5 pacientes en formato papel.
6. A las 6:27 h. se recuperan las aplicaciones asistenciales.
7. El personal de admisión y sanitario agregan toda la documentación, tanto administrativa como sanitaria, en el sistema sin ningún problema.

Valoración, problemas detectados, mejoras…

Todo el personal sabía cómo acceder y dónde se ubicaba la documentación relativa al Plan de Contingencia.
Se avisó según la forma prevista al personal de informática por parte de la supervisora de enfermería y admisión.
La activación del Plan fue realizada por el Jefe de Hospital quien se encargó de avisar a todas las áreas del centro.

Conclusiones

Todos los pasos del plan de contingencia se han realizado satisfactoriamente, en este caso la jefa de hospital sabía a quién avisar así como dónde acceder a las plantillas y como activar el plan de contingencia.

El personal de enfermería, es este caso la supervisora de urgencia, sabía cómo actuar e indicó a su personal cómo trabajar durante la parada, sobre todo en triaje.

Admisión registró la información del paciente en papel y se lo pasó a triaje correctamente, también sabía dónde estaba la documentación y el circuito a realizar.
dicha información sobre cómo actuar en una contingencia.

A la vista de la prueba realizada, no se va a realizar ningún cambio en el plan de contingencia.

2.2.3 AUDITORIAS DE LOS SISTEMAS Y LOPD.

Se realizan auditorias bianuales sobre LOPD por empresas externas al hospital, en dichas auditorias se informa al centro de las mejoras a realizar para la correcta aplicación de ley de LOPD en el hospital.

Además anualmente se realizan por parte de la Consejería un plan de actuación de LOPD en el centro, en dicho plan se especificarán las deficiencias observadas en el centro con respecto a la LOPD, para realizar dicho plan se realiza una visita física al hospital por parte del auditor de la consejería.

Tras dichas auditorias y en función de las “no conformidades” encontradas se ponen en marcha acciones de mejora para su corrección. El seguimiento de estas acciones de mejora se centraliza en el Comité de Seguridad del Hospital

En referencia a los accesos a las aplicaciones mensualmente se realizan seguimientos de accesos al sistema HIS del centro, realizando un seguimiento aleatorio de accesos al HIS del centro y verificando su correcto acceso a los datos médicos, si no es así se ha especificado un protocolo por parte de la comisión de seguridad del centro para tomar las medidas oportunas.

Se adjunta ejemplo: 
INFORME DE AUDITORÍA MAYO 2(

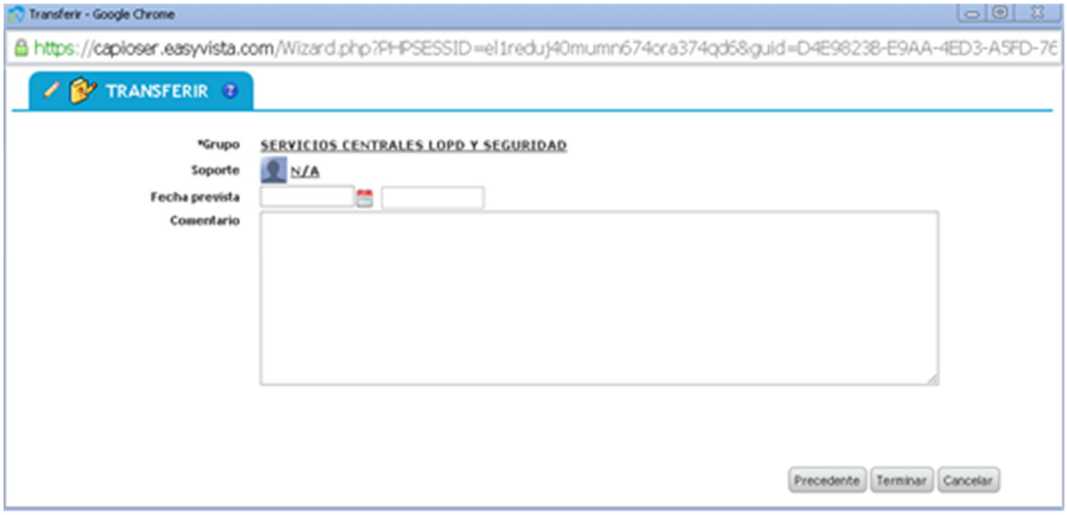
Mensualmente también se realizan un seguimiento de accesos a HORUS para verificar su correcto acceso a los datos de los pacientes.

Se adjunta ejemplo:


082015_acta.doc

En relación a la formación de LOPD se realizan dos formaciones anuales para todos los empleados del centro, una es realizada por parte del centro y otra por personal de la Consejería de Sanidad.

En el hospital existe un procedimiento de notificación de incidencias de LOPD, dichas notificaciones se realizan a través de la aplicación de EASYVISTA y se asignaran al grupo de seguridad.



2.2.4 REVISION DE POLITICAS DE BACKUP Y PRUEBAS DE RESTAURACION

Se han definido políticas de Backup de las diferentes BBDD que contienen información sensible en cuanto a tratamiento se refiere. Por este motivo se han establecido diferentes tiempos de restauración online de estas BBDD, dicha información se especifica en el documento BIA donde se identifican los tiempos RTO/RPO de las distintas aplicaciones. Se adjunta archivo:

ES3-ZH022_BIA_Caracterizacion_servicio

Como mínimo se verifican semestralmente la correcta restauración de las copias de seguridad cumpliendo con los objetivos del contrato marco.

Informe restauración 2do se

Se ha recogido en un protocolo como realizar la restauración de estas BBDD por parte del personal técnico del centro.

Hospital Universitario Rey Juan Carlos Comunidad de Madrid	
PROCEDIMIENTO DE RESTAURACIÓN DE COPIAS DE SEGURIDAD DE BBDD- HIS (GHOSP)	**CÓDIGO:** MO/PES12/POC01 **EDICIÓN:** 2.0

Realizado por: Equipo de Sistemas HURJC	**Aprobado por:** Responsable de sistemas HURJC. Supervisión de servicios centrales de sistemas del Grupo IDC
Destinatarios: Dirección de Sistemas, Responsables de Sistemas, Gerentes	**Fecha Aprobación:** Noviembre 2014
A conocer por: Miembros NPC, Dirección de sistemas, Responsables de Sistemas, Responsables de Compras, Gerentes	**Fecha última revisión:** Septiembre 2015

Tras la realización se cumplimenta un cuestionario para la verificación de la correcta realización o de las deficiencias detectadas.

Hospital Universitario Rey Juan Carlos
Comunidad de Madrid

INFORME DE RESTAURACIÓN DE COPIAS DE SEGURIDAD DE BASES DE DATOS EN EL HOSPITAL UNIVERSITARIO REY JUAN CARLOS

SEGUNDO SEMESTRE DE 2015

1.- OBJETO

El presente informe tiene por objeto detallar una de las pruebas de restauración realizada en la BBDD durante el primer semestre tanto en IMDH como en Casiopea1.

2.2.5 IMPLEMENTACION DE MEJORAS DE SEGURIDAD.

Anualmente se identifican e implementan como mínimo dos mejoras de seguridad en el centro, dichas mejoras son aprobadas en el comité de seguridad del hospital.

Las mejoras realizas en el centro este año son:

- Mejorar la seguridad para los dispositivos móviles (portátiles) comprando candados especiales para su fijación al sitio de trabajo.

- Proyecto de virtualización del puesto de trabajo para una mejor movilidad del trabajos y seguridad de acceso a los datos.

2.2.6 FORMACION E INNOVACION

Se identifican las necesidades de formación para el equipo técnico de sistemas de información del centro para su correcto desempeño del puesto, para ello se exponen las necesidades para la búsqueda de cursos internamente y también con la oferta para los centros sanitarios propuesta por la Consejería de Sanidad.

Cada año se realizan como mínimo dos formaciones.

Las iniciativas tanto corporativas como del centro se proponen en la Comisión de Dirección del centro y se valora su desarrollo e implantación en el centro, existe un grupo de mejora para el HIS de forma corporativa para su valoración y planificación de desarrollo.

En el último año y con proyección de ampliar su desarrollo a futuro se han comenzado con las siguientes:

- **Portal del paciente**, permite al usuario el acceso desde su casa a datos médicos, como informes de alta, resultado de pruebas, así como interactuar con los profesionales del centro.

- Creación de **e-consultas** por parte de los profesionales de los centros de Salud de la zona de referencia del Hospital con el fin de facilitar el flujo de comunicación entre Atención primaria y especializada

- Implantación de nueva **aplicación para anestesia** para la toma de constantes de forma automática de los distintos dispositivos utilizados en quirófano así como realización de informes sobre el proceso de anestesia.

- Diferentes mejoras en el sistema HIS del centro, en nuestro caso un desarrollo interno llamado Casiopea 2.0

2.2.7 REINGENIERIA DE PROCESOS.

Constantemente se están analizando los circuitos que siguen los pacientes para ser atendidos dentro del hospital, con el fin de ir mejorando la calidad de la atención prestada. En este sentido se recogen las posibles mejoras y/o necesidades de los profesionales trasladándolas a un grupo corporativo para su análisis y posterior implementación.

Paralelamente se están desarrollando herramientas para la explotación de información que permiten tener una visión más global sobre el funcionamiento de estos circuitos y tomar decisiones que aporten una mejora de los mismos.

2.2.8 CONTROL Y ADMINISTRACION DE LA ACTIVIDAD TIC.

Para un mejor control y administración del departamento de informática y cumpliendo también con los objetivos marcados en el contrato marco se realizan las siguientes tareas:

- ✓ Actualización de inventario del equipamiento de microinformática del centro (ordenadores, impresoras, etc..), indicando la ubicación de los equipos. (ANEXO)

A	B	C	D	E	F	G	H
AREA	Descripción	Nombre del Equip	Descripcion completa	Serial	Marca	Nº inventario	º serie impre
HOS	Hospitalizacion	HRJC-HOS5UC1	UNIDAD DE CONTROL	J6L0J5J	DELL	MS18105	XEY2212323
HOS	Hospitalizacion	HRJC-HOS5UC2	UNIDAD DE CONTROL	CZC2013QC8	HP	MS04222	XEY2212323
HOS	Hospitalizacion	HRJC-HOS5UD1-2	DESPACHO1	CZC2013Q8V	HP	MS04174	XEY2212326
HOS	Hospitalizacion	HRJC-HOS5UD1-1	DESPACHO1	4JKV95J	DELL	MS18112	XEY2212326

- ✓ Administración del antivirus a través de una consola centralizada tanto para ordenadores como para servidores.

- ✓ Administración de toda la red del hospital manteniendo en todo momento un inventario actualizado de los equipos así como el grado de utilización de los mismos.

HRJCLMS - Detailed Device Report

Generated on Sep 21 2015 17:17:45 Central European Summer Time(GMT +02:00:00)

Summary

Total number of devices	34
Devices with Report Data	33
Devices without Report Data	1 (FW-HRJC-01)

10.166.200.10 : System Information

Updated At	Mar 29 2015 11:36:00
System Name	GW.HRJC.01
Domain Name	
Description	Cisco IOS Software, C2900 Software (C2900-UNIVERSALK9-M), Version 15.1(4)M9, RELEASE SOFTWARE (fc3)

- ✓ Administración del entorno virtual y del almacenamiento de los servidores de forma que en todo momento podemos saber consumos de espacio con el fin de poder hacer proyecciones a largo plazo de necesidades de almacenamiento.

Virtual Disks By Host Report #1

martes, 29 de septiembre de 2015 8:32:33

Ordered by Virtual disk name, Ascending
Servers (all)
Hosts (all)
Virtual disk groups (all)
Virtual disk types (all)

Host: HRJCESX6

Virtual disks: 23 Total size: 57,47 TB Total allocated space: 43,72 TB

Virtual Disk	Size	Allocated Space	Type	Preferred Server	Alternate Server	Storage Profile	Recovery Priority	Replication Status	Data Status
Replica_test	200,00 GB	48,75 GB	Mirrored		HRJCDTCORE03	Archive			Up to date
Temp_FJD	4,88 TB	4,85 TB	Mirrored		HRJCDTCORE03	Archive			Up to date
Temp_FJD_2	1,00 TB	827,75 GB	Mirrored		HRJCDTCORE03	Archive			Up to date
VMware_High_1	500,00 GB	367,25 GB	Mirrored		HRJCDTCORE03	Low			Up to date
VMware_High_2	2,00 TB	1,21 TB	Mirrored		HRJCDTCORE03	High			Up to date
VMware_LAB	1,00 TB	554,00 GB	Mirrored		HRJCDTCORE03	Low			Up to date
VMware_Low_1	1,46 TB	1.004,63 GB	Mirrored		HRJCDTCORE03	Archive			Up to date
VMware_Normal_1	1,50 TB	934,25 GB	Mirrored		HRJCDTCORE03	Low			Up to date

2.2.9 HIMSS EUROPE

El Hospital Universitario Rey Juan Carlos fue reconocido en Noviembre de 2013 por el HIMSS con el Stage 6 en la cuarta edición de la cumbre HIMSS Europe CIO Summit, una de las máximas calificaciones de HIMSS.

HIMSS (Sociedad de Sistemas de Información y Gestión en Sanidad) es una organización profesional exclusivamente enfocada en promocionar el liderazgo y la utilización óptima de las tecnologías de la información en Salud.

El Modelo Europeo de Adopción del Historial Clínico Electrónico (EMRAM por sus siglas en inglés) clasifica los hospitales en función de su progreso en la finalización de 8 fases para crear un entorno electrónico de registros sobre pacientes.

2.3 RESUMEN SITUACION

Partimos de un plan de actuaciones presentado en 2013 bajo el marco del Plan Athene@

Oficina Técnica del Plan Athene@

- Información relativa al análisis y diagnóstico de la situación actual elaborado dentro del marco del Plan Athene@, con indicación de un resumen de situación, fortalezas y debilidades en los siguientes ámbitos
  1. Sistemas de Información
  2. Comunicaciones - LAN
  3. Servidores
  4. Almacenamiento y BackUp
  5. Puestos de trabajo

- Información específica relativa a los inventarios TIC remitidos por los Centros en los siguientes ámbitos:
  1. Sistemas de Información
  2. Comunicaciones - LAN
  3. Servidores
  4. Almacenamiento y BackUp
  5. Puestos de trabajo

- **Oficina de Seguridad Sistemas de Información**
  - **Situación Actual**: Deficiencias y carencias observadas durante los estudios y diagnósticos realizados.
  - **Proyectos de mejora**: Relación de proyectos para abordar las deficiencias críticas en materia de seguridad.

- **Otras iniciativas:** Descripción de las otras actuaciones que se precisan para alcanzar el nivel mínimo de protección de seguridad de la información.

Resumen de la situación existente por ámbito, especificación de los riesgos identificados por la situación actual e identificación de las necesidades de dotación y/o adquisición de componentes, productos y servicios (como base a los proyectos a abordar a corto/largo plazo).

Ámbito	Situación Actual	Riesgos Existentes	Necesidades Detectadas	2015-2018
Sistemas de Información	Hospital en un alto grado de digitalización. En constante proceso de evolución y renovación. En proceso de implantación en del proyecto CASIOPEA 2.0	Complejidad de integración. Migración. Periodo de transición y gestión del cambio.	Renovación y Evolución. Proyecto principal Casiopea 2.0	Prioridad Alta Consecución a medio plazo
Infraestructuras Servidores y Almacenamiento	Dimensionadas de acuerdo a los servicios actuales. Se está trabajando en el proyecto de centralización de CPD en relación a todos los hospitales gestionados por IDCSalud	Dificultad de gestión. Infraestructura diversificada.	Proyecto de Centralización de CPD´s del grupo y CPD de respaldo.	Prioridad Alta Consecución a corto plazo
Comunicaciones	Diversificación de las líneas de comunicaciones con diferentes operadores	Riesgo de dependencia de operador minimizado.		
Puesto de trabajo	Entorno “standard” de escritorio, basado en soluciones Microsoft. Incorporación de entornos móviles para el puesto de trabajo	Obsolescencia de versiones y de PC´s	Valorar soluciones de escritorios móviles (centralización de puestos de trabajo).	Prioridad Media Consecución a largo plazo (previo

Ámbito	Situación Actual	Riesgos Existentes	Necesidades Detectadas	2015-2018
				análisis de factibilidad)
Seguridad	Todas las aplicaciones generan logs de acceso Aumento de la utilización de dispositivos móviles Todos los equipos disponen de un sistema de antivirus actualizado que se monitoriza a través de consolas centralizadas. Se ha incorporado un sistema UTM de última generación que garantiza la seguridad perimetral de las comunicaciones. Se realizan auditorías perimetrales tipo caja negra en cuanto se modifican partes de la arquitectura externa. Se realizan auditorías bianuales en materia de protección de datos.	Que se produzcan accesos inadecuados con una detección tardía. Acceso a información protegida Problemas con Malware y backbone que no detecta el Antivirus Las fuentes de información son diversas y resulta complejo disponer de la información ordenada y en tiempo real	Incorporación de un sistema MDM que ayude a gestionar y securizar dispositivos móviles	Prioridad Media Consecución Medio Plazo

3. LINEAS DE ACTUACION

En función de todo lo descrito anteriormente respecto a la situación actual del departamento TIC, así como la identificación de las necesidades detectadas pasamos a resumir las líneas de actuación para el período 2015-2018:

- ✓ Cumplimiento anual de los objetivos establecidos en el Contrato Marco.
- ✓ Alineación con los proyectos estratégicos de la Comunidad de Madrid en materia de Tecnologías de la información y Comunicaciones
- ✓ Consecución de implantación de nuestro principal proyecto de Historia Clínica (Casiopea 2.0)
- ✓ Centralización de CPD`s y CPD de respaldo
- ✓ Identificación de sinergias con el fin de ser más eficientes en la atención del paciente.
- ✓ Desarrollo de nuevos canales para mejorar la seguridad del paciente
- ✓ Desarrollo de nuevos canales de comunicación con el paciente
- ✓ Desarrollo de nuevos canales de comunicación con residencias del área de referencia