



INFORMATICA Y SALUD

Especial: La Seguridad de la Información Sanitaria

V Reunión del Foro de Interoperabilidad en Salud

XII Foro de Seguridad y Protección de Datos de Salud

Presentación del Índice SEIS

Entidades Asociadas



Director

Salvador Arribas

Comité editorial

Luciano Sáez
Marcial García Rojo
Julio Moreno
Emilio Aced

Consejo de Redacción

Rodrigo García Azurmendi
Miguel Chavarría
Fernando Bezares
José Quintela
Alberto Gómez Lafón
Jesús Galván
María Rovira
José Luis Monteagudo
Cristina Cuevas
Begoña Otalora
Fernando Escolar
Carlos García Codina
Vicente Hernandez
Carlos Hernández
Juan Fernando Muñoz
Juan Manuel de León
Carlos Parra
Antonio Poncel
Francisco Javier Francisco Verdú
Carlos Royo
José Lagarto
Isabel Aponte
Guillermo Vázquez
Javier Carnicero

Colaborador Técnico

Diego Sáez

Información, Publicidad,

Suscripciones y DISTRIBUCIÓN:

CEFIC. C/ Enrique Larreta, 5 Bajo Izda
28036 Madrid
Tlfn: 913 889 478 • Fax: 913 889 479
e-mail: cefic@cefic.es

Producción Editorial:

Tel. 902 271 902 • 987 27 27 27
E-mail: mic@editorialmic.com
www.editorialmic.com



Editorial MIC

DL: M-12746-1992
ISSN: 1579-8070

COLABORADORES TECNOLÓGICOS

AGFA
HealthCare

CSC

INFORMATICA
Sistemas Integrados

INTERSYSTEMS

EMC

intel

gmv

•••••Systems•

AtoS

SIEMENS

FUJITSU

Los artículos revisiones y cartas publicadas en I+S, representan la opinión de los autores y no reflejan la de la Sociedad Española de Informática de la Salud

ABELLO LINDE

COLEGIO OFICIAL DE FARMACÉUTICOS DE CÁCERES

COLEGIO OFICIAL DE FARMACÉUTICOS DE BADAJOZ

COMPLEJO HOSPITALARIO UNIVERSITARIO DE SANTIAGO DE COMPOSTELA

CONSEJO GENERAL DE COLEGIOS OFICIALES DE FARMACÉUTICOS

EMERGRAF, S.L. CREACIONES GRÁFICAS

HOSPITAL CLINIC. SISTEMAS DE INFORMACIÓN

IDCSALUD

MUTUA UNIVERSAL

MUTUAL CYCLOPS-CENTRE DOCUMENTACIÓ

OSAKIDETZA - SERVICIO VASCO DE SALUD

Eficiencia de las Inversiones TIC en el Sistema Sanitario

Hemos presentado los resultados del Índice SEIS 2014, estudio sobre la situación de la implantación de las TIC en el Sistema Nacional de Salud correspondiente al año 2014. Este estudio se realiza en colaboración con los responsables TIC de los Servicios de Salud, del Ministerio de Sanidad Servicios Social y de Red.es, a los que agradecemos su trabajo, que nos permite disponer ya de tres años de información sobre las inversiones y gastos en proyectos TIC en el sistema sanitario público. Esto va a permitir valorar la situación real ajustando el factor temporal, ya que muchos proyectos tienen unos tiempos de ejecución superior al año.

Los datos obtenidos del ejercicio 2014 reflejan un cambio importante en cuanto a la tendencia. Por una parte, el gasto sanitario se ha mantenido prácticamente igual al del 2013, con un importe de 51.857.952.000 euros, una disminución de 539 millones de euros; sin embargo, el gasto TIC en los Servicios de Salud se incrementó un 5,82% respecto al 2013, llegando a un total de 660.972.000 euros. Estos datos reflejan un cierto optimismo en cuanto a la priorización de los proyectos de innovación por parte de las autoridades sanitarias de las CC AA.

Es más significativo el incremento producido en las inversiones del Ministerio de Sanidad Servicios Sociales e Igualdad y del Ministerio de Industria a través de Red.es del 15,92% y del 79,51% respectivamente. Siendo en conjunto el incremento del 7,55%, con una cifra total de 701 millones de euros y un porcentaje global sobre el gasto sanitario del 1,27%, cifra a todas luces muy lejana para una organización con un presupuesto de más de 51 mil millones de euros y en un sector como el sanitario, donde su principal materia prima es la información y el conocimiento.

De la información que se obtiene de los datos del Índice SEIS 2014 destacaríamos algunos hechos significativos. Por ejemplo, la disminución del

número de CPD, el incremento de los puestos de trabajo con herramientas tecnológicas, el escaso presupuesto dedicado a la seguridad y la falta de recursos humanos.

Sin embargo, podemos destacar la eficiencia de estas inversiones, ya que con los reducidos recursos dedicados a las TIC, se está consiguiendo la implantación de importantes proyectos innovadores en el sector sanitario. Tenemos que hacer una valoración del retorno real de esta inversión, ya que hoy solo podemos comparar con lo que otros países de nuestro entorno han invertido y lo que han puesto en marcha. No disponemos de indicadores globales, que cuantifiquen tanto en términos económicos como en resultados en salud lo que aportan estos proyectos.

Desde la Sociedad Española de Informática de la Salud estamos promoviendo la realización de una metodología con la identificación de indicadores que se incorporen a todos los proyectos TIC, de forma que seamos capaces de cuantificar los beneficios de la innovación. Este será el objetivo de las próximas Jornadas Nacionales de Informática Sanitaria en Andalucía "Innovación y Salud", que con el lema "Midiendo el impacto de las TIC en salud", se celebrarán los días 17 a 19 de junio.

Se están desarrollando proyectos en todos los Servicios de Salud para mejorar la eficiencia de los propios recursos TIC, que suponen en términos económicos el 1,27% del presupuesto sanitario, pero mantenemos que si el mismo esfuerzo se realizase en mejorar la eficiencia del 98,73% restante el resultado sería abrumador.

Es necesario convencer a las autoridades que para mejorar la eficiencia del sistema sanitario y sociosanitario, hay que incrementar las inversiones en proyectos TIC y que se considere la utilización de las TIC como una acción prioritaria en sus líneas de gobierno.

La Seguridad de la Información Sanitaria

Coordinador: **Juan Díaz García**

Responsable Unidad de Gestión de Riesgos Digitales, Servicio Andaluz de Salud

El año 2015 se inicia con un ataques masivo a la segunda mayor organización sanitaria de norteamérica, "Anthem" con un robo de datos de mas de 78 millones de pacientes afectados y el año anterior otra gran organización sanitaria "Community Health Systems" perdía mas de 4,5 millones de registros de pacientes. Haciéndose realidad un informe del FBI donde avisaba de lo vulnerable del sector sanitario a los ciberataques, debido a las pobres estrategias de seguridad contra las ciberamenazas que pueden afectar a los datos de salud.



Los sistemas sanitarios se convierten en objetivos especiales por poseer información confidencial que refleja el estado de salud actual, afecta a grandes volumen de pacientes, y está muy expuesta por la necesidad de la accesibilidad del paciente a su asistencia e información.

Las organizaciones sanitarias pueden estar condicionadas con un factor humano que se encuentra sobrepasado por los recortes, poco motivado y con falta de conocimiento de los riesgos digitales. El factor tecnológico a su vez es afectado por la obsolescencia programada, con escaso mantenimiento y una débil inversión en relación al valor que aporta a la organización y la dependencia operativa que genera. Por último se suma el factor organizacional que tiene que responder a las nuevas demandas de la sociedad, con limitación de recursos y prestaciones. Debiendo evolucionar a una corresponsabilidad sanitaria junto

al paciente constantemente conectado con su E-Salud.

Este marco implica que las organizaciones sanitarias tienen "puntos débiles" y se convierte en objetivos prioritarios del crimen organizado. En contraposición de la banca y las grandes empresas que tienen una gran inversión en tecnología y cultura de la seguridad.

Recogemos en este monográfico algunos ejemplos de organizaciones sanitarias que hacen de la Seguridad de la Información Sanitaria un objetivo irrenunciable y consiguen que repercuta en una mejora de la asistencia sanitaria y confianza del paciente.

Esperemos que sea de vuestro interés y que os ayuden a encontrar respuestas a vuestras problemáticas. Y recordad "La Seguridad de la Información Sanitaria es un deber de todos".

Manifiesto de Valencia sobre Seguridad de la Información y Privacidad en el Sector Sanitario

JuanMiguel Signes Andreu¹, Ricard Martínez Martínez², Cayetano Hernández Marín³

1. Socio de ISACA-CV, AVISA y SEIS; 2. Ricard Martínez Martínez. Presidente de APEP; 3. Presidente de AVISA y socio de SEIS.

By failing to prepare, you are preparing to fail
Benjamin Franklin

Nunca antes que ahora la actividad asistencial y la salud de los pacientes han dependido tanto de la información y de las tecnologías asociadas. Nunca antes que ahora ha sido tan necesario fundamentar la confianza en la tecnologías, en los servicios que se basan en ellas y en los profesionales que los hacen posible.

Las enormes ventajas que han aportado las tecnologías de la información a la actividad asistencial y a la salud de la población durante los últimos 30 años son indudables. Pero esas ventajas no han venido solas: la tecnología y la dependencia tecnológica entrañan riesgos que es necesario conocer y tratar adecuadamente so pena de incurrir en lo que sería una clara demostración de gobierno y gestión irresponsables.

Estas reflexiones salieron a relucir en una jornada técnica celebrada en Valencia en octubre de 2014 con el título "Las tensiones entre funcionalidad, seguridad y privacidad en el sector sanitario". A la cita, convocada por el capítulo de Valencia de ISACA, AVISA y APEP, asistió un numeroso grupo de profesionales entre los que se contaban muchos socios de estas asociaciones y de la SEIS.

El título de la jornada quería centrar los debates en las dificultades para compaginar esos tres objetivos, a menudo contrapuestos, y que suelen recibir una atención muy desigual por parte de los actores que intervienen en el sector sanitario. El objetivo de la jornada era doble. En primer lugar exponer los problemas desde los puntos de vista de los distintos tipos de profesionales allí reunidos: técnicos, gestores, desarrolladores, directivos, auditores, médicos, abogados, especialistas en seguridad y en protección de datos personales, etc. En segundo lugar apuntar soluciones poniendo énfasis en las que pudieran realizarse directamente por dichos profesionales o por las asociaciones representadas. Una de tales soluciones resultó ser la redacción del Manifiesto que aquí se presenta.

El Manifiesto cumple una doble función. Por un

lado es una declaración de intenciones dirigida fundamentalmente a los titulares de la información y a los clientes y usuarios de las tecnologías que intervienen en su tratamiento. Esta declaración pretende fundamentar su confianza en el cuidado y saber hacer de los profesionales que participan en el gobierno, gestión, operación y provisión de los servicios tecnológicos. Por otro lado, es un compromiso que obliga a los profesionales miembros de las entidades que suscriban el Manifiesto a satisfacer las expectativas generadas. Ambas funciones son inseparables y complementarias.

El Manifiesto también tiene su importancia por otros motivos. Uno de ellos es porque no existe un código de conducta para los profesionales implicados que cumpla adecuadamente este propósito de generar confianza (esta circunstancia se explica por la escasa regulación de estas profesiones, en parte debido a que aún son muy recientes, y también por la tolerancia general que se tiene con los fallos en los productos informáticos). Otro motivo es que puede servir para evitar males mayores. A este respecto vale la pena recordar la dureza de las penas que imponen los tribunales por delitos de revelación de secretos relacionados con la información clínica, o la cuantía de las sanciones que impone la Agencia Española de Protección de Datos por incumplimiento de la normativa en esa materia.

Los dieciocho puntos que contiene el Manifiesto recogen otros tantos principios básicos de actuación. Estos puntos evidencian que la solución al problema de encontrar un punto de equilibrio entre funcionalidad, seguridad de la información y protección de datos personales no es y no puede ser solamente tecnológica.

El Manifiesto apuesta por los sistemas que abordan la seguridad y la privacidad desde las primeras fases del ciclo de vida, lo que contrasta con algunas opiniones y costumbres que es necesario cambiar. Por ejemplo, cuando los clientes exigen funcionalidad olvidando o relegando los aspectos de seguridad y

Especial Seguridad de la Información Sanitaria

privacidad hasta una fase tardía, la calidad del producto final se resiente y el resultado suele ser tan caro como ineficaz. Además, en caso de tener que rendir cuentas, los sobrecostes causados por esa mala praxis se camuflan haciéndolos pasar por algo normal e inevitable: ya se sabe, con la informática siempre pasan este tipo de cosas.

Una actuación responsable, sea de gobierno, de gestión, de operación o de provisión, supone un

conocimiento de los componentes esenciales de la calidad del producto o servicio en cuestión, así como valorarlos y exigirlos en su justa medida. El Manifiesto aporta su grano de arena a la hora de hacer patente esta situación y reivindicar la contribución de la seguridad y la privacidad a la calidad de los sistemas de información. Como alguien ha escrito, si piensa que la seguridad es cara, pruebe con la inseguridad.

MANIFIESTO DE VALENCIA SOBRE PRIVACIDAD Y SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN SANITARIOS

Las organizaciones abajo firmantes, todas ellas sin ánimo de lucro y representantes de varios colectivos de profesionales cuya actividad interesa o se desarrolla en el sector sanitario, concedoras

- de la importancia de las tecnologías de la información y las comunicaciones para la sostenibilidad y la calidad de la asistencia sanitaria,*
 - del carácter especialmente sensible de los datos relativos a la salud de las personas,*
 - de la necesidad de establecer controles que sustenten la confianza en las actuaciones de los profesionales y entidades involucradas,*
 - y del deber de rendir cuentas por esas actuaciones,*
- con objeto de contribuir a generar confianza en los sistemas de información y en los profesionales que se ocupan de ellos, manifiestan lo siguiente:*

- 1. que el enorme potencial de la tecnología debe aprovecharse sin mermar derechos reconocidos ni introducir o incrementar vulnerabilidades de las que nadie se hace responsable;*
- 2. que la adopción de la tecnología debe pasar por una revisión a fondo de los procedimientos existentes, no limitarse a su mecanización;*
- 3. que la privacidad y la seguridad son una necesidad, un deber y una exigencia legal;*
- 4. que la privacidad y la seguridad dependen de todos los miembros de una organización, desde directivos hasta personal subalterno o de servicios;*
- 5. que la seguridad y el buen gobierno son condiciones inseparables;*
- 6. que la seguridad es un componente imprescindible y un buen indicador de la calidad;*
- 7. que la privacidad y la seguridad son necesarias para generar confianza;*
- 8. que la seguridad es un motor para mejorar las organizaciones, ya que les exige alcanzar un nivel de madurez alto en el desempeño de sus funciones;*
- 9. que el nivel de diligencia necesario en la selección, aplicación y vigilancia de los controles de seguridad exige a entidades y profesionales un esfuerzo continuado de formación y sensibilización;*

10. que la diligencia en el aprovisionamiento de tecnología exige la comprobación previa del nivel de seguridad que permite alcanzar;

11. que las consideraciones sobre la privacidad deben ser tenidas en cuenta desde las primeras fases de desarrollo de los proyectos (privacy by default, privacy by design);

12. que las consideraciones sobre seguridad deben ser tenidas en cuenta desde las primeras fases de desarrollo de los proyectos (security by default, security by design);

13. que los sistemas de información deben hacer públicas sus funciones y ceñirse a ellas, sin puertas traseras ni actuaciones ocultas;

14. que la información objeto de tratamiento en dichos sistemas lo será únicamente por las entidades legitimadas y para los fines declarados;

15. que las cinco dimensiones principales de la seguridad de la información son: autenticidad, confidencialidad, integridad, disponibilidad y trazabilidad;

16. que la salud del paciente y la calidad de la asistencia sanitaria dependen en gran medida de la integridad, disponibilidad y autenticidad de la información;

17. que la separación de funciones y responsabilidades entre quienes se ocupan de la información, de los servicios, de la seguridad y de la aplicación de la tecnología es un principio organizativo básico para satisfacer los requisitos de seguridad;

18. que ninguna entidad ni parte de ella se bastan a sí mismas para hacer frente a todos los retos que plantea la seguridad, por lo que la colaboración con otros agentes es una necesidad ineludible; y se comprometen a actuar conforme a estos principios, a promover su cumplimiento, exigirlos cuando corresponda, y darles la oportuna publicidad, e invitan a otras entidades a hacer lo mismo declarando su adhesión a este manifiesto.

Las cuatro asociaciones promotoras del Manifiesto (ISACA-CV, AVISA, APEP y SEIS) harán oficial la firma del mismo en un acto conjunto en Valencia durante esta primavera. Tras la firma se iniciará una campaña de difusión en la que se invitará a los agentes que operan en el sector sanitario a declarar su adhesión al mismo.

Manifiesto de Valencia sobre Seguridad de la La Seguridad en el Contrato Programa

José Manuel Laperal González

Responsable de la Oficina de Seguridad en la Dirección General de Sistemas de Información Sanitaria

Servicio Madrileño de Salud; Jefe de Área de Consultoría, Integración y Soluciones; Dirección de Planificación y Coordinación para el ámbito Sanitario. Agencia de Informática y Comunicaciones de la Comunidad de Madrid.

INTRODUCCIÓN

Es muy posible que un título algo más poético hubiera quedado más sugerente o elegante, pero finalmente me he decidido por la trasmisión de un mensaje claro y directo: el Contrato Programa de los centros sanitarios debe incorporar, sin excusa posible, indicadores de seguridad. Es el camino correcto y el que lleva a la obtención de resultados tangibles, como intentaré argumentar en este artículo en base a una experiencia probada.

El Contrato Programa es el documento que recoge el acuerdo (en el caso del SERMAS) entre la Viceconsejería de Asistencia Sanitaria y los Gerentes de cada hospital donde se especifican objetivos de actuación para hospitales de la Red Sanitaria Pública de la Comunidad de Madrid. En este acuerdo se recogen indicadores de seguridad, de calidad, de farmacia, de continuidad asistencial, de atención al paciente y de sistemas de información que deberán ser alcanzados por cada centro, incluyéndose en anexos al mismo las metas concretas, fórmulas de cálculo, aclaraciones y criterios de cumplimiento.

Cualquier organización lleva trabajando tiempo en la mejora de su seguridad informática (¡por supuesto!), encontrándonos lógicamente, con diferentes estrategias con las que se puede abordar la seguridad informática y con distintos procesos de evolución de las mismas, entre los cuales, un proceso evolutivo frecuente es el que describo a continuación.

En los primeros estadios, en las organizaciones se actuaba en los puestos de trabajo instalando programas antivirus, a la par que también se protegían los servidores incorporando a la red dispositivos cortafuegos y otros elementos que mejoraban la seguridad perimetral. A continuación, cuando uno se decidía de una vez por abordar el cumplimiento de la regulación normativa (casi de inmediato, por supuesto) la organización acometía el asunto de las declaraciones de ficheros, los documentos de seguridad y las auditorías bienales. Los más intrépidos abordaban incluso un Plan Director de Seguridad. En este camino se iba

mejorando y ya íbamos cumpliendo. La cosa estaba más presentable, pero desgraciadamente al cabo de cierto tiempo se entraba en un cierto estancamiento. Porque tras el avance inicial y la superación del miedo a la reprimenda legal, el asunto pasaba a un segundo plano donde solamente hacían avanzar la concienciación y los incidentes. El Plan se iba olvidando, acuciados por asuntos más urgentes del día a día (sanitario en nuestro caso), que es cosa complicada como todos sabemos.

En el año 2008, en el Servicio Madrileño de Salud empezamos a trabajar en la creación de una cultura corporativa de seguridad con un Plan Director de Seguridad. Lo abordamos de una forma bastante creativa, con la que se conseguía empezar a institucionalizar los pilares principales de una estrategia de seguridad corporativa, pero adaptada a la realidad de cada centro según sus características especiales. En esta idea, el Plan se configuraba en cada centro a su medida mediante la elección de proyectos e iniciativas a modo de créditos (como en una formación universitaria) según sus posibilidades y circunstancias. Con esto conseguíamos que manteniendo como obligatorios una serie de proyectos corporativos ("troncales") el Plan de Seguridad de cada centro era finalmente personalizado (completando los proyectos troncales con otros proyectos optativos y de libre elección) según sus posibilidades y circunstancias. Evitábamos, en definitiva, el café para todos (imagínense la viabilidad de un plan recetado que tuviera que servir tanto para un hospital de 70 camas como para una ciudad sanitaria de más de 1600, un SUMMA, un Centro de Salud, etc).

En este estadio se consiguieron progresos significativos en materia de seguridad y se empezó a avanzar en una cultura de seguridad común.

En los años siguientes se fueron desarrollando las iniciativas del Plan Director y se colaboraba desde la Oficina de Seguridad de la Dirección General de Sistemas de Información con los centros en el apoyo que demandasen para su despliegue.

A partir de ese estadio, la concienciación de la direc-

Especial Seguridad de la Información Sanitaria

ción con la seguridad era determinante en el grado de avance, teniendo que competir en recursos con otras necesidades TIC y además de las necesidades propias del centro. Para tener posibilidades en esta competición, era necesario redoblar las actuaciones de formación y concienciación, una y otra vez. Si además acontecía una situación de limitaciones presupuestarias generalizada, avanzar era cada vez un reto más complicado, donde el desánimo, la resignación, el conformismo jugaban en contra.

Cabía entonces hacer la reflexión de si podía existir otro camino. El avance de la Historia Clínica Digital (HCDSNS) se imponía, la relación de los pacientes con la Sanidad por medios electrónicos aumentaba, aparecían nuevas regulaciones normativas (LSSI, ENS, ENI), nuevos impulsos a la telemedicina y a las aplicaciones móviles, mHEALTH, BYOD y un larguísimo etcétera.

En definitiva era y es un hecho que la prestación sanitaria ya se ha unido a la tecnología hasta el punto que va siendo cada vez más difícil considerar que puede prestarse la una sin la otra. Entonces, ¿cabe considerar ni por un instante que puede prestarse asistencia sanitaria de una forma no segura?

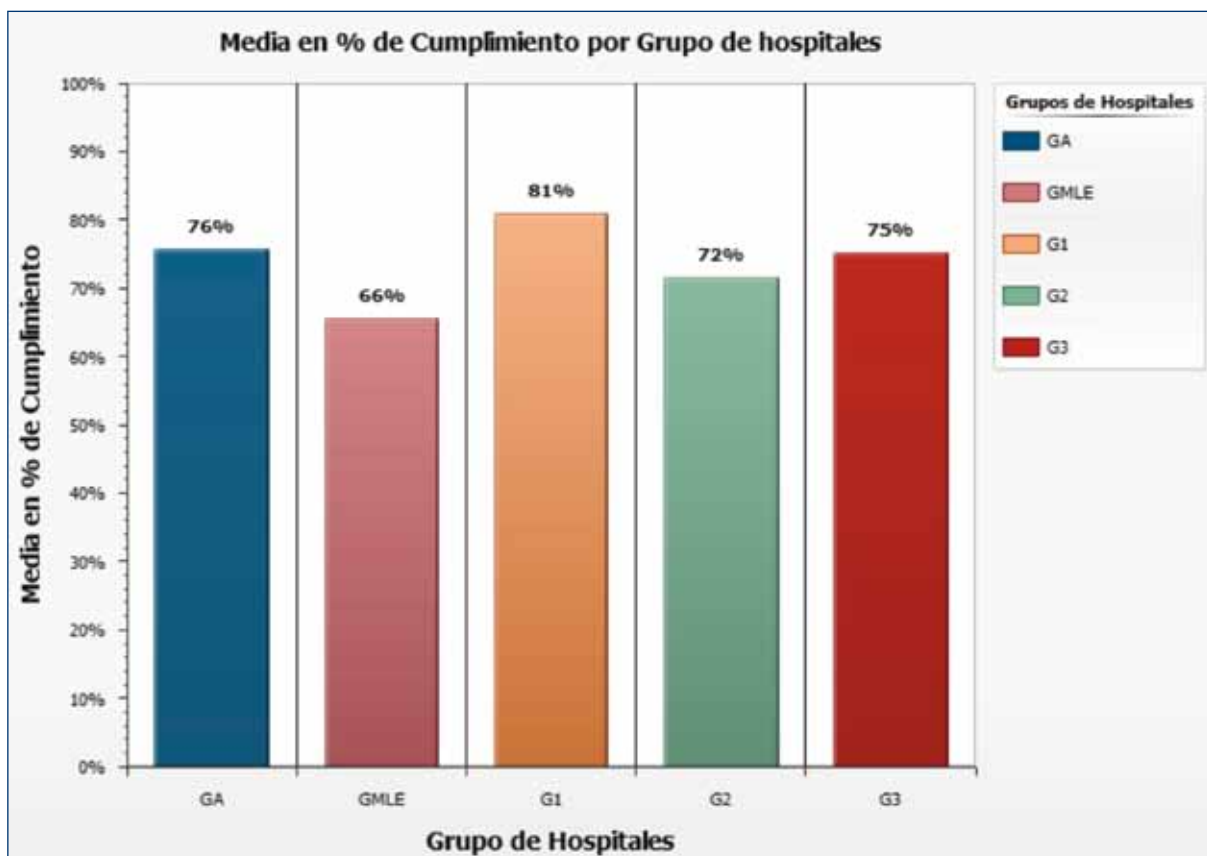
Del fruto de esta unión, aparece por sí sola una lógica consecuencia: al estar embebida la tecnología en la propia prestación sanitaria, en los indicadores

de control de ésta deben incluirse también indicadores de control de la gestión tecnológica y de su seguridad, puesto que todo es ya una misma cosa. ¿Funcionará?

Inicio del Contrato Programa

En el año 2011 el Servicio Madrileño de Salud incorporó indicadores TIC e indicadores de seguridad en los denominados Contratos Programa de Centro, establecidos e impulsados por el Servicio Madrileño de Salud (SERMAS) desde 2009, y se encargó a la Oficina de Seguridad (OSS) de la Dirección General de Sistemas de Información Sanitaria llevar a cabo la elaboración, definición y seguimiento de las metas fijadas en los mismos en lo relativo a indicadores de seguridad. Para lograr un desarrollo de actividades homogéneo, la OSS elaboró para su distribución una guía de apoyo a los Hospitales, donde se definió una metodología de trabajo y unas guías de actuación, acompañadas de unos flujos de comunicación y colaboración permanente, para facilitar el cumplimiento de los objetivos fijados.

La tipología de los indicadores para ese año, y los siguientes fueron el resultado del análisis de las necesidades detectadas en los Diagnósticos de Seguridad que se realizan con regularidad, las auditorías LOPD y las auditorías técnicas de los Centros de



Procesos de Datos que se venían realizando periódicamente.

De dicho análisis previo, se perfilaron los siguientes grupos de indicadores e indicadores:

- GCP_1.A: Plan de Continuidad del Servicio
- GCP_1.B: Constitución Comité de Seguridad de la Información
- Los resultados obtenidos para el contrato programa 2012 fueron buenos (ver gráfico anterior).

La mejora pues, estaba probada y el análisis detallado de los datos, marcó las bases de continuidad para los años siguientes:

- Constitución formal del Comité de Seguridad de la Información y Protección de Datos de Carácter Personal, con el apoyo de la gerencia del Hospital, tal y como se establece en el control 6 de la norma ISO/IEC 27002/2005. Conseguido al 95%.
- Realización del Diagnóstico de Seguridad y auditoría CDP. Auditorías LOPD. Conseguido al 97%.
- Constitución de la Unidad Independiente de Gestión de la Seguridad. Conseguido al 85%
- Número de acciones en materia de mejora de la Seguridad de la Información. Conseguido al 80%.
- Formación y concienciación en protección de datos. Conseguido al 60%.

Continuidad del Contrato Programa

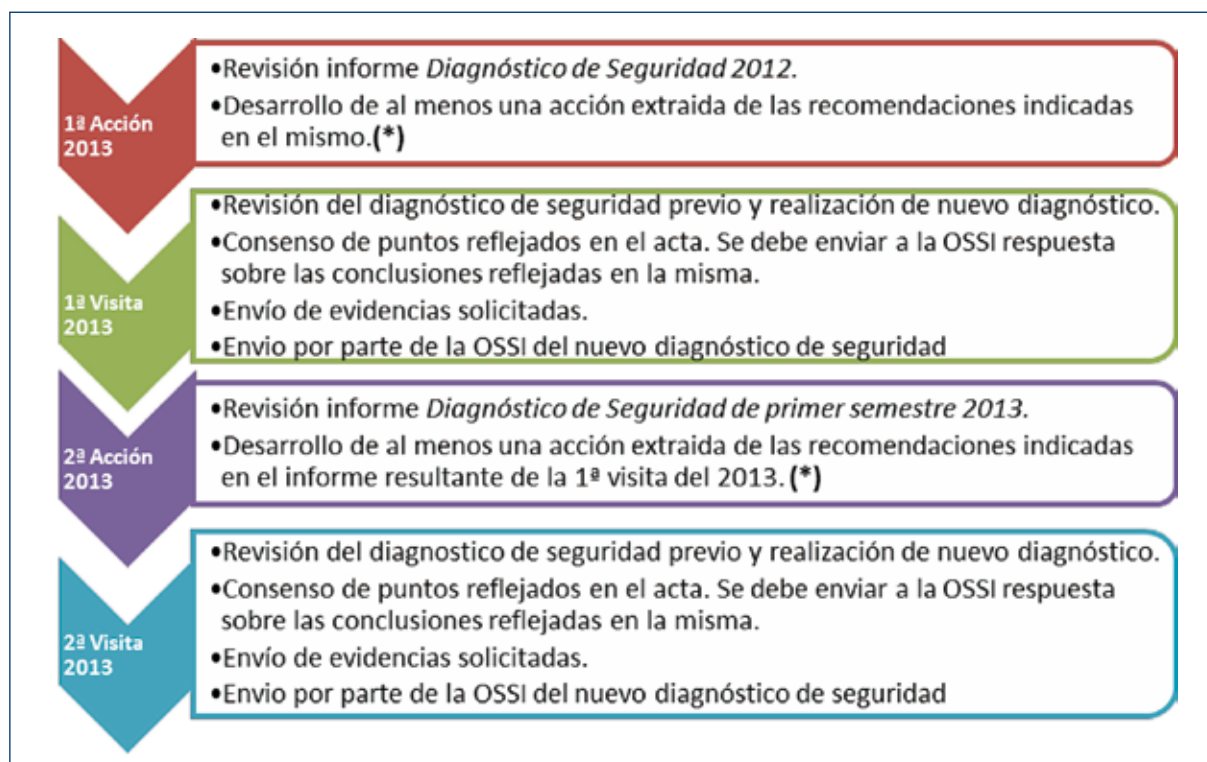
Era pues, uno de los objetivos claros, la consolidación y continuidad de las buenas prácticas

adquiridas en el Contrato Programa 2012. Para mantener un proceso de mejora continua se mantuvieron ciertos indicadores, subiendo su nivel de exigencia, y se dio un mayor peso a aquellos que no pudieron ser completados anteriormente. Se focalizó en la obligación de una planificación más exhaustiva que obligara a abordarlos por fases a lo largo del todo el año, y se hizo hincapié en la recopilación de evidencias para poder evaluar más objetivamente los niveles de calidad alcanzados. Se elaboró nuevamente una metodología y guía de apoyo para los Hospitales, y se mantuvo el flujo de trabajo colaborativo entre la Oficina de Seguridad y los centros.

Se profundizaba en los aspectos de contingencia y recuperación y en la presentación de resultados a alto nivel, esto en la Junta Técnico Asistencial:

- GCP_5.1: Actualización plan de continuidad de servicio

Indicador
GCP_5.1.1-Realización del diagnostico de seguridad 2013
GCP_5.1.2-Definición tiempos recuperación (RTO/RPO) para nuevos sistemas
GCP_5.1.3-Actualización del Plan de Contingencia
GCP_5.1.4-Aprobación y comunicación de nuevas versiones de los planes
GCP_5.1.5-Pruebas del Plan
GCP_5.1.6-Presentación en sesión de la Junta-Técnico Asistencial



Especial Seguridad de la Información Sanitaria

- GCP_5.2: Mejoras en el ámbito de la seguridad de la información

Indicador
GCP_5.2.1-Auditorías de accesos a los sistemas
GCP_5.2.2-Unidad independiente gestión seguridad (Dedicada)
GCP_5.2.3-Presentación del Plan de Seguridad TIC en sesión de la Junta-Técnico Asistencial
GCP_5.2.4-Conformidades en las auditorías LOPD
GCP_5.2.5-Actuaciones de seguridad en Puesto de Trabajo
GCP_5.2.6-Iniciativas Comité de Seguridad

Pese a que el nivel de exigencia aumentó, los niveles de calidad se mantuvieron, creciendo incluso en algunos grupos de centros.

El proceso de mejora se mantenía, los centros reaccionaban positivamente y bajo la implicación de la Dirección los niveles de mejora aumentaban:

- Del objetivo inicial de revisión de planes de contingencia en los que se requería "Los servicios críticos deben disponer del plan completo y en todo caso al menos el 70% de los servicios deben tener desarrollado el plan de contingencia correspondiente" fueron revisados planes de contingencia de los servicios más críticos por un 80% de los Hospitales de la Comunidad de Madrid. (Frente al 35% del año anterior)
- En cuanto a las conformidades en las auditorías

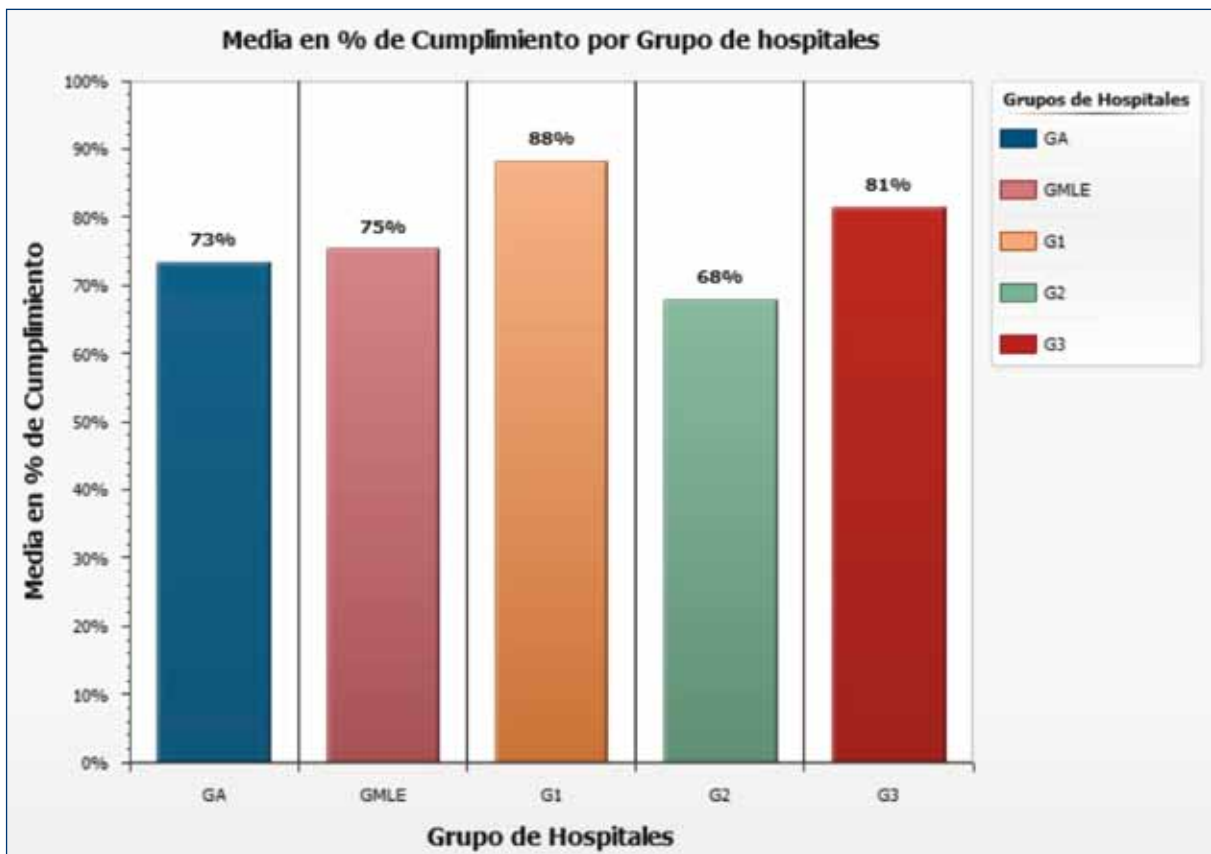
LOPD, aproximadamente un 80% de las no conformidades y recomendaciones extraídas de los correspondientes informes fueron abordadas.

- En lo referente a formación y concienciación en protección de datos, la OSSI impartió formaciones a más del 75% de los Hospitales. (Frente al 60% del año anterior)
- Se realizaron auditorías de accesos a los sistemas de información en el 75% de los Hospitales.
- Se revisaron los tiempos de recuperación RTO/ RPO de los sistemas de información. Realizado 85% de los Hospitales. (Año anterior 30%).

La estrategia no solamente funcionaba, sino que funcionaba muy bien. Habíamos conseguido que la dirección de cada centro estuviera implicada en la mejora de la seguridad y por tanto fuera consciente de las problemáticas y necesidades; la función TIC se elevó de nivel y empezaba a formar parte de los Comités de Dirección del Centro al mismo nivel que otras áreas.

Consolidación

Se puede considerar el año 2014 como el año de consolidación del Contrato Programa. Una de las metas marcadas desde la OSSI ha sido la consecución de aquellos objetivos no conseguidos en años anteriores.



Especial Seguridad de la Información Sanitaria

Por ello, se definieron los siguientes indicadores y grupos de indicadores:

Indicador
GCP_5.1.1-Pruebas del Plan de Contingencia.(Una por semestre)
GCP_5.1.2-Auditoría de los sistemas y LOPD
GCP_5.1.3-Revisión de políticas de backup y pruebas de restauración
GCP_5.1.4-Implementación de mejoras de seguridad
GCP_5.4.2-Gestión correcta de los usuarios de los sistemas de información

En la misma línea que en años anteriores, la OSSl elaboró para su distribución una guía de apoyo a los Hospitales, donde se define una metodología de trabajo así como las plantillas necesarias que facilitan el trabajo en la consecución de ciertos indicadores.

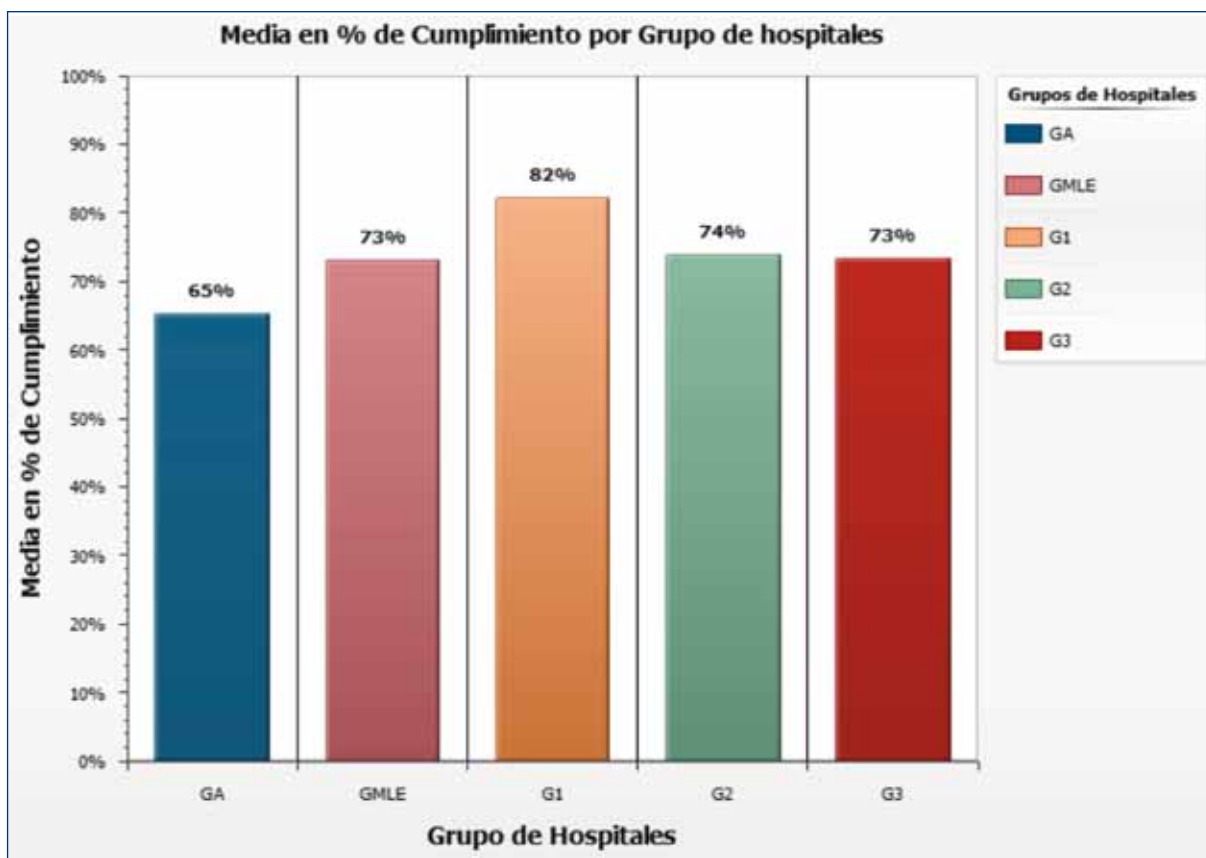
El nivel de exigencia seguía subiendo y los buenos resultados se mantenían (ver gráfico inferior):

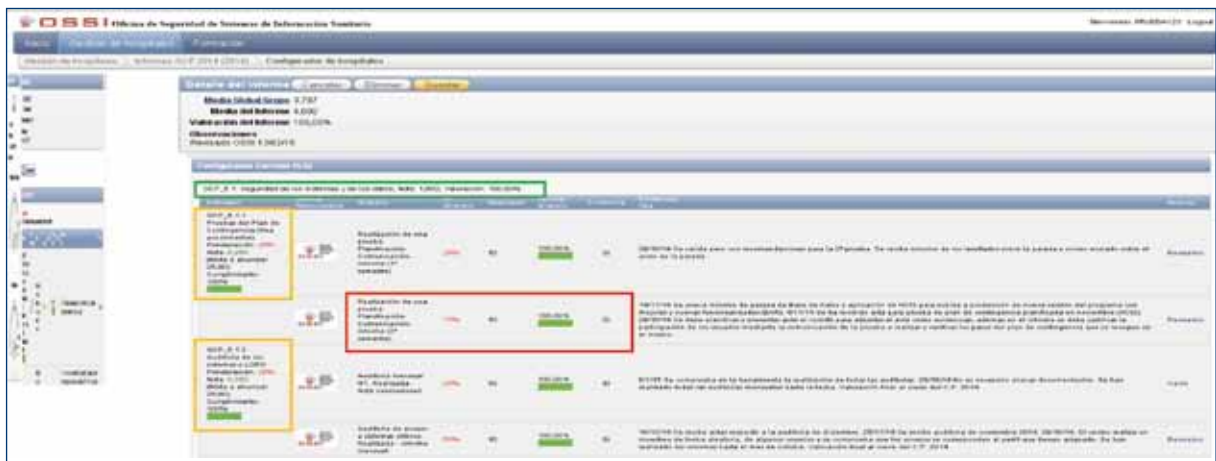
En el momento en el escribo estas líneas el Contrato Programa 2014 se encuentra en proceso de cierre y análisis pero se pueden extraer algunas conclusiones:

- Auditoría de los sistemas y LOPD. Se ha alcanzado la regularización de auditorías de sistemas y la implementación de las mejoras reflejadas en el

informe de auditoría de LOPD en cada centro. La totalidad de los hospitales ha realizado acciones al respecto.

- Revisión de políticas de recuperación y pruebas de restauración. Se han revisado y desarrollado, en algunos casos, las políticas y procedimientos de recuperación de los sistemas de información catalogados como críticos. Se ha conseguido llevar a cabo las pruebas de restauración. De los 35 Hospitales de la Comunidad de Madrid tan solo un 11 % de los centros no han realizado aún acciones al respecto.
- Implementación de mejoras de seguridad. Sobre la base de las recomendaciones extraídas del informe de Diagnóstico de Seguridad, o bien iniciativas propias (o derivadas de las recomendaciones de la auditoría del CPD). Se destaca como dato relevante que la totalidad de los centros han realizado alguna acción al respecto.
- Formación y concienciación en protección de datos. La OSSl impartió formación al 98% de los Hospitales frente al 75% del año anterior.
- Gestión correcta de los usuarios de los sistemas de información. Revisión trimestral de usuarios en los principales sistemas de información y DA. De los 35 Hospitales de la Comunidad de Madrid tan solo un 20% no ha realizado aún acciones al respecto.





Valoración de la experiencia

En términos generales, es un hecho que la inclusión de indicadores de seguridad en el Contrato Programa, con el seguimiento y participación de la OSSI en los objetivos marcados en el Contrato Marco, ha facilitado la materialización e implementación de mejoras en cuestiones de seguridad de los sistemas de información, en un salto cualitativo de calidad.

Se ha contribuido a alcanzar un nivel elevado de compromiso y coordinación entre los distintos centros de la Sanidad madrileña, Hospitales y servicios centrales.

En la actualidad cada centro funciona con un Comité de Seguridad (cuyo máximo representante es el propio gerente del Hospital), se establecen agendas de trabajo en materia de seguridad con reuniones periódicas de seguimiento donde se revisan los tiempos de respuesta y recuperación, se revisan y aprueban planes de contingencia y pruebas de continuidad del servicio, se detectan nuevas necesidades y carencias que son elevadas a la Gerencia del Centro, donde son analizadas con el nivel de implicación adecuado, dando como resultado nuevas medidas y estrategias de seguridad.

Estos planes, una vez aprobados por el Comité de Seguridad, son difundidos a todo el personal del centro y se planifican simulacros de pruebas de los mismos con el objetivo de comprobar su efectividad.

En la actualidad los centros disponen un sistema de información denominado SGOSSI, concebido como una herramienta centralizada para la gestión de la información de las distintas líneas de servicio

en materia de seguridad de la información (cumplimiento LOPD, diagnósticos de seguridad, Contrato Programa), la cual les permite:

- Acceso directo a información en tiempo real.
- Consultar informes históricos.
- Posibilitar a los Hospitales la generación de informes propios.
- Disponer de gráficos comparativos entre líneas de servicio.
- El hospital puede adjuntar documentos y/o evidencias que justifiquen el cumplimiento del objetivo marcado en cada caso y acceder online a la evaluación que realiza la OSSI sobre las evidencias recibidas.

Con todo, se ha logrado incluso generar proactividad en actividades tales como:

- Revisión de los registros de acceso a sistemas de información de alta criticidad como los relacionados con historias clínicas.
- Revisiones proactivas en la gestión de usuarios y perfiles.
- Formación y concienciación en materia de seguridad de la información.
- Pruebas de restauración de sistemas considerados críticos.
- Pruebas de planes de contingencia.

En definitiva, la experiencia en la participación del Contrato Programa, ha sido y es un éxito y como comentaba al principio del artículo, es un camino probado donde el reto ahora consiste en mantener el rumbo, recordando:

“La Seguridad no es solo un proceso tecnológico... Es un Proceso Organizacional”.

Seguridad de la Información Sanitaria y la Investigación Médica en Hospitales

Esther Elvira Andrés

Jefe de Sección de Informática – Hospital Universitario de Cruces

Los científicos e investigadores han analizado datos desde siempre. No hace tantos años y sin el mundo de Internet, la investigación en un Hospital era a menor escala : con una muestra reducida de pacientes y con la Historia clínica en papel. Toda la labor de estudio estaba muy limitada y controlada porque el volumen de datos a manejar suponía ya en si mismo una limitación.

En la actualidad nos enfrentamos a un gran desafío : la escala en la que los datos son generados. Hablamos de Petabyte 10¹⁵, Exabyte 10¹⁸, Quintillón 10³⁰, En un artículo he leído que con todas las redes sociales, fotos, vídeos, ubicación geográfica mediante GPS, en definitiva toda actividad diaria que realiza cualquiera de nosotros con los smartphones, se generan alrededor de 2,5 quintillones de bytes diarios en el mundo. ¡Impresionante! 2.500.000.000.000.000.000.000.000.000

Hay un gran entusiasmo a nivel mundial en las expectativas sobre Big Data aplicado al entorno Salud, ya que este último cumple una serie de requisitos que lo hace "atractivo".

Dada la cantidad de datos médicos registrados por paciente y el nº de casos tratados, junto a las nuevas herramientas que facilitan el tratamiento de la información, volumen y velocidad de procesamiento, el mundo de la investigación médica se ha profesionalizado en auténticos institutos, anexas a los centros Sanitarios y cuyo personal se entre mezcla. A lo largo de los años, la labor asistencial se ha compaginado con una potente labor investigadora; no sólo en líneas de investigación, ensayos clínicos y proyectos mundiales, sino en trabajos universitarios, docentes y procesos de mejora de procedimientos aplicados a las técnicas usadas con pacientes.

Esta explosión de "grandes datos" está transformando la manera en que se conduce la Investigación y adquiere fuerza el uso de Big Data (así como el uso de software libre y gratuito) para resolver problemas complejos relacionados con el descubrimiento científico, investigación biomédica y salud, entre otros.

Por definición, se denomina Big Data a la gestión

y análisis de enormes volúmenes de datos que no pueden ser tratados de manera convencional, ya que superan los límites y capacidades de las herramientas de software habitualmente utilizadas para la captura, gestión y procesamiento de datos. Dicho concepto engloba infraestructuras, tecnologías y servicios como: imágenes digitales, datos de formularios, emails, mensajes en redes sociales, señales de móvil, archivos de audio, sensores, datos de encuestas, logs, que pueden provenir de escáneres médicos, micrófonos, cámaras, telemedicina, electrocardiogramas, espirómetros, sensores, ... y en general, cualquier aparato de electromedicina. Sin olvidar la explosión en nuestras vidas de lo que se denomina "Internet de las cosas", como por ejemplo, relojes que permiten llevar un seguimiento de varios parámetros relacionados con la salud del individuo gracias a varios sensores y un software.

El objetivo de Big Data es convertir el dato en información que facilita la toma de decisiones en tiempo real. Más que una cuestión de tamaño, es una oportunidad de negocio. Las empresas ya están utilizando Big Data para entender el perfil, las necesidades y el sentir de sus clientes respecto a los productos y servicios vendidos.

En este contexto, las Organizaciones Sanitarias encajan perfectamente ya que existe una gran actividad asistencial, tanto a nivel quirúrgico como de Urgencias y tanto para adultos como para pediatría. El volumen de información que se maneja es enorme y el perfil de las personas atendidas también. Además, son Organizaciones que cuentan con gran cantidad de tecnología aplicada a las últimas técnicas. Tecnología que ya no consiste en un aparato aislado, sino en una inteligencia inte-

grada y conectada a nuestros Sistemas de Información propios y al mundo Internet.

El uso de Big Data, así como el uso de software libre y gratuito cada vez más extendido entre estos profesionales investigadores, va más allá, incluso proyectos mundiales con Bases de Datos que no se sabe dónde residen ni las medidas de seguridad que cumplen, por no mencionar el fin último de los datos que se recogen al finalizar el estudio o proyecto. Adquiere especial relevancia los criterios de seguridad que recoge la Ley Orgánica de Protección de Datos (LOPD), ¿dónde quedan conceptos como "utilización del dato exclusivamente para el fin que fue recogido", "consentimiento expreso del paciente"....?

Vemos en nuestras organizaciones sanitarias que se incorporan profesionales investigadores jóvenes muy acostumbrados ya a la tecnología y el software gratuito (en la mayoría de los casos también software libre). En el mejor de los casos, los profesionales TIC del propio Centro únicamente nos vemos implicados en estas herramientas porque nos necesitan para instalarlas en los ordenadores del Hospital, y de esta manera se nos plantea la disyuntiva de permitir o no estas herramientas y encajarlas con el cumplimiento de la LOPD y las medidas de seguridad aprobadas por el Centro. Ellos nos ven como poco facilitadores para su trabajo, pero nosotros tenemos la obligación de hacerles reflexionar en cuestiones como:

- ¿Dónde se ubican las BBDD con los datos de pacientes del centro tras esas URL mundiales que les facilitan en los proyectos y qué medidas de seguridad aplican?
- ¿Qué tipo de consentimiento tienen de los pacientes? El paciente cuando da su consentimiento para participar en un proyecto de investigación mundial, ¿conoce los riesgos implícitos de la tecnología usada?
- Aunque haya voluntad de disociar y anonimizar los datos, ¿qué herramientas se usan para ello?. No existen estándares seguros y formalmente reconocidos y aceptados que garanticen los principios básicos de: romper la relación entre dato y titular, ser irreversible y equivaler a un borrado permanente.
- ¿Qué personal maneja estos datos? ¿Son profesionales propios o externos: institutos de investigación, laboratorios, universidades, patrocinadores, empresas colaboradoras, ...?
- ¿Cómo se regula esas relaciones estrechas entre la actividad asistencial (hospitales y centros de sa-

lud) y la investigadora (Institutos de Investigación públicos y privados)?

- Los consentimientos de los pacientes recogen expresamente el fin para el que se usan, pero ¿cuál es el destino final de los datos recogidos y tratados al finalizar el proyecto o ensayo clínico?
- ¿Por qué en el ámbito de la investigación hay tanto software gratis?. ¿Cual es el negocio?

En todo software gratuito, la estrategia empresarial no se basa en vender productos, sino servicios. Para estas empresas el negocio no es tanto el desarrollo de software, que también, sino que como en la mayoría de los casos este software además es libre, se benefician de las aportaciones que hacen los diseñadores que tocan el código fuente. El producto puede ser gratuito, pero no todo el mundo sabe código. Hay muchas cosas que adaptar dependiendo del tipo de negocio al que esté enfocado el programa, y pueden surgir problemas. Además hay que ocuparse del mantenimiento y estar pendiente de las nuevas actualizaciones que llegan al mercado. ¿Quién puede hacer todo eso? ¿Por qué voy a centrarme en vender un solo producto una vez si puedo cobrar pequeñas cantidades a lo largo de mucho tiempo?

Debido al gran avance que existe día a día en las tecnologías de la información, los profesionales de TI de los Servicios de Salud nos tenemos que enfrentar a nuevos desafíos que permiten analizar, descubrir y entender más allá de las herramientas tradicionales y programas propietarios ad hoc. Y dado el gran crecimiento de las aplicaciones disponibles en internet, nunca vamos a poder competir con las virtudes que este tipo de software (que las tiene) les ofrece. Incluso, si no estamos dispuestos a pasar por este software, los investigadores pueden tener la tentación de buscar vías alternativas con prácticas ilegales de piratear programas. Lo que si sabemos es que somos nosotros quienes tenemos las aptitudes técnicas para valorar y elegir de entre todo el software que se ofrece y modificarlo si hiciera falta, teniendo en cuenta aspectos muy importantes de seguridad. En entornos de información tan sensible como es el de Salud, todos estos rápidos avances en tecnología que abren las puertas hacia un nuevo enfoque de entendimiento y toma de decisiones, exigen profesionales cualificados y especializados en Seguridad y TI.

Evidentemente la tecnología está ahí y hay que aprovechar las ventajas que ofrece a todos los profesionales, saber adaptarla a cada ámbito, cono-



ciendo los riesgos que puede haber tras herramientas tan potentes y que los datos de salud que se utilizan para un fin tan loable como contribuir a la investigación y a la ciencia no caigan en manos de terceros, porque “los malos” están ahí a la escucha , en esta era hiperconectada y donde la “información de las personas” es el verdadero negocio, por no mencionar intereses de terceros. Numerosos artículos recogen ya el precio en el mercado negro de datos de salud y cómo se ha multiplicado el nº de ataques a Hospitales :

“La información médica de las personas puede llegar a valer diez veces más que el número de una tarjeta de crédito para los ciberdelincuentes ...”

Tenemos por delante una tarea de concienciación, de transmitir la importancia de utilizar esta tecnología de una manera adecuada, controlada y legislada.

CONCLUSIONES

La naturaleza de la información hoy es diferente a la información en el pasado.

En Investigación Médica, ¿por qué limitarse a una muestra reducida de pacientes, con el sesgo que ello conlleva, si tenemos al alcance una gran cantidad de información que podemos tratar a una gran velocidad e incluso repetir una y otra vez aplicando distintas fórmulas y patrones?

El uso de Big Data ayuda a los investigadores a descubrir cosas que les podrían llevar años por sí mismos sin el uso de estas herramientas. Debido a la velocidad del análisis, es posible que el investigador pueda cambiar sus ideas basándose en el resultado obtenido y trabajar el procedimiento una y otra vez hasta encontrar el verdadero valor al que se está tratando de llegar. Ofrece la facilidad de describir enormes cantidades de datos (estructurados, no estructurados y semi estructurados) que de otra forma tomaría demasiado tiempo y sería muy costoso cargarlos a una base de datos relacional para su análisis, así como desarrollar de forma propia el código correspondiente.

El hecho de pensar en cosas gratis o libres, nos pone los pelos de punta pensando ¿por qué es libre o gratis? El conocimiento es algo que se comparte y todos los profesionales de TI en Sanidad nos deberíamos de preocupar por mantener una estrecha relación con el Investigador y brindarle el soporte adecuado. La tendencia global es orientar las tec-

nologías al servicio y soporte; y no al licenciamiento. Además el software libre/OpenSource/gratis puede llegar a ser más seguro que el software propietario : al propietario no hay manera de ver “sus puestas traseras”; sin embargo, al libre cuando su código fuente es tratado por una persona entendida es mucho más difícil la inclusión de dichas puertas traseras (verdaderos agujeros de seguridad). Lo importante es que se facilite el código fuente del software elegido para que pueda ser revisado por profesionales cualificados, los investigadores sanitarios no tienen estas capacidades y es por ello que deben de ir de la mano de los profesionales de TI de sus Centros.

Los profesionales de TI en Salud llevamos ya una trayectoria de años concienciados de los riesgos del exterior y de las exigencias legales, merece la pena formar y concienciar también a estos profesionales de la Investigación de la importancia de hacer las cosas bien desde el principio, aunque esto les parezca una “piedra en su camino”, con todos los agentes implicados: investigadores, juristas y profesionales de IT y seguridad (Privacidad en el diseño).

La información y los servicios están sometidos a riesgos, no sólo malintencionados o ilícitos, sino también fallos y accidentes. La sociedad espera que los servicios que se prestan con sus datos sean de total confianza y seguridad, en esto las Administraciones Públicas debemos de dar ejemplo.

El hecho de que tecnológicamente determinados patrones se puedan estudiar y aplicar resulta cuanto menos inquietante.

¿Contempla la legislación vigente esta nueva forma de tratar la información? ¿Dónde se traspasa la frontera con la legislación sobre derechos fundamentales de los ciudadanos en cuanto a su privacidad? ¿Deberíamos pensar que en un futuro no muy lejano ya no habrá datos personales ni privados y que nuestra información estará “ahí” accesible para su tratamiento?

¿Estamos preparados para este nuevo escenario?

“El hecho de pensar en cosas gratis o libres, nos pone los pelos de punta pensando ¿por qué es libre o gratis? El conocimiento es algo que se comparte y todos los profesionales de TI en Sanidad nos deberíamos de preocupar por mantener una estrecha relación con el Investigador y brindarle el soporte adecuado”

Oficina de Seguridad de la Información Servicio Canario de la Salud

XXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

El Servicio Canario de la Salud, como el resto de Sistemas Regionales de Salud, explota en el ejercicio de sus atribuciones un conjunto heterogéneo de sistemas de información que gestionan una gran cantidad y diversidad de datos, siendo especialmente sensibles los relacionados con la información de salud de los pacientes.

La identificación y registro de los accesos a esta información es, además de una buena práctica generalmente recomendada, un requisito legal que garantiza al ciudadano la seguridad de que sus datos son tratados con la confidencialidad debida.

Normativa

El Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de protección de datos de carácter personal específica en su artículo 103 que “de cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado”. En el apartado 2 del citado artículo indica que “en el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido”. El objetivo es, según informe 0584/2009 de la Agencia Española de Protección de Datos, ser capaz de establecer las acciones realizadas por un determinado usuario respecto a un registro accedido. El resto del artículo 103, establece que “los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos” y se fija en dos años el periodo mínimo de conservación de los datos registrados. El responsable de seguridad tiene a su cargo “revisar al menos una vez al mes la información de control registrada” y elaborar “un informe de las revisiones realizadas y los problemas detectados”.

Disponer de un registro de accesos no es únicamente un requisito de la normativa de protección de datos; desde el ámbito de la administración electrónica, el Esquema Nacional de Seguridad, ENS, también exige en su punto [op.exp.8] que se

registren “todas las actividades de los usuarios en el sistema”, en especial, “la de los operadores y administradores del sistema” y, en su punto [op.exp.10], fija la protección de estos registros de actividad, de manera que se asegurará la fecha y hora de los accesos y que los registros no puedan ser “ser modificados ni eliminados por personal no autorizado”.

La propia Política de Seguridad del SCS, basada en las mejores prácticas incluidas en la ISO27002, incluye un apartado dedicado a la clasificación de la información, para adecuar las medidas de seguridad de una manera proporcionada al activo protegido, y señala, en el apartado dedicado a la monitorización de eventos, la necesidad de disponer de registros de la actividad de los usuarios, así como garantizar su protección.

Punto de partida y objetivos

En el punto de partida del proyecto, la identificación y registro de los accesos a la información calificada de nivel alto por la normativa de protección de datos y el ENS y aquella información categorizada como confidencial, de acuerdo con la Política de Seguridad de la organización, se realizaba de manera ad-hoc en cada uno de los sistemas. Este enfoque precisaba de una mejora de cara a una gestión y tratamiento automatizados para poder dar cumplimiento a los requerimientos normativos, así como a los requisitos internos del SCS.

Así pues, el objetivo era la implantación de un sistema homogéneo y centralizado que permitiera la generación, identificación y registro de los accesos a los datos de los sistemas de información del SCS, teniendo en cuenta el entorno distribuido de los mismos, informática y geográficamente hablando, de manera que el acceso al registro de accesos resultante fuera centralizado en un único sistema, independientemente de la ubicación del registro accedido. En este

repositorio común, se consolidarían y custodiarían los registros de accesos de los sistemas que se categoricen con el máximo nivel de protección, ya sea por protección de datos, ENS o política interna.

Estrategia

Se partía de un conjunto heterogéneo de sistemas, tanto por arquitectura como por tecnología (sistemas basados en SAP, aplicaciones desarrolladas en Java y .NET, etc.), distribuidos geográficamente a lo largo y ancho del archipiélago y cuyo punto en común es el Sistema Gestor de Base de Datos, SGBD, basado en Oracle.

También el grado de cumplimiento de la obligación de disponer de un registro de accesos era variado; había aplicaciones que disponían de un registro de accesos correctamente implantado, otras que lo tenían parcialmente (por no recoger la totalidad de la actividad de los usuarios; por no tener en cuenta accesos de tipo lectura; por considerar únicamente los accesos realizados desde la aplicación y no haber contemplado los accesos directos a la base de datos; por no proteger adecuadamente el registro de accesos resultante, etc.) y una pequeña porción que no disponía de registro de accesos.

Además, se decidió incluir el registro de accesos a carpetas y/o directorios en servidores Windows de especial protección, así como la actividad de los administradores en sistemas unix y otros dispositivos de red.

En respuesta a esta situación de partida, se optó por descomponer el problema en varios escenarios, buscando una solución para cada uno de ellos, dando así respuesta a toda la casuística planteada. Así, se crearon diferentes soluciones para diferentes problemas:

- Activación de la auditoría a nivel de base de datos para el conjunto de usuarios autorizados a acceder directamente: Se activa para las operaciones de lectura, pues, como veremos en el punto siguiente, las operaciones de modificación y borrado se manejan de otra manera. Este punto debe contar con un prerrequisito básico, y beneficio colateral de la implantación de esta solución, que es la eliminación de usuarios genéricos o no asociados a una persona concreta.
- Elaboración de un mecanismo de recogida de la actividad de modificación y/o borrado de datos realizada directamente sobre la base de datos mediante el tratamiento de los archivologs generados por el SGBD Oracle. Este punto exige el prerrequisito de trabajar en modo archivolog.

- Elaboración de una API para aquellas aplicaciones que no estaban recogiendo la actividad de los usuarios. Esta API se insertó en todos aquellos lugares del código de la aplicación donde se tratan datos de nivel alto o de carácter confidencial, ya sea de lectura, modificación o borrado.
- Elaboración de un sistema de recogida de los logs de las aplicaciones que generaban un registro de accesos correcto, complementado con un procedimiento de parseo de la información recogida para poder almacenarla en un formato normalizado.
- Recolección de logs mediante conectores prediseñados para sistemas propietarios, como SAP, de logs basados en syslog o de actividad de Active Directory de servidores basados en Windows.

Todo esto debe ir acompañado de

- un sistema de normalización de toda la información recogida procedente de orígenes heterogéneos
- un sistema de compresión de los logs recogidos que permita reducir la ocupación en disco de la ingente información recolectada
- un sistema de firma de los logs recogidos que garantice su integridad y autenticidad

Usos previstos

Además de dar cumplimiento a las exigencias normativas que se han repasado en los apartados anteriores, la recolección de toda la actividad sobre los datos susceptibles de un nivel alto de protección, el sistema resultante permite

- explotar los datos de acceso, pudiendo así cuantificar el número de accesos, por perfil, por fechas, por horas, por aplicación, etc. Esta foto dinámica permitirá identificar actividad (por números de accesos, por horario, etc.) que se sale de la norma
- auditar la actividad de los usuarios privilegiados (administradores)
- realizar auditorías de la actividad de usuarios escogidos
- realizar auditorías de los accesos a los datos de determinados pacientes
- atender las reclamaciones realizadas ante la Oficina de Defensa de los Derechos de los Usuarios Sanitarios
- atender las solicitudes de los usuarios que demandan conocer quién ha accedido a su Historia Clínica
- realizar auditorías aleatorias de acceso a datos sensibles

Auditorías aleatorias y sus beneficios

Al margen del obvio beneficio del cumplimiento normativo y del beneficio colateral de haber reducido al mínimo el número de usuarios genéricos tanto en las aplicaciones como en los accesos directos a base de datos, el beneficio de la implantación de este sistema que más se está aprovechando es el derivado de las auditorías aleatorias.

Las auditorías aleatorias consisten en escoger, mediante una función tipo random, una serie de accesos a datos sensibles de un número prefijado de usuarios de los sistemas de información del SCS, a los que se requerirá justificación para los mismos. Para ello, se escogen accesos muy recientes (de las últimas dos semanas), de manera que sean capaces de poder justificarlos.

La comunicación de la auditoría se hace formalmente, mediante una carta dirigida al usuario, que le es entregada por el Responsable de Seguridad delegado de la Gerencia en cuestión, habilitado para ello por el Responsable de Seguridad.

En esta misiva, se le informa de la normativa de protección de datos y del programa de auditorías que se lleva a cabo desde la Oficina de Seguridad de la información.

“Las auditorías aleatorias consisten en escoger, mediante una función tipo random, una serie de accesos a datos sensibles de un número prefijado de usuarios de los sistemas de información del SCS, a los que se requerirá justificación para los mismos. Para ello, se escogen accesos muy recientes (de las últimas dos semanas), de manera que sean capaces de poder justificarlos”

Se le señalan dos o tres accesos realizados por él en los últimos días y se le solicita que justifique los mismos.

Por justificación, se espera que indique su puesto de trabajo, indicando si es personal sanitario (conforme a la Ley 44/2003 de Profesiones sanitarias tituladas), si el acceso se realizó durante su jornada de trabajo habitual, si se hizo desde su centro de trabajo y si el acceso se produjo mientras el pacien-

te estaba en el centro asistencial.

Estos datos resultan suficientes para determinar si el acceso es compatible con la Política de Seguridad del SCS, la normativa de protección de datos y la Ley 41/2002, de Autonomía del Paciente.

Se hace hincapié en que no se haga alusión en la respuesta a datos de salud y/o clínicos del paciente, de manera que la propia auditoría no resulte en un tratamiento de nivel alto.

La respuesta del usuario, que se se remite por correo electrónico, suele ser del tipo:

El Servicio Canario de la Salud forma e informa a sus trabajadores en el momento en que se incorporan a la organización acerca del conjunto de deberes y obligaciones que asumen desde ese preciso instante y las cuestiones de protección de datos y privacidad son parte integrante de esta información.

Así, el personal conoce las obligaciones que emanan, entre otras, de la Ley de Autonomía del Paciente, de la Ley Orgánica de Protección de datos y de la normativa autonómica de aplicación. A pesar de ello, la noticia de que sus accesos están siendo auditados, noticia que se extiende rápidamente con la recepción de las cartas de auditoría en las Gerencias, tiene un gran impacto; el usuario conoce, repentinamente, que sus accesos se están registrando de manera automatizada, que estos registros quedan almacenados y protegidos y que se le puede requerir para que los justifique.

Esta noticia supone que incluso el usuario más consciente de sus obligaciones reflexione sobre la naturaleza de sus accesos a la Historia Clínica y se cuestione si todos sus accesos estaban realmente justificados.

El resultado es un usuario más concienciado, más cuidadoso con que sus accesos deben estar siempre asociados a la actividad asistencial, consiguiendo así un efecto de autocontrol que es, más allá del mero cumplimiento de la normativa interna, la mejor medida de seguridad.

Datos del Sistema

- 40 millones de registros semanales procesados
- 27 sistemas de información de nivel alto integrados
- 350 GB de información registrada desde el inicio de puesta en marcha del sistema
- 3 servidores; un servidor de integración de los registros recogidos, un servidor de explotación de los registros procesados (basado en el Novell Sentinel Log Manager) y una cabina de almacenamiento de 10 TB.

Seguridad de la información para la seguridad del paciente. Eventos relacionados con las Tecnologías de la Información Sanitaria

Manuel Jimber del Río¹, Martín Tejedor Fernández², Juan Díaz García³

1. Responsable de Seguridad de la Información. Hospital Reina Sofía.

2. Jefe de Servicio de Calidad. Hospital Reina Sofía.

3. Responsable Unidad de Gestión de Riesgos Digitales. Servicio Andaluz de Salud

Habitualmente se identifica el origen de los eventos adversos que alcanzan al paciente con las prácticas clínicas y los errores humanos, pasando desapercibido que las Tecnologías de la Información Sanitarias (TIS) están involucradas o incluso están en el origen de algunos de estos eventos.

Sin duda las TIS aportan innumerables ventajas a los profesionales sanitarios en su labor para la asistencia sanitaria, pero al mismo tiempo, con la creciente introducción de las tecnologías de la información se están introduciendo nuevos riesgos para el paciente derivados de una mala implementación, un mal funcionamiento o un mal uso de las TIS que pueden acabar ocasionando eventos adversos sobre el paciente.

¿Cuáles son los posibles orígenes de los problemas con los sistemas de información que utilizamos habitualmente? Recordemos que un sistema de información consta básicamente de Máquinas (hardware), Programas (Software) y el más importante las personas (usuarios y técnicos). Un cuarto componente del sistema son los "interfaces" o sistemas y mecanismos de comunicación entre los componentes anteriores. Por supuesto, no podemos olvidarnos de otro componente fundamental, los datos.

Un fallo o error en cualquiera de estos componentes podría ocasionar un incidente que afecte a la seguridad del paciente.

EVENTOS ADVERSOS RELACIONADOS CON LAS TIS

Entre enero de 2008 y julio de 2010 se realizó un estudio con el objetivo de mejorar una clasificación de los problemas con las TIS relacionados con eventos de seguridad del paciente. El estudio analizó 899.768 informes, de los cuales 1.100 estuvieron relacionados con las TIS y, de éstos, 436 describían eventos. El examen de los 436 eventos reveló 712

problemas de los cuales, el 96% estaban relacionados con los sistemas informáticos y el 4% eran problemas con la interfaz hombre-máquina. Casi la mitad de los eventos (46%) estuvieron relacionados con circunstancias peligrosas y 46 causaron daño al paciente, incluyendo 4 muertes.

El estudio concluye con una clasificación de 36 tipos de problemas clasificados por un lado, como problemas "humanos", y por otro, como problemas relacionados con la "máquina". Con mayor grado de detalle se clasifican problemas en la entrada de información, en la transferencia de información y en la salida de información. También se añade una categoría de problemas "Técnicos Generales" que representan los problemas hardware y software no incluidos en las categorías anteriores y otra categoría de "Factores Contribuyentes" que representa la contribución de las variables socio-técnicas a los problemas TIS.

Los "Problemas de entrada de la Información" relacionados con "Captura de datos caída o no disponible" tuvieron su origen fundamentalmente en retrasos y fallos en la captura de datos de los dispositivos PACS: Pérdida de imágenes, imágenes distorsionadas, invertidas lateralmente, transmitidas en orden incorrecto, almacenadas en el expediente del paciente equivocado e intercambiadas en el proceso de transmisión de las imágenes. La mayoría de estos problemas obligó a repetir las pruebas con la consiguiente sobreexposición innecesaria a la radiación del paciente. También se encontraron este tipo de problemas en los sistemas de prescripción electrónica provocando la administración de dosis incorrectas y de la corrupción de los registros de la HCE del paciente.

Especial Seguridad de la Información Sanitaria

Los errores en la introducción de datos y manipulación de registros se identificaron en sistemas de laboratorio y de petición electrónica y derivaron en problemas de identificación del paciente y la selección errónea de órdenes de prescripción, teniendo su origen en un diseño pobre de la interfaz de usuario. Como resultado se realizaron pruebas incorrectas, administración de radiación innecesaria, errores en la medicación y cirugía al paciente equivocado. En un caso, la escasa visibilidad de la dosis debido al uso de fuentes de letra de pequeño tamaño ocasionó una sobredosis de adrenalina 10 veces superior a lo prescrito, dando lugar a un infarto de miocardio en el paciente. En otro caso, un paciente sufrió una sobredosis de anticoagulantes. Se encontraron ejemplos de una interfaz mal diseñada en un sistema CPOE en el que el médico tenía que desplazarse por una lista desplegable de 225 opciones ordenadas alfabéticamente, resultando en la prescripción de una sobredosis de digoxina 4 veces superior a lo previsto.

El mismo estudio detectó un caso en el que se fusionaron datos de la base de datos de prueba con los datos de los pacientes reales (errores en la manipulación de datos), lo que acabó llevando a un paciente al quirófano innecesariamente.

Los "Errores en la transferencia de información" estuvieron relacionados con problemas en la redes y paradas no planificadas de los sistemas de prescripción electrónica, y también tuvieron sus consecuencias, tales como no comunicar los cambios en las recetas de farmacia de forma que los pacientes recibieron medicamentos incorrectos o medicamentos correctos pero con frecuencias equivocadas.

También se identificaron problemas de integración entre sistemas de información de forma que los sistemas "integrados" recibían información incorrecta o incompleta. Por ejemplo, se detectó un caso en el que una caída del sistema de prescripción electrónica retrasó el tratamiento de un paciente después de una cirugía, resultando en una discapacidad musculoesquelética permanente. En otro caso, el paciente murió cuando se produjo un problema en la red del PACS, retrasando la transmisión de imágenes al sistema remoto para su diagnóstico.

En la categoría de mantenimiento y actualización de sistemas en explotación, se detectó un caso en el que se sobrescribió la información de alergias durante un proceso de actualización de una base de datos, lo que llevó a la administración de un medicamento que provocó una reacción alérgica en un paciente. En la categoría de "errores en la transferencia de información" se identificaron errores

relacionados con fusiones de historias clínicas de pacientes distintos con el mismo nombre y apellidos, a su vez, relacionados con problemas con la interfaz de usuario, comentados antes.

En cuanto a los "problemas con la salida de la información", los errores más numerosos suelen estar relacionados con los sistemas PACS. Una fecha y hora erróneas de la imagen llevó a un neuroradiólogo a concluir que la enfermedad de su paciente había disminuido cuando en realidad había progresado. En otro caso los marcadores y la orientación de las imágenes llevaron a un cirujano a operar el lado equivocado de la cabeza del paciente debido a que el PACS le mostró la imagen invertida de izquierda a derecha. Problemas con el envío de las imágenes a estaciones de visualización para su análisis y diagnóstico hacia sistemas de información de terceros. Por ejemplo, un sistema de visualización basado en web rotaba aleatoriamente las imágenes al recibirlas. En otro caso, se invirtió una imagen TAC de los senos de una paciente al enviarla desde el PACS a una grabadora de CD, lo que llevó al cirujano a operar el seno equivocado. Otro PACS invertía sólo la mitad de las imágenes cuando el técnico lo ordenaba. Otro ejemplo muy llamativo fue el caso de un sistema PACS basado en web que mostraba los datos de un paciente pero las imágenes del paciente anterior que estaban almacenadas en la memoria caché del navegador.

Algunos otros ejemplos son; no visualizar alertas sobre alergias, retrasos inaceptables en la visualización de datos de una HCE que provocaba que el usuario hiciera clic varias veces seguidas, firmando documentos y aceptando mensajes sin tener conciencia de ello, listas de trabajo incompletas que dejaban a los pacientes sin órdenes de tratamiento o listas de tratamiento que mostraban los medicamentos del periodo de 24h siguientes en lugar del actual.

Más ejemplos; problemas con los formatos de salida de la información que pueden resultar confusos. Un sistema que mostraba órdenes médicas recientes junto con órdenes antiguas, de forma que no se podía distinguir unas de otras. Otro CPOE redondeaba las dosis pediátricas al mostrarlas en pantalla, por ejemplo, la desmopresina 0,025 ml = 0,1 mg se redondeaba a 0,03 ml = 0,12 mg, aumentando la dosis en un 20%). Otro sistema era incapaz de mostrar dosis con volúmenes inferiores a 0,01 ml, lo que obligaba al personal de enfermería a calcular los volúmenes a mano.

El estudio también encontró numerosos problemas técnicos generales (16%), relacionados con las funcionalidades del software, su configuración, los

interfaces entre dispositivos médicos y otros sistemas de información y la configuración de las redes. Estos son sólo algunos de los problemas detectados por el mencionado estudio, con un impacto lo suficientemente importante como para tomar conciencia de que las TIS constituyen una variable más a considerar en relación con la seguridad del paciente.

UNA RESPONSABILIDAD COMPARTIDA. MODELOS Y METODOLOGÍAS

El reto para las organizaciones sanitarias consiste en identificar los problemas de las TIS relacionados con la seguridad del paciente antes de que éstas se implanten, pero también estar preparadas para detectar este tipo de problemas, una vez puestas en explotación, tan pronto como sea posible para poder adoptar las medidas necesarias y corregirlos antes de que se ocasione un daño al paciente.

El enfoque de las organizaciones sanitarias respecto de la seguridad de las TIS debe apoyarse en una orientación colectiva multidisciplinar tanto de expertos internos como externos y que comprende a todos los implicados, desde diseñadores hasta usuarios de los sistemas TIS, y sólo desde un abordaje global y al más alto nivel por parte de las organizaciones sanitarias y con la ayuda de los responsables de TI oportunos será posible atajar un incremento constante de los eventos adversos relacionados con las TIS.

Recientemente se han desarrollado modelos, metodologías y marcos para ayudar a las organizaciones sanitarias a detectar y corregir los incidentes de seguridad del paciente relacionados con las TIS. En la figura siguiente se muestra el modelo socio-técnico de análisis de eventos que surge con el fin de tratar de entender el origen de los eventos y parte del hecho de que las causas interaccionan entre sí en un modelo de 8 dimensiones.



Modelo Socio-técnico

Un examen de los incidentes TIS en el contexto del modelo socio-técnico permite a las organizaciones mirar más allá del incidente y entenderlo en el contexto de las personas que utilizan los sistemas, otras tecnologías y los procesos afectados por las TIS. La comprensión de estas interacciones permitirá a las organizaciones sanitarias hacer mejoras en sus sistemas TIS cuando se identifiquen fallos que pueden conducir a un daño al paciente.

Por otro lado, con el apoyo de la Oficina del Coordinador Nacional para la Tecnologías de la Información de la Salud (ONC) de los EEUU se ha utilizado un proceso riguroso e iterativo para desarrollar un conjunto de 9 herramientas de autoevaluación para optimizar la seguridad y el uso seguro de la HCE. Estas herramientas, referidas como "Safety Assurance Factors for EHR Resilience" o guías SAFER, se pueden utilizar para auto-evaluar la seguridad y eficacia de las implementaciones de la HCE, identificar áreas específicas de vulnerabilidad y crear soluciones y un cambio de cultura para mitigar los riesgos.

Como complemento al abordaje específico de los modelos anteriores, nos gustaría añadir COBIT® 5 como un marco para el abordaje global de los problemas antes comentados. Porque pensamos que los problemas TIS relacionados con la seguridad del paciente no son más que un problema de falta de alineación entre las metas de TI y los objetivos de las organizaciones sanitarias.

Por último, terminaremos con una interesantísima reflexión del señor Thomas H. Davenport (Mastering Information Management Paperback – March 24, 2000) que resume a la perfección de que tenemos que preocuparnos en realidad cuando hablamos de TIS.

"Imaginen un mundo obsesionado con la fontanería. En este extraño lugar, centenares de libros y revistas, e incluso algunos canales de televisión, cubren extensamente la actualidad del sector de la fontanería, celebrando los últimos avances en válvulas, soldaduras y cañerías. Las conversaciones de café están dominadas por el tema de si una marca de desagües vacía más rápido que otra. Los magnates del equipamiento para fontaneros aparecen en las portadas de las revistas de negocios, incluso de las publicaciones de interés general, y se convierten en las personas más ricas del mundo. Las compañías pagan millones y billones para conectar todos sus artefactos y asegurar que las cañerías lleguen a los lugares más remotos. Solamente hay un tema que en este mundo tan extraño se pasa por alto: ¡el agua! ¿Es limpia y fresca? ¿Es agua lo que los consumidores quieren beber? ¿Tienen sed?"

La estrategia “SWARMING” para la protección de datos sanitarios

Juan Díaz García, Rafael Marín Jiménez

Unidad de Gestión de Riesgos Digitales, Servicio Andaluz de Salud

La estrategia militar más efectiva también funciona cuando el objetivo es la protección de datos en particular y la seguridad de la información en general. En la actualidad, en el Servicio Andaluz de Salud, existen evidencias objetivas de adecuación a la normativa de protección de datos en diferentes áreas, que han ido surgiendo en paralelo al impulso de las estrategias de seguridad de la información, las actividades internas de sensibilización y formación.

No cabe duda que para ganar una guerra no basta con ganar una batalla por lo que resulta interesante analizar la estrategia empleada en los casos de éxito para potenciarla en el resto. Intentaremos presentar una visión lo más imparcial posible de como se ha desarrollado en nuestro sistema de salud.

“El Swarming, cuya traducción literal en castellano sería Enjambre, es una estrategia militar en la cual una fuerza militar ataca a un enemigo desde múltiples direcciones diferentes para después reagruparse. El swarming puede ser más efectivo que cualquier otra estrategia militar y permite a un ejército vencer cuando su número y equipamiento es inferior al del rival.”

Cuando nuestra misión es defender la intimidad, la privacidad, la confidencialidad y la protección de los datos personales en las organizaciones sanitarias, hemos de asumir que somos inferiores en número y que no contamos con suficientes recursos. De ahí la importancia de la optimización de los medios, de la necesidad de maximización de los beneficios obtenidos con ellos y del establecimiento de alianzas con otros incondicionales que permitan alcanzar nuestros objetivos, ya que de lo contrario podríamos ser considerados obstáculos al progreso y al desarrollo tecnológico.

Elegir unas tácticas de alineación en detrimento de otras no parece adecuado, mejor combinarlas hasta conseguir su confluencia. Es posible trabajar con la dirección siguiendo un enfoque top-down y buscar la complicidad y el apoyo del personal base aplicando un enfoque bottom-up. (Explicar)

La ignorancia, el desinterés, la falta de procedimientos, la carga de trabajo, las instalaciones, la dispersión geográfica, la ausencia de controles, la falta de reconocimiento, las prioridades establecidas, etc. son factores a tener en cuenta para focalizar las acciones a desarrollar, siempre marcando objetivos o hitos muy concretos, alcanzables y de impacto.

La estrategia debe plasmarse en un plan que contemple tácticas y cualidades eficaces como:

- Un sistema de comunicación versátil y fiable, que garantice la transmisión de información tanto a nivel interno como externo.
- Movilidad que facilite el acercamiento a objetivos distantes, poco accesibles o atrincherados. Fomentando el contacto humano y detectando las carencias y necesidades.
- Autonomía por parte de la unidad. Afecta a los recursos humanos, materiales y económicos.
- Evitar el fuego enemigo mediante perfeccionado del sistema de coordinación. La jerarquía, las funciones, los tiempos, los métodos, todo debe estar bien organizado.
- Perseverar.

El plan ha de contemplar el ataque desde múltiples direcciones, por ejemplo:

- Formación que contrarreste la ignorancia y que sensibilice a los profesionales, persiguiendo que elementos clave de otras áreas se sumen a nuestro bando y mediante sus actuaciones vayan sembrando nuevas competencias entre sus subordinados y superiores. Desde 2008 se realizan diferentes acciones de sensibilización y formación, segmentadas por perfiles profesionales y ejecutadas con metodología presencial, semipresencial y teleformación.
- Infiltración en otras unidades de la organización, estableciendo la relación como una oportunidad de simbiosis difícil de rechazar y permita alcanzar un objetivo común. Se establece una especial relación con la Agencia de Calidad Sanitaria de Andalucía para converger en estándares de acreditación que potencien el cumplimiento y las buenas prácticas en protección de datos y seguridad de la información.

- Realizar una revisión sistemática de la situación de la organización, amparados en la obligación legal de realizar auditorías. Generando como valor añadido, el plan de acción a acometer con las tareas para solucionar las no conformidades detectadas. A lo largo de estos años se han realizado varios planes de auditorías presencial en el Servicio Andaluz de Salud, afectando a hospitales, áreas de gestión sanitaria, distritos sanitarios y centros de transfusión. También se han realizado autoevaluaciones de cumplimiento y se ha automatizado mediante una plataforma digital que permite auditar en dos fases, la primera no presencial y la segunda de recogida de evidencias. En paralelo a la ejecución de estas acciones se ha ido conformando un equipo humano de profesionales de la organización, que además de desempeñar las funciones asociadas a su puesto de trabajo, actúa como auditores internos tras acreditar sus competencias como CISAs de acuerdo a ISACA.

Son precisas algunas herramientas de apoyo a las tácticas y las acciones emprendidas, como un número de teléfono y correo electrónico de contacto como un medio rápido y accesible para que los profesionales puedan consultar dudas y proponer sus ideas. Un website, intranet, que posibilite la publicación de contenidos y la localización de los mismos, un espacio para la reutilización, la información. Es conveniente disponer de una plataforma de teleformación, en esta caso accesible no sólo desde la red corporativa sino desde internet y si es posible, una herramienta automatizadas de gestión de auditorías y completándose con una plataforma colaborativa y videoconferencia, que permite salvar la dispersión geográfica y facilita la cooperación.

Repasaremos las conquistas que se han alcanzado, con el esfuerzo y mérito de muchos profesionales en diversas áreas de competencia, dando lugar a un nivel de madurez organizativo importante en la materia objeto de debate, aunque no por ello suficiente.

Hitos Internos:

- La Dirección General de Asistencia Sanitaria y resultados de salud han emitido diferentes instrucciones sobre el cumplimiento en materia de protección de datos.
- La Dirección General de Gestión Económica y Servicios ha normalizado los pliegos de contratación recogiendo especialmente el cumplimiento del artículo 12 de la LOPD.
- La Dirección General de Profesionales mantiene

desde 2007 un Plan de Concienciación y Formación en protección de datos y seguridad de la información.

- La Asesoría Jurídica informa y hace recomendaciones prácticas de casos de uso.
- La Secretaria General realizó instrucciones sobre Investigación y Videovigilancia.
- Se han definido estándares de acreditación para las competencias profesionales, Unidades Clínicas de Gestión y páginas web, relativos a la confidencialidad y privacidad en general y los particulares del cumplimiento de la normativa de protección de datos.



- Por parte de la Consejería de Salud y Políticas Sociales, a través de la iniciativa Red Salud Andalucía, se ha desarrollado la Guía de usos y estilo en las redes sociales del Sistema Sanitario Público de Andalucía.
- El Biobanco del Sistema Sanitario Público de Andalucía (SSPA) ha redactado la Guía para el uso de muestras biológicas y datos de origen humano en investigación biomédica.
- La web de procedimientos para la atención ciudadana, puesta a disposición de los profesionales del Sistema Sanitario Público de Andalucía (SSPA) por la Dirección General de Asistencia Sanitaria y Resultados en Salud. En ella pueden encontrarse procedimientos específicos para para la protección de datos de personas en situación de especial riesgo y para el de acceso, rectificación y cancelación en la historia clínica.
- La Agencia de Calidad Sanitaria de Andalucía ha establecido un Programa de Certificación de páginas web sanitarias.
- Se ha establecido una Estrategia de calidad y seguridad en aplicaciones móviles de salud, creado el Distintivo AppSaludable, como sello de garantía para reconocer aquellas aplicaciones móviles que sean fiables para los usuarios.

Especial Seguridad de la Información Sanitaria

- La Subdirección de Tecnologías de la Información del SSPA ha incorporado nuevas funcionalidades a los sistemas de información asistenciales centralizados, que permitan el ejercicio de oposición.
- Se ha establecido planes de Formación de Formadores en protección de datos y seguridad.
- Se ha creado un Grupos de Auditores CISA y expertos CISM de ISACA.
- Se dispone de una Intranet especializada en seguridad y protección de la información por la Unidad de Gestión de Riesgos Digitales, así como servicios de consultaría, etc.

Hitos Externos:

- Se colabora con la Consejería de Economía, Innovación, Ciencia y Empleo para la actualización y cumplimiento de la Política de Seguridad de las Tecnologías de la Información y Comunicaciones en la Administración de la Junta de Andalucía.
- Se participa en el Grupo de Expertos en Seguridad Digital de la J.A.
- Se ha establecido acuerdo de servicio con el Centro de detección y respuesta ante incidentes de seguridad Andalucía CERT.

- Se colabora con las asociaciones de profesiones para la difusión de estas materias como el libro "Mitos y Leyendas de la LOPD" de APISA.

CONCLUSIONES

Presentada la estrategia en este artículo, otro sería objeto para la evaluación de cada una de los hitos conseguidos, sus bondades y sus defectos, en pro de la consecución del consenso de todos los agentes implicados y persiguiendo siempre la mejora continua. Muy probablemente haya de considerarse la existencia de múltiples agentes dinamizadores en la proliferación de buenas prácticas, procedimientos, estándares de acreditación, etc, relativos a la seguridad de la información y la protección de datos personales.

La palabra clave es la Cooperación con todos los agentes presentes en nuestras organizaciones sanitarias, ya que todos pueden aportar. Debemos buscar alianzas y objetivos comunes que refuercen la consecución de nuestras metas.



Nuestros productos

GESCOT: Gestión de Costes Hospitalarios

mira: Estaciones Clínicas de trabajo

miranda: Planes de cuidados de enfermería

SAVAC GM: Gestión integral del Medicamento

BDCM: Gestión y política centralizada de productos hospitalarios

SAVAC Integración: Gestión Hospitalaria Integral (HIS)

Continuum: Gestión Integral Socio Sanitaria

SAVAC Diets: Gestión integral de Dietas y nutrición

P4H: Análisis y predicción de reingresos

Chronotime: Gestión de turnos

V Reunión del Foro de Interoperabilidad en Salud

“La nueva ola: aplicando la experiencia a los retos innovadores”

Organizado por la Sociedad Española de Informática de la Salud (SEIS), con la colaboración de red.es, Ayuntamiento de Barcelona y TicSalud, los pasados 22 y 23 de abril, la Sala de Actos Cibernàrium del Growth Center acogió la celebración de la V Reunión del Foro de Interoperabilidad en Salud. Durante el encuentro se celebraron cinco sesiones, además del acto inaugural y la clausura. La asistencia de público fue numerosa, circunstancia que demuestra que cada vez hay más interés por los retos innovadores.

ACTO INAUGURAL

La mesa estuvo presidida por **Francesc García Cuyás**, coordinador general de las Tecnologías de Información y Comunicación del Departamento de Salut de la Generalitat Catalana. Comenzó el encuentro **José Luis Monteagudo**, presidente del Comité Ejecutivo de la reunión demostrando su satisfacción personal por poder celebrar estas Jornadas Técnicas. No olvidó el agradecimiento a la Fundación TicSlut, a **María Rovira**, a **Carlos Gallego** y al Comité Organizador por “habernos preparado un programa que cubre muchos aspectos de actualidad sobre temas relevantes como es el desarrollo de la historia clínica electrónica”.

Luciano Sáez, Presidente de la SEIS agradeció la ayuda y la hospitalidad que en esta ocasión brindó la Consejería de Sanidad de la Generalitat de Catalunya y el especial apoyo de María Rovira y Carlos Gallego. Y, por supuesto a Francesc García Cuyás que presidió el acto inaugural.

Destacó el presidente de la SEIS que “nos constan los esfuerzos realizados en Cataluña en materia de interoperabilidad y cómo han priorizado estos proyectos. Fueron reconocidos con el Premio Nacional de Informática y Salud de 2014 por la creación y puesta en marcha de los estándares en interoperabilidad”.

Agradeció el responsable de la SEIS el trabajo de José Luis Monteagudo, presidente del Comité Ejecutivo y Presidente del CTN de AENOR, organi-

zación con la que la SEIS se siente muy vinculada desde hace muchos años, “no sólo por ser miembro de la misma sino también por el convenio de colaboración con el que damos soporte a la Secretaría del CTN139”. Además, expresó su agradecimiento a Adolfo Muñoz, coordinador general de esta V Reunión así como a todas las personas que han colaborado en este acto.

Anticipó Luciano Sáez que “hemos propuesto al Ministerio de Sanidad, Servicios Sociales e Igualdad la necesidad de crear un apartado especial para la interoperabilidad en el documento sobre Estrategia y Salud Electrónica que se elaboró en el seno del Consejo Asesor y la propuesta de creación de una Oficina Nacional de Interoperabilidad”.

Francesc García, durante su intervención, recordó que esta reunión sobre interoperabilidad “es como la piedra roseta para acercarnos a las TIC, dar respuesta a nuestros ciudadanos y poderles ofrecer una buena asistencia”. Se sirvió de una serie de diapositivas para explicar el sistema sanitario catalán, que es un modelo multiproveedor integrado en una sola red de utilización pública y en el que se potencia la autonomía de gestión de cada uno de los centros. “Toda la atención está centrada en el ciudadano”. Proyectó un video en el que se presentó la HC3 (Historia Clínica Compartida de Cataluña), que da apoyo a la atención adecuada y de calidad en Cataluña.

SESIÓN PRIMERA. "LA NUEVA GENERACIÓN DE NORMAS"



Moderó esta primera sesión **Jordi Gabaldà Azofra**, responsable del Centro de Competencia Tecnológica de la Direcció de Sistemes d'informació de Cat Salut.

Durante la primera intervención, **David Moner**, investigador del grupo de Informática Biomédica (IBIME) del Instituto ITACA de la Universitat Politècnica de València, presentó el estado actual y la evolución futura de la norma ISO 13606. Esta norma tiene como objetivo facilitar la comunicación e interoperabilidad semántica de la información de salud contenida en la historia clínica electrónica. La norma ha evolucionado desde su origen en una serie de proyectos de investigación europeos a comienzos de los años 90, a convertirse en norma europea y española (norma UNE-EN 13606) y desde 2008, en norma internacional ISO 13606. Desde entonces, la norma está siendo utilizada tanto para definir modelos de información clínica, por ejemplo en el proyecto de Historia Clínica Digital del Sistema Nacional de Salud en España y el proyecto de Historia Clínica Nacional Unificada en Uruguay; o para crear repositorios de historia clínica electrónica. Un buen ejemplo de repositorio nativo de historia clínica electrónica ISO 13606 está en el Estado de Minas Gerais (Brasil) donde se da servicio a una población de 20 millones de personas.

Recientemente, explicó David Moner, se ha iniciado el proceso de revisión de la norma ISO 13606 con el objetivo de realizar los ajustes oportunos que faciliten su uso e implementación, así como alinearla con otros desarrollos y estándares existentes. Uno

de los principales criterios de la renovación será evitar cambios profundos para que la transición de las actuales implementaciones a la nueva versión sea lo más transparente y sencilla posible. El proceso de renovación, en el que participan varios expertos españoles en delegación de AENOR, se espera que finalice a finales de 2016. Entre los cambios, actualmente en discusión, destaca la creación de un nuevo conjunto de tipos de datos según la norma ISO 21090, la definición de un modelo de información demográfica que sea compatible con el uso de arquetipos, la actualización del modelo de arquetipos o la creación de arquetipos de referencia acordes a la norma ISO 13940. "Con estos y otros cambios aún pendientes de estudio, la norma ISO 13606 servirá mucho mejor a su objetivo de facilitar la interoperabilidad semántica y será aún más sencilla de utilizar para el desarrollo de sistemas de historia clínica electrónica".

Francisco Pérez Fernández, presidente de HL7 España, trató la cuestión de las novedades en HL7, centrándose en FHIR (Fast Healthcare Interoperability Resources). De momento se trata solo de un borrador y se espera que el próximo año esté disponible. Comentó Pérez Fernández, que el FHIR, que es una nueva propuesta de especificación de estándares HL7 para el intercambio electrónico de información médica, tiene valor para mejorar las infraestructuras y la forma de interoperar y poder adaptarlo a los tiempos de movilidad que estamos viviendo. FHIR se presentó en San Diego en el 2011 y está construida sobre la simplicidad

de V2.x. Cuenta con estándares modernos como XLM, JSON, http, REST y UML y está tomando impulso muy rápidamente.

El presidente de HL7 España proyectó una serie de ejemplos en los que se vio como FHIR permite el acceso a datos en JSON de una manera controlada a través de HTTP. Usa V2.x porque aunque funciona V3, es más difícil. Por otro lado, HL7 V2 necesitaba una evolución. Los nuevos mercados y las nuevas necesidades son las aplicaciones basadas en Smartphone o tablets, la nube y los dispositivos personales (Wearable).

Con esta situación, el ponente manifestó que surgen preguntas: "La primera de ellas sería ¿cómo hago para que mi app en android/iOS reciba los datos de mi servidor? ¿cómo conecto mis actuales aplicaciones utilizando el almacenamiento en la nube? y, por último ¿cómo puedo estandarizar el acceso a nivel de registro a mi historia clínica electrónica?, se trata de una API gratuita, simple y abierta". Soporta escenarios comunes y la inclusión de los casos se basa en la regla del 80%, es decir que sólo se incluye en la especificación algo que pida el 80% de los implementadores. En cuanto al foco de implementación señaló que FHIR se testea antes de la publicación y que el código abierto está disponible con la especificación de Java. Además proporcionó múltiples ejemplos que resultan muy fáciles de entender. También mencionó los recursos FHIR que son unidades pequeñas de intercambio de datos, con significado y conducta definidos y ubicación conocidas, representando la unidad más pequeña de transacción. Comentó algunos ejemplos de recursos. "Otra ventaja es su legibilidad".

Raimundo Lozano-Rubí, consultor sénior del Hospital Clinic de Barcelona, disertó sobre la "Nueva versión de UNE-EN ISO 13940" (ContSys), que resulta ser una de las menos conocidas aunque continuamente se hacen referencias a ella. Es una norma que define un sistema de conceptos y que está orientada a la continuidad de los cuidados. Pretende establecer una base común de conceptos que sirva para los servicios sanitarios y que constituya el fundamento tanto para la interoperabilidad semántica como para describir los conceptos necesarios para el desarrollo de la información en el ámbito sanitario. El núcleo lo constituye la interacción entre pacientes y profesionales y considera los aspectos clínicos, de gestión y de recursos.

Después de enumerar la génesis de ContSys desarrolló el proceso clínico con sus inputs que se transforman en outputs. Las áreas que cubre son la de actores (healthcare actors), las cuestiones de salud (health issues), la actividad (activity), los procesos de salud (process), el tiempo (time-related concepts), la gestión del conocimiento y el soporte a la toma de decisiones (clinical knowledge and decision support), la responsabilidad (responsability) y la gestión de la información (health information management). Definió el consultor sénior del Hospital Clinic de Barcelona el concepto de actores sanitarios, los temas de salud que divide en health matter y health issue, las actividades cuyo objetivo es mejorar o mantener el estado de salud y los procesos que transforman los inputs en outputs. En cuanto al tiempo destacó la diferencia que hay entre periodos e episodios.

SESIÓN SEGUNDA. "NUEVAS APROXIMACIONES INNOVADORAS EN HCE: REQUERIMIENTOS EN INTEROPERABILIDAD Y SOLUCIONES PROPUESTAS"

Como conclusión expuso que se trata de una norma extensa, con un marco conceptual rico y en conformidad con la norma. Además, es imprescindible para los procesos clínicos compartidos y tiene un amplio consenso.

Moderó el debate de esta segunda sesión, **Adolfo Muñoz Carrero**, secretario del CTN139 de AENOR y delegado de interoperabilidad en la SEIS. Además es el Coordinador General de la V Reunión.

En primer lugar tomó la palabra Carlos Gallego Pérez, responsable de la Oficina de Estándares e Interoperabilidad,

TicSalut de la Generalitat de Catalunya. Presentó la Historia Clínica Compartida de Cataluña (HC3), ofreciendo muchos datos sobre la actividad de la misma: tienen más de 100 millones de documentos normalizados; mensualmente, unos 27.600 profesionales diferentes acceden al visor con unos 28.000 accesos diarios y comentó, a modo de anécdota, que mientras dura la mesa habrá unos 2.200 accesos a la HC3. 4.800 personas acceden mensualmente ya a sus datos de salud. 12.400 ciudadanos diferentes han accedido a sus datos de salud durante este año. El 100% de los centros públicos de salud está conectado a la historia compartida.

Actividades de la SEIS



“En Cataluña hay un proyecto de corresponsabilidad y el hecho de compartir ha introducido un alto grado de madurez entre los proveedores de salud lo que permite seguir trabajando en un plan de salud y en beneficio del ciudadano que se relaciona con la aseguradora, con urgencias, cuando va al hospital, etc”. Considera Carlos Gallego Pérez que “la información ya no es de una comunidad o de un servicio de salud, es del ciudadano y se comparte. Este canal de salud es un espacio de alta seguridad. El ciudadano tiene una nueva forma de relacionarse”. En cuanto al proceso, añade Gallego Pérez, se proporciona un identificador común alrededor del cual los profesionales actúan. En Cataluña todo esto lleva a la atención no presencial y termina hablando de cómo enfrentarse a la movilidad.

Pablo Serrano, director de Planificación del Hospital 12 de Octubre, comentó que la Comunidad de Madrid está evolucionando Horus como repositorio de las HCE para responder a las estrategias de atención de pacientes crónicos y continuidad de la asistencia.

En resultados anteriores se había demostrado la combinación de información de orígenes heterogéneos. Se obtiene “la foto”, una composición instantánea (ejemplo: el resumen del paciente), pero es necesaria “la película”, la secuencia son las múltiples relaciones entre “fotogramas”. El desafío, considera Pablo Serrano, es pasar de los actuales repositorios documentales, que se pueden ordenar por sus metadatos de contexto, sin significado clínico, sin navegación entre documentos ni componentes, hacia un repositorio de componentes de registro, con relaciones, tanto las convencionales

de contención como las trascendentales con significado clínico entre cualquiera de los componentes. “La principal expectativa de los profesionales sobre la información clínica es que esté ordenada con sentido clínico”.

El objetivo del proyecto ha sido la definición de un modelo de información clínica normalizado, longitudinal y de continuidad entre niveles, para un uso compartido de la HCE, a partir de los modelos de las HCE existentes. Sobre este modelo, en definitiva, “se desarrolla un nuevo módulo de visualización que marque la evolución de HORUS, que dé respuesta a las necesidades de los profesionales visualizando la información ordenada con sentido clínico pleno”, explica Pablo Serrano.

Como metodología se han utilizado las normas ISO de informática sanitaria: de conceptos de Continuidad de la asistencia (UNE-EN ISO 13940) y del modelo de HCE (UNE-EN ISO 13606). Un grupo de trabajo de expertos de los diferentes ámbitos definió un caso de uso que implica a primaria, especializada y la farmacia para pacientes crónicos en atención ambulatoria.

En la modelización se han utilizado las clases de información de contexto con sus atributos, tanto opcionales como requeridos. Se han detallado en los extractos y en los arquetipos de los componentes de registro: composición, entrada e ítem.

En los sistemas Atención Primaria, eReceta, eCita y Hospital se han identificado los campos equivalentes dentro del modelo de datos, analizando tipos de datos, opcionalidad y multiplicidad. Se ha comprobado la equivalencia para los metadatos de un repositorio de documentos IHE XDS. Se ha diseñado la ordenación y presentación requerida para

la continuidad de la asistencia combinando la información clínica con sentido. Se han identificado los componentes de 13.940 problemas de salud, motivo de contacto, evolución, alergia, reacción adversa, alerta, derivación, cita, seguimiento, estratificación, prescripción, dispensación y orden diagnóstica. Se han editado las versiones 2 de los arquetipos 13606 del CMDIC, con el contexto completo.

En el modelo se han utilizado las clases AUDIT INFO (firma y versiones) y FUNCTIONAL ROLE (autores). Para representar las relaciones se han requerido 4 tipos enlaces LINK: ordenación por problema de salud, interpretación revisada, flujo de órdenes y suplemento de información. Estos componentes de registro clínico y sus enlaces, que representan los flujos de trabajo clínico, recogen plenamente el significado existente en los sistemas actuales y prevé la evolución futura. El modelo representa los enlaces existentes y permite la ordenación de los componentes en el repositorio con sentido clínico avanzado. Además, permite la presentación que demuestre la utilidad clínica y concrete los conceptos abstractos del modelo.

Por último, **Manuel Pérez Vallina**, vicepresidente de HL7 España, Dirección Técnica de Sistemas de

Información de Sacyl habló sobre “Normalización Terminológica. Estrategia y Metodología”. Expuso que los objetivos generales son la utilización de estándares que “nos lleven a la interoperabilidad, la centralización de recursos terminológicos y la sistematización de procesos para obtener una mayor calidad”. Los objetivos estratégicos son: ayudar en la continuidad asistencial y seguridad del paciente, permitir intercambio de información normalizada entre sistemas, dar soporte a los procesos de Business Analytics y Business Intelligence, BigData y permitir crear nuevas aplicaciones relacionadas con: toma de decisiones, análisis de riesgos, investigación y estudios sobre la salud. El proyecto se ha dividido en 4 fases.

Pérez Vallina defendió como conclusiones que “la información asistencial estandarizada, recursos terminológicos sincronizados, centralizados y actualizados, mapas de procesos de gestión de recursos terminológicos y responsables de calidad y mantenimiento de los recursos terminológicos nos conduce a explotar la información asistencial e igualmente a la continuidad de la asistencia”.

Terminada las intervenciones de los ponentes, dirigido por **Adolfo Muñoz** comenzó un animado debate que hubo que cortar por agotarse el tiempo.

SESIÓN TERCERA. AVANCES DE INVESTIGACIÓN



La tercera sesión dedicada a avances en la investigación fue moderada por **Montserrat Robles Viejo**, directora del Instituto Universitario de Investigación en Tecnologías de la Información y Comunicaciones (ITACA) de la Universitat Politècnica de València, quien resaltó que conseguir un alto nivel de inter-

operabilidad es uno de los más importantes retos de cara a un uso significativo de la HCE y que el poder asegurar una consistencia a nivel de significado es un requerimiento básico para mejorar la asistencia sanitaria y el uso óptimo para investigación y docencia.

Actividades de la SEIS

En primer lugar, **Xavier Pastor**, jefe de informática Médica del Hospital Clínico de Barcelona, aportó la experiencia adquirida en su organización sobre el concepto de interoperabilidad y lo concretó en una serie de ejemplos, tanto bajo el punto de vista técnico, como semántico u organizativo. Así, puso de manifiesto que, tras un periodo en el que se han consolidado buenos modelos basados en la interoperabilidad técnica, se ha llegado a un punto en el que es necesario compartir en tiempo real el proceso asistencial. Este se extiende más allá de las paredes del hospital, conectando con diversos dispositivos asistenciales y esto obliga a plantear nuevas arquitecturas de los sistemas de información que den respuesta a las necesidades reales de los clínicos, sin abandonar lo mucho que se ha conseguido puertas adentro de las organizaciones.

Destacó Xavier Pastor el hecho de que, si bien el profesional especifica una recogida de información muy estructurada al filo de sus necesidades, posteriormente la realidad demuestra que en la inmensa mayoría de los casos se opta por el formato de texto libre en lenguaje natural con todas sus características, con lo cual, si se desea aprovechar esta información para interoperar entre sistemas de HCE y profesionales, se requiere como paso previo una extracción de conceptos contenidos en los cursos clínicos y en los informes asistenciales y representarlos debidamente. Para ello propuso como nuevo paradigma, la elaboración de recursos de conocimiento biomédico basados en ontologías y la creación de repositorios clínicos de datos del paciente que puedan ser compartidos en tiempo real por profesionales sanitarios distintos trabajando en organizaciones con sistemas informáticos diferentes. Para ello, se ve necesaria la adopción de estándares para la representación de los datos clínicos y la promoción de los repositorios de conocimiento. En este momento, el Hospital Clínico de Barcelona desarrolla una serie de proyectos piloto como la codificación automática de diagnósticos, la construcción de un servidor de conocimiento basado en ontologías (OntoKS) y un repositorio nativo conforme a la norma UNE-EN ISO 13606 de datos clínicos de pacientes (OntoCR®) accesible mediante servicios web desde las estaciones de trabajo de los sistemas de atención primaria y de los hospitales.

Roberto Somolinos, investigador de la Unidad de Investigación en Telemedicina y eSalud del Instituto de Salud Carlos III, reflexionó sobre la Anonimi-

zación de la Información Clínica para uso secundario. La historia clínica electrónica permite registrar y almacenar grandes cantidades de información clínica que también podría ser utilizada para fines secundarios (docencia, estadística, investigación). Para ello es necesario cumplir los requisitos sobre protección de la privacidad de datos que establecen las leyes de cada país. De forma general, el intercambio de datos para uso secundario sólo es posible si los datos han sido previamente anonimizados.

Explicó Somolinos que la anonimización (ISO/TS 25237) es el proceso que elimina todos los enlaces entre un conjunto de datos y el propietario de los mismos. Ya existen diversas soluciones que la implementan y modelos de clustering (k-anonimity, l-diversity, t-closeness) que cuantifican el riesgo de re-identificación de registros de-identificados.

La norma UNE-EN ISO 13606, que normaliza la transferencia de historias clínicas electrónicas entre sistemas heterogéneos, presenta algunas características idóneas para la anonimización: dispone de un paquete demográfico independiente dentro del modelo de referencia y posee un tipo de datos II para representar objetos identificadores.

La Unidad de Investigación en Telemedicina y eSalud del Instituto de Salud Carlos III, confirmó Roberto Somolinos, ha diseñado y desarrollado un sistema pseudonimizador basado en la norma UNE-EN ISO 13606 que facilita la realización de anonimización de forma sistemática de acuerdo a un conjunto de parámetros (sexo, fecha de nacimiento, lugar de residencia). Este sistema sirve como herramienta de ayuda para grupos de investigación que desean dejar disponibles los datos clínicos recopilados en sus proyectos para uso secundario de terceras partes. Estos grupos pueden seleccionar el grado de especificidad de los parámetros con los que se realiza la pseudonimización de los registros, de tal forma que se asegure que el riesgo de re-identificación sea tan bajo que los datos se consideren anonimizados.

En la conclusión de la jornada, **José Alberto Maldonado**, investigador del grupo de Informática Biomédica (IBIME) del Instituto ITACA de la Universitat Politècnica de València, presentó uno de los últimos desarrollos de la IHSDO para la explotación de SNO-MED CT. Concretamente la propuesta de lenguaje para el enlace terminológico con los modelos de información tales como plantillas, arquetipos, mensajes o formularios electrónicos de entrada de datos.

Este lenguaje se encuentra en estado de borrador aunque está muy avanzado tras casi dos años de elaboración. Define una sintaxis para especificar los dos tipos de enlaces terminológicos posibles: enlaces semánticos y de contenido (también llamados de valor). Con el primero se asocia un término de la terminología a una entidad del modelo de información para describir su significado, por ejemplo diagnóstico principal, presión sistólica, severidad, etc. Por el contrario con el enlace de contenido se indica el conjunto de posibles valores que un atributo codificado puede contener, por ejemplo todos los tipos de diabetes mellitus. Por tanto, es un lenguaje que permite definir subconjuntos. Es importante destacar además que es compatible con otras especificaciones de la IHSTDO, por un lado es una extensión de la gramática composicional la cual nos permite post-coordinar conceptos y por otro es un subconjunto del futuro lenguaje de consulta. El lenguaje permite definir expresiones complejas que combinan operadores sobre la jerar-

quía de SNOMED CT (ascendientes, descendientes) con operaciones de conjuntos (unión, intersección, diferencia), lógicas y de cardinalidad.

El grupo IBIME, añadió José Alberto Maldonado, ha desarrollado un analizador sintáctico y semántico y un motor de ejecución para este lenguaje. Actualmente se encuentra disponible una versión beta en <http://diebosto2.pc.upv.es:8080/SnomedQuery/>, la cual permite validar y ejecutar expresiones del lenguaje. El objetivo final del grupo de investigación es incorporar este lenguaje a su plataforma LinkEHR para la normalización de la historia clínica electrónica. Es un primer paso para definir enlaces terminológicos avanzados con modelos de información de historia clínica electrónica ya que actualmente todas las herramientas disponibles son muy limitadas en este tema. Ya dentro del ámbito de la investigación se pretende aumentar la capacidad expresiva de los arquetipos y plantillas al incorporar restricciones complejas sobre los datos para la validación y evaluación de la calidad de los datos clínicos.

SESIÓN CUARTA. NUEVOS DESARROLLOS COMERCIALES



Los nuevos desarrollos comerciales centraron la cuarta sesión de trabajo, que estuvo moderada por **Isidro Fàbregues i Aladren**, presidente del Forum Cis.

En primer lugar habló **Félix Villar**, socio director de IN2, sobre "Interoperabilidad con dispositivos móviles wearables". Expuso que "hasta el día de hoy se entiende la Interoperabilidad como la capacidad de los sistemas de información sanitarios de inte-

grarse para poder compartir toda la información de los pacientes recogida por los profesionales de la salud, es decir, la historia clínica electrónica compartida. La Interoperabilidad por lo tanto es un trabajo colaborativo entre los centros sanitarios, ya sean hospitales, centros de asistencia primaria, centros privados, o centros de diagnóstico por imagen, para llevar a cabo una mejor atención al paciente y garantizar la seguridad de sus datos".

Con los avances en tecnología y los distintos dis-

Actividades de la SEIS

positivos, añadió Félix Villar, "los pacientes también generan otros datos de salud que ya no provienen de fuentes médicas". Estos datos, que suelen ser generados de forma constante, provienen de aplicaciones en dispositivos móviles o wearables que disponen de múltiples sensores en contacto con la piel que permiten conocer el pulso (frecuencia cardíaca), saturación de oxígeno, temperatura, si se descansa adecuadamente... y lo que depare el futuro (hematocrito, recuento leucocitario, número de plaquetas...), es decir, "información muy valiosa para el seguimiento y para la salud preventiva de los pacientes que de ser incorporada en la historia clínica electrónica compartida aportaría aún mayor valor".

Este nuevo paradigma, entiende el socio director de IN2, "nos plantea nuevos retos, en primer lugar el enorme volumen de información no estructurada que deberemos procesar separando el polvo de la paja, en este punto las nuevas tecnologías de BIG DATA pueden ser la solución. Por otro lado tenemos la fiabilidad de los datos, para garantizarla deberemos establecer mecanismos para controlar el origen y certificar aplicaciones y dispositivos. Y por último, la identificación unívoca de los pacientes/ciudadanos de manera que sepamos en cada momento a quién corresponde la información que se está suministrando al sistema, más que un problema tecnológico es un problema político que implicará el establecimiento de acuerdos de confianza entre las partes certificados por un tercero".

Las ventajas del sistema "son obvias" y se traducen, a juicio de Félix Villar, en una "mejor información para el personal sanitario, seguimiento de la adherencia al tratamiento, empoderamiento del paciente en el cuidado de su salud, poder aplicar con mayor facilidad y garantías políticas de salud preventivas y predictivas personalizadas a cada paciente".

Sobre "HealthShare Personal Community" intervino **José Carlos Ruiz**, Project Manager Iberia, InterSystems Iberia S.L. InterSystems HealthShare Personal Community ofrece a las empresas y a las redes de información de atención sanitaria una solución completa y ampliable como apoyo para la creación de comunidades de pacientes activos y comprometidos.

Después de la etapa de "interoperabilidad" para conectar a los profesionales adecuados, de forma que dispongan en sus entornos de toda la información de los pacientes, llega una nueva etapa en la que nuevos agentes, no sólo personal de asistencia sanitaria, necesitan tener una visión com-

pleta de la información del paciente. Uno de los más importantes es el propio paciente, "al que ya no le basta con ser un mero observador de su salud y de sus cuidados", concluye José Carlos Ruiz y añade que "al nuevo perfil de paciente lo denominamos paciente comprometido y éste gestiona activamente y de manera informada su salud y su bienestar, así como los de otras personas a su cargo. Revisan y gestionan las historias clínicas, se informan de las condiciones, adoptan hábitos saludables, adquieren productos sanitarios con información suficiente e interactúan con los proveedores sanitarios como socios".

Personal community es un módulo del ecosistema de productos HealthShare, que facilita la interconexión de múltiples agentes como generadores y/o consumidores de información.

Entre sus funcionalidades destacan:

- Cronograma personal de salud intuitivo y visual con toda la información clínica, social y administrativa.
- Mensajería segura para comunicación con profesionales de entidades de salud.
- Registro seguro y gestión de representantes legales (para casos de menores o incapacitados).
- Servicios administrativos adicionales, como citación, registros de lista de espera o renovación de medicaciones.
- Contenido educativo personalizado, donde el paciente puede seleccionar entre canales de su interés y tiene acceso a un calendario de eventos y citas personales en cualquier centro de la red sanitaria.

Toda la arquitectura interna de la herramienta está basada en estándares, destacando el uso de FHIR (estándar de HL7 para interoperabilidad granular), mediante servicios REST en formato JSON. Además HealthShare está certificado en la mayoría de circuitos IHE disponibles.

El acceso a la información puede hacerse a través de web y también está optimizado para acceder por medio de dispositivos móviles como tabletas o teléfonos inteligentes.

Personal community avanzó José Carlos Ruiz ya está siendo utilizado en tres organizaciones del noroeste de los Estados Unidos (Hixny, Baystate Health y Hunteerton Healthcare) y la plataforma de HealthShare tiene una fuerte presencia en los estados de Texas, New York, Missouri, Illinois y Rhode Island. Además en Europa HealthShare gestiona la historia nacional de salud de Suecia (9.400.000 pacientes) y hay proyectos de implantación en Reino Unido.

La cuarta sesión de trabajo concluyó con la intervención de **Andrea Barbiero**, consultora TIC de BITAC MAP SL, que presentó el “Estudio del impacto de la transición de CIE9 MC a CIE10ES en los sistemas de información de las autoridades sanitarias”.

BITAC MAP, de la mano de Andrea Barbiero, presentó su cartera de servicios. BITAC MAP es un referente en la implantación de servicios terminológicos especializados que permiten a los profesionales de la salud compartir su información en entornos de e-Salud. Proporcionan a través de herramientas y servicios propios, la posibilidad de minimizar el coste y la complejidad de la adopción de estándares terminológicos dentro de las organizaciones sanitarias.

Están focalizados en promover y facilitar la interoperabilidad semántica; liderar la adopción y consolidación de terminologías tales como SNOMED-CT y LOINC; y actualmente se encuentran centrados en acompañar de sus clientes en la inminente transición del cambio del sistema de codificación clínica CIE9MC a CIE10ES. Esta transición, explicó Andrea Barbiero, implica un cambio en tres dimensiones: organizativa en cuanto al

cambio de los procesos actuales de trabajo de las organizaciones; en relación a la formación sobre la nueva codificación que los diferentes profesionales requerirán; y en relación a los sistemas de información sanitarios.

BITAC colabora con las diferentes administraciones y organizaciones sanitarias en mitigar el riesgo relacionado con esta transición a través de sus servicios de “Estudio del impacto de la transición de CIE9 MC a CIE10ES (MC/PCS) en los sistemas de información de las organizaciones sanitarias”.

Para garantizar la información asistencial y económica es necesario el análisis del estado actual de los Sistemas de Información (HIS, explotación de datos, etc.) involucrados en las organizaciones sanitarias de cara a la adaptación a la nueva codificación clínica.

Para llegar, BITAC MAP plantean el análisis en tres fases metodológicas:

- Análisis y diagnóstico de la situación actual.
- Valoración de los Sistemas de Información.
- Resultados de la valoración, obteniendo un foto completa de las necesidades a cubrir en lo referente a Sistemas de Información en cada uno de las organizaciones sanitarias.

SESIÓN QUINTA. IMPACTO DEL USO DE CIE10 EN LOS SISTEMAS PÚBLICOS



Mercedes Alfaro Latorre, subdirectora general de Información Sanitaria e Innovación del Ministerio de Sanidad, Servicios Sociales e Innovación, moderó la mesa dedicada al “Impacto del uso de CIE10 en los sistemas públicos”. En su intervención avanzó que

en el Ministerio de Sanidad, con objeto de intentar apoyar todo este proceso de cambio, los trabajos preparatorios se iniciaron en el 2009 cuando ya se supo que la CIE9 MC iba a dejar de ser actualizada y que no quedaba más remedio que migrar hasta

Actividades de la SEIS

otro sistema de clasificación, se comenzó reuniendo a las CCAA para encontrar un primer consenso técnico al cual se llegó en cuanto a plazos y necesidades. En el Ministerio “se intentó disponer de los materiales de referencia”, explicó Mercedes Alfaro Latorre. Por otra parte, añadió, “se han iniciado ya algunas actividades de formación tanto a la pública como a la privada. Se han organizado tres foros con expertos de varios países. Además los sistemas de información de carácter estatal los estamos adaptando”. El Ministerio, también intenta dar a las CCAA una ayuda económica para que el cambio sea menos gravoso.

El Jefe del Servicio de Documentación Clínica de la Xerencia de Xestión Integrada de Pontevedra, José **Antonio Falagán**, disertó sobre los cambios para pasar del CIE9-MC al CIE10-S. Realizó un breve repaso de lo que son los sistemas de información referidos a los hospitales en los que se basan en el paciente y fundamentalmente a dos preguntas: qué le pasa al paciente (diagnósticos) y qué le hemos hecho (procedimientos).

La información que se debe recoger se estableció en 1987 con el CMBD. Previamente, en septiembre de 1984 se publicó una orden del Ministerio de Sanidad por la que el informe de alta se decide que sea obligatorio. Posteriormente el CMBD se recogía de este informe de alta o de la propia historia clínica.

Falagán explicó que la CIE es la herramienta que permite traducir conceptos relevantes expresados en lenguaje natural a otro documental a base de códigos, básicamente numéricos. Se desarrolló en EEUU en 1977, el mismo año en que fue aprobada como sistema obligatorio por el Consejo Interterritorial. Con el tiempo, llegaron las actualizaciones por la aparición de nuevos códigos aunque mantenía la misma estructura pero aparecen problemas de actualización de las tablas y notificación de novedades a los codificadores. En España aparecieron 9 ediciones.

Comparó José Antonio Falagán las diferencias estructurales entre CIE-9-MC a CIE-10-ES y explicó el código de diagnósticos y el código de procedimientos que tienen una estructura de 7 caracteres, que según su posición tiene un significado distinto. Puso múltiples ejemplos sobre los procedimientos de CIE-9-ES y la CIE-9-MC y una interesante explicación sobre el procedimiento de Whipple.

Como resumen concluyó que un código CIE-9MC es igual a 8 códigos CIE-10-PCS.

Según Falagán los retos que se presentan son:

- Formación del personal codificador.
- Difusión entre los clínicos.
- Adaptación de los programas de codificación y explotación.
- El problema singular de la Lista de Espera Quirúrgica.
- Reformulación de los Sistemas de Información basados en la codificación.

Montserrat Bustins Poblet, responsable de la División de Análisis de la Demanda y la Actividad de la Generalitat de Catalunya, tomó la palabra para hablar del impacto del uso de CIE 10 en los sistemas públicos que afecta a todos los registros de morbilidad, tanto del CMBD en todos los ámbitos hospitalarios como el CMBD en el sector socio sanitario: salud mental, atención primaria, emergencias y farmacia. Hay impactos seguros en la disminución de la calidad y de la productividad, así como retrasos en los envíos.

Tras el encuentro con los responsables de los hospitales para analizar las consecuencias de los cambios, Montserrat Bustins Poblet comentó el impacto sobre la financiación de los centros sanitarios y afirmó que la experiencia demuestra que un cambio significativo en los sistemas de información supone que los datos pierdan calidad, afectando más a los dispositivos con recursos menores. Sobre el análisis de la información los impactos van a las modificaciones en todos los repositorios de información.

En 2016 se llevará a cabo un pilotaje en varios hospitales con la doble codificación para agrupar la actividad y valorar los cambios más significativos en la financiación. Además tendrán en cuenta hacer los ajustes necesarios para no poner en peligro la buena marcha de los centros, concluyó Montserrat Bustins Poblet.

Manuel Regaña Valero, coordinador TIC de la Subdirección de Sistemas de Información para la Salud de la Consejería de Sanidad de la Generalitat Valenciana, disertó sobre la transición de CIE9-MC a CIE10-ES. Consideró que “en la transición a la nueva clasificación clínica CIE10-ES, un aspecto que requiere de un profundo análisis es el de los Sistemas de Información, que cubren los requerimientos de servicio de la Conselleria de Sanitat (CS), y que se encuentren directa o indirectamente implicados en la adaptación a la nueva codificación”.

Según el MSSSI es imprescindible que todos los Servicios de Salud autonómicos estén adoptando medidas para posibilitar el correcto cumplimiento de lo dispuesto en el Real Decreto y llevar a cabo

esta transición en los centros sanitarios, tales como:

- La adaptación de los modelos de datos de los sistemas de información hospitalarios al nuevo modelo RAE-CMBD y a la nueva clasificación.
- Verificación cumplimiento de planes de formación para codificadores y usuarios de la nueva clasificación.
- Desarrollo o adaptación de herramientas de soporte incluyendo aplicaciones de ayuda a la codificación con la nueva clasificación.

Para abordar las medidas necesarias para cumplir lo dispuesto en el punto 1, “necesitaremos alternativas temporales tales como realizar la codificación en CIE10-ES a través de herramientas preparadas para ello pero sin integrarse con los sistemas clínico/asistenciales y posteriormente ir revertiendo la medida y llegar la codificación CIE10-ES de nuevo al origen, esto es, a los sistemas de HCE”, explicó Regaña Valero. El punto 3, añadió, supone un reto aún mayor, ya que asociado a esta transición está la evidencia de no continuidad de las revisiones de la

CIE9-MC, es decir, la paulatina desaparición del uso de esta clasificación en los SS. II. Así, los principales puntos de atención deben ser:

- Código fuente afectados.
- Bases de datos.
- Integraciones.
- Extracciones de información (ETL y BI).

El proyecto de transición, desde el punto de vista de SS. II., debe tener como principales objetivos:

- Ofrecer una relación completa del grado de afectación de los SS.II.
- Establecer prioridades.
- Conseguir el apoyo de la Dirección.
- Mantener un grupo dedicado a la coordinación de las distintas tareas.
- Plantear alternativas de abordaje según priorización del MSSSI (big-bang, doble codificación, periodo transitorio,...)
- Diseñar hoja de ruta de la transición a CIE10.
- Proponer soluciones corporativas a implementar por los diferentes SS. II.

CLAUSURA



Adolfo Muñoz, como Coordinador General del Foro, inició el discurso final con el turno de agradecimientos: a los anfitriones por su buena acogida, centrándose en **María Rovira**, como coordinadora del Comité Local por toda su labor; a los patrocinadores sin cuya contribución el Foro no sería posible; a los ponentes y moderadores “porque comunicando su saber y experiencia construyen el encuentro”, a CEFIC por la ayuda pres-

tada y, por supuesto, a todos los asistentes, “razón última de que, año tras año, se siga celebrando el evento”.

Por su parte, **Mercedes Alfaro** agradeció a la SEIS el trabajo que viene realizando señalando que sus acciones “son sinérgicas” con el trabajo del Ministerio de Sanidad, Servicios Sociales e Igualdad.

García Cuyás dio por finalizado el foro.

XII Foro de Seguridad y Protección de Datos de Salud

“El ciclo de vida del Big Data sanitario: del internet de las cosas a la Protección de datos desde el diseño”

La Sociedad Española de Informática de la Salud (SEIS) celebró, los pasados 24 y 25 de marzo, un nuevo Foro de Seguridad y Protección de Datos, con la colaboración del Gobierno de Aragón. Más de 150 personas asistieron al encuentro que se estructuró en cinco sesiones, además del acto inaugural y la clausura. La SEIS repitió escenario –Sala de Conferencias y Exposiciones del Gobierno de Aragón- donde se celebró la IV Reunión del Comité Técnico de Seguridad de la Información Sanitaria.

MESA INAUGURAL



Estuvo compuesta por Luciano Sáez, Ramón Miralles, María José Blanco, Iñaki Pariente y José Antonio Gil-Lahorra.

Luciano Sáez, presidente de la SEIS, confirmó que la Sociedad Española de Informática de la Salud está celebrando, anualmente, estos Foros de Seguridad y Protección de Datos. El primero se celebró en el 2004. “Su objetivo era y lo sigue siendo compartir experiencias y conocimientos sobre un tema tan importante como la protección de datos de salud”,

defendió el presidente. Confirmó el presidente que se había celebrado una reunión del Comité Técnico de Seguridad de la Información Sanitaria en la que, entre otros temas, se aprobó un documento de concienciación de directivos sanitarios en materia de seguridad de la información.

Ramón Miralles, representante de la Autoridad Catalana de Protección de Datos disculpó a la directora de la misma, María Àngels Barbará i Fondevilla que no pudo estar presente en el acto inaugural.

Defendió la continuidad del Foro a lo largo de estos doce años y añadió que en esta edición se va a hablar de un tema que puede ser del futuro como es Big Data. "Sin duda vamos a asistir a un Foro de sumo interés".

María José Blanco, secretaria general de la Agencia Española de Protección de Datos, opinó que en estos años ha madurado el concepto de protección de datos y que desde la reunión anterior se han producido hechos muy importantes. "Internet ha cambiado el marco de nuestra sociedad", señaló.

"Tenemos muchos retos por delante y necesitamos un marco legal". Destacó que no solo se trata de resolver los interrogantes, sino que "es necesario hacer una reflexión sobre los límites de la tecnología que utilizamos".

Iñaki Pariente, director de la Agencia Vasca de Protección de Datos, señaló que este tipo de encuentros tienen un diseño muy "interesante" ya que reúne a empresas, administración y agencias, que son las entidades más involucradas en el tema. Consideró que "estamos en un momento crucial con respecto a los datos vinculados a la salud, cada vez se generan más datos y por ello Big Data es el presente y el futuro. Aspiro a aprender de todos".

José Ángel Gil-Lahorra, gerente del Sector III del Servicio Aragonés de Salud, recordó que desde que fue médico de primaria en Fuerteventura ya se interesó por la recogida de datos de pacientes y su tratamiento. "En el momento actual, las TIC nos permiten manejar una enorme cantidad de información que requiere confidencialidad. El Gobierno de Aragón va a publicar una orden para garantizarla".

SESIÓN PRIMERA. SOLUCIONES TECNOLÓGICAS PARA LA SEGURIDAD EN SALUD



María Ángeles Rincón Viñegla, directora general de Nuevas Tecnologías del Departamento de Industria e Innovación del Gobierno de Aragón, fue la encargada de moderar la sesión.

Intervino en primer lugar **Gonzalo Salas Claver**, Senior Manager de Sistemas Informáticos Abiertos, que dedicó su intervención a "La concienciación como pilar estratégico de la seguridad: canales y medios", idea en la que intentó centrarse y ver dónde se está para poder desarrollar un centro de concienciación.

Informó de que tienen múltiples entornos (primaria, receta electrónica, etc.) que interactúan con la historia clínica electrónica, con el historial de farmacia y en definitiva con el SNS. También se ocupan de la investigación y docencia centrada en ensayos clínicos.

En diversas diapositivas mostró varios casos en los que no se ha actuado con la suficiente seguridad. Citó el caso de una funcionaria que divulgó la historia clínica de su marido, estudiante de medicina, entre otros ejemplos. Según Salas Claver hay tres

Actividades de la SEIS

tipos de responsabilidades: la administrativa, la civil y la responsabilidad patrimonial del Estado.

Concluyó enumerando que para abordar un plan de concienciación es necesario: definición y alcance, diseño del material, ejecución del plan y medición del éxito.

Julio Vivero, jefe de Área de Consultoría e Infraestructura de GMV, dedicó su tiempo a "Big Data y la Seguridad de la Información del entorno Sanitario". Habló de los riesgos en Big Data mencionando que el proveedor maneja la información, el posible acceso de terceros y las nubes públicas con equipos compartidos. La forma de evitar los riesgos, según Vivero, sería confiar en el proveedor, mantener una política de seguridad, transparencia en los procesos y creatividad. Citó las ventajas de Researchkit o Google Wallet. Gracias a Big Data y Google se puede predecir, por ejemplo, la evolución de la gripe, en función de las búsquedas.

En cuanto a Big Data y su relación con las redes sociales, comentó Julio Vivero que en LinkedIn hay más de 100 ingenieros trabajando únicamente en el motor de recomendación de contactos, Facebook puede predecir el futuro de una pareja y Twitter ofrece una forma potente de predecir tendencias y revueltas.

El ponente concluyó que cada vez hay una mayor dependencia de proveedores de servicios de Internet. Se incrementan las capacidades pero también los riesgos. "Hay que contemplar un doble enfoque, como consumidor o como cliente. Como cliente, es vital gestionar los riesgos, conocer el proveedor y sus políticas y establecer contramedidas". Como consumidor si bien Big Data "tiene numerosas ventajas como la cantidad de datos, alcance, visibilidad, también se debe ser crítico con los datos propor-

cionados".

Juan Díaz, coordinador del Comité Técnico de Seguridad de la Información Sanitaria de la SEIS, habló del CTSIS, la red de responsables de seguridad de la información en salud. Según una encuesta se ve "el grado poco avanzado de la seguridad de la información", apostilló Díaz. Al tiempo, informó sobre ANTHEM, la principal aseguradora de EEUU. "Su presidente dice a los miembros de la misma que la protección de los datos personales, financieros y médicos es una prioridad para la empresa, a pesar de haber perdido, por un ataque cibernético, 78 millones de datos", compartió Juan Díaz. Sobre el futuro opinó que hay que transmitir confianza en la seguridad de la información, que es preciso crear un modelo organizativo de la seguridad de la información y garantizar la firma electrónica.

Juan Miguel Signes Andreu, miembro del Comité Técnico de Seguridad de la SEIS que coordina junto con Juan Díaz, defendió que "nunca antes que ahora, tantas cosas habían dependido de las TIC, sobre todo la actividad asistencial". Por ello ha sido necesario actuar para aumentar la confianza en las TIC. Citó el caso de condenas de dos años de prisión, cinco años de inhabilitación y unas multas muy elevadas, no por difundir información confidencial de los pacientes sino por el hecho de haber accedido a la información sin estar habilitados para ello. Por ese motivo, un grupo de profesionales pertenecientes a varias sociedades científicas, se reunieron en Valencia hace tan solo unos meses y aprobaron el Manifiesto de Seguridad y Privacidad para los datos asistenciales con el objetivo de garantizar la privacidad y seguridad de los datos de los pacientes. En el manifiesto se enumeran los dieciocho principios que deben regir la gestión de la seguridad.

SESIÓN SEGUNDA. LAS FUENTES DEL BIG DATA. EL INTERNET DE LAS COSAS

La sesión fue moderada por **Iñaki Pariente** de Prada, director de la Agencia Vasca de Protección de Datos.

Aitor Moreno Fernández de Laceta, del Instituto Iberoamericano de Innovación fue el primero en hablar enumerando lo que su empresa está haciendo sobre la salud. Llevan diez años dedicados a Big Data y durante ese tiempo han pasado del control al caos. En el momento actual "dejan que los profesionales médicos escriban lo que quieran y que

sean sistemas inteligentes los que normalicen esa información", adelantó Moreno Fernández. "Ahora se guarda toda la información y aquel que sea capaz de manejar la más relevante, en el momento adecuado para aplicarla en una toma de decisión, es el que triunfará".

Citó Moreno Fernández de Laceta el Big Analysis → sistemas de apoyo a la decisión y la validación de teorías científicas-. "Hay que saber sacar los datos relevantes y no toda la información ya que hay mucho ruido y también hay que dejar que las máqui-



nas hagan el trabajo de análisis de la información. El tiempo dedicado para analizar los datos en cualquier sector, como en sanidad, es ingente”, precisó. Habló sobre algunos ejemplos de proyectos dedicados al cuidado y vigilancia de los pacientes, así como el trabajo que están desarrollando para Osakidetxa, persiguiendo una teleasistencia inteligente. Para finalizar, citó a Lynx y mencionó que “tienen plataformas para resolver un gran número de temas”.

Concepción Sánchez Montero, representante para España y Portugal de Fitbit, expuso las ventajas de las smartbands. Lo que diferencia a Fitbit, según la ponente, es “la variedad, innovación, compatibilidad, comodidad y marca, que refuerza todos los niveles de fitness”.

La tercera intervención corrió a cargo de **Jesús Gago Centeno**, director de Desarrollo de Negocio de Big Data y Análisis de IECISA. Empresa que lleva muchos años posicionada como socio estratégico para la modernización del sector sanitario. Comentó Gago Centeno que Big Data y el IoT son tecnologías que usadas “adecuadamente” pueden contribuir a la mejora de la gestión en sanidad, a la innovación en salud y en general al bienestar social. Citó el proyecto AD-TIPS que están desarrollando para mitigar el alto impacto social y económico que la enfermedad de Alzheimer supone. En su

opinión, discernir el mejor tratamiento es complejo por la cantidad de factores a tener en cuenta: comorbilidades, factores de riesgo, resistencia al tratamiento, medio social, intolerancias, suspensión de la medicación, efectividad a corto y largo plazo, etc. En este proyecto se usan las tecnologías Big Data para gestionar este volumen creciente de información con tres objetivos:

- Tipificar segmentos de pacientes con el mayor detalle posible, a partir de toda la información disponible.
- Identificar empíricamente tratamientos “idóneos” de acuerdo a diferentes métricas: efectividad, coste, calidad de vida, prevención de la exacerbación, y conformidad.
- Usar este conocimiento terapéutico acumulado para proporcionar información personalizada a través de dispositivos portátiles a disposición tanto de pacientes como de cuidadores.

Otro proyecto que comentó Jesús Gago Centeno fue text mining de historias clínicas que consiste en la extracción de datos estructurados de la información a partir del texto en lenguaje natural contenido en historias clínicas y otros documentos asistenciales.

Para cada paciente hay ya muchos datos presentes en la codificación sanitaria: patología, procedimientos, diagnóstico, terapia, etc. Esta información combinada con la experiencia del profesional se

Actividades de la SEIS

usa actualmente para mejorar las prescripciones y actuaciones sanitarias.

Señaló que puede haber mucha más información relevante en los textos que redacta el profesional del caso clínico. Esta información está disponible solo en lenguaje natural y puede incluir datos de mucho interés como son hábitos vitales del paciente, otras patologías, incidencias en la administración de fármacos, factores sociales, etc.

IECISA aplica la tecnología de OCR y text mining para obtener información estructurada del texto disponible en historias clínicas de pacientes con objeto de segmentar con mayor precisión el universo de pacientes para cada patología y asesorar al profesional en la elección de la mejor terapia para cada caso.

“Si hoy por hoy tenemos problemas para señalar con seguridad qué datos son relativos a la salud, el cruce y análisis masivo de datos hará esta operación mucho más difícil”

El ponente **Xesús Pérez López**, profesor de la Universidad Rey Juan Carlos de Madrid, intervino en su calidad de asesor jurídico de proyectos de investigación industrial, aludió a las dificultades que implica la recogida de datos de salud para el despliegue de proyectos industriales de investigación en un contexto “Big Data”, partiendo de su propia experiencia en los proyectos ANR.

Se trata de proyectos multi-actores franceses, en los que colaboran grandes empresas y Pymes con diferentes organismos de investigación públicos y con Fuerzas y Cuerpos de Seguridad del Estado, con la finalidad de crear un prototipo industrial funcional. El Estado cofinancia el proyecto a través de la Agence Nationale de la Recherche, con tres condiciones: una, que exista un interés público en el prototipo; dos, que el Estado sea copropietario de los resultados; y tres, que exista un acompañamiento jurídico cuando el sistema a desarrollar sea susceptible de presentar un perfil problemático desde el punto de vista del derecho de la protección de datos.

Destacó Xesús Pérez López que la presencia de juristas en los proyectos permite la implantación de un acompañamiento “privacy by design”. Éste consiste en identificar las funciones del prototipo susceptibles de generar una problemática importante desde el punto de vista de la protección de

datos; y en proponer, sobre la base de un intercambio con los desarrolladores, soluciones técnicas que imposibiliten, en la medida de lo posible, cualquier uso exorbitante del sistema final.

El ponente aludió especialmente a su experiencia en el proyecto ANR ROLOSEP, dirigido por el Grupo Airbus, que consiste en desarrollar un sistema de geolocalización personal robusto que debe operar en condiciones extremas (humo, fuego, interior de edificios o bajo tierra, etc.), destinado principalmente a los bomberos, a la policía y a los trabajadores aislados de la EDF. Lo que es más interesante, con la finalidad de garantizar la seguridad de los portadores, el sistema recupera datos fisiológicos del portador mediante captosres especiales y los envía al puesto de mando, de modo que el status físico del portador sea monitorizado en todo momento desde el mismo.

El asesor jurídico de proyectos de investigación industrial destacó dos problemas que centraron la atención de los juristas en lo tocante a los datos relativos a la salud de las personas. En primer lugar, una parte de los problemas jurídicos tienen que ver con la categorización de los datos fisiológicos recuperados por el sistema como datos de salud o como simples datos personales, al tratarse de un sistema que, sin estar directamente ligado al ámbito sanitario, pueden suministrar datos de salud al responsable del tratamiento. En segundo lugar, el sistema ROLOSEP se cuenta entre los sistemas que recogen datos de salud e integran otros tipos de datos personales al mismo tiempo, como, por ejemplo, datos de geolocalización. Esta acumulación de datos diferentes multiplica la información que puede obtenerse del sistema y complica así la consideración jurídica de estos sistemas. Ambos problemas son comunes a casi cualquier “wearable” orientado hacia la salud (e-health, quantified self).

El ponente señaló cómo la aplicación de un enfoque “Big Data” es susceptible de exigir un esfuerzo “mucho mayor” para encontrar un marco viable. Por una parte, “si hoy por hoy tenemos problemas para señalar con seguridad qué datos son relativos a la salud, el cruce y análisis masivo de datos hará esta operación mucho más difícil”. Por otra, si la integración de dos fuentes de recogida de datos supone una gran complicación desde el punto de vista jurídico, “¿qué nivel de complicación se alcanzará cuando se emplee un enfoque “Big Data” para analizar los datos recogidos por una “Smart City”, es decir, por una ciudad entera repleta de captosres?”.

SESIÓN TERCERA. CASOS PRÁCTICOS



Los casos prácticos de la experiencia de las autoridades de protección de datos centraron los contenidos de la tercera sesión. Estuvo moderada por **Pedro Alberto González González**, responsable del registro de ficheros y nuevas tecnologías de la Agencia Vasca de Protección de Datos. El objetivo, apuntó, es “compartir lo que han sido casos reales analizados y resueltos en el último año por las Autoridades de Protección de Datos y que nos pueden servir como paradigma”.

Los ponentes que participaron en la tercera sesión fueron: **Ana Aperribal Ulacia**, jefa de la Asesoría Jurídica de la Agencia Vasca; **Andrés Garijo**, instructor en la Subdirección General de Inspección de datos de la Agencia Española y **Carles San José i Amat**, jefe del Área de Inspección en la Autoridad Catalana.

Andrés Garijo explicó un caso que tiene que ver con las justificaciones de las ausencias de trabajo. En la Diputación de Salamanca se exigía a sus trabajadores que al cuarto día de ausencia al trabajo deberían aportar un certificado de un médico del sector público donde figurara la patología, las prescripciones y la duración de la ausencia. Durante la investigación del procedimiento se concluyó que no hay ninguna ley que habilite el tratamiento de estos datos ya que la LOPD determina que los datos de salud deben estar protegidos. Se publicó que en este caso se había infringido la ley.

Ana Aperribal comentó que tiene varias consultas vinculadas al tratamiento de datos para ITs y para baja laboral. Mencionó un caso en el que se exige no solamente el parte de baja sino también, por parte de la administración, informe del médico de primaria. La cuestión estaba relacionada con el cobro del 100% de las prestaciones de IT por contingencias comunes. Es estos casos se exigía un informe del médico, lo cual resultaba a todas luces excesivo.

Otro caso explicado por la jefa de la Asesoría Jurídica de la Agencia Vasca guardaba relación con el uso de la historia clínica para resolver cuestiones de responsabilidad patrimonial. La historia clínica, sin duda es el documento más relevante de cualquier paciente, con una finalidad asistencial. Y también es la prueba reina que puede servir para evaluar la asistencia dispensada y es fundamental cuando se trata de probar una mala praxis. En este caso, un ciudadano presentó una reclamación por mala praxis (extracción pieza dental equivocada). El instructor del expediente para resolver el expediente de responsabilidad patrimonial reclamó información del servicio afectado. Se remitió e incorporó al expediente la totalidad de la historia clínica, consistente en más de 150 páginas sobre otras patologías (dándose la circunstancia de que, además, en ninguna parte de la historia aparece el episodio que genera el expediente). Este caso está suficientemente claro y se entiende que solicitar la historia clínica completa resulta excesivo. El instructor cumple con

Actividades de la SEIS

pedir el informe del servicio correspondiente. Se sancionó al Servicio Vasco de Salud. Es un ejemplo de la calidad.

El moderador propuso a partir de las intervenciones anteriores pasar al principio de derecho de acceso a la historia clínica por parte del ciudadano.

Andrés Garijo comentó el caso de una paciente que solicitó su historia clínica al servicio de salud donde había sido tratada, pidiendo que, por vivir en otra ciudad, se la mandara por correo certificado. La clínica, debido a la naturaleza de los datos consideró que no era el medio adecuado para darle la información solicitada, sugiriendo que la interesada se trasladara al centro y allí poder acreditar su personalidad. La Agencia entendió que la solicitud de esta paciente estaba ajustada a derecho y ordenó al centro de salud que mandara la historia por correo certificado.

Se citó, también, el caso de otra paciente que quiso acceder a su HC y en este caso, el odontólogo que la trató le mandó un informe en el que se recoge todo el proceso asistencial. La solicitante no queda conforme porque ella quiere la HC completa. El médico alega que el informe es mucho más entendible que la historia. La señora también pedía unas radiografías digitales alegando el médico que como no las había pagado, no se sabe la causa de la gratuidad, eran de su propiedad. Estudiando el caso, la Agencia estimó la reclamación, entendiendo que el hecho de haberlas cobrado o no, no afecta al derecho de acceso a la HC.

Las intervenciones sobre el derecho de rectificación o cancelación comienzan con **Carles San José i Amat** quien citó el caso de una persona que fue atendida en un hospital y una vez finalizada la asistencia se le hizo un informe de alta en el que constaban datos relativos a trastornos de personalidad y conducta paranoide, así como antecedentes de tóxicos y un consumo abusivo de alcohol hace 30 años. La persona atendida consideraba excesiva esta información y se solicitó la cancelación de esa información en el informe de alta. La primera consideración a tener en cuenta es el tiempo de conservación de la información médica, que para el informe de alta es de 15 años. Respecto de la información de ese proceso asistencial, se negó la cancelación y además el hospital esgrimió de manera razonable la necesidad, desde el punto de vista médico, de conservar esos datos y por lo tanto se desestimó la reclamación en esa parte. Pero, por otro lado, en el informe de alta se mencionaban antecedentes de 30 años atrás. Aquí

no se podía tener en cuenta los 15 años porque se trataba de una información que había superado ese plazo. No obstante, el hospital justificó la necesidad de esa información amparándose en la pertinencia de aquella información para evaluar la situación actual del paciente. En consecuencia, se desestimó la petición de esa rectificación, respetando el criterio de los profesionales médicos.

Ana Aperribal Ulacia defendió que el derecho de acceder y cancelar los datos de salud es un derecho de todo ciudadano. Explicó un caso, de hace tiempo, en el que estimaron la rectificación porque la administración sanitaria no justificó en ningún modo las razones por las que las solicitudes de rectificación que formulaba la persona no se podía llevar a cabo. En este caso lo que reclamaba era el cambio en la historia clínica de "acoso laboral" por el de "acoso sexual". No se trataba de una información clínica. En este caso la administración sanitaria no justificó adecuadamente las razones para denegar la rectificación.

Algo que preocupa a **Ana Aperribal**, en materia de rectificación son las segundas opiniones. "Los ciudadanos se quejan de que cuando haya dos opiniones médicas divergentes tienen que figurar las dos en el historial", reflexionó.

Carles San José i Amat expuso un caso que trataba de un demandante que alegaba que datos de su historia clínica, por medio de una filtración, habían llegado a una tercera persona y el reclamante, seguro de que alguien estaba filtrando información a esta persona, solicitó que sus datos solo pudieran ser consultados por el médico que le atiende. Se denegó dicha solicitud por falta de justificación de las sospechas del reclamante y porque podría perjudicarse a la propia persona afectada en caso de atención urgente.

Ana Aperribal Ulacia presentó un caso curioso en el que la AVPD atendió un caso de rectificación de historia clínica derivado de la ejecución de una sentencia, en la que el condenado había usurpado la identidad de una tercera persona, a fin de hacerse prescribir ansiolíticos. Una vez resuelta la responsabilidad penal del condenado, el juzgado acuerda cancelar los datos de las falsas prescripciones de la historia del tercero suplantado, a fin de no perjudicarlo en su historial médico. Aunque la sentencia ordena la cancelación a la Agencia, no le corresponde a ésta la materialización de dicha cancelación, ni siquiera su tutela, pues no deviene del ejercicio de derechos previsto en la

legislación sobre protección de datos. En cualquier caso, se facilitó la gestión de dicha cancelación ante el Servicio Vasco de Salud.

Respecto a las medidas de seguridad, **Carles San José i Amat** presentó el caso de unos familiares que, tras solicitar el acceso a la historia clínica de un familiar fallecido, denunciaron la falta de medidas de seguridad en el acceso a la historia clínica que se mantiene "a pie de cama". Se trata de una

información que podía leer cualquiera que pasara por la UCI. El hospital alegó que no había otra forma de guardar esos datos y que de hacerlo en otro lugar no sería bueno para la asistencia de ese paciente. Se hizo un requerimiento para la mejora de las medidas de seguridad y el hospital modificó sus normas de trabajo imponiendo una medidas de seguridad muy originales por lo cual fue posteriormente premiado.

La coordinadora de la sesión fue **Maria Àngels Bar-**

SESIÓN CUARTA. EL TRATAMIENTO MASIVO DE LOS DATOS DE SALUD. PROYECTOS Y REALIDADES DE BIG DATA



bará i Fondevila, directora de la Autoridad Catalana de Protección de Datos. Comentó, durante su intervención, los objetivos de las autoridades de protección de datos como son el involucrar al conjunto de los agentes del sector en un diálogo constructivo para evitar, por un lado, infringir el derecho y por otro, intentar mantener un alto nivel de innovación. Añadió que los beneficios de las tecnologías son incuestionables para todos, aunque tienen el peligro de impactar en "nuestros derechos", sobre todo en el sector sanitario. Comentó, posteriormente, la importancia de la tecnología de Big Data que, "sin duda, puede mejorar la gestión de nuestra salud, aunque hay que intentar que ninguna persona pueda ser identificada".

Ramón Maspons Bosch, ingeniero industrial y coordinador de innovación de la Agencia de Cali-

dad y Evaluación Sanitarias de Cataluña (AQuAs), presentó algunas características del proyecto VISC+ que trata sobre el incremento de la competitividad de la investigación del sistema sanitario. El objetivo, defendió el ponente, es poner en Cataluña la información del sistema sanitario para que los investigadores puedan mejorar la calidad de sus proyectos. Esta información se ofrecerá de forma anonimizada y segura. Pidió que nunca las empresas privadas tuvieran acceso a la información mientras que esta no fuera totalmente anónima. El proyecto tendrá un único perfil de clientes que serán los centros de investigación de cualquier procedencia.

Para terminar su intervención, el ponente reitera la idea clave que es la mejora de competitividad del sistema.

Actividades de la SEIS

Elisabet Vilella Cuadrada, directora del Área de Investigación del Hospital Universitario Instituto Pere Mata, ha trabajado, durante más de dos años, en el proyecto dinámico para poder disponer de la información de los pacientes que está mecanizada desde hace varios años. Explicó que las características socio económicas de la provincia de Tarragona representan a la media europea por lo cual los datos son extrapolables al resto de Europa. El Grupo Pere Mata, con sus diferentes hospitales, atienden a todas las personas que presentan problemas de salud mental de cualquier edad, desde los niños hasta los ancianos, lo cual permite realizar estudios de salud mental con los datos de que disponen. Han encontrado en su trabajo varios retos que agruparon en los que están relacionados con los datos y los relacionados con la actividad. En relación con los datos comprobaron que tener un número abundante de ellos no es suficiente ya que hay que estructurarlos y enumerar los que estén duplicados. Tuvieron en cuenta la seguridad y privacidad más allá del uso primario y que el proyecto fuera sostenible y buscaron varias soluciones.

Concluyó, para sintetizar, que en el modelo que utilizan hay que pasar la información de la base de datos a una plataforma donde estarán disociados y anonimizados. Finalmente los datos se utilizarán para la gestión propia e interna de la institución y también para compartir con empresas e instituciones.

Victor Rocabert, experto en Big Data de Bismart, explicó que cuando en el año 2012 se empezó a popularizar todo lo relacionado con Big Data su empresa ya había terminado el primer proyecto. A partir de ese momento han desarrollado diferentes proyectos de Big Data dentro del ambiente sanitario. Cuando hablan desde el punto de vista sanitario tienen especial relevancia los aspectos de seguridad y privacidad. Destacó que la gran mayoría de proyectos de Big Data tienen fines estadísticos y analíticos y que el objetivo es estudiar un gran volumen de datos para generar conclusiones de valor que ayuden a prevenir ciertos riesgos y disponer de más información para una toma de decisiones sin llegar, en ningún caso, a los datos individualizados.

Avanzo que Bismart está trabajando en proyectos de análisis de redes sociales que constituyen

una fuente de información de gran valor. Por otro lado se ocupan de generar señales para farmacovigilancia y de buenos hábitos alimenticios y de salud. También trabajan en pulseras que se usan de forma permanente para controlar el sueño, el pulso, etc. Están implicados, además, en temas de tele asistencia y tele medicina en fase de desarrollo unas veces y otras en fases de implantación.

Alberto Sotomayor, responsable del área de Big Data de Ibermática, presentó, en primer lugar a la empresa a la que pertenece. Ibermática lo que hace es tomar la tecnología que aparece en el mercado y trasladarla y aplicarla a casos concretos para el sector público. Una de las "patas" de Big Data, que es la inteligencia artificial, es la que más han desarrollado. Muchos de los proyectos en este ámbito tienen que ver con la IA.

Durante su intervención, el ponente se hace una pregunta, "¿qué hacemos cuando queremos entender una realidad que presenta muchas variables y que es compleja?" Citó, como ejemplo, el clima que aunque es una realidad hay que estudiar una serie de variables que pueden incidir en él. Lo mismo ocurre en el ámbito de la salud. "A veces no se trabaja con todos los datos y lo que se hace es tomar sólo una muestra aunque se pueda introducir un sesgo". Big Data –añadió Sotomayor– introduce la tecnología necesaria para el almacenamiento de todos los datos que puede tener esa realidad que se está estudiando. Citó algunos proyectos que tienen en marcha relacionados con el ámbito hospitalario como el que han desarrollado, entre otros, para el hospital de Cruces.

El último en intervenir fue **Marc Blasi**, subdirector Centro de Excelencia de Big Data de Barcelona (Fundación Barcelona Digital). En el Centro de Excelencia trabajan con el concepto "casi en tiempo real", es decir, del acceso continuo a los datos y por tanto no se procesa en batch sino en tiempo real. "Para dar respuesta a ello se deben responder con la rapidez que debe tener la empresa para proporcionar seguridad a los consumidores", explicó Blasi y confirmó que han introducido el término de procesamiento distribuido apareciendo plataformas de servicio. Destacó la importancia de la seguridad y la anonimización de los datos. Un aspecto importante es quién tiene que hacer el trabajo de encriptación.

SESIÓN QUINTA. DERECHOS DE LOS CIUDADANOS Y PROTECCIÓN DE DATOS DESDE EL DISEÑO. EVALUACIONES DE IMPACTO EN LOS DATOS DE SALUD



Coordinó la sesión **María José Blanco Antón**, secretaria general de la Agencia Española de Protección de Datos. Los ponentes fueron: **Emilio Aced Féliz**, **Santiago Farré Tous**, **Julio Mayol Martínez** y **Daniel A. López Carballo**.

María José Blanco comenzó formulando a los ponentes la pregunta sobre cuáles consideran que son los retos más importantes que se presentan en el tratamiento de los datos con Big Data e Internet de las Cosas, en relación con las personas en este ámbito sanitario.

Comenzó respondiendo **Julio Mayol**, director de Innovación del Hospital Clínico de Madrid. Bajo su punto de vista, la sanidad representa un sector “clave” en todas las sociedades occidentales y hay que tener en cuenta que en la práctica asistencial se hacen cuatro cosas diferentes, que no pueden separarse, y que son asistencia, docencia, investigación y gestión. Los médicos tienen datos muy relevantes para la toma de decisiones. Pero la sociedad no considera que los datos sanitarios sean de la misma naturaleza que el resto de la información, por ejemplo, los datos bancarios.

Las compañías tecnológicas –reflexionó Julio Mayol- sobre todo en USA deciden que las TIC hay que utilizarlas en el sector salud porque es el nicho que les queda y el más potente. “Nos convierten así en el centro sanitario del futuro, nos monitorizan allá

por donde vamos lo cual crea datos que no sabemos para qué sirven, pero que son datos sanitarios, con lo que ello implica”, explicó y añadió que “tenemos los que se recogen de todos los sitios, ya que hay sensores por todas partes. No se aplican tratamientos secundarios. La mayoría no están aquí y es información que podría ser relevante o no, para la asistencia, docencia e investigación, pero se controlan en Silicon Valley donde dicen que ellos no venden datos”. Entiende el ponente que “llegamos a una situación en la que los datos de nuestros pacientes, que porten sensores, no están disponibles, siendo dudosa su calidad. También hay problemas semánticos”. Por otro lado, los ciudadanos piensan que sus datos están recogidos y que deberíamos dar solución a sus problemas, pero el sanitario no es capaz porque no tienen acceso a esa información. “No es posible la interoperabilidad”. Por otro lado hay que tener en cuenta que un paciente puede negarse a que sus datos estén en una base automatizada y “no en papel como siempre”.

Daniel A. López Carballo, abogado y asociado Sénior TIC, Privacidad y Protección de Dato de Écija, comenzó hablando de los escenarios actuales. De presente y futuro en el que intervienen nuevos sistemas de tratamiento de datos. “Hemos evolucionado ya que ahora no se pide información al paciente, sino que se le da a par-

Actividades de la SEIS

tir de los procedimientos tecnológicos que se le aplican”, explicó López Carballo. Entiende que “ante los actuales métodos que se emplean, los actuales retos son los antiguos, es decir que los problemas de tratamiento de datos existían ya de toda la vida”. Citó el concepto de finalidad, es decir, “para qué estamos utilizando los datos que estamos cediendo continuamente a partir de los teléfonos móviles, de las pulseras, etcétera, datos estos que aprovechan las empresas para darnos consejos sobre hábitos saludables”. Hay que tener en cuenta, insistió López Carballo, “la madurez de las personas”.

Presentó el ejemplo en el mundo audiovisual aquellos dibujos de rombos que nos daban cierta información de la película, o la etiqueta de las prendas que nos ilustran sobre su lavado y planchado. Otro reto es la transparencia, es decir, como vamos a utilizar la información para buscar el punto de equilibrio entre los datos del paciente y el cumplimiento de la norma.

Santiago Farré Tous, responsable de la Asesoría Jurídica de la Autoridad Catalana de Protección de Datos, sostuvo que Big Data tiene grandes retos para el tratamiento de la información, no sólo por su cantidad sino también por proceder de diferentes fuentes.

Distinguió tres elementos a tener en cuenta en este fenómeno y son:

- No todo aquello que técnicamente sea factible es jurídicamente y éticamente admisible.
- Lo que nos ofrece Big Data es la posibilidad de obtener perfiles en cualquier ámbito.
- El principio de minimización.

Internet de las cosas también presenta, según el ponente, grandes retos para la protección de datos sobre todo en medicina.

Emilio Aced Félez, jefe de Área de la Unidad de Apoyo al Director de la Agencia Española de Protección de Datos y Coordinador General del Foro, intentó resumir unos aspectos desde la perspectiva de protección de datos, centrándose en los retos que para determinadas personas se pueden presentar.

Le llamó la atención lo “opacos” que son los tratamientos de Big Data para las personas y afirmó que legalmente sí existen tratamientos secundarios en el ámbito de Big Data. En el momento actual, además de la historia clínica “se capturan datos sobre salud de muchísimas fuentes como redes sociales, chats, etc”. Además de la tecnología que se usa ac-

tualmente y que produce información de “dónde vamos, cuántos pasos damos, qué establecimientos frecuentamos y no pensamos que de toda esa información hay alguien que se apodera y que puede ser utilizada con diversos fines”.

Precisó Aced Félez que la manera de mejorar este tipo de retos es “la transparencia”. Habló de lo que él llama “irresponsabilidad” cuando se refiere a lo difícil que es, para la persona común, saber quién es el responsable de ciertos tratamientos de los datos. “Muchas veces no se sabe quién está trabajando con los datos de quiénes y para qué se están utilizando”.

En tercer lugar, mencionó la dificultad de supervisión. Como experto en protección de datos afirmó que se trata de una cuestión enormemente compleja. La correcta supervisión es un verdadero reto. También, comentó Aced Félez las predicciones que podría ser la finalidad última del manejo de tanta información. Y esas predicciones se aplican a personas concretas. “Predecir el futuro, conocerle y mejorarle podría ser el objetivo de Big Data, sin olvidar que las predicciones pueden ser acertadas o erróneas”.

En una segunda ronda, **María José Blanco** preguntó a los ponentes si consideran que estos conceptos que pueden derivarse del proyecto del Reglamento Europeo son aplicables a los actuales entornos, si pueden aportar beneficios y qué soluciones pondrían para abordar estos problemas.

Julio Mayol explicó que en el New York times leyó algo sobre los médicos utilizando la historia clínica electrónica. Uno de ellos, que trabaja en un hospital de Phoenix anunciaba que “ni tenemos ni vamos a tener historia clínica electrónica”. También contó la historia de un paciente que dejó de ir a su médico porque este “había desaparecido detrás del ordenador”. En el sector médico los ordenadores no están diseñados para la atención a los usuarios, los sistemas de información sanitaria, comentó el ponente, “son malos o muy malos” según la percepción de los usuarios. Se presenta un problema grave ya que los sistemas de información necesitan un replanteo global urgente.

López Carballo comenzó su intervención diciendo que “una de las cuestiones que en protección de datos nos encontramos es cómo hablar el mismo lenguaje y cómo aplicar la norma de protección de datos al tipo de tratamiento que estamos hacien-

do". Con respecto a la LOPD "es complicado empezar de cero". Al final hay que avanzar hacia "un equilibrio, un compromiso entre todos los actores".

Defiende López Carballo que la Agencia Española, la Vasca y la Catalana deberían difundir ese mensaje, pero añade que también es un concepto de cultura. "Al final los conceptos de privacidad en el diseño, lo que provocan es que en un mismo foro, en la misma empresa, juristas, informáticos e instituciones nos sentemos y pensemos sobre la información, a dónde queremos llegar, qué vamos a hacer con la información y las medidas a tomar no sólo desde un punto de vista técnico sino también desde el jurídico".

Santiago Farré opinó que, precisamente, es en este entorno donde pueden desplegarse los mejores efectos de estas herramientas, principalmente en la cuestión de privacidad. "Cuando se habla de protección de datos tenemos que ser conscientes de que un mal tratamiento de la información puede provocar perjuicios irreparables y la reparación de estos perjuicios difícilmente será completa y desde luego es muy difícil". La autoridad catalana ha impulsado la privacidad por diseño desde hace unos años y "creemos que este es el camino a seguir".

"Desde el punto de vista del ciudadano, lo que aporta la privacidad en el diseño es que le permite el control de su información, porque en este entorno, para controlar la información, es preciso tener una formación y unos conocimientos de los cuales la mayoría de los ciudadanos no disponen", defendió Farré y añadió que "además, para los desarrolladores de soluciones o productos, incorporar la privacidad en el diseño debería ser visto como un activo, como un elemento que permite que sus soluciones sean las más competitivas". Habló de las Smart TV que recogen información sobre el uso de las mismas por parte del propietario. Y esos datos podrían estar relacionados con la salud. "Lo que está claro es que quien ha diseñado esa TV no ha tenido en cuenta la privacidad".

Emilio Aced Féllez expuso que en "el entorno en el que estamos hablando de Big Data, una app puede tener diez millones de descargas. El primer baluarte para la protección de datos debe partir del propio responsable, que debe estar convencido de que la privacidad es un elemento crucial de su negocio". Por ello, añadió Aced Féllez, "hay que partir de un concepto respetuoso con la privacidad desde que se diseñan los productos". En este entorno, "las evaluaciones de impacto en la protección de datos son un herramienta crucial. Es necesario fomentar una cultura proactiva. Se debe recordar que detrás de los datos hay personas". Entiende que "en el uso, todas las herramientas que existen deben tener en cuenta desde el principio este aspecto de la privacidad. Tiene que haber un equilibrio entre lo que es posible y lo que es ético". En este entorno, una herramienta muy interesante es la guía de la Agencia Española para ayudar a los que estén interesados en estas nuevas técnicas para las evaluaciones de impacto. Son importantes porque ayudan a que desde un primer momento "nos preocupemos y seamos capaces de llegar de detectar los riesgos que hay para las personas en los tratamientos que se realicen".

Lo primero que habría que hacer –añadió Aced Féllez– es identificar "qué riesgos tengo y si no puedo eliminarlos, al menos mitigarlos". Este tipo de procesos ayudan a desarrollar una cultura proactiva del tratamiento de datos dentro de las instituciones, pero también, desde el punto de vista del propio interés ya que "podemos evitar daños reputacionales a una organización o incluso sanciones económicas". Por lo tanto, también es importante para las organizaciones integrar en sus procesos de desarrollo las evaluaciones de impacto para respetar los derechos de las personas.

"Big Data e Internet de las Cosas pueden aportar muchos beneficios pero siempre hay que tener en cuenta que detrás de los tratamientos hay personas y que las decisiones que se toman basadas en estos paradigmas las afectan grandemente", concluyó.

CLAUSURA

Emilio Aced se mostró agradecido a todos los que han hecho posible la organización de este Foro, especialmente a los miembros del Comité Local, **Antonio Poncel** y **Marta Trigo**.

Extendió su agradecimiento a las empresas que han colaborado en la realización del evento y a la Secretaría Técnica de la SEIS por su trabajo "callado y eficiente".

Actividades de la SEIS



“Este Foro comenzó por una reunión del Comité Técnico de la Seguridad de la Información y prácticamente se ha terminado con un documento de concienciación a directivos, que esperamos esté disponible en breve y que creemos facilitará la seguridad de la información que se maneja. También, estamos empezando a trabajar en un nuevo documento sobre la seguridad en el ámbito sanitario”, concluyó Emilio Aced, al tiempo que avanzó que se ha presentado el Manifiesto de Valencia sobre la importancia de la seguridad en nuestro ámbito. Agradeció la asistencia de todos y les anunció que el próximo Foro de Interoperabilidad se celebrará en Barcelona los días 22 y 23 de abril.

María Àngels Barbará señaló que los objetivos de este Foro se han superado con creces. Las ponencias, en su opinión, “nos han aportado a todos nuevos puntos de vista que permitirán seguir avanzando en la garantía de la privacidad”. Concluyó que “las tecnologías que hemos tratado en esta ocasión están en una primera línea de evolución pero ya están demostrando que en el ámbito de la salud van a permitir enormes avances, tanto para mejorar la salud como para la calidad de vida de las personas. Se deben evaluar y minimizar los riesgos”.

Ángel Sanz Barea, director Gerente del Servicio Aragonés de Salud, disculpó al consejero que no puede estar presente en el encuentro. Defendió Sanz Barea que “uno de los temas principales de la

actualidad es el impacto de las TIC en nuestro mundo y sus consecuencias, tanto para las personas y organizaciones como para la sociedad en sí misma”. Actualmente, “las personas y nuestros ciudadanos en general y los pacientes en particular exigen a los servicios de salud los mismos servicios que encuentran en otros ámbitos de la vida”. Recordó Sanz Barea que “se piden citas por internet, se consultan resultados y otras muchas cosas”.

“En los últimos años se han producido en España grandes avances. Aún quedan muchas cosas por hacer, sobre todo en la relación telemática con nuestros pacientes, pero para que podamos consolidar estos ritmos de crecimiento y avance hacen falta seguridad y confianza”, apuntó el director gerente del Servicio Aragonés de Salud. “Sólo si sentimos seguridad, los nuevos servicios serán eficaces y útiles. El mundo de la salud por la esencia de la información que se maneja requiere un especial cuidado en todo lo relacionado con la seguridad”.

“El avance de las TIC nos plantea nuevos retos que requieren la tecnología en todos los niveles, cortafuegos, antivirus, firmas, etc., para lo cual se requiere organización, sentido común y proporcionalidad en las medidas de seguridad. En Aragón, recientemente, se ha aprobado la creación del Comité de Seguridad” concluyó, no sin antes animar a la SEIS a que siga con la organización de estos foros.



Presentación del Índice SEIS

El pasado día 19 de mayo se presentó en el Salón de Actos del Ministerio de Industria, Energía y Turismo el Índice SEIS 2014

Como es sabido se trata de un estudio sobre la situación de la implantación de las TIC en el Sistema Nacional de Salud. En este caso se ofrecían los datos correspondientes a 2014.

El Índice SEIS se realiza en colaboración con los responsables TIC de los Servicios de Salud de las Comunidades Autónomas, el Ministerio de Sanidad, Servicios Sociales e Igualdad y Red.es.

Con este Índice 2014, ya son tres años los que la SEIS ofrece información fiable sobre las inversiones y gastos en proyectos TIC en el sistema sanitario público.

Computerworld ha editado un especial en el que se incluye este tercer estudio, que fue repartido entre todos los asistentes.

El acto fue presentado por **Francisco Javier García Vieira**, director de Servicios Públicos Digitales de Red.es, que dio la bienvenida a todos a este acto en la Secretaría de Estado de Comunicaciones.

A continuación tomó la palabra **María José Marzal**, directora de Computerworld, para indicar que, en esta nueva edición del Índice, se puede apreciar un

aumento del 5,6% sobre el 2013 del gasto de tecnologías de la información en Sanidad, que aunque es bien acogido, todavía queda lejos de lo deseado, pues solo representa el 1,27% del gasto global sanitario.

Seguidamente intervino **Luciano Sáez Ayerra**, presidente de la SEIS. Después de agradecer a María José Marzal su colaboración, comentó que el objetivo del Índice es dar a conocer los datos de la inversión TIC en Sanidad. Agradeció también al equipo de la SEIS que ha colaborado en este trabajo, destacando especialmente la participación de **Carlos García Codina** y a **Francisco Martínez del Cerro**.

Su intervención sirvió también para anunciar las jornadas de Andalucía, cuyo lema será "Viviendo el impacto de las TIC en salud". Sáenz afirmó que "sentaremos una bases metodológicas que incluyan los aspectos que deberían valorarse y las formas de incorporar los procesos de evaluación en los modelos de contratación".

Añadió que es importante disponer de profesionales cualificados, tanto en tecnología como en el

Actividades de la SEIS



negocio sanitario. “Hay que priorizar la formación”, dijo.

Zaida Sampedro, vicepresidenta de la SEIS, demostró su satisfacción por este Índice en su tercer año consecutivo y agradeció a todos los que colaboraron en su realización.

Según su punto de vista, hay que contemplar la situación bajo tres puntos de vista: medir, conocer y compartir. En cuanto a los presupuestos y recursos humanos, hemos estado expuestos a muchas críticas. Desde el punto de vista público y privado e incluso el empresarial, cada uno de nosotros debe tener el convencimiento de que los recursos empleados aún son insuficientes.

El Índice SEIS tiene que servir de ayuda para comparar lo que es la productividad de los recursos humanos TIC y que el esfuerzo que se haga a nivel institucional no solamente sea económico sino en recursos que necesariamente tienen que ser capaces de dirigir y recorrer toda la andadura que tenemos hoy. Finalizó poniendo como ejemplo a la Agencia Tributaria, que dispone de grandes presupuestos en tecnología.

Carlos García Codina, responsable del Índice, comentó los objetivos, los principios seguidos y la metodología empleada para la elaboración del Índice

SEIS 2014, y presentó un resumen de los resultados obtenidos.

Indicó que el Índice se puede consultar en la web de la SEIS, además de en el suplemento de Computerworld distribuido a los asistentes al acto (<http://82.98.165.8/documentos/acuerdosyconvenios/INDICE2014.pdf>)

Señaló como característica significativa que el Índice 2014, contempla datos de los índices de 2012 y 2013, mostrando directamente la evolución experimentada en la mayoría de los indicadores, lo que facilita el trabajo de análisis.

Concluyó diciendo, que a su juicio, el Índice SEIS aporta información, que hasta ahora no se disponía, sobre la implantación de las TIC en la sanidad pública española, y que, a su juicio, ésta información es muy valiosa para todos los implicados en el sector sanitario, así por ejemplo:

- A los gestores, les suministra índices generales sobre la inversión en TIC, lo que les permite establecer comparaciones con otros sectores tanto públicos como privados, nacionales o extranjeros.
- A los responsables TIC de los Servicios de Salud les permite conocer su situación con respecto al resto de las CCAA y servir de apoyo en la definición de estrategias y en la defensa de proyectos y actuaciones concretas.
- A las empresas del sector les da información sobre:
 - La distribución del presupuesto entre las diferentes partidas.
 - La situación de los proyectos corporativos.
 - Los proyectos prioritarios que los servicios de salud van a abordar próximamente.

Finalmente intervino **Juan Fernando Muñoz**, subdirector general del Ministerio de Sanidad, Servicios Sociales e Igualdad, que felicitó a todos los que han trabajado para conseguir los datos del Índice, pues es consciente de la dificultad que implica. Incluso dijo que a él mismo le ha costado mucho trabajo encontrar alguna información medianamente fiable de otras fuentes para constatar los datos del Índice. Ofreció datos comparativos de la implantación de las TIC en general, señalando la posición de cabecera que España ocupa en la mayoría de las áreas e insistiendo en la similitud entre los datos de la SEIS y los obtenidos por otros organismos nacionales e internacionales.

Terminado el acto, el numeroso público asistente intercambió impresiones mientras se servía un vino español.

Con el apoyo de la **Agenda Digital** para España

Innovación y Salud

XXII Jornadas Nacionales de Informática Sanitaria en Andalucía



Síguenos en twitter:
@SEISeSalud
@jisa2015

Midiendo el Impacto de las TIC en Salud

Organiza



Con la colaboración de



red.es



JUNTA DE ANDALUCÍA
CONSEJERÍA DE IGUALDAD, SALUD Y POLÍTICAS SOCIALES

PROGRAMA PRELIMINAR

MÁLAGA

17, 18 y 19 de junio de 2015

HOTEL SOL PRÍNCIPE
Paseo Colorado, 26
29620 Torremolinos

COLABORADORES TECNOLÓGICOS



XXII Jornadas Nacionales de Informática Sanitaria en Andalucía

Málaga, 17, 18 y 19 de junio de 2015

INTRODUCCIÓN

Un año más Málaga nos volverá a acoger en el mes de junio, esta vez durante los días 17, 18 y 19, para celebrar las Jornadas de Informática Sanitaria en Andalucía en la que será su edición número XXII, bajo el lema "Midiendo el impacto de las TIC en salud".

Son ya demasiados los años en los que el pretexto de la crisis ha condicionado la inversión TIC en el ámbito sanitario, afectando no en sentido positivo, como indicaría la lógica derivada de una convicción firme en su aportación a la eficiencia, sino, antes bien, en una reducción generalizada de los presupuestos TIC. Esto pone de manifiesto que dicha convicción está seguramente poco arraigada en los gestores, algo que debería hacernos reflexionar sobre la forma en la que ponemos en valor la aportación de las TIC a la mejora de la calidad y la eficiencia de la asistencia sanitaria y su capacidad para transformar un modelo asistencial que comienza a presentar rasgos de anacronismo.

Por ello, en momentos en los que los recursos escasean y hay que justificar cada euro gastado, es importante disponer de argumentos para defender la utilización de las TIC en el ámbito asistencial como un elemento en el que merece la pena invertir. Esto supone disponer de metodología que permita poner cifras a los retornos que generan las TIC tanto de forma directa como indirecta, subrayando además, que el principal retorno de los servicios asistenciales está en el valor del servicio que se presta a la sociedad.

OBJETIVOS

Ahondando en estos planteamientos, este año nos proponemos abordar el reto de realizar una primera aproximación al complejo tema de dimensionar con rigor y precisión razonable el impacto de las TIC en la salud. Para ello trataremos cuestiones como:

- Cómo debería enfocarse el análisis de la evidencia del impacto de las TIC en salud para zanjar el debate de su contribución real a la mejora de la calidad y la eficiencia de la asistencia sanitaria
- Cómo generalizar el hábito de la evaluación del impacto de proyectos TIC y sentar unas bases metodológicas elementales que incluyan:
- Aspectos que deberían valorarse

- Identificar los diferentes ámbitos en los que las TIC aportan valor, con especial énfasis en aspectos indirectos
- Elementos a tener en cuenta a priori para facilitar la evaluación de dichos impactos
- Forma de medir algunos impactos indirectos
- Forma de incorporar el proceso de evaluación en los modelos de contratación vigentes

La colaboración entre proveedores de salud, empresas y profesionales del sector TIC en sanidad, intercambiando sus experiencias y puntos de vista, en un trabajo altamente participativo y creativo contribuirá, como en anteriores ediciones, a generar un debate enriquecedor del que se espera obtener un documento de consenso que recoja algunas recomendaciones esenciales sobre las cuestiones mencionadas.

METODOLOGÍA

Como en la última edición, mantendremos un esquema de trabajo con tres partes bien diferenciadas:

- En la sesión inicial del miércoles por la tarde se pretende revisar algunos de los aspectos básicos relacionados con el tema, con la finalidad de normalizar conceptos y terminología. Para ello se realizará una primera sesión de carácter teórico a la que seguirá una mesa con experiencias prácticas y debate en la que estarán representados los principales agentes de interés: servicios de salud públicos y privados, proveedores de tecnología y pacientes. Su objetivo es generar en la audiencia una base de conocimiento compartido sobre los temas que serán objeto de debate en los talleres.
- A lo largo del jueves se desarrollarán tres/cuatro talleres paralelos en los que mediante el método del caso se analizarán en profundidad algunas situaciones reales, buscando dar respuesta a cuestiones concretas sobre los aspectos mencionados en la introducción.
- La documentación y las propuestas generadas el jueves serán elaboradas y discutidas en la sesión plenaria del viernes, para generar un documento de consenso en el que se recojan las conclusiones y las recomendaciones aprobadas como resultado de las Jornadas.

PROGRAMA PRELIMINAR

MIÉRCOLES, 17 DE JUNIO DE 2015

16.00 - 16.30 Registro de Participantes

16.30 - 17.00 Inauguración

17.00 - 18:30 SESIÓN DE APERTURA **“Aspectos conceptuales de la medición del impacto de las TIC en salud”**

Coordinan:

- Sr. D. Jesús Galván Romo, *Viceconsejero Consejería de Sanidad y Asuntos Sociales de Castilla-La Mancha*
- Sr. D. Miguel Ángel Montero Martínez, *Director de Sanidad y Servicios Sociales Informática El Corte Inglés*

Interviene:

- Sr. D. Ramón Maspons Bosch, *Coordinador d'Innovació Agència de Qualitat i Avaluació Sanitàries de Catalunya*

18.30 - 18.45 Pausa

18.45 - 20.15 MESA REDONDA **“Evidencias del impacto de las TIC en Salud”**

Modera:

- Sra. D^a Zaida Sampedro Préstamo, *Directora General de Sistemas de Información Sanitaria Servicio Madrileño de Salud*

Intervienen:

- Sra. D^a Ana Miquel Gómez, *Gerente Adjunta de Planificación y Calidad Gerencia de Atención Primaria. Responsable de la Estrategia de Atención a Pacientes con Enfermedades Crónicas. Servicio Madrileño de Salud*
- Sra. D^a Cristina Granados Ulecia, *Directora Gerente Complejo Hospitalario de Toledo*
- Sr. D. Ángel Blanco Rubio, *Director de Organización, Procesos y TIC Idc Salud*
- Sra. D^a Piedad López Roldán, *Subdirectora de Información y Atención al Paciente Dirección General de Atención al Paciente Servicio Madrileño de Salud*
- Sr. D. Enrique Palau Beato, *Director de Estrategia y Portfolio en Salud Atos Iberia*
- Sr. D. Francisco Javier García Vieira, *Director de Servicios Públicos Digitales Red.es*

21.30 Inicio Moraga

JUEVES, 18 DE JUNIO DE 2015

9.30 - 11.30 TALLERES PARALELOS. Primera Sesión

Taller 1: “Telemedicina”

Coordinan:

- Sr. D. Alberto Mateos Gala, *Subdirector de Sistemas de Información Servicio Extremeño de Salud*
- Sr. D. Pablo Camba, *Healthcare Sales Director T-Systems*

Dinamizadores:

- Sr. D. Rafael Artalejo Gutiérrez, *Director Técnico de Tecnologías de la Información para la Salud Servicio de Salud de Castilla La Mancha*
- Sra. D^a Ana Moraga Ferreira, *Consultora de Sanidad Informática El Corte Inglés*
- Sr. D. Cayetano M. Hernández Marín, *Presidente Asociación Valenciana de Informáticos de Sanidad. AVISA*
- Sr. D. Fernando Hernández Segado, *Responsable Proyectos Telemedicina en eHealth Telefónica*
- Sra. D^a Elvira Muslera Canlini, *Coordinadora Servicio de Coordinación Asistencial y Cuidados Servicio de Salud del Principado de Asturias. SESPA*
- Sr. D. Luis Camacho Murcia, *Subdirector General de Gestión Económica y Contratación SEPAD. Servicio Extremeño de Salud*

Taller 2: “Gestión digital del consentimiento informado”

Coordinan:

- Sr. D. Carlos Gallego Pérez, *Responsable Oficina d'Estàndards i Interoperabilitat Tic Salut. Generalitat de Catalunya*
- Sr. D. Juan Carlos Muria Tarazón, *Consultor de Sanidad Fujitsu*

Dinamizadores:

- Sr. D. Ángel Luis García García, *Account Manager Área Salud Fujitsu*
- Sr. D. Manuel Escudero Sánchez, *Subdirector General de Tecnologías de la Información Servicio Murciano de Salud*
- Sr. D. Xavier Oliva Suárez, *Subdirector de Tecnologías de la Información Servei de Salut de les Illes Balears*
- Sr. D. José Manuel Morales Pastora, *Director Técnico de Sistemas de Información Gerencia Regional de Salud de Castilla y León*
- Sr. D. José Cañete Aguado, *Gestor de Producto de la Unidad de Seguridad Telefónica*
- Sr. D. Rodolfo Cantabrana Virumbrales, *Gerente de Sanidad y Bienestar Social Connectis*

Taller 3: “Impacto en Salud de la Nueva Generación de Historias de Salud Electrónicas Inteligentes”

Coordinan:

- Sr. D. Francisco José Sánchez Laguna, *Responsable del Servicio de Coordinación de Sistemas de Información Servicio Andaluz de Salud*
- Sr. D. Pablo Sánchez Cassinello, *Managing Director Sector Sanidad Accenture*

Dinamizadores:

Actividades de la SEIS

- Sr. D. Francisco Javier Pérez Fernández, *Healthcare Product Senior Manager Indra Sistemas S.A*
- Sr. D. Carlos Piqueras Picón, *Director de Sanidad Intel Corporation Iberia*
- Sr. D. Juan Lucas Retamar Gentil, *Subdirector General de Tecnologías de la Información Servicio Andaluz de Salud*
- Sra. D^a Inmaculada Concepción Castejón Zamudio, *Coordinadora de Proyectos de Innovación Dirección General de Calidad, Investigación, Desarrollo e Innovación Consejería de Igualdad, Salud y Políticas Sociales de la Junta de Andalucía*
- Sr. D. Cesar Wagener Moriana, *Director de Productos de Salud Connectis*
- Sra. D^a Lola Ruiz Iglesias, *Experta de Historia Clínica Electrónica*
- Sr. D. Guillermo Vázquez González, *Subdirector de Tecnologías de la Información Gerencia de Gestión Integrada de A Coruña Representante de ATOS*

Taller 4: "Imagen Clínica Digital"

Coordinan:

- Sr. D. Martín Begoña Oleaga, *Subdirector de Organización y Sistemas de Información Servicio Vasco de Salud*
- Sr. D. Sergio Irayzoz Del Castillo, *IT Manager South Europe Agfa Healthcare*

Dinamizadores:

- Sr. D. Pedro Totoricagüena Arana, *Jefe de Servicio Servicio Vasco de Salud. Osakidetza*
- Sr. D. José Juan Moratilla Villaverde, *Business Manager Syngo Siemens, S.A. Healthcare Sector*
- Sra. D^a Marisa Correcher Palau, *Directora de Gestión Sanitaria de Sistemas de Información Conselleria de Sanitat de la Generalitat Valenciana*
- Sr. D. Antonio Orduña Galán, *Hospital La Fe de Valencia*
- Sr. D. Daniel Raduan Munem, *Responsable de Imagen Médica Digital en eHealth Telefónica*
- Sr. D. Javier Sánchez, *Director Comercial de Administración Pública EMC*

11:30 - 12:00 Pausa Café

12:00 - 14:00 Talleres Paralelos. Segunda Sesión
Taller 1, 2, 3 y 4

14:00 - 16:30 Almuerzo

16:30 - 20:30 Talleres Paralelos. Tercera Sesión
Taller 1, 2, 3 y 4

20:30 Vino Español

VIERNES, 19 DE JUNIO DE 2015

9:30 - 11:30 Sesión de Presentación y Discusión de las conclusiones de los Talleres

Modera:

- Sr. D. Ángel Sanz Barea, *Director Gerente Servicio Aragonés de Salud*

Intervienen:

- Sr. D. Alberto Mateos Gala, *Subdirector de Sistemas de Información Servicio Extremeño de Salud*
- Sr. D. Pablo Camba, *Healthcare Sales Director T-Systems*
- Sr. D. Carlos Gallego Pérez, *Responsable Oficina d'Estàndards i Interoperabilitat Tic Salut. Generalitat de Catalunya*
- Sr. D. Juan Carlos Muria Tarazón, *Consultor de Sanidad Fujitsu*
- Sr. D. Francisco José Sánchez Laguna, *Responsable del Servicio de Coordinación de Sistemas de Información Servicio Andaluz de Salud. SAS*
- Sr. D. Pablo Sánchez Cassinello, *Managing Director Sector Sanidad Accenture*
- Sr. D. Martín Begoña Oleaga, *Subdirector de Organización y Sistemas de Información Servicio Vasco de Salud*
- Sr. D. Sergio Irayzoz Del Castillo, *IT Manager South Europe Agfa Healthcare*

11:30 - 12:00 Pausa Café

12:00 - 13:00 Presentación y aprobación del documento final

Modera:

- Sr. D. Juan Fernando Muñoz Montalvo, *Subdirector General de Tecnologías de la Información Ministerio de Sanidad, Servicios Sociales e Igualdad*

Intervienen:

- Sr. D. Carlos Luis Parra Calderón, *Coordinador General de las Jornadas*
- Sr. D. Gregorio Gómez Soriano, *Coordinador General de las Jornadas*

13:00 - 13:30 Clausura

SECRETARÍA TÉCNICA

CEFIC SL

C/Enrique Larreta, 5 - Bajo izq - 28036 Madrid

e-mail: secretaria.tecnica@cefic.es

Tel: 91 388 94 78

FORO DE INTEROPERABILIDAD

Coordinador: Adolfo Muñoz Carrero

Alineamiento de UNE-EN ISO 13606 con HL7 FHIR

En el número de diciembre de 2014 de esta misma sección se hablaba de la nueva especificación que está creando HL7 para el intercambio de información clínica: FHIR (Fast Healthcare Interoperability Resources). Como ya se comentó, durante el mes de mayo de 2015 se espera que se publique el segundo DSTU (Draft Standard for Trial Use) y que la especificación completa se publique a mediados de 2016.

De igual manera, dentro de su ciclo de vida preestablecido, la norma UNE-EN ISO 13606 ha entrado en su proceso de revisión normativo, con la creación de varios grupos de trabajo (que cuentan, por cierto, con importante presencia española) para tratar diversos aspectos de la norma y cómo mejorarlos, introduciendo los resultados de varias encuestas realizadas entre los implementadores y usuarios de la misma.

Uno de los temas que han surgido entre los grupos de expertos ha sido, precisamente, que aprovechando que se está trabajando en ambas especificaciones de forma paralela, se debería intentar alinear sus desarrollos para poder intercambiar información entre ambos formalismos de manera sencilla. Por esta razón, se creó un nuevo grupo de trabajo que, liderado por un experto de cada una de las normas (Helen Broberg, por parte de 13606 y Gary Dickinson por FHIR), se ha reunido ya en varias ocasiones (la última durante la reciente reunión del TC 215 de ISO, en San Francisco, en el abril pasado). El objetivo de este grupo es crear mecanismos normalizados para poder “traducir” la información entre ambas normas: una tabla de mapeo (mapping table) en la especificación de 13606 y un perfil del extracto en FHIR (HL7 FHIR 13606 extract profile). Junto a estos dos mecanismos, y siguiendo las recomendaciones/quejas que se han formulado últimamente por la dificultad de la implementación de este tipo de normas, también se va a producir una detallada descripción (o guía de implementación) sobre como emplearlos en escenarios reales.

En cuanto al calendario, en el caso del perfil de FHIR, las fechas con las que se trabaja es que se incluya

en la votación normativa que ocurrirá en 2016, de manera que esté disponible en 2017. En el caso de 13606, la tabla de mapeo se espera que el primer borrador esté preparado en septiembre de 2015 y la versión definitiva en enero de 2016.

El trabajo de este grupo de expertos está consistiendo en localizar aquellas áreas problemáticas en la intersección entre los recursos definidos por FHIR y las clases de 13606 que dificulten el paso de uno a otro, y proponer cambios en las especificaciones para superarlas. Así, por ejemplo, se ha propuesto la definición de nuevos recursos para FHIR (Folder, Record Component, Demographic, ...) o modificaciones en los existentes, como la inclusión de un atributo territory en el recurso Composition, para indicar el territorio en el que se ha generado la composición. Igualmente, para 13606 se han propuesto modificaciones, como la inclusión de un atributo Status dentro del EHR_EXTRACT para marcar el estado en el que se encuentra el extracto.

Sin embargo, el mayor punto de fricción entre ambas especificaciones viene de las diferencias en las propias filosofías internas de ambos formalismos: mientras 13606 se diseña para poder trabajar con cualquier información definida a través de un arquetipo (sea un arquetipo actual o uno desarrollado en el futuro) FHIR no parece encontrarse muy a gusto acomodando recursos genéricos (su regla del 80% en el que sólo se crea un recurso nuevo cuando es adecuado para al menos el 80% de las situaciones). Este problema se está investigando por el grupo de trabajo y será tenido en cuenta en las especificaciones finales

FORO DE TELEMEDICINA

Coordinador: O. Moreno

La telemedicina reduce kilómetros y costes

Otro pequeño ejemplo más de cómo la telemedicina puede favorecer el ahorro de costes y la reducción de las distancias entre pacientes y médicos, en este caso, desde la antípodas. Tal y como se comenta en la prensa neozelandesa, se trata del tratamiento para pacientes infantiles con diabetes.

Los pacientes infantiles con diabetes de la región de Otago Central (la tercera región más poblada de la Isla Sur de Nueva Zelanda) se empezarán a ahorrar miles de kilómetros de viaje debido a un servicio clínico de medicina remota implementado desde el Hospital de referencia de Dunedin.

En el ejemplo que se cita, una familia tiene dos hijas de 10 y 12 años con diabetes tipo 1 y que necesitan cuatro consultas médicas al año con el endocrinólogo pediátrico Dr. Ben Wheeler.

En lugar de los 4 viajes al año a Dunedin, sólo necesitarán visitarle una vez al año y el resto de visitas pueden ser dirigidas a través de un enlace tecnológico con la Clínica Dunstan en Clyde.

Los padres de las niñas preguntaron hace varios meses al Dr. Wheeler de empezar algún tipo de iniciativa para reducir a la familia los 600kms en total por cada viaje. Esto implicaba la pérdida de un día de trabajo de uno de los padres y del día de clase de las niñas.

En las sesiones en la Clínica Dunstan, la familia está acompañada, en el lado clínico, por una enfermera especialista en diabetes. El Dr. Wheeler es capaz de revisar los resultados de las pruebas y comentar el tratamiento o cualquier otro tema con los pacientes vía un enlace de video. En Dunstan, la enfermera examina a las pacientes, descarga los datos de los glucómetros y de las bombas de insulina, los sube a la web y prescribe la medicación junto con un dietista, que ofrece consejos sobre la dieta a seguir en la misma sesión clínica.

La sesión clínica empezó en enero pasado y es la primera experiencia formal de telemedicina de la Junta de Salud del Distrito Sur -Southern District Health Board- (que es la organización financiada por el gobierno responsable de la atención primaria y especializada en las regiones de Otago y Southland).

La diabetes tipo 1 es muy adecuada para telemedicina debido a que implica análisis de los datos y tareas educativas más que una exploración física. El

Dr. Wheeler planea ofrecer el mismo servicio para los pacientes de Oamaru.

La Junta de salud tiene problemas presupuestarios y la telemedicina es una forma de reducir los costes. Se espera que la sesión clínica de diabetes ahorre a la Junta al menos 1.000 dólares por paciente al año en gastos de viaje y ocho horas en tiempo de viaje a los pacientes.

El Dr. Wheeler atendió a la petición de este servicio calificándolo como útil y después de haberlo considerado durante algún tiempo. El equipamiento extra cuesta una cantidad mínima y le gustaba el hecho de que la sesión pudiera realizarse desde el ordenador de su trabajo, en lugar de establecer un vínculo tecnológico engorroso.

El Dr. Wheeler dijo que, "la primera sesión clínica fue un gran éxito. Los padres y las niñas estaban felices de verse más cerca de casa y estamos en condiciones de proporcionar la misma alta calidad de la atención, sin la necesidad de que los pacientes y sus familias tengan que viajar tantas veces".

"Estoy encantado de que las sesiones clínicas hayan comenzado y lo bien que han ido. Este es un gran ejemplo para la Junta de Salud del Distrito Sur de proporcionar la atención adecuada en el lugar y momento correctos y dar a los pacientes un mejor acceso a la atención médica", comentó el Director General de Salud de la Junta de Salud del Distrito Sur, el Dr. David Tulloch.

La iniciativa de telemedicina fue posible gracias a la financiación concedida a través de la iniciativa Southern Innovation Challenge. Se lanzó la idea a un panel de evaluadores y recibió la financiación para la compra de la cámara y altavoces para que dicha iniciativa se creara.

Más información:

Scoop Health - <http://www.scoop.co.nz/stories/GE1501/S00024/first-patients-for-paediatric-diabetes-telemedicine-clinic.htm>

Otago Daily Times - <http://www.odt.co.nz/news/dunedin/338457/telemedicine-cuts-down-kilometres-and-costs>

FORO DE SEGURIDAD Y PROTECCIÓN DE DATOS

Coordinador: Emilio Aced

Apple ha lanzado ResearchKit, una aplicación para trasladar la investigación médica de los laboratorios a la calle

Esta nueva herramienta permitirá que todas aquellas personas que tengan un iPhone o un AppleWatch y que deseen contribuir a la investigación científica puedan hacer llegar sus datos de salud a los distintos grupos de investigación que pongan en marcha iniciativas basadas en esta tecnología, ayudando en uno de los puntos más complicados en cualquier estudio o investigación: el reclutamiento de pacientes.

ResearchKit es una plataforma de *software* de código abierto que las entidades sanitarias y los centros de investigación pueden utilizar para crear aplicaciones de diagnóstico y de recogida de datos relevantes para dichas investigaciones. A través de ella, los pacientes podrán hacer llegar sus datos de salud directamente a los investigadores a través de los distintos dispositivos de Apple equipados con esta herramienta.

De acuerdo con la información suministrada por Apple, cualquier información que se comparte a través de ResearchKit se mantendrá confidencial: la persona elige en qué estudios desea participar y mantiene el control sobre la información que proporciona. Es decir, según Apple, esta compañía nunca tiene acceso a los datos de los pacientes que se recogen a través de las aplicaciones desarrolladas por las instituciones sanitarias y que se alojan en un servidor de un tercero de confianza (Sage Bionetworks, una institución médica sin ánimo de lucro localizada en Seattle) donde se guardan cifrados y cumpliendo los estándares de la legislación americana de sanidad. Se asegura que los únicos que tienen acceso a los datos son los investigadores del estudio.

El punto de partida de Apple ha sido transformar la forma en que los estudios médicos se llevan a cabo y que no ha cambiado en las últimas décadas basándose en la captación individual de los pacientes cuando van a la consulta o por otros medios explicándoles la finalidad y el alcance del estudio e informándoles de los derechos que les asisten.

En cambio, con ResearchKit todo el proceso es electrónico y se realiza a través de un terminal

que esté habilitado para utilizar la plataforma y, a pesar de las implicaciones éticas y prácticas del sistema, los comités éticos de las cinco instituciones que han diseñado las primeras aplicaciones aprobaron el proceso de concesión electrónica de consentimiento dentro de la aplicación. No obstante, esta nueva posibilidad no deja de suscitar preocupaciones.

Distintas fuentes han señalado los posibles riesgos que puede conllevar como, por ejemplo, la facilidad de falsificar la edad para entrar en un estudio (los menores lo tienen prohibido salvo consentimiento paterno); la suplantación de identidad o la utilización fraudulenta de las aplicaciones por personas que no forman parte de los grupos de estudio (ya sea por mera diversión o con fines espurios) o los posibles riesgos de reidentificación de la información por no hablar de las consecuencias de las posibles brechas de seguridad.

Otros riesgos se concretan en la posibilidad de que la plataforma puede ser utilizada, por ejemplo, por empresas farmacéuticas para obtener información de los usuarios de Apple y generar beneficios a través de ella; en la desviación en el tipo de población que participa en los estudios (personas de países ricos, con alto poder adquisitivo y que se toman en serio su enfermedad y el cómo mejorarla); y en las dudas sobre la obtención de un consentimiento realmente informado a través de la información que se proporciona en una aplicación dirigida a todo tipo de usuarios y sin que queda clara la implicación de los Comités de Ética en la supervisión de todas las aplicaciones antes de su lanzamiento.

Marcial García Rojo

Director UGC Anatomía Patológica. Hospital de Jerez, Cádiz. Vicepresidente de la SEIS.

Jose Sacristán París

Coordinación y Sistemas Información. Área de Tecnologías de la Información. Servicio de Salud de Castilla-La Mancha.



Los profesionales de la salud andaluces pueden notificar incidencias en los centros sanitarios, a través de una aplicación para móviles

La aplicación Avizor es una iniciativa del Observatorio para la Seguridad del Paciente de la Consejería de Igualdad, Salud y Políticas Sociales de la Junta de Andalucía, que tiene como objetivo que los profesionales sanitarios del sistema sanitario público de Andalucía, puedan notificar riesgos, eventos adversos o incidentes de seguridad para el paciente, en el centro sanitario. Esta notificación puede realizarse en tiempo real y en el punto de atención, de manera rápida, muy sencilla y garantizando el anonimato.

Fuente: 07/04/2015. Observatorio para la Seguridad del Paciente.
<http://www.juntadeandalucia.es/agenciadecalidadsanitaria/observatorioseguridadpaciente/opencms/es/apps-salud/index.html>

El Hospital de Campdevàrol implanta tabletas para la firma de documentos

El Hospital de Campdevàrol, en la provincia de Girona, ha implantado el uso de tabletas táctiles para la firma de documentos con información de salud; concretamente, utiliza la firma biométrica para los documentos que hacen referencia a la Ley Orgánica de Protección de Datos (LOPD) y a los consentimientos informados. Como la prueba piloto en el Servicio de Cirugía se valoró muy positivamente, se

decidió dar continuidad al proyecto y ahora se está preparando el despliegue a todos los servicios del centro.



Gracias a dicho sistema, los pacientes firman los documentos en una tableta táctil en lugar de hacerlo en un papel impreso. Después, estos documentos digitales son almacenados de manera segura en la historia electrónica del paciente. Además, el sistema ha sido recibido muy positivamente por parte del personal administrativo del centro, porque ahorra tiempo y no hay que almacenar todos los documentos en papel. Además, la firma biométrica agiliza los procedimientos y evita pérdidas de documentos.

Fuente: 02/02/2015. Acta Sanitaria.
<http://www.actasanitaria.com/el-hospital-de-campdevanol-implanta-las-tabletas-tactiles-para-la-firma-de-documentos/>

Plataforma de receta médica online para el sector privado en España

Un equipo de médicos, farmacéuticos e informáticos ha desarrollado la primera plataforma de receta médica online en España, cuyo objetivo es facilitar la renovación de recetas a los profesionales sanitarios del sector privado y a los pacientes; según sus creadores, "Receta Médica Online" (<https://www.recetamedicaonline.es/>) es una herramienta tecnológica que permite a médicos y farmacéuticos comunicarse con su paciente vía telemática y renovar la receta sin necesidad de desplazarse.

Cualquier médico colegiado puede registrarse sin coste y comunicarse vía telemática con su paciente para recetarle los medicamentos que previamente se le han indicado. Una vez autorizada la receta



electrónica, se le envía al paciente a su smartphone, tablet u ordenador para que pueda imprimirla y retirar su medicina en cualquier farmacia de España.

Fuente: 23/04/2015. Acta Sanitaria.

<http://www.actasanitaria.com/nace-una-plataforma-de-receta-medica-online-en-espana/>



Aplicación para la rehabilitación de dedos y manos en esclerosis múltiple.

Genzyme, filial de la francesa Sanofi, ha colaborado con la empresa dedicada a realidad virtual Virtualware para el desarrollo de EM One Hand, una herramienta para la rehabilitación fina de dedos y manos en formato virtual para pacientes con esclerosis múltiple (EM).

El sistema utiliza un dispositivo de captura e interpretación de los movimientos llamado Leap Motion, que permite utilizar la tecnología del videojuego con fines terapéuticos.

Fuente: 30/04/2015. Diario Médico. <http://www.diariomedico.com/2015/04/30/area-profesional/gestion/genzyme-virtualware-rehabilitacion-em-one-hand>

NOTICIAS DE EMPRESAS

Gfi España y Gfi Francia unifican sus soluciones clínicas asistenciales con mira®

Gfi España y Gfi Francia unifican sus soluciones de Software para las estaciones clínicas asistenciales y acuerdan que mira® (de la empresa de Gfi Savac) sea la solución de continuidad para sus clientes del sector Salud tanto en Francia como en España. El acuerdo reafirma la estrategia emprendida por Gfi (Savac) hace más de 4 años de diseñar y crear una Estación Clínica como una capa Software independiente e interconectable con cualquier HIS, así como la inversión conjunta de más de un millón y medio de euros. Las primeras instalaciones en Francia se llevarán a cabo durante el segundo semestre de 2016.

mira® es la Estación clínica de trabajo pensada por y para los médicos, personal de enfermería y profesionales clínicos. Permite el acceso a toda la información de un paciente, incorporando

todas las gestiones que realizadas en relación con el mismo. De esta forma, la recogida de antecedentes, las órdenes médicas (prescripción farmacológica, petición de pruebas complementarias, etc.) el diseño y ejecución de planes de cuidados, etc. se incorporan a la Historia Clínica Electrónica, que puede ser compartida con otras organizaciones. Además, dispone de un sistema de alertas, creación de plantillas, consulta de resultados de pruebas, entre otras utilidades y permite la personalización individual de las pantallas de cada usuario y su integración con cualquier Sistema de Información Hospitalario. Todo ello, para simplificar el trabajo del personal asistencial y aumentar el tiempo dedicado a los pacientes.

Más información: www.gfi.es

Coordina: **Alberto Gómez Lafón**

Vocal Asesor de la DGCBSNS y Farmacia

Proyecto FOGA-Farmacia (Fondo de Garantía Asistencial)

El Real Decreto 16/2012 introdujo modificaciones muy importantes en el contexto de la prestación sanitaria en nuestro Sistema Nacional de Salud e incorporó en su Artículo 8 ter, la Cartera Común Suplementaria que básicamente incluye todas aquellas prestaciones cuya provisión se realiza mediante dispensación ambulatoria y están sujetas a aportación del usuario.

Comprende esta cartera las siguientes prestaciones:

- Prestación farmacéutica.
- Prestación ortoprotésica.
- Prestación con productos dietéticos.

FOGA Farmacia constituye un subconjunto que opera de manera autónoma, aunque forma parte del concepto general de compensación financiera y, por tanto, del sistema de gestión e información cuya titularidad la ostenta la Dirección General de Cartera Básica de Servicios del SNS y Farmacia.

Conceptualmente, el sistema se ha diseñado contemplando los siguientes epígrafes:

- Farmacia
- Atención Primaria
- Informes Foga (incluye a los dos anteriores)
- Explotación
- Administración.

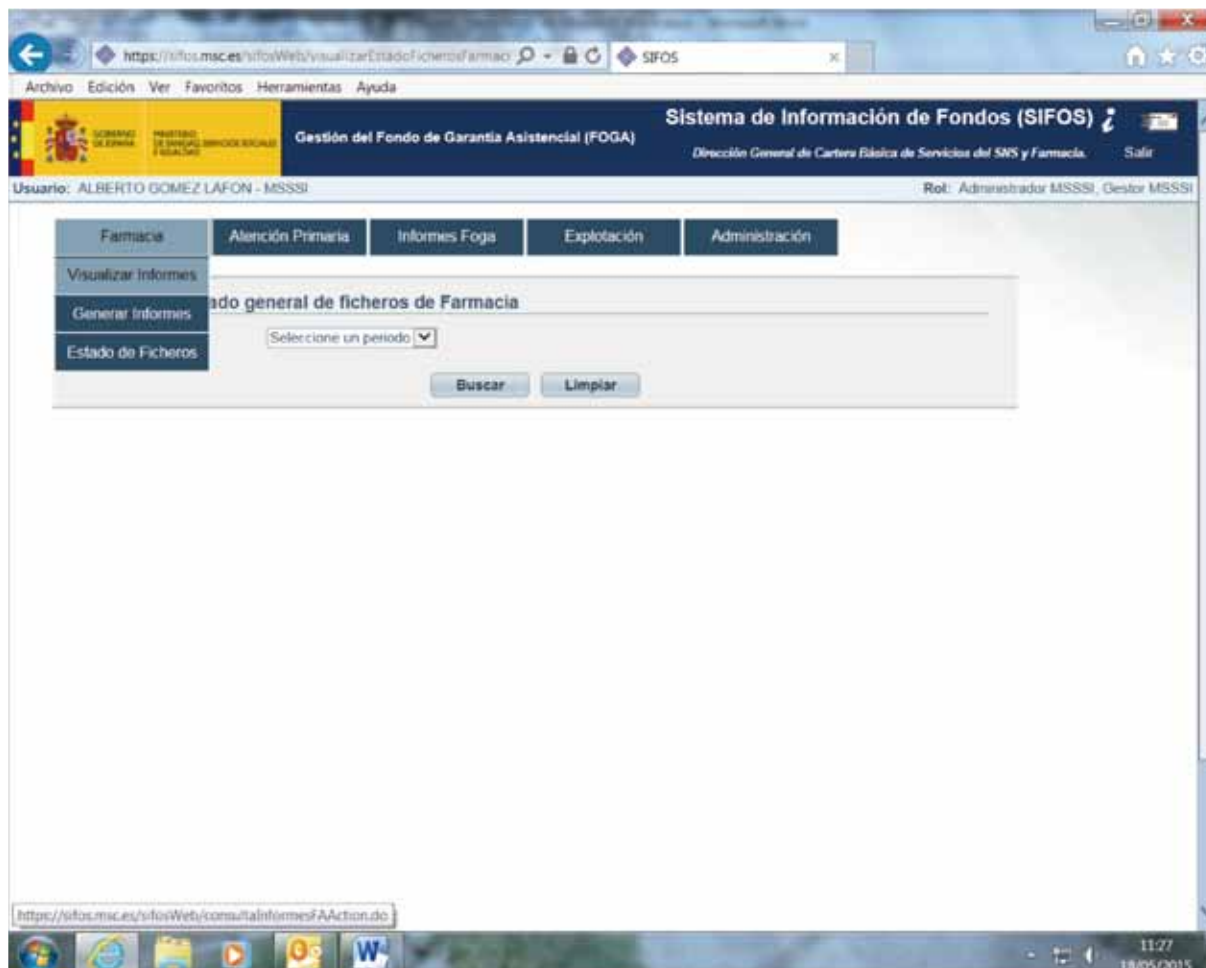
En el primer apartado de farmacia, hay disponibles tres opciones como son:

- Visualizar informes
- Generar informes
- Estado de los ficheros.

Los ficheros contienen todas las recetas que han pasado varios filtros entre los que caben destacar dos. El primero separa las recetas que han sido informadas en el apartado CIP (código de identificación personal), es decir, contiene información sobre el asegurado al que le ha sido prescrita la receta, para posteriormente validar que el mismo no pertenece a la Comunidad Autónoma en la que se ha realizado la dispensación (facturación).

El CIP se valida en la base de datos de tarjeta sanitaria y, si existiera alguna referencia, será objeto de compensación económica. El segundo filtro importante afecta a las recetas que no vienen in-





formadas en el apartado CIP. En este caso el sistema valida la primera letra del apartado correspondiente a su número de indentificación, que señala en que CA se realizó la prescripción y además, que esta es diferente de la CA en la que se facturó, ya que en esos casos la receta es objeto de compensación. No es difícil entender que la información obtenida es mucho mas fiable con el primer filtro que con el segundo y por ello, se considera que el segundo filtro deberá quedar con el tiempo en una opción minoritaria y exclusivamente aplicable a determinadas situaciones en las cuales la prescripción se realiza en soporte impreso. Por el momento, esta opción se está aplicando en aquellas CCAA todavía no preparadas para incorporar el CIP en sus procesos de captura de datos.

Todos los ficheros con los resultados de compensación serán accesibles por parte de los responsables autonómicos, para que puedan verificar cada receta sujeta a compensación y así tener la posibilidad de ejercitar las acciones que consideren oportunas.

Existirán dos tipos de usuarios de carácter autonómico que operarán en FOGA Farmacia. Por una parte los gestores, que serán los encargados de remitir los ficheros y que probablemente serán los mismos que actualmente se encargan de enviar los ficheros de facturación mensualmente y por otra los supervisores, que podrán acceder a toda la información de su CA. Además, estos supervisores pueden ser los mismos o no que los titulares en Atención Primaria, y podrán acceder tanto a la información de Farmacia como a la global.

La primera fase de FOGA comprendió los seis últimos meses de 2012 y todo 2013 y los datos correspondían a los obtenidos aplicando el segundo filtro anteriormente mencionado. La información que corresponde a 2014 se encuentra formada por una mezcla todavía importante como resultado de aplicar ambos filtros. Ciertamente y en base a las disponibilidades técnicas y tecnológicas de cada CA, las cifras que se obtengan marcarán las diferencias de aplicar uno u otro criterio, que en todo caso se espera que para 2015 será mas uniforme.

App Centradas en los Pacientes y sus Necesidades: Apps de Cuidados

Ruth Molina Fuillerat¹, Mercedes Muñoz Becerra²

1. Enfermera en la Unidad de Diálisis del Complejo Hospitalario Universitario de Granada. @RuthMoli

2. Enfermera en la Unidad de Diálisis del Complejo Hospitalario Universitario de Granada. @merchezul @Dialisis24h <http://www.dialisis24h.com/>

Hoy en día titulares como estos leemos a diario... "Un paciente experto y formado mejora en su salud" ó "el 20% de los pacientes crónicos usa móvil para temas relacionados con su salud". Conceptos como el de la mSalud y mHealth están ya presentes en nuestras consultas médicas y de enfermería, en la relación del día a día con nuestros pacientes, convirtiéndose en poderosos instrumentos para la gestión de las enfermedades crónicas, la promoción de hábitos saludables y el empoderamiento de los pacientes. Enfermería debe de estar presente en todos los canales donde el paciente está y reclame, empezando a liderar iniciativas y proyectos de la mSalud, y aplicaciones móviles de cuidados para pacientes.

Usar la tecnología para personalizar los cuidados, porque nosotras entendemos que para que la tecnología funcione debe de existir contacto directo. Apps que estén centradas en el paciente y sus necesidades, de persona a persona. Cuidados innovadores que unan la ciencia, la tecnología y el arte de Enfermería. Existe gran cantidad de Apps de cuidados para pacientes crónicos: hipertensos, diabéticos, anticoagulados... etc. ¿Pero realmente se ha tenido en cuenta las necesidades del paciente? ¿Estas apps están lideradas o realizadas por Enfermería, protagonista esencial de la prestación de cuidados? ¿Se posibilita la participación activa de los pacientes en el diseño, contenido y desarrollo de las apps de cuidados?

Buscamos que los pacientes se hagan más responsables de su enfermedad. Estas herramientas educativas son complementarias a lo que ya estamos trabajando, es decir, a un enfoque que potencie que el paciente esté formado e informado en su enfermedad.

Nuestra app Diálisis24h, aplicación de ayuda y soporte para el paciente renal en diálisis, surge de una necesidad sentida y demandada a lo largo del tiempo por parte de nuestros pacientes. "Traigo 4kg y solo he bebido dos vasos de agua" es la frase más oída y repetida en nuestras salas de diálisis. El control de la ingesta de líquidos es fundamental para el autocuidado de los pacientes renales en programa

de diálisis. Sin embargo, la experiencia clínica muestra que, ése es el aspecto del tratamiento donde se produce mayor grado de incumplimiento, debido al desconocimiento y manejo insuficiente de su balance hídrico y manejo nutricional. A la hora de crear una app de cuidados con éxito y que funcione es importante tener en cuenta a los pacientes, porque si de verdad queremos que el centro de atención sea el paciente, hay que escucharlos, que se sientan escuchados, valorados e identificados.

Nosotras abordamos esta necesidad creando Diálisis24h, una app centrada en las necesidades del paciente, a pie de cama, posibilitando la participación activa de ellos mismos en el diseño y contenido de la app, todo un proceso enriquecedor donde han dado su punto de visto y sugerido mejoras. En definitiva ellos mismos, los pacientes, la han hecho suya. Han pasado de ser un elemento pasivo a activo, a querer saber más sobre su enfermedad e involucrarse. A ser más proactivos en la gestión de su propia salud. Las apps de cuidados pueden ser positivas no sólo para los pacientes, que reciben un nuevo estímulo para el aprendizaje, sino también para los profesionales implicados en su cuidado, disponiendo de nuevas herramientas para su tarea educativa.

Las APPS no están concebidas dentro del sistema sanitario como parte del tratamiento de un paciente o como instrumento de ayuda en el cuidado de la salud y queda mucho por hacer aún, pero lo importante es que Enfermería ha iniciado el paso en este campo. Se necesitan más estudios sobre cuál es la mejor intervención además de pretender aportar conocimientos e idear diferentes métodos en este área, dando un aire nuevo y atractivo en la educación sanitaria de nuestros pacientes. Y la demostración científica de la viabilidad de las apps de cuidados dará pie a explorar aún más en la línea de investigación sobre intervenciones de salud móvil en el comportamiento de los enfermos y en especial, de los pacientes crónicos. Mejorando e impulsando la mejora y apoyo del abordaje integral de los pacientes.



CLINICAL COLLABORATION PLATFORM

Sistemas ayudó a Juan cuando se asustó por un latido irregular.

COLABORACION ENTRE LOS DISTINTOS SISTEMAS SANITARIOS.

El médico de cabecera de Juan lo derivó a un cardiólogo de otro centro hospitalario. Una plataforma informática avanzada, puso a disposición los datos de Juan, para que el cardiólogo los pudiese consultar.

Juan consiguió a tiempo una atención especializada – y ahora su corazón funciona como un reloj.

Connecting people and data. Anywhere.

Carestream

Vue

The power of together.

Lea el caso de estudio: carestream.es/ccp-es





Actividades de la SEIS

Agenda'15



XXII JORNADAS DE INFORMÁTICA SANITARIA EN ANDALUCÍA:

“INNOVACIÓN Y SALUD”

Sede: Málaga - Torremolinos

Fechas: 17, 18 y 19 de Junio 2015.

V REUNIÓN DEL FORO PARA LA GOBERNANZA DE LAS TIC EN SALUD

Sede: Bilbao

Fechas: 6 y 7 de Octubre de 2015

XIII REUNIÓN DEL FORO DE TELEMEDICINA Y

II CONGRESO IBEROAMERICANO

DE TELESALUD Y TELEMEDICINA Y XII FORO IBÉRICO

Sede: Sevilla

Fechas: 23 al 25 de Noviembre de 2015

IV REUNIÓN DE LA PLATAFORMA TECNOLÓGICA

PARA LA INNOVACIÓN EN SALUD

Sede: Sevilla

Fechas: 25 al 26 de Noviembre de 2015



2ª Edición

MÁSTER EN DIRECCIÓN DE SISTEMAS Y TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES PARA LA SALUD

El objetivo del máster es la especialización de profesionales en la gestión directiva de las TIC en Salud en el ámbito público, privado y de las empresas proveedoras de soluciones tecnológicas, revisión de casuísticas que se producen en el ámbito de las TIC de la salud, con la presentación de casos de éxito que ayuden a su resolución.

DIRIGIDO A:

- * Directivos de las Administraciones autonómicas y estatales en el área de Salud
- * Directivos de organizaciones privadas aseguradoras o proveedoras de servicios de salud
- * Responsables de informática, comunicaciones y sistemas de información (CIOs) de Hospitales y otras organizaciones públicas y privadas proveedoras de servicios sanitarios y sociales
- * Gestores de TIC en empresas de aseguramiento sanitario
- * Gestores de proyectos de TIC para la salud en empresas consultoras
- * Directivos y profesionales de empresas tecnológicas proveedoras de herramientas, servicios y soluciones TIC en Salud
- * En general profesionales que deseen desarrollar su carrera en la Dirección TIC para la Salud

PROGRAMA

A1: Marco de Referencia y Bases de las TIC en Sanidad

A2: Gestión Directiva de las TIC en Salud

A3: Las TIC en el Sistema Sanitario

A4: Tecnologías y Soluciones TIC en Salud

Comienzo: noviembre 2015

Fecha de Matriculación: a partir del 20 de junio de 2015

Duración: 1 año académicos 60 ECT's

Metodología: Presencial y Virtual. Las clases presenciales suponen 2 días al mes (normalmente jueves y viernes) incluyendo las visitas y asistencia a Congresos y Jornadas Técnicas. Para aquellos alumnos que puedan tener dificultades para desplazarse a sesiones presenciales, se establecerá un programa personalizado alternativo que les permita obtener la titulación.

Institución Docente: Escuela Nacional de Sanidad (ENS) Instituto de Salud Carlos III (c/ Monforte de Lemos 5, Pabellón 8) Madrid

EQUIPO DOCENTE

Estará formado por profesionales de reconocido prestigio en el sector sanitario y tecnológico, tanto del sector público como del privado y de entidades generadoras de innovación.

