NÚMERO
122

I+S

ABRIL
2017

REVISTA DE LA SOCIEDAD ESPAÑOLA DE INFORMÁTICA Y SALUD



ESPECIAL

SEGURIDAD Y PROTECCIÓN DE DATOS

Preparándonos para el Nuevo Reglamento de Protección de Datos

ENTIDADES ASOCIADAS

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD































































SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

Director
Salvador Arribas Valiente

Comité Editorial
Jesus Galván Romo
Alberto Gómez Lafón
Francisco Martínez del Cerro
Julio Moreno González
Luciano Sáez Ayerra
Zaida Sampedro Préstamo
Guillermo Vázquez González

Consejo de Redacción
Elvira Alonso Suero
Martín Begoña Oleaga
Ángel Blanco Rubio
Javier Carnicero Giménez de Azcárate
Inmaculada Castejón Zamudio
Miguel Chavarría Díaz
Juan Ignacio Coll Clavero
Juan Díaz García
Francisco Javier Francisco Verdú
Carlos Gallego Pérez
Carlos García Codina
Gregorio Gómez Soriano
Vicente Hernández
Javier López Cavero
José Luis Lorenzo Romero
Raul Martínez Santiago
José Luis Monteagudo Peña
Adolfo Muñoz Carrero
Juan Fernando Muñoz Montalbo
Carlos Luis Parra Calderón
José Quintela Seoane
Dolores Ruiz Iglesias
José Sacristán Paris

Colaborador Técnico
Diego Sáez

Información, Publicidad, Suscripciones y Distribución:
CEFIC. C/ Enrique Larreta, 5
Bajo Izda 28036 Madrid
Tlfno: 913 889 478
e-mail: cefic@cefic.es

Producción Editorial:
EDITORIAL MIC
Tel. 902 271 902 · 987 27 27 27
www.editorialmic.com

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

5 **EDITORIAL**

6 **ESPECIAL:** SEGURIDAD Y PROTECCIÓN DE DATOS

6 Preparándonos para el Nuevo Reglamento de Protección de Datos
7 Desvinculando datos personales: Seudonimización, Desidentificación y Anonimización
10 El nuevo Reglamento Europeo de Protección de Datos
13 Los Datos de Salud en el Nuevo Reglamento Europeo de Protección de Datos
15 La aplicación del Reglamento General de Protección de Datos en el Sector Salud de Datos
18 Plataforma centralizada de logs del Ib-Salut
22 Esquema Nacional de Seguridad en el Servicio Aragonés de Salud
28 Protección de datos en estudios de investigación biomédica desde la perspectiva del Reglamento Europeo
30 Los directivos ante la transformación digital

33 **ACTIVIDADES DE LA SEIS**

33 XIV Foro de Seguridad y Protección de Datos en Salud
48 VII Reunión del Foro de Interoperabilidad en Salud
51 XXIV Jornadas Nacionales de Innovación y Salud en Andalucía
52 XXII Premios Nacionales de Informática y Salud 2016

82 **FOROS Y SECTORES**

58 Foro de Protección de Datos en Salud
59 Foro de Gobernanza
60 Foro Telemedicina
61 Foro de Interoperabilidad
62 Sector de Enfermería
63 Sector de Informática Médica
64 Sector de Farmacia

68 **NOTICIAS DEL SECTOR**

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.
Queda prohibida la reproducción total o parcial sin citar su procedencia.

ENTIDADES
COLABORADORAS

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

CONSEJO GENERAL DE COLEGIOS OFICIALES DE FARMACÉUTICOS

OSAKIDETZA - SERVICIO VASCO DE SALUD

COLEGIO OFICIAL DE FARMACÉUTICOS DE CÁCERES

COLEGIO OFICIAL DE FARMACÉUTIOS DE BADAJOZ

IDCSALUD

MUTUAL CYCLOPS-CENTRE DOCUMENTACIÓ

EMERGRAF, S.L. CREACIONES GRÁFICAS

HOSPITAL CLINIC. SISTEMAS DE INFORMACIÓN

COLABORADORES TECNOLÓGICOS

Atos · connectis · FUJITSU

gmv · Ibermática · indra

Informática El Corte Inglés · intel · InterSystems Health | Business | Government

PHILIPS · SIEMENS Healthineers · T-Systems

La **Seguridad** una **prioridad vital** en las organizaciones sanitarias

Dada la relevancia de los temas de seguridad y protección de datos en el ámbito de la salud, dedicamos este número esencialmente a ello, además coincidiendo con la celebración en Sevilla el pasado mes de febrero de la XIV Reunión del Foro de Seguridad y Protección de Datos de Salud, donde analizamos la situación para la reutilización de la información de salud y del nuevo reglamento.

La transformación digital del sector salud, se está produciendo de una forma lenta pero ineludible: la tecnología disponible, el cambio cultural y la demanda del ciudadano provoca que nuestro sector este incorporando nuevas formas de trabajar y de ofrecer los servicios de salud por medios electrónicos.

Un freno para esta transformación puede ser la disponibilidad de los sistemas con las garantías adecuadas y su seguridad. Planteo esto a raíz de los datos que observamos en el INDICE SEIS, de los que podemos deducir que la inversión en seguridad de los sistemas si bien va incrementándose, no llega a cumplir unos porcentajes adecuados a las necesidades de nuestro sistema sanitario. Aunque podríamos argumentar que el presupuesto TIC global dedicado en sanidad es muy insuficiente, tampoco cumple en lo referente a los recursos humanos y organizativos dedicados a esta tarea.
Es necesario hacer esfuerzos adicionales en materia de seguridad, ya que además de las consideraciones técnicas y de las obligaciones derivadas del marco legal, el factor resistencia al cambio en las organizaciones utiliza argumentos de muchos tipos, pero el más habitual es sobre los efectos producidos por falta de disponibilidad de servicios y la seguridad de la información, provocando desconfianza tanto en los profesionales responsables de la atención sanitaria, como en los directivos y autoridades, e incluso en el ciudadano. Cualquier eventualidad será magnificada y supondrá un importante freno a la transformación. Debemos considerar este factor clave para el avance en la incorporación de nuevos proyectos, tenemos muchos ejemplos de paralizar importantes proyectos por esta causa, siempre además muy bien recogida por los medios de comunicación.
Todas las organizaciones sanitarias deben disponer de un análisis de riesgos de todos los sistemas de información, valorando las necesidades y requerimientos indispensables para poder cumplir, con las garantías acordes a los efectos que pueden producirse, la alta disponibilidad de los servicios electrónicos y de la seguridad y confidencialidad de la información.

Aunque se ha avanzado, todavía queda camino por recorrer no solo desde la perspectiva de disponer de los recursos tecnológicos necesarios, sino desde el punto de vista organizativo y de recursos humanos especializados.

Debería ser una prioridad en nuestras organizaciones este tema tan vital para nuestro sector.

Preparándonos para el Nuevo Reglamento de Protección de Datos

Juan Díaz
Coordinador del Comité Técnico de Seguridad de la Información de Salud

LOS MESES PASAN Y ESTAMOS LLEGANDO AL ECUADOR DEL PERIODO TRANSITORIO PARA LA ENTRADA DEFINITIVA DEL NUEVO REGLAMENTO DE PROTECCIÓN DE DATOS UE 2016/679 EL PRÓXIMO 25 DE MAYO DE 2018.

Las organizaciones sanitarias son subsidiarias de aplicar la mayoría de los requerimientos del Reglamento Europeo de Protección de Datos, ya que requieren un tratamiento de información especial "Salud" y de manera masiva afectando a toda la población en caso de la administración pública o en gran volumen como los centros sanitarios privados.

> ***El reglamento añade nuevos principios como la Transparencia, Minimización de datos utilizados y la Responsabilidad proactiva de las organizaciones, el establecimiento de políticas de protección de datos y la adhesión a códigos de conducta***

En su artículo 9 incluye a los datos relativos en la salud entre las categorías especiales de datos, hasta ahora conocidos como datos sensibles (salud, origen racial, religión) que cuentan con obligaciones reforzadas. Las entidades cuya actividad principal consista en el tratamiento a gran escala de categorías especiales de datos personales -hospitales, clínicas, aseguradoras médicas, mutuas y, eventualmente, laboratorios y empresas farmacéuticas- estarán obligadas a nombrar un delegado de protección de datos.

El reglamento añade nuevos principios como la Transparencia, Minimización de datos utilizados y la Responsabilidad proactiva de las organizaciones, basada en la existencia de procedimientos auditados, el establecimiento de políticas de protección de datos y la adhesión a códigos de conducta y certificaciones en materia de protección de datos.

El nuevo marco permite una aplicación flexible de medidas de seguridad en función de los requerimientos de cada tipo de tratamiento de datos, adecuando proporcionalmente las salvaguardas en función de los riesgos detectados. Las organizaciones sanitarias tendrán que realizar un análisis de riesgo de los tratamientos que realizan (PIA Privacy Impact Analysis) para determinar qué medidas tienen que aplicar y como hacerlo.

Con carácter general debemos revisar la información que trata la organización, los datos personales recogidos, de dónde vienen y con quién los comparte, constituyendo un registro obligatorio de tratamientos realizados. También debemos revisar los textos de los avisos, consentimientos y cláusulas de privacidad actuales para su actualización.

Tenemos que facilitar el conocimiento y concienciación en toda la organización ante este nue-vo marco y en especial a sus responsables, para priorizar las áreas que podrán causar problemas de cumplimiento. Será necesario que las organizaciones afectadas identifiquen a su Delegado de Protección de Datos que velará por el cumplimiento legal, contando con el apoyo y la autoridad para hacerlo con eficacia.

Por tanto debemos iniciar con premura una adaptación progresiva al Reglamento antes de que sea aplicable, consiguiendo que nuestras organizaciones estén preparadas para cuando entre en vigor en nuevo reglamento. Los siguientes artículos nos enseñan como abordarlo en algunos de sus puntos claves.

Desvinculando datos personales: Seudonimización, Desidentificación y Anonimización

Ramón Miralles López
Coordinador de Auditoria i Seguridad de la Información en la Autoridad Catalana de Protección de Datos

EN LA REUTILIZACIÓN DE LA INFORMACIÓN OBTENIDA A PARTIR DE LOS PROCESOS ASISTENCIALES RELACIONADOS CON LA SALUD DE LAS PERSONAS CONCURREN AL MENOS 2 CUESTIONES QUE, A PRIORI, PUEDEN RESULTAR ANTAGÓNICAS Y DE DIFÍCIL CONJUGACIÓN.

Por un lado el alto valor que puede tener esa información para la investigación médica, y por otro el hecho de que los datos relacionados con la salud son datos personales de carácter sensible, para los que el marco jurídico impone una serie de cauteles en forma de requisitos o limitaciones en su uso y tratamiento.

El Reglamento (UE) 2016/679 del parlamento europeo y del consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, en adelante el RGPD), que será aplicable a partir del 25 de mayo de 2018, y viene a ampliar el significado de los denominados «datos de salud».

El todavía vigente marco jurídico del derecho a la protección de los datos de carácter personal, que será desplazado por el RGPD a partir de mayo de 2018, define los datos personales relacionados con la salud, como las informaciones referidas a «la salud pasada, presente y futura, física o mental», de una persona, incluyendo su información genética.

Con el RGPD el legislador Europeo ha redefinido los datos relativos a la salud, obviamente manteniendo su esencia, en cuanto a que se refieren a la salud física y mental de una persona, pero pasando también a ser considerados como tales las informaciones derivadas de la prestación de los servicios de atención sanitaria, en tanto puedan revelar el estado de salud de las personas.

Por tanto incluye información sobre la persona, recogida con ocasión de su inscripción en registros a efectos de asistencia sanitaria o con ocasión de la propia prestación de la asistencia; también cualquier número, código, símbolo o dato «asignado a una persona física que la identifique de manera unívoca a efectos sanitarios»; y continúa describiendo el considerando 35 del RGPD «la información obtenida de pruebas o exámenes de una parte del cuerpo o de una sustancia corporal, incluida la procedente de datos genéticos y muestras biológicas, y cualquier información relativa, a título de ejemplo, a una enfermedad, una discapacidad, el riesgo de padecer enfermedades, el historial médico, el tratamiento clínico o el estado fisiológico o biomédico del interesado, independientemente de su fuente, por ejemplo un médico u otro profesional sanitario, un hospital, un dispositivo médico, o una prueba diagnóstica in vitro».

Ahora se definen de manera separada los «datos genéticos» y se les da una relevancia propia, siendo aquellos «datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona».

Y el RGPD pasa a considerar tanto los datos relativos a la salud, como a los datos genéticos, como categorías especiales de datos persona-

les, lo que tiene como primera consecuencia que queda prohibido su tratamiento, obviamente estableciendo el RGPD en que circunstancies no aplica la mencionada prohibición, es decir, se van a establecer para ese tipo de datos toda una serie de cauteles en cuanto al uso que puede llegar a dárseles.

Pero no es la intención de este artículo abordar de qué manera se regulan los datos relativos a la salud en el RGPD, ni profundizar en su régimen jurídico en el RGPD, sino que la intención es conectar algunos contenidos del Reglamento con la ejecución de proyectos que puedan tener por objeto el tratamiento masivo de información, o en su caso la aplicación de técnicas de "big data" en los que se puedan ver involucrados datos relativos a la salud o a la genética.

El "big data" realmente no aparecen de una manera explícita en el Reglamento General de Protección de Datos, lo que por otra parte resulta adecuado, ya que eso redunda en su neutralidad tecnológica, y por tanto en su perdurabilidad como instrumento jurídico destinado a regular situaciones en las que las tecnologías de la información y la comunicación, y su continua evolución, están muy presentes.

> ***El reto y la dificultad será crear un conjunto de datos protegidos, que, sin identificar directamente a las personas, resulten útiles a la finalidad del posterior tratamiento.***

Sí que hay una referencia del Reglamento que si nos puede ser de utilidad, concretamente cuando el reglamento describe los que denomina "operaciones de tratamiento a gran escala", que son aquellas "que persiguen tratar una cantidad considerable de datos personales a nivel regional, nacional o supranacional y que podrían afectar a un gran número de interesados".

Desde la perspectiva del RGPD estaríamos situados en ese tipo de tratamientos, que vendrían a estar relacionados con el tratamiento masivo o incluso con el "big data".

En el RGPD esa característica de a "gran escala", en líneas generales, considera que supone un potencial escenario de "alto riesgo" para los derechos y libertades de las personas, por lo que se exige también para ese tipo de operaciones de tratamiento unas mayores cautelas.

Por descontando las decisiones sobre cómo llevar a cabo ese tipo de tratamientos se van sustentar en la gestión de ese riesgo, que es uno de los pilares de la nueva arquitectura Europea del derecho fundamental a la protección de los datos de carácter personal.

Ese enfoque al riesgo, que deberá estar presente en todas y cada una de las decisiones relacionadas con las operaciones de tratamiento de datos personales, implicará identificar, analizar y valorar el riesgo, y en función de esa valoración deberán ser tomadas las decisiones adecuadas para tratar o controlar el riesgo, fundamentalmente en el sentido de reducir su probabilidad y gravedad, decisiones que implicarán la adopción de medidas técnicas y organizativas.

Pues bien, entre las medidas que prevé el RGPD para proteger los datos de carácter personal se encuentra la «seudonimización», que el propio Reglamento define como un tratamiento de datos personales, cuyo resultado es que ya no puedan atribuirse (vincular) esos datos «seudonimizados» a una persona concreta, a no ser que se utilice información adicional para volver a vincular los datos a esa persona, debiendo figurar esa información adicional por separado y sujetá a medidas técnicas y organizativas destinadas que impidan que los datos personales se atribuyan a una persona física identificada o identificable.

En primer lugar quisiera hacer una breve referencia a 3 conceptos que me parecen claves en toda esta cuestión de proteger los datos personales en base a su transformación, vendrían a ser 3 posibles niveles de desvinculación de los datos personales.

Por un lado tenemos la «seudonimización», a la que ya me he referido, que implica eliminar de un conjunto de datos personales la vinculación con la persona, manteniendo separadamente la información necesaria para volver a vincular la información (re-identificar). Aquí los riesgos girarán en torno a esos datos que permiten la re-identificación y al uso de otras fuentes de información que permitan la re-identificación.

En un segundo nivel tendríamos lo que se denomina «desidentificación», que sería llevar a cabo el mismo proceso pero destruyendo los datos que permitirían la re-identificación directa. De manera que el riesgo quedaría limitado a que no se pueda re-identificar a personas en base al uso de otras fuentes de información.

Y finalmente la «anonimización», que implicaría que una vez realizada la «desidentificación», se aplican operaciones adicionales sobre los datos ya desvinculados, de manera que no se pueda producir la re-identificación en base a otras fuentes de información (aquí se aplicarían funciones criptográficas, perturbación de datos, reducción de datos, etc.)

En el siguiente enlace puede encontrarse información, elaborada por "Future of Privacy Forum" (https://fpf.org) que describe esos diferentes mecanismos de desvinculación y sus particularidades en cuanto a la protección de los datos personales.

Al final de lo que se trata es de llevar a cabo una serie de operaciones de transformación, sobre un conjunto de datos personales, que da como resultado otro conjunto de datos, que no identifican de manera directa a las personas a las cuales hacen referencia, pudiendo aplicar diferentes niveles de protección respecto del riesgo de re-identificación.

En cualquier caso, no debemos perder de vista que todo ese proceso de transformación implica llevar a cabo un tratamiento de datos personales, al cual le serán de aplicación la normativa de protección de datos; lo que llevaría a que, por ejemplo, una re-identificación no autorizada será considerada una violación de la seguridad de los datos.

El reto y la dificultad será crear un conjunto de datos protegidos, que, sin identificar directamente a las personas, resulten útiles a la finalidad del posterior tratamiento.

Por tanto, lo que podríamos denominar el «ciclo de la desvinculación de datos personales» implicará disponer de las tecnologías, las personas y los procesos adecuados que permitan reducir al máximo el riesgo de re-identificación.

Ese ciclo estaría dividido en una serie de fases que pueden describirse brevemente de la siguiente manera:

1. Debe iniciarse con el diseño del método de desvinculación, es decir, cómo tenemos previsto transformar los datos personales para protegerlos, obviamente incluyendo aquí potenciales evaluaciones de impacto, análisis de riesgos, etc.
2. La segunda fase del ciclo será la aplicación del método diseñado.
3. La tercera fase será verificar, antes de liberar la información, que efectivamente el riesgo de re-identificación está dentro de los márgenes aceptables y que la información resultante es de utilidad.

   Así en función del método de transformación, a efectos de re-identificación habrá que verificar si:
   - ¿Se puede singularizar a una persona concreta?
   - ¿Se pueden vincular registros relativos a una persona?
   - ¿Se puede inferir información relativa a una persona?

4. Y la última fase del ciclo será revisar periódicamente el proceso de desvinculación, a fin de valorar si el diseño inicial sigue siendo válido, y en caso de no serlo deberá procederse a su rediseño, iniciándose de nuevo el ciclo.

De este modo, aplicando un proceso sistemático, estaremos dando respuesta a la protección de los datos personales, especialmente en escenarios de tratamiento de datos a gran escala que requieren de garantías adicionales, como sería el caso de la reutilización de datos de salud y datos genéticos.



Ciclo de desvinculación de datos personales

El nuevo Reglamento Europeo de Protección de Datos:

Una oportunidad para avanzar en investigación biomédica con las garantías adecuadas para los pacientes

Amelia Martín Uranga
Responsable Plataforma Medicamentos Innovadores. FARMAINDUSTRIA

ES IMPORTANTE RESALTAR EL COMPROMISO QUE ASUME LA INDUSTRIA FARMACÉUTICA CON LA INVESTIGACIÓN EN NUESTRO PAÍS, INVIRTIENDO MÁS DE 1000 MILLONES DE EUROS EN I+D. ESPAÑA SE ENCUENTRA ENTRE LOS MEJORES PAÍSES EUROPEOS PARA REALIZAR INVESTIGACIÓN CLÍNICA, CON LA FINALIDAD DE QUE LOS PACIENTES TENGAN ACCESO A FÁRMACOS INNOVADORES, AL MISMO TIEMPO QUE A LOS INVESTIGADORES LES OFRECE LA OPORTUNIDAD DE ADQUIRIR EXPERIENCIA REAL SOBRE FÁRMACOS EN DESARROLLO Y LA INDUSTRIA FARMACÉUTICA DISPONGA DE UN ENTRAMADO CIENTÍFICO, ÉTICO Y JURÍDICO DE PRIMER NIVEL.

La apuesta de la industria por la investigación clínica, por los pacientes y por la sociedad española en su conjunto, es una realidad que pone de manifiesto la apuesta que el sector desarrolla de forma coordinada con hospitales, centros de investigación, profesionales sanitarios y administraciones públicas. Por ello, una interpretación restrictiva de la normativa de protección de datos, así como de determinadas normas de aplicación sectorial en las que incide dicha normativa, puede poner en peligro el trabajo realizado en los últimos años, dado que afectaría significativamente a la capacidad de los sistemas sanitarios europeos y de los investigadores para avanzar en investigación biomédica y aprovechar todo el potencial que las diferentes fuentes del Big Data (ensayos clínicos, historia clínica electrónica, registros de pacientes, receta electrónica etc…) ofrecen a las autoridades sanitarias, a los investigadores y, por supuesto, a los pacientes. No se puede ignorar que todo ello ayuda en la toma de decisiones de forma rápida y eficaz, a realizar análisis predictivos, así como a una mejora continua de los sistemas de trabajo y de la eficiencia en cuestiones tan sensibles como la asistencia sanitaria, con la finalidad de impulsar mejoras en el sistema sanitario y en su sostenibilidad.

En el presente artículo, y con el nuevo Reglamento Europeo de Protección de Datos[1] (en adelante RGPD), que será plenamente aplicable en mayo de 2018, la autora se plantea diversas cuestiones relacionadas con la seguridad jurídica para los agentes públicos y privados que intervienen en la I+D de medicamentos, ¿discurren en paralelo la protección de datos y los avances científicos y tecnológicos?; ¿podemos usar los datos para fines distintos y compatibles[2] para los que el sujeto consintió? En este sentido, el art. 6.4 del RGPD recoge esta situación al establecer que "cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta (…)". En efecto, los datos no se agotan cuando se usan, se pueden reutilizar y su valor se incrementa cuando se conectan con otros datos, tal y como también se contempla en el espíritu del Reglamento, que

ya prevee el Big Data en salud[3]. Como señalábamos anteriormente, en la actualidad, el valor de la información ya no reside tanto en su uso primario como en los usos secundarios que se pueden hacer de esa información, por lo que evidentemente habrá que tomar las garantías adecuadas, que podrán incluir el cifrado o la seudonimización[4] (art. 6.4.e) del RGPD) y además los proyectos en los que se vaya a reutilizar información tendrán que ser aprobados por un Comité de ética de investigación que proteja los derechos e intereses de los participantes en el mismo. En este sentido ya existen Proyectos IMI como el Harmony, coordinado desde España, en el que en los 5 años de duración con 51 socios (públicos y privados , entre los que se encuentran 7 empresas farmacéuticas) de 11 países europeos, van a crear una plataforma de gestión de Big Data para integrar y compartir datos que permitan dar respuesta a los problemas más acuciantes de los tumores hematológicos y mejorar los tratamientos de los pacientes que los sufren[5].

¿Se pueden tratar datos personales sin el consentimiento del interesado, existen excepciones al consentimiento? En este sentido resultan relevantes los conceptos de interés público y salud pública (definidos en el Considerando 54 del RGDP)[6] y el artículo 9 i), j) del RGPD que introducen una legitimación específica para realizar investigación científica (definida a su vez en el Considerando 159 del RGDP)[7], siempre unido a dos elementos principales: existencia de una Ley de la Unión o de un EM[8] y las garantías y excepciones aplicables al tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos (art. 89 RGPD). En este sentido resulta necesaria una armonización a nivel europeo de los conceptos de interés público y de investigación científica ya que la investigación es actualmente internacional y los consorcios son de carácter paneuropeo

1. Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
2. Considerando 50 del RGPD "El tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial (...)" y el artículo 5.1b) del RGPD " los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»)
3. Considerando 157 del RGDP "Combinando información procedente de registros, los investigadores pueden obtener nuevos conocimientos de gran valor sobre condiciones médicas extendidas, como las enfermedades cardiovasculares, el cáncer y la depresión. Partiendo de registros, los resultados de las investigaciones pueden ser más sólidos, ya que se basan en una población mayor. Dentro de las ciencias sociales, la investigación basada en registros permite que los investigadores obtengan conocimientos esenciales acerca de la correlación a largo plazo, con otras condiciones de vida, de diversas condiciones sociales, como el desempleo y la educación. Los resultados de investigaciones obtenidos de registros proporcionan conocimientos sólidos y de alta calidad que pueden servir de base para la concepción y ejecución de políticas basada en el conocimiento, mejorar la calidad de vida de numerosas personas y mejorar la eficiencia de los servicios sociales. Para facilitar la investigación científica, los datos personales pueden tratarse con fines científicos, a reserva de condiciones y garantías adecuadas establecidas en el Derecho de la Unión o de los Estados miembros"
4. Definido en el art. 4.5) RGDP la «seudonimización como el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable"; La anonimización conforme a lo que establece la AEPD no se puede asegurar al 100%, además el RGDP no contempla la anonimización. De todos modos, en este ámbito es recomendable la seudonimización, minimizando riesgos de reidentificación, al mismo tiempo que se preserva el uso de los datos finales
5. https://www.imi.europa.eu/content/harmony
6. Considerando 54 del RGDP: El tratamiento de categorías especiales de datos personales, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública. Ese tratamiento debe estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y libertades de las personas físicas. En ese contexto, «salud pública» debe interpretarse en la definición del Reglamento (CE) n.o 1338/2008 del

de modo que no deberían utilizarse dentro de la UE conceptos diferentes sobre cuestiones relevantes para la salud de los ciudadanos.

Las investigaciones genéticas requieren en no pocas ocasiones el uso de muestras biológicas, bien de los sujetos que participan en el ensayo, bien de otras personas ajenas al mismo. En todo caso, los resultados de los análisis y de las demás pruebas pueden ser de gran utilidad para el progreso de las investigaciones en determinadas áreas como la genómica; en estos proyectos de investigación biomédica nos podríamos plantear la posibilidad de prestar un consentimiento más amplio de cara a futuras líneas de investigación que no estén inicialmente previstas. Es cierto que en muchas ocasiones, y a priori en el momento de la recogida de los datos personales con fines de investigación científica/biomédica, no es posible determinar con exactitud la finalidad del tratamiento que se va a dar a esos datos, pero se ha de permitir a los interesados dar su consentimiento para determinados ámbitos de la investigación científica siempre que se respeten las normas éticas reconocidas para la investigación científica, tal y como se recoge en el Considerando 33 del RGPD. En este sentido el Grupo de Comités de Ética y FARMAINDUSTRIA, están trabajando en colaboración para elaborar una Guía de Consentimiento Informado y Hoja de Información al Paciente que recoja esta posibilidad.

La nueva normativa comunitaria potencia además los denominados códigos de conducta (art. 40 y sss), como modelo de corregulación en el que las responsabilidades y derechos sean compartidos entre todos los agentes. Estos códigos éticos en materia de protección de datos, es algo en lo que FARMAINDUSTRIA se inició en 2009 con la publicación del Código Tipo de Protección de Datos para Investigación Clínica y Farmacovigilancia que va a ser actualizado conforme al nuevo marco normativo. Esta herramienta de FARMAINDUSTRIA proporciona un notable valor añadido y seguridad jurídica en el manejo de los datos de salud en el ámbito de la investigación clínica y la farmacovigilancia; aumentando, más si cabe, la confianza en una industria que siempre ha sido extremadamente escrupulosa en el tratamiento de este tipo de datos y en proteger adecuadamente los derechos e intereses de los pacientes.

En definitiva, el nuevo RGPD debe ser una oportunidad para seguir avanzando en proyectos de investigación biomédica que contemplen la reutilización de datos, o el uso de datos de salud "a gran escala", incluyendo las garantías adecuadas para asegurar el máximo beneficio de los pacientes, siempre bajo la supervisión de los comités de ética de investigación. Se ha de tener presente el mecanismo de coherencia del Reglamento Europeo, para que todas las autoridades estén alineadas en esta materia, con la finalidad de conseguir una adecuada armonización que otorgue seguridad jurídica y permita a nuestros investigadores mantener un liderazgo en el ámbito de consorcios paneuropeos de investigación biomédica presentes y futuros, buscando y respetando siempre un adecuado equilibrio entre la protección de datos de los participantes, y otros valores sociales como la salud pública, el interés público y la promoción de la investigación biomédica en el mayor beneficio de los pacientes.

Parlamento Europeo y del Consejo (1), es decir, todos los elementos relacionados con la salud, concretamente el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, *los recursos asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria,* y las causas de mortalidad (…)".

7. Considerando 159 del RGDP: " El presente Reglamento también debe aplicarse al tratamiento datos personales que se realice con fines de investigación científica. El tratamiento de datos personales con fines de investigación científica debe interpretarse, a efectos del presente Reglamento, de manera amplia, que incluya, por ejemplo, el desarrollo tecnológico y la demostración, la investigación fundamental, la investigación aplicada y la investigación financiada por el sector privado. Además, debe tener en cuenta el objetivo de la Unión establecido en el artículo 179, apartado 1, del TFUE de realizar un espacio europeo de investigación. Entre los fines de investigación científica también se deben incluir los estudios realizados en interés público en el ámbito de la salud pública. (…)"
8. En España la Ley 14/2007 de Investigación Biomédica; Real Decreto 1716/2011, de 18 de noviembre, por el que se establecen los requisitos básicos de autorización y funcionamiento de los biobancos con fines de investigación biomédica y del tratamiento de las muestras biológicas de origen humano, y se regula el funcionamiento y organización del Registro Nacional de Biobancos para investigación biomédica

Los Datos de Salud en el Nuevo Reglamento Europeo de Protección de Datos

Iñaki Pariente de Prada
Socio Director Fundador DAYNTIC LEGAL. Consultoría en Derecho Digital y Protección de Datos. Abogado. ExDirector Agencia Vasca de Protección de Datos.

EL 25 DE ENERO DE 2012 LA ENTONCES COMISARIA EUROPEA VIVIANNE REDING PRESENTÓ UN AMBICIOSO PROYECTO DE ELABORACIÓN DE UNA NORMA EUROPEA DE PROTECCIÓN DE DATOS QUE FUERA DIRECTAMENTE APLICABLE EN TODOS LOS ESTADOS MIEMBROS Y QUE UNIFICARA LA INTERPRETACIÓN Y APLICACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS EN EL ÁMBITO EUROPEO.

El día 4 de mayo de 2016 finalmente se publicó en el Diario Oficial un Reglamento Europeo que después de muchas idas y venidas contenía una serie de principios esenciales que vienen a renovar la normativa de la protección de datos de forma importante.

En el ámbito de la salud, se introduce en la definición de datos de salud la información proveniente de la asistencia sanitaria, de forma expresa. No creo que hubiera ninguna duda al respecto, pero el proceso legislativo y las sucesivas reformas que ha sufrido el proyecto original, con enmiendas de las distintas instituciones participantes, ha incluido expresamente esta mención. El dato de salud sigue refiriéndose a la salud pasada, presente y futura, y no creo que en su aplicación práctica tengamos ningún ejemplo de problemas prácticos en cuando al concepto.

Se definen expresamente los datos genéticos, como aquellos datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona. Entre las tareas pendientes una vez que este Reglamento entró en vigor el día 25 de mayo de 2016, se encuentra la de revisar la normativa interna incompatible, lo que supondrá que la normativa sobre estudios genéticos, uso de material genético o investigación deberá adaptarse tanto a este principio general, como al resto de principios generales del Reglamento.

Ambos, junto con otros como los datos biométricos, se incluyen dentro de la categoría de "categorías especiales de datos", que requieren, en cuanto a la prestación del consentimiento, un consentimiento explícito de la persona para su tratamiento, salvo en aquellos supuestos en que se utilice una causa de licitud para el tratamiento distinta. El consentimiento en estos casos debe ser explícito para el tratamiento de los datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado.

El artículo 9 plantea una situación algo distinta a la que venía aplicándose en España de acuerdo con el la normativa interna en vigor. En efecto, la licitud para el tratamiento de datos personales de salud en el momento actual en España pasa por el consentimiento expreso como causa ordinaria, que en su caso puede sufrir excepciones.

En la situación actual tras la aprobación del Reglamento Europeo ya no tiene como principal causa de licitud el consentimiento, sino que

partimos de un principio general de prohibición general del tratamiento, con las excepciones previstas en el artículo 9, entre las cuales se encuentra el consentimiento, pero también otras condiciones de licitud, en concreto las siguientes:

- Apartado h) El tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;
- Apartado i) El tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional,
- Apartado j) El tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

En los tres supuestos que mencionamos, debemos tener en cuenta que cualquier tratamiento de datos de salud sin consentimiento que se base en una de las tres causas expuestas, debe apoyarse en una norma del Derecho de la Unión o de los Estados miembros.

En el caso de diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social (llamo la atención sobre la asistencia social), la norma de Derecho interno no requiere un contenido mínimo, y además podrá basarse el tratamiento en la existencia de un contrato con un profesional sanitario.

En el caso de la salud pública, habrá que tener en cuenta la definición de salud pública que se establece en el Reglamento (CE) 1338/2008 del Parlamento Europeo y del Consejo, es decir, todos los elementos relacionados con la salud, concretamente el estado de salud, con inclusión de la morbilidad y la discapacidad, los determinantes que influyen en dicho estado de salud, las necesidades de asistencia sanitaria, los recursos asignados a la asistencia sanitaria, la puesta a disposición de asistencia sanitaria y el acceso universal a ella, así como los gastos y la financiación de la asistencia sanitaria, y las causas de mortalidad. Este tratamiento de datos relativos a la salud por razones de interés público no debe dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines.

Esa interpretación que se haga en el futuro, así como los límites de la misma, nos darán la clave de hasta dónde podemos tratar datos personales de salud sin el consentimiento de las personas.

Y por último lugar, la previsión del apartado j) para supuestos de investigación científica, que requiere una norma interna o europea que regule esta cuestión y que como mínimo sea proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado. Nos remite al artículo 89 del Reglamento en cuanto a las garantías del interesado.

En resumen, un panorama interesantísimo en el que nuevamente juristas y tecnólogos debemos ir de la mano en una interpretación dinámica de estos contenidos normativos, que debe tener como elemento esencial también a las agencias española y autonómicas de protección de datos.

La aplicación del Reglamento General de Protección de Datos en el Sector Salud de Datos

Vidal Valdunciel
Key Account Manager. Panda Security

LO GRAN MAYORÍA DE LOS DATOS QUE SE GENERAN Y MANEJAN EN EL SECTOR SALUD SON DE NATURALEZA PERSONAL, CONFIDENCIAL Y VITAL, Y SON AMPLIAMENTE COMPARTIDOS POR LOS DISTINTOS ACTORES Y PROVEEDORES QUE INTERVIENEN EN LA RED ASISTENCIAL.

La obligatoriedad de adaptar las prácticas de protección de datos de prácticamente todas las organizaciones y empresas que trabajan en el sector Salud al RGPD es un hecho.

Las organizaciones que no lo hagan, se enfrentarán a sanciones y otros problemas. Afrontarlo cuanto antes debe verse como una prioridad y a la vez como una oportunidad, que ayudará a tener una mayor visibilidad y control de los datos, un mayor nivel de protección e incluso un nuevo factor diferencial con la competencia.

SANCIONES Y OTROS PROBLEMAS DERIVADOS DEL INCUMPLIMIENTO DEL REGLAMENTO

Si las empresas no cumplen con el Reglamento a partir de la fecha de aplicación, el 25 de mayo de 2018, se enfrentan a:

- Daños económicos directo o indirectos ocasionados por incidentes de seguridad provenientes del exterior o por los propios empleados y colaboradores.
- Daños reputacionales derivados de que el incidente de seguridad debe notificarse públicamente.
- Pérdida de clientes actuales y potenciales cuando la empresa no puede demostrar que se encuentra en conformidad con la regulación.
- Riesgo de limitación o prohibiciónde procesamiento de datos que las DPAs pueden imponer, afectando la actividad normal de la empresa.
- Posible suspensión de los serviciosa los clientes, con el consecuente abandono de estos o incluso posibles acciones legales de los clientes, por la limitación para procesar los datos.
- Indemnizaciones que en virtud del nuevo Reglamento ya que los interesadostienen derecho a reclamar en caso de infracción.
- Así como las costosas multas de administraciónque pueden alcanzar hasta 20.000.000€ o el 4% del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

Con el cumplimiento del Reglamento las empresas evitarán los problemas anteriores y ganará la confianza de los consumidores y como tal una ventaja competitiva.

MECANISMO DE CERTIFICACIÓN APROBADO

Los legisladores han reconocido que para muchas empresas ser capaces de demostrar que se adhieren al RGPD será una ventaja. Para ello se está empezando a introducir los mecanismos de certificación de protección de datos y los sellos y marcas de protección de datos.

El RGPD habla incluso de la posibilidad de llegar a un sello europeo común de protección de datos, y aunque por ahora el RGPD proporciona escasos detalles, es de esperar que este mecanismo para mostrar la adhesión, se desarrollará en los próximos meses.

PLAN DE ACCIÓN PARA PREPARARSE PARA EL RGPD

Para adaptar las prácticas empresariales al RGPD, las empresas deben comenzar por entender su actual posición en la conformidad del reglamento. Un primer paso importante será que las organizaciones tengan bajo control los procesos de tratamiento de datos personales, incluyendo:

- Qué datos personales se tratan, incluyendo la recogida, tránsito, almacenamiento y procesamiento.
- Donde está esta información y quien tiene acceso a ella, través de su organización, incluyendo terceras empresas y colaboradores.
- Cuando se transfiera desde y hacia, incluido a terceros y transfronterizos.
- Cuáles son las medidas de seguridad a lo largo de su ciclo de vida.
- Cómo se almacena la información que permite la identificación del resto de la información.
- Cómo se permite la identificación, modificación, borrado o transferencia de los datos personales de un interesado si así lo solicitara.
- Cómo se comunica la política de privacidad y como se guarda y hace uso en el tratamiento de los datos, las respuestas.

PANDA ADAPTIVEDEFENSE AYUDA A CUMPLIR CON EL RGPD

El proceso de adecuación a las exigencias del RGPD requiere de un gran esfuerzo de concienciación, formación,análisis e implantación de nuevas prácticas y tecnología. Todo este esfuerzo corre el riesgo de acabar por no servir de nada si, la elección no es la acertada y por un fallo de seguridad en los sistemas, los datos que están siendo gestionados por la empresa se pierden o un atacante logra acceder a ellos.

Panda AdaptiveDefense reduce al mínimo estos riesgos y ayuda al cumplimiento del RGPD asentándose en dos pilares fundamentales:SeguridadyGobernanza de la Información.
Y es que estas son las dos claves, un buen control de los datos que se recogen, almacenan y tratan en los diferentes departamentos de la empresa tanto en los equipos como en los servidores, y la adopción de las medidas de seguridad necesarias para protegerlos de atacantes, adversarios o fallos de seguridad.
A partir de estas bases, se marcan tres líneas de acción que permiten garantizar la seguridad de los datos:

1. Preparación

La actitud proactiva por parte de las empresas es muy importante, teniendo que estar preparadas para la prevención de cualquier incidente de seguridad con el fin de neutralizarla lo antes posible o el bloqueo del atacante en el caso de que logre entrar en los sistemas, y lo mismo en lo referido a disponibilidad de realizar investigaciones forenses detalladas en cada momento.
Además, AdaptiveDefense permite realizar auditorías internas para verificar, el estado de seguridad del parque en cualquier momento, incluido antes del despliegue de la solución, en la puesta en marcha del plan de acción para el cumplimiento del RGPD o periódicamente.

2.Protección

Las verdaderas soluciones de seguridad deben combinar tecnología avanzadas e inteligencia humana y computacional, machine learning en manos de expertos en seguridad. Para que una solución de seguridad sea tomada en seria, debe ofrecer el tipo de prevención, detección, visibilidad e inteligencia que pueda detener y prevenir ciber-atacantes de cualquier tipo una y otra vez.
Las exigencias de protección de una empresa, incluida las exigencias del RGPD, que obliga a notificar en las primeras 72 horas del incidente el detalle de lo sucedió, impacto y acciones tomadas hasta el momento, obliga a que las soluciones de seguridad cubran los siguientes aspectos claves, que AdaptiveDefenseproporciona:

3. Visibilidad y Control

Los datos están vivos: crecen, cambian e incluso se mueven. Organizar la gestión de los mismos para adecuarse a la nueva norma es solo el principio. Una vez que todo esté como debe es imprescindible mantener un control constante sobre losmismos, con el fin de comprobar si se produce algún movimiento anómalo sobre ellos.

AdvancedReportingTool (ART), el módulo de AdaptiveDefense, es una herramienta de Informes Avanzados que genera automáticamente inteligencia de seguridad y de actividad a nivel de endpoints.
Esta Inteligencia permite a las empresas identificar ataques y comportamientos inusuales, así como mal uso interno, basados en los eventos continuamente monitorizados en los endpoints.
Panda AdaptiveDefense vela por la seguridad de la empresa y sus datos y ayuda en la gobernanza de la información. Las empresas que confían en Adaptivedefense tiene ya un camino recorrido en el cumplimiento del RGPD, aportando:

- Protección de los datos personales procesado en los sistemas de la empresa, evitando por ejemplo la ejecución de cualquier proceso no confiables en los servidores corporativos.
- Reducción del riesgo de ser objeto de ataques de seguridad e indicadores claves de la actividad y estado de los endpoints que ayudan a establecer las medidas de seguridad: Equipos vulnerables, actividad de red anómala entre dispositivos o entre dispositivos de dentro de la empresa hacia el exterior, etc.
- Herramientas para satisfacer la obligatoriedad de notificar los incidentes de seguridad en las primeras 72 horas.
  Gracias a las herramientas de análisis forense, alertas, visibilidad y control de AdaptiveDefense, la empresa estará en condiciones de notificar tanto el detalle del incidente como del plan de acción para solventar y evitar el incidente en el futuro.
- Mecanismos de control y gobierno del dato al DPO, que será notificado en tiempo real, no solo de los incidentes de seguridad y si en estos están involucrados los ficheros con datos personales.
  Tanto ART, a través de alertas en tiempo real, paneles de control e informes, como el sistema de notificación del SIEM corporativo alertarán al DPO en tiempo real de accesos anómalos a los ficheros con datos personales.

AGENDA 2017

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

VII REUNIÓN DEL FORO DE INTEROPERABILIDAD
Lugar: Salamanca • **Fechas:** 26 y 27 de abril de 2017

XXIV JORNADAS NACIONALES DE INNOVACIÓN Y SALUD EN ANDALUCÍA
Lugar: Málaga - Torremolinos • **Fechas:** 7, 8 y 9 de junio 2017

VII REUNIÓN DEL FORO PARA LA GOBERNANZA DE LAS TIC EN SALUD
Lugar: Extremadura • **Fechas:** 27 y 28 de Septiembre de 2017

XV REUNIÓN DEL FORO DE SALUD CONECTADA
Lugar: Aragón • **Fechas:** 25 y 26 octubre

VI REUNIÓN DE LA PLATAFORMA TECNOLÓGICA PARA LA INNOVACIÓN EN SALUD
Lugar: País Vasco • **Fechas:** 22 y 23 de Noviembre de 2017

Plataforma centralizada de logs del Ib-Salut

Miguel Ángel Benito Tovar[1], Esther Álvarez Salazar[2]
1. Responsable de la Oficina de Seguridad de la información Ib-Salut
2. Senior Manager del área de IT Risk en Ernst & Young

PALABRAS CLAVES
Seguridad de la información, protección de datos, esquema nacional de seguridad, ISO/IEC 27002:2013, QRADAR.

INTRODUCCIÓN

La información representa uno de los activos más importantes para cualquier organización. Es por ello que deben tomarse las medidas oportunas para garantizar unos niveles adecuados de seguridad de la información y esto incluye, entre otros aspectos, la monitorización de sistemas para poder conocer el uso que se le da a los sistemas de la organización y poder actuar ante errores o problemas detectados.

La trazabilidad de las acciones realizadas por los usuarios de los sistemas de información, así como por los propios sistemas de información autónomamente, representa un aspecto primordial para poder saber lo que está pasando en los sistemas de información, poder corregir malos usos, errores o vulnerabilidades y poder atribuir la responsabilidad de las acciones realizadas a la entidad adecuada.

Para garantizar la trazabilidad es necesario disponer de trazas de actividad o "logs" que podríamos definir como registros de eventos ocurridos en los sistemas de información que permiten saber quién, qué, cuándo, cómo y porqué ocurren dichos eventos.

La gestión de "logs" consiste por lo tanto en monitorizar adecuadamente los eventos de seguridad configurados en los sistemas y analizar los registros generados por dichos eventos de seguridad para poder actuar en consecuencia.

En el ámbito de la administración pública actualmente existen diversos requisitos legales para garantizar la trazabilidad, entre los que es necesario mencionar:

- Artículo 103 del Reglamento de Desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, LOPD, aprobado por el Real Decreto 1720/2007, de 21 de diciembre. Dicho artículo relativo al registro de accesos y de obligado cumplimiento para aquellos sistemas que traten datos de salud, establece 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. Y en el caso de que el acceso haya sido autorizado, será preciso guardar también la información que permita identificar el registro accedido.
- Artículo 23 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. Dicho artículo relativo al Registro de actividad establece que se registrarán las actividades de los usuarios, reteniendo la información necesaria para monitorizar, analizar, investigar y documentar actividades indebidas o no autorizadas, permitiendo identificar en cada momento a la persona que actúa.

De igual modo, alineándose con la Norma ISO/IEC 27002:2013 Código de prácticas para los controles de seguridad de la información, la gestión de "logs" facilitará el cumplimiento de los siguientes objetivos de control establecidos en la Norma:

12.4 Registro de actividad y supervisión.
12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información.
12.4.3 Registros de actividad del administrador y operador del sistema

PLATAFORMA CENTRALIZADA DE LOGS DEL IB-SALUT

El cumplimiento de los preceptos legales anteriormente citados supone un gran reto para un entorno como es el sanitario especialmente debido al elevado número de sistemas de información que tratan datos de salud, y por ende de nivel alto según el Reglamento de Desarrollo de la LOPD, así como por el alto volumen de accesos efectuados diariamente por parte de los profesionales a dichos datos.

Es por ello, que por parte de la Subdirección de Tecnologías y Sistemas de Información del Servicio de Salud de las Islas Baleares (Ib-Salut) se ha impulsado la implantación de una solución centralizada de "logs" que venga a dar no sólo el cumplimiento a los imperativos legales sino que también demuestre a los ciudadanos de las Islas Baleares el compromiso del Ib-Salut con respecto a la confidencialidad sus datos.

Atendiendo a todo lo anteriormente expuesto, los principales motivos para la puesta en marcha de la citada plataforma centralizada de logs fueron:

- Cumplimiento de la normativa de Protección de Datos y el Esquema Nacional de Seguridad.
- Detención proactiva de accesos potencialmente indebidos.
- Tratar y correlar de forma centralizada los eventos/logs de los sistemas asistenciales y TIC.
- Presentar, a través de cuadros de mando personalizados, información relevante sobre el uso de los sistemas del Servicio de Salud.
- Disminución del esfuerzo de analizar los eventos/logs de cada sistema de forma separada y con la intervención de múltiples equipos (sistemas, soporte de aplicaciones, oficina de seguridad de la información, ...)
- Posibilidad de realizar investigaciones dirigidas sobre el uso de los sistemas.
- Garantizar la validez jurídica en lo referente a la integridad, conservación y tratamientos de los eventos/logs.

Para la puesta de la plataforma centralizada de logs se siguieron las siguientes fases:

1. Selección de la tecnología a utilizar: Por parte de la Oficina de Seguridad de la Subdirección de Tecnologías y Sistemas de Información se evaluaron diferentes alternativas tecnológicas tanto comerciales como Open Source decantándose finalmente por la solución Qradar de IBM. Dicha solución ha sido catalogada como la número uno en la Forrester 1Q 2017 Security Analytics Wave Report.
2. Identificación de los sistemas a integrar: En una primera fase se estimó que los sistemas a integrar fueran los sistemas asistenciales de referencia utilizados en atención especializada y atención primaria. Destacar igualmente que en todas las licitaciones para la adquisición de nuevos sistemas de información por parte del Ib-Salut, ya se incluye la obligación de que éstos se integren con la plataforma centralizada de logs. Igualmente dentro de esta primera fase se incluyó la integración de sistemas TIC tales como cortafuegos, antivirus, servidores DNS, directorios activos, sistemas de detección/prevención de intrusiones (IDS/IPS) y servidores de correo.
3. Identificación de casos de riesgos para cada uno de los sistemas: Tal como se expuso anteriormente, una de las principales motivaciones de la puesta en marcha del proyecto fue la de detectar de una manera proactiva aquellos accesos que no se ajustaran a priori a un uso correcto de los sistemas. Para esta fase se contó con la colaboración del equipo de la Dirección Asistencial desde donde se definieron los casos de riesgo a implementar en la plataforma centralizada. A modo de ejemplo, se consideran casos de riesgos un acceso masivo a la historia clínica de un paciente por distintos profesionales, el acceso a datos clínicos por personal no asistencial o por ejemplo los accesos que se produzcan entre los propios profesionales sin una debida justificación. Es importante destacar que dichos casos de riesgos no son estáticos y que los mismos se van modificando de su propio análisis.
4. Implantación y puesta en marcha de la plataforma centralizada de logs



Figura 1. Plan de proyecto

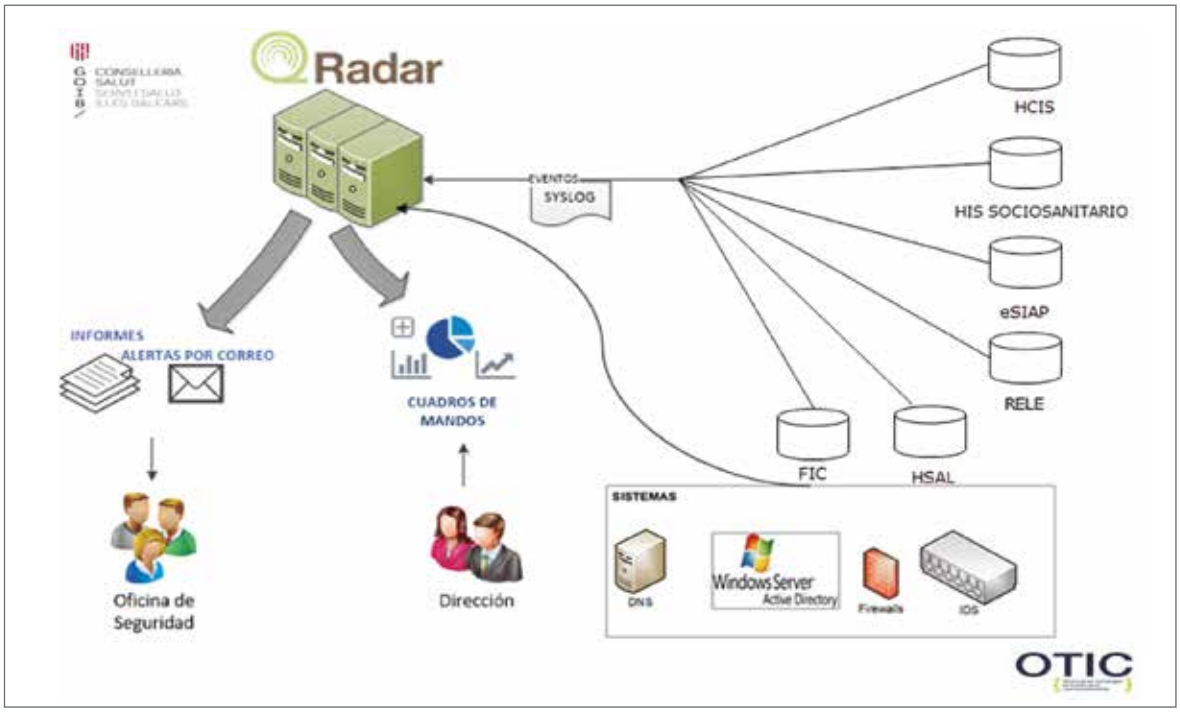


Figura 2. Resumen implantación

ELABORACIÓN DE INFORMES

Dentro de los objetivos del proyecto se encontraba enmarcado el de proporcionar a cada una de las Gerencias del Ib-Salut cuadros de mando personalizados que permitieran conocer y explotar en tiempo real los accesos de los profesionales sobre sus sistemas.

Para ello por parte de la Oficina de Seguridad de la Información se ha elaborado diferentes vistas mediantes las cuales la Dirección y los Responsables de Seguridad de las Gerencias pueden analizar en cualquier momento los accesos efectuados por sus profesionales y especialmente aquellos que requieran una atención inmediata como pudiera ser el acceso masivo a una historia clínica lo cual es considerado como un caso de riesgo tal como se explicó con anterioridad.

Asimismo, cada una de las Gerencias cuenta con la posibilidad de generar sus propias vistas así como de elaborar informes de las revisiones de acceso que vengan a dar cumplimiento a los preceptos establecidos por el citado artículo 103 del Reglamento de Desarrollo de la LOPD.

SOLUCIÓN TECNOLÓGICA SELECCIONADA

Tal como se indicó anteriormente, la solución seleccionada para el proyecto ha sido IBM Security Q Radar Log Manager. Las principales características por las que se optó por la citada solución son:

- Posibilidad de capturar y procesar grandes volúmenes de logs/eventos
- Integración nativa de los dispositivos TIC existentes en el Ib-Salut.
- Posibilidad de generar cuadros de mando personalizable basados en roles y funciones.
- Proporciona funcionalidades de creación de informes extensivos para el cumplimiento normativo y la gestión de amenazas.
- Análisis y correlación de diversos datos de registro y sucesos para proporcionar conocimientos procesables en riesgos de conformidad, posibles ataques, acceso inadecuado a datos, amenazas internas y mucho más.
- Generación de alarmas en tiempo real de accesos de profesionales a información sin justificación necesaria.

CONCLUSIONES

El cumplimiento de la legislación vigente en materia de seguridad de la información y protección de datos es un reto al que se tienen que enfrentar las organizaciones sanitarias tanto públicas como privadas.

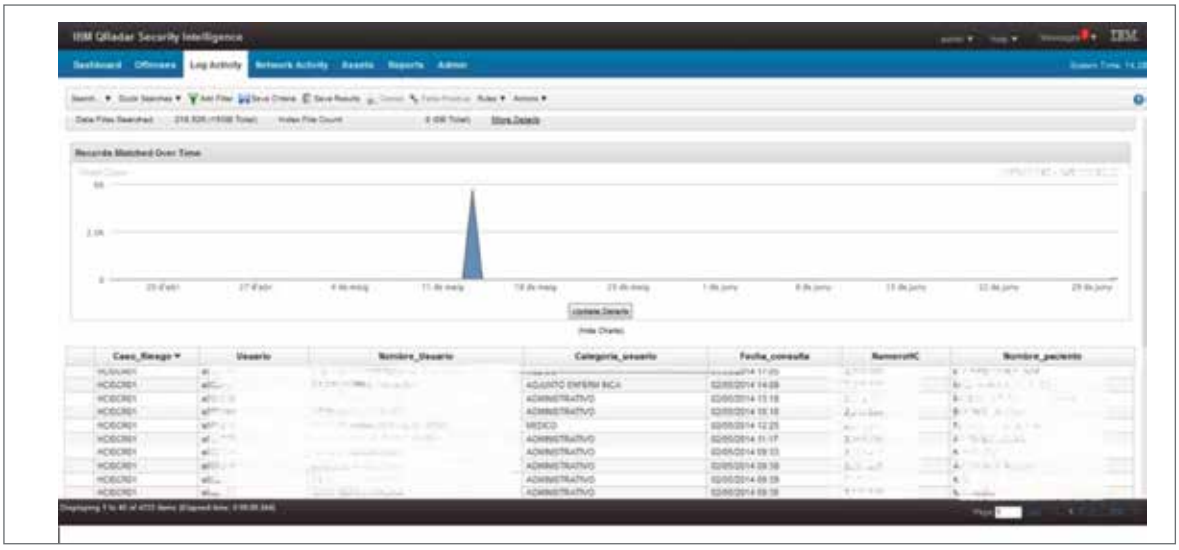


Figura 3. Informe anonimizado caso de riesgo HCISCR01



Figura 4. Vista cuadro de mando

Para afrontar dicho reto, es necesario contar con las soluciones tecnológicas adecuadas pero para garantizar el éxito de cualquier proyecto o iniciativa en materia de seguridad de la información es necesario contar con el compromiso y sensibilidad de la dirección en cuanto al cumplimiento de la legislación y la confidencialidad de los datos de los pacientes como es sin lugar a duda el caso del Servicio de Salud de las Islas Baleares.

REFERENCIAS

[1] Servicio de Salud de las Islas Baleares. https://www.ibsalut.es/ibsalut/es

[2] Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750

[3] Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. https://www.boe.es/buscar/act.php?id=BOE-A-2008-979

[4] Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-1330

[5] IBM Security QRadar SIEM. http://www-03.ibm.com/software/products/es/qradar-siem

Esquema Nacional de Seguridad en el Servicio Aragonés de Salud

Nuria Borque Modrego; Marta Trigo Cabrejas
Centro de Gestión Integrada de Proyectos Corporativos, del Servicio Aragonés de Salud

EL ESQUEMA NACIONAL DE SEGURIDAD (ENS), REGULADO POR EL REAL DECRETO 3/2010, DE 8 DE ENERO, TIENE POR OBJETO ESTABLECER LA POLÍTICA DE SEGURIDAD EN LA UTILIZACIÓN DE MEDIOS ELECTRÓNICOS Y ESTÁ CONSTITUIDO POR PRINCIPIOS BÁSICOS Y REQUISITOS MÍNIMOS QUE PERMITAN UNA PROTECCIÓN ADECUADA DE LA INFORMACIÓN.

Será aplicado por las Administraciones Públicas para asegurar el acceso, integridad, disponibilidad, autenticidad, confidencialidad, trazabilidad y conservación de los datos, informaciones y servicios utilizados en medios electrónicos que gestione en el ejercicio de sus competencias.
La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, estableciaprincipios y derechos relativos a la seguridad en relación con el derecho de los ciudadanos a comunicarse con las Administraciones Públicas a través de medios electrónicos; y su artículo 42 creaba el Esquema Nacional de Seguridad.Las 75 medidas de seguridad que recoge el ENS se agrupan según el esquema siguiente.

PLAZOS DE CUMPLIMIENTO DEL ENS

En la disposición transitoria del Real Decreto 3/2010 se articulaba un mecanismo escalonado para la adecuación a lo previsto en el Esquema Nacional de Seguridad de manera que los sistemas de las administraciones deberían estar adecuados a este Esquema en un plazo que vencía el 30 de enero de 2014.No obstante, con la publicación citada el 4 de noviembre de





2015 en el BOE del Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, se abre un nuevo plazo de adecuación al Esquema Nacional de Seguridad que vence el próximo 4 de noviembre de 2017.

ESQUEMA NACIONAL DE SEGURIDAD EN EL SERVICIO ARAGONÉS DE SALUD

En aras de cumplir con el presente Esquema Nacional de Seguridad, el Servicio Aragonés de Salud publicó en el Boletín Oficial de Aragón la Orden de 16 de marzo de 2015, del Consejero de Sanidad, Bienestar Social y Familia, por la que se aprueba la Política de Seguridad de las Tecnologías de la Información y la Comunicación en el Servicio Aragonés de Salud y se crean el Comité de Seguridad de la Información y la figura del Responsable de Seguridad. El objetivo por un lado era establecer directrices básicas y duraderas para una protección eficaz de la información, y por otro instaurar el compromiso del organismo con la seguridad de los sistemas de información, asentando los pilares de su marco normativo, concretados en el Comité de Seguridad de la Información, y en la figura del Responsable de Seguridad, sobre la que se apoya el gobierno de la seguridad en el Servicio Aragonés de Salud.

El ámbito de aplicación de la política de seguridad incluye a todos los hospitales, centros de salud, centros de salud mental, consultorios, centros de atención especializada, centros de atención sociosanitaria, puntos de atención continuada, servicios de urgencia de atención primaria, 061 y centros directivos y de administración del Servicio Aragonés de Salud en la Comunidad Autónoma de Aragón en los que los empleados acceden a los sistemas de información del Servicio Aragonés de Salud, así como las empresas proveedoras de servicios

relacionados. Además, la política de seguridad es aplicable a todos los sistemas de información del Servicio Aragonés de Salud y/o que den soporte a sus procesos, así como todos los activos de información sustentados en ellos.

Para divulgar esta política de seguridad de la información, la Gerencia del Servicio Aragonés de Salud ha elaborado una web informativa dedicada a los profesionales sanitarios sobre seguridad de la información en el entorno sanitario y protección de los datos personales. En la página se proporcionan pautas de comportamiento seguro en el uso de las nuevas tecnologías para mejorar la seguridad de la información que se gestiona y la cultura de la propia institución, así como el contenido de esta política, la legislación aplicable en esta materia, además de los derechos y obligaciones de los usuarios y un decálogo de seguridad destinado a ayudar a los profesionales en su labor, que resume el manual de "Normas de Uso de los Sistemas de Información del Servicio Aragonés de Salud", donde se detallan los diferentes aspectos de la seguridad de la información.

Especial relevancia tiene el apartado de Actualidad,relacionado con la Protección de Datos en nuestro ámbito, y donde podemos encontrar una relación de todas las Resoluciones de la Agencia Española de Protección de Datos relativas al Servicio Aragonés de Salud, ordenadas por artículo vulnerado y por orden cronológico.

El Comité de Seguridad de la Información tiene reservada también otra sección donde se puede consultar su actividad y sus líneas actuales de trabajo.

Por último, existe una sección donde se puede descargar toda la documentación importante, como normas, procedimientos o plantillas de uso frecuente; otra sección de Preguntas Frecuentes (FAQ) y una sección de Consultas, en la que se puede enviar cualquier duda o sugerencia relacionada con la Seguridad de la Información a personal especializado de la organización.

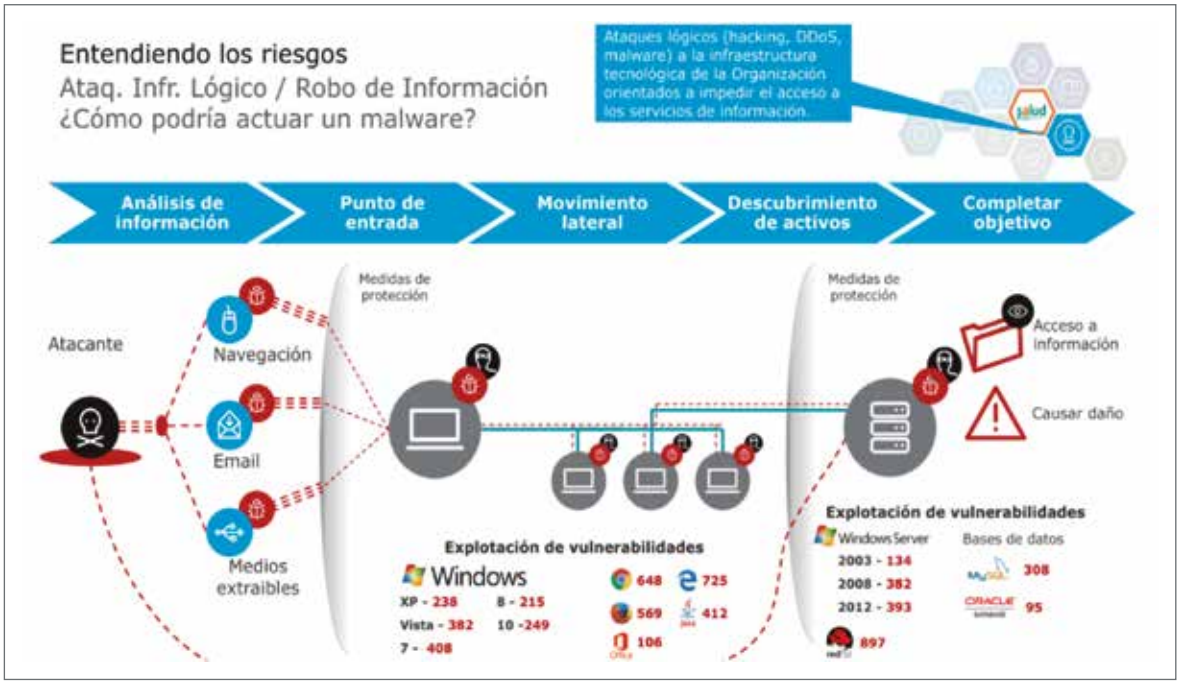
La web pretende ser un portal abierto y dinámico, adaptada la idiosincrasia sanitaria, en el que los profesionales sanitarios puedan expresar todos los aspectos diversos de la Seguridad de la Información que les preocupe de su organización, tanto los actuales como los que vayan surgiendo y con la que gracias a la contribución de todos, se pueda perfeccionar la cultura en materia de Seguridad de la Información.

Además actualmente el Servicio Aragonés se encuentra inmerso en la implantación del Esquema Nacional de Seguridad, cuyo enfoque metodológico concibe la elaboración del Plan de Adecuación como un ejercicio de reflexión estratégica que se articula en 3 fases diferenciadas.

Cada una de las fases se subdivide a su vez en otras dos, en función de los perfiles que dentro de la organización deberán desarrollar las tareas asociadas a cada una de ellas:

- Perfiles técnicos, no necesariamente personal TI, multidisciplinares, cuyos miembros son parte del Comité de Seguridad de la Información y son los encargados de recopilar la información necesaria para una adecuada toma de decisión por parte de la Dirección del proyecto.
- Perfiles directivos, que a partir de la información obtenida del trabajo realizado por las áreas técnicas deberá tomar las decisiones respecto al modelo de seguridad de la información a implantar.





DESCRIPCIÓN DE LA FASE I DEL PLAN DE ADECUACIÓN AL ENS: ANÁLISIS PRELIMINAR DE RIESGOS

Una vez identificados los interlocutores claves que participarán posteriormente en cada una de las etapas del proyecto, se establece la planificación a alto nivel de las siguientes fases del proyecto y se prepara la Presentación de inicio del Proyecto para la Dirección del Proyecto, con el siguiente contenido:

- Introducción a las amenazas de seguridad de la información.
- Motivaciones del proyecto.
- Marco Metodológico del Proyecto.
- Planificación del trabajo y colaboración esperada por parte de los interlocutores.

Posteriormente se realiza "El análisis preliminar de riesgos", que pretende conseguir doble objetivo:

- Ayudar a los responsables a entender los riesgos que amenazan la seguridad de los activos de información de su Organización.
- Captar la sensibilidad de la Dirección Gerencia de la Organización respecto a cada uno de dichos riesgos.

Para ello:

- Se parte de un inventario de riesgos estándar, fácil de entender por todos los interlocutores, con el fin de facilitar la toma de decisiones.
- Se mantienen entrevistas con los interlocutores clave de Servicio Aragonés de Salud para obtener una visión preliminar de:
- Los principales procesos de negocio de Servicio Aragonés de Salud y los activos de información que dan soporte a dichos procesos de negocio.
- Los cambios previstos en la Organización en el corto y medio plazo, tanto desde un punto de vista de sus procesos como de los sistemas de información que les dan soporte.
- La organización del área TIC de Servicio Aragonés de Salud y sus procesos de gestión.
- Estado de las iniciativas de seguridad desarrolladas recientemente o en curso en Servicio Aragonés de Salud.
- El estado actual de seguridad de Servicio Aragonés de Salud. Para ello, se pueden analizar los últimos informes de auditoría de seguridad realizados (LOPD, otros), los últimos incidentes de seguridad ocurridos, etc.
- Para cada uno de los riesgos anteriores, se presenta por parte del equipo de proyecto, información clave para la toma de decisiones por parte de la Dirección Gerencia de Servicio Aragonés de Salud, a dos niveles:



- Interna, que permita de manera preliminar evaluar el nivel de exposición de la propia Organización frente a dicho riesgo.
- Externa, que permita evaluar la evolución de las amenazas que pueden materializar dicho riesgo.

Una vez entrevistadas las personas clave en la organización, que pueden aportar suficiente información sobre la identificación de activos de información, sus vulnerabilidades y las amenazas a los que se encuentran expuestos, así como su probabilidad de ocurrencia y el impacto de las mismas, se lleva a cabo la priorización de los riesgos, para la cual, los miembros del Comité de Seguridad participan en una votación, en la que individualmente asignan una puntuación a cada riesgo, de 1 a 9, donde 9 es el riesgo que más le preocupa y 1 el que menos. No es posible asignar la misma puntuación a dos riesgos.

La metodología propuesta pretende, en este punto del proyecto, abstraer a la Dirección Gerencia de la Organización y al Comité de Seguridad del conocimiento de las medidas de seguridad técnica a aplicar, y centrarse más en entender las amenazas y valorar el impacto sobre su Organización, compartiendo la percepción del riesgo actual al que se encuentran sometidos sus activos de información.

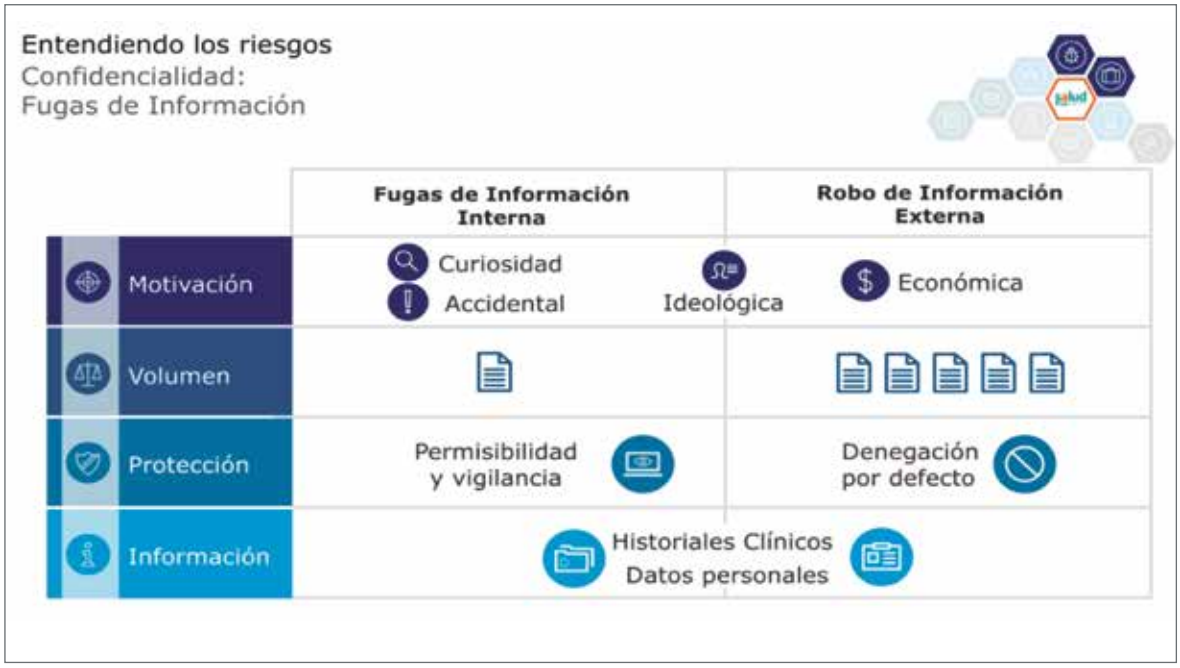
Dejando para fases futuras la determinación de los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo.

Los 9 riesgos a priorizar surgen de la combinación de las dos variables que componen un riesgo:

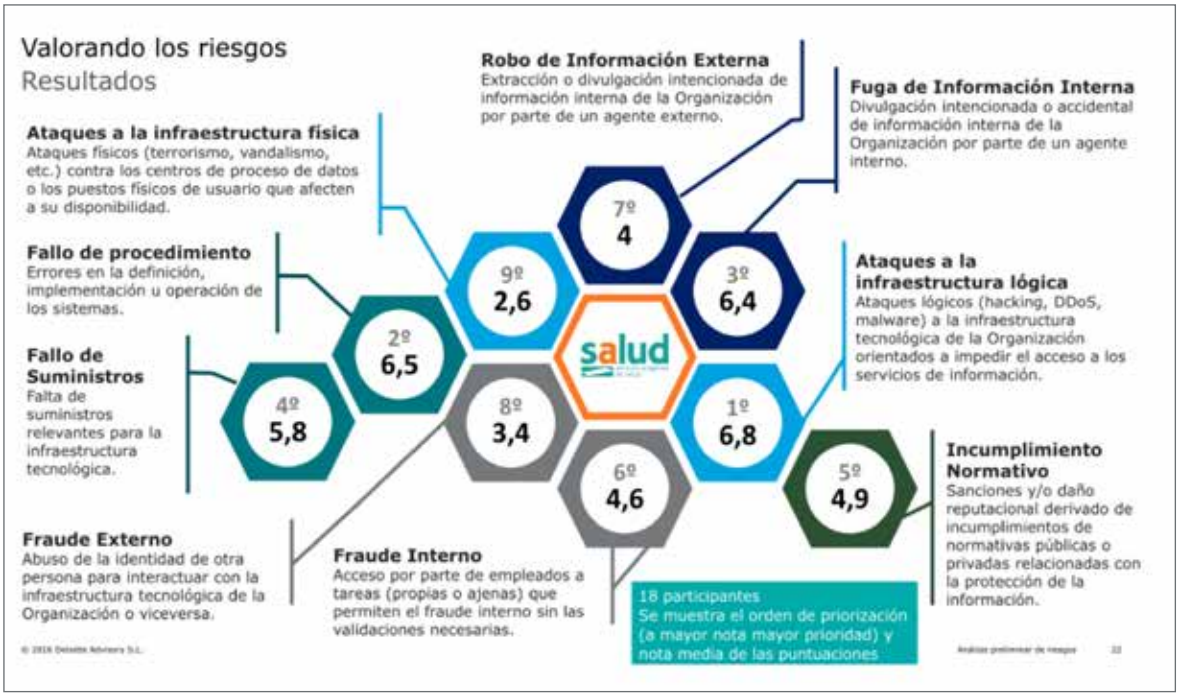
- El impacto, sobre cada uno de las variables de la seguridad de la información: Confidencialidad, Disponibilidad e Integridad.
- El agente de amenaza que puede afectar a dichas variables: Agente Externo, Agente Interno y Fallos/Errores.

El análisis preliminar de riesgos se articula en una única reunión de 2 horas, en la que participan los miembros del Comité de Seguridad y la Dirección Gerencia del Servicio Aragonés de Salud, y está orientado a la toma de decisiones y cuya estructura es:

- Presentación de la metodología.
- Presentación de los 9 riesgos: Ataques a la infraestructura física, ataques a la infraestructura lógica, incumplimiento normativo, fuga de información interna, robo de información externa, fallo de procedimientos, fallo de suministros, fraude externo y fraude interno.



- Votación de riesgos para priorizar los riesgos en función del nivel de preocupación que desde la Dirección de Servicio Aragonés de Salud se perciba de cada uno de ellos.
- Análisis preliminar de los resultados: Priorización de los riesgos en función del nivel de preocupación que desde el equipo designado por Servicio Aragonés de Salud se perciba de cada uno de ellos.



Finalizado dicho análisis preliminar de riesgos, se puede iniciar la fase siguiente, de "Análisis detallado de riesgos." En la que está inmerso actualmente el Servicio Aragonés de Salud.

Protección de datos en estudios de investigación biomédica desde la perspectiva del Reglamento Europeo. Disociación, Codificación, Seudonimización y Reutilización. Nuevo Paradigma

Álvaro Hornero Díezs
Abogado. CISA. CISM. Auditor con capacidad de firma frente a la Dirección General de Ordenación del Juego. Grupo SIA

EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS[1] (GDPR) ESTABLECE UNA SERIE DE CONDICIONES PARA EL TRATAMIENTO DE DATOS ESPECIALMENTE PROTEGIDOS RELATIVOS A LA SALUD, EN RELACIÓN CON NECESIDADES ESPECÍFICAS Y, EN PARTICULAR, SI EL TRATAMIENTO DE ESOS DATOS LO REALIZAN, CON FINES RELACIONADOS CON LA SALUD, PERSONAS SUJETAS A LA OBLIGACIÓN LEGAL DE SECRETO PROFESIONAL.

Estos requerimientos se refuerzan con la obligación de protección de datos personales y garantías de confidencialidad, derivada de aplicar la Ley 14/2007, de 3 de julio, de Investigación biomédica[2], que establece diversas previsiones con la finalidad de proteger la confidencialidad y la intimidad relativas a la información que resulten de la actividad de investigación biomédica.

Toda esta normativa hace necesario incorporar al uso de las tecnologías de la información y de la comunicación las prácticas que permitan garantizar un entorno seguro para el tratamiento adecuado de la información.

> ***La aplicación de la seudonimización a los datos personales puede reducir los riesgos para el afectado por el tratamiento o "sujeto fuente" y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos***

Estas garantías deben asegurar que se aplican medidas técnicas y organizativas para que se observe, en particular, los principios de "minimización de los datos", atendiendo a la proporcionalidad y necesidad del tratamiento, y los principios de "integridad y confidencialidad", de tal manera que se garantice una seguridad adecuada de los datos personales.

La aplicación de la seudonimización a los datos personales puede reducir los riesgos para el afectado por el tratamiento o "sujeto fuente" y ayudar a los responsables y a los encargados del tratamiento a cumplir sus obligaciones de protección de los datos.

Para ello, la ponencia de Grupo SIA propuso analizar las particularidades del marco jurídico específico en el ámbito sanitario, centrándose en algunos de los aspectos esenciales como son la protección de datos de carácter personal en estudios de investigación biomédica, el tratamiento de datos disociados, codificados o seudonimizados, y la reutilización de la información desde la perspectiva del

Reglamento General de Protección de Datos.
Desde esta perspectiva, se presentaron soluciones y servicios orientados a la firma digital y a la custodia de documentos electrónicos, con soluciones innovadoras para optimizar la experiencia del usuario con plataformas móviles, como nuestras soluciones de Portafirma, Custodia Digital y Firma Centralizada (firma en la nube).
Dicha tecnología se compone por la familia SIAVAL que es un equipamiento appliance pensado para soluciones corporativas, que permite licenciar las funcionalidades de forma independiente, diseñados para cumplir los estándares de la industria y compatibles con múltiples certificados de distintas PKI, ya sean internas o públicas.
Asimismo, como Prestador de Servicios de Confianza, SIA proporciona los servicios de emisión de certificados reconocidos, servicios de firma, sellado de tiempo, etcétera, además de servicios de consultoría jurídica, como apoyo de los propios departamentos jurídicos internos en las distintas fases de los proyectos de adecuación de procesos a la Firma Electrónica.
Por otro lado, se presentó la plataforma de autenticación Entrust IdentityGuard mediante la cual se obtiene una solución versátil y flexible de autenticación fuerte para usuarios y aplicaciones, evitando el robo de identidad y protegiendo la confidencialidad de la información sensible mediante el uso de la mayor gama del mercado de factores de autenticación, que evolucionan sin tener que hacer continuos y costosos cambios para la adaptación e integración de aplicaciones.
Para el cumplimiento de las medidas de cifrado y seudonimización que propone el GDPR, se presentaron soluciones de cifrado y seudonimización de datos, proceso este último por el cual se reemplazan los datos personales con un valor sustituto. Como ya mencionábamos, dicho proceso reduce significativamente los riesgos de exposición de los datos, ya que los datos se cifran y almacenan en un repositorio seguro, y en la organización se procesa el dato seudonimizado.

OBJETIVOS

Por último, para enfrentar la problemática expuesta del proceso de adecuación al GDPR con plenas garantías de éxito, Grupo SIA propone la realización de un Assessment previo orientado a la consecución de los siguientes objetivos:

- Conocer el impacto del GDPR en los procesos de negocio de la organización.
- Evaluar el grado de cumplimiento actual de los requisitos introducidos por el GDPR.
- Identificar el gap de cumplimiento existente.
- Identificar y valorar las diferentes variables que contribuyan a determinar la importancia de los diferentes requisitos.
- Establecer la estrategia más adecuada y eficiente para cumplir el GDPR, así como el plan de proyectos a acometer.
- Establecer la planificación más idónea en base a las prioridades identificadas.

Aconsejando seguir de manera temprana un enfoque progresivo para la adaptación de los elementos afectados a los nuevos requisitos.

> ***SIA proporciona los servicios de emisión de certificados reconocidos, servicios de firma, sellado de tiempo, etcétera, además de servicios de consultoría jurídica, como apoyo de los propios departamentos jurídicos internos en las distintas fases de los proyectos de adecuación de procesos a la Firma Electrónica***

1. REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) http://www.boe.es/doue/2016/119/L00001-00088.pdf
2. Ley 14/2007, de 3 de julio, de Investigación biomédica http://www.boe.es/boe/dias/2007/07/04/pdfs/A28826-28848.pdf

Los directivos ante la transformación digital

Juan Miguel Signes[1], Juan Díaz García[2]
1. Conselleria de Sanitat Universal i Salut Pública.
2. Servicio Andaluz de Salud.

ÚLTIMAMENTE SE VIENE HABLANDO MUCHO DE TRANSFORMACIÓN DIGITAL Y POR MUY BUENAS RAZONES. ESTA EXPRESIÓN SIRVE PARAR REFERIRSE A LA REVOLUCIÓN TECNOLÓGICA QUE ESTAMOS VIVIENDO Y QUE AFECTA A TODOS LOS ÁMBITOS DE ACTIVIDAD, PÚBLICOS O PRIVADOS. PERO POR OTRO LADO TAMBIÉN ES ÚTIL PARA SUBRAYAR LOS CAMBIOS QUE DEBEN REALIZAR LAS ENTIDADES PARA SEGUIR EN ACTIVO, APROVECHANDO LAS OPORTUNIDADES QUE BRINDA LA TECNOLOGÍA Y HACIENDO FRENTE A LOS RIESGOS.

Precisamente la envergadura y el alcance de esos cambios explican que se hable con propiedad de la transformación digital de las entidades. Se trata de un asunto principal del que deben ocuparse activamente quienes ostentan las funciones de gobierno.

Las tareas de gobierno asociadas a la transformación digital se pueden resumir en cuatro: fijar objetivos, asignar tareas y responsabilidades, dotar de recursos y pedir cuentas. En cuanto al señalamiento de objetivos, parte de ellos están en las normas y regulaciones del sector, que a menudo incluyen la obligación de cumplir unos requisitos mínimos en unos plazos o con una cadencia determinados. A partir de ahí, cada entidad debe identificar tareas y responsabilidades y asignárselas al órgano competente que corresponda. Y aquí es donde empiezan los problemas: si los objetivos no se reconocen como objetivos de la entidad, o se asignan a un órgano sin competencia, capacidad, autoridad o recursos suficientes, las probabilidades de que se cumplan se desvanecen y los riesgos para la entidad aumentan.

> ***La creciente dependencia de las tecnologías de la información y su penetración en todas las áreas de las entidades hacen que ocuparse de la seguridad de la información (y particularmente la privacidad cuando se manejan datos personales) sea una necesidad, además de una exigencia legal***

La creciente dependencia de las tecnologías de la información y su penetración en todas las áreas de las entidades hacen que ocuparse de la seguridad de la información (y particularmente la privacidad cuando se manejan datos personales) sea una necesidad, además de una exigencia legal. Esta necesidad surge de la confianza que cada entidad debe tener en sus posibilidades de conseguir sus propios objetivos dentro de los marcos presupuestario y temporal previstos, así como la confianza que debe transmitir a los titulares de la información que maneja y al resto de agentes con los que interactúa en el desarrollo de su actividad.

La normativa sobre privacidad[1] y seguridad[2] aplicable a las Administraciones Públicas españolas, así como las buenas prácticas y recomendaciones generalmente aceptadas[3], establecen una serie de capacidades de las que es preciso dotarse, así como la independencia que deben mantener esas capacidades entre sí y respecto a otras dentro de la misma entidad. Entre esas capacidades destacan las de auditoría, gestión de riesgos, privacidad, seguridad y asesoramiento legal.

A menos que estos asuntos reciban la atención que merecen por parte de quienes desempeñan las funciones de gobierno en cada entidad,

ésta no dispondrá de las capacidades mencionadas, o las tendrá en precario a menudo basándose en el voluntarismo y en la sobrecarga de tareas de los profesionales de las tecnologías de la información (¿acaso no han sido ellos quienes han traído estos problemas?), por mucho que la normativa diga otra cosa. Es decir, que la transformación digital y la seguridad de la información son asuntos tan trascendentales para las entidades que no se pueden despachar endosándoselos a los órganos responsables de las tecnologías de la información. El cumplimiento de la normativa sobre esas materias tampoco.

Las capacidades mencionadas anteriormente son especialidades profesionales diferenciadas. Requieren una preparación específica y un esfuerzo de formación continuo que hace que quienes se dedican a ellas difícilmente puedan compatibilizarlas con otras funciones manteniendo un nivel digno de desempeño profesional. Esta circunstancia encaja mal en las Administraciones Públicas, cuya gestión del personal no se caracteriza precisamente por su agilidad a la hora de responder a los cambios.

Por otro lado, la necesidad de especializarse y de mantener un bonito nivel de competencia profesional no es la única razón para que quienes desempeñen esas capacidades deban abstenerse de participar en otras actividades. De hecho los conflictos de intereses son otra poderosa razón para mantener una saludable separación de funciones. Los profesionales, de otro modo, terminarían siendo a la vez juez y parte, lo que minaría la credibilidad de sus dictámenes y los objetivos de confianza que se persiguen.

A continuación se destacan algunas características de estas capacidades.

AUDITORÍA

La cualificación para desempeñar estas funciones puede venir avalada por alguna de las certificaciones disponibles en el mercado (quizás la más reconocida con carácter general sea CISA de ISACA[4]). Disponer de una capacidad de auditoría interna redunda en un menor impacto de las auditorías en el funcionamiento normal de la entidad, así como un menor coste y un mayor aprovechamiento de los resultados: el conocimiento de los auditores internos del funcionamiento de la propia entidad marca las diferencias. La independencia de los auditores respecto a los órganos responsables de los servicios auditados resulta esencial. Los auditores de sistemas de información no pueden depender del responsable de dichos sistemas.

GESTIÓN DE RIESGOS

El análisis y la gestión de riesgos deben orientar las actuaciones en materia de seguridad. Quienes desempeñen esas funciones deben tener un conocimiento profundo de los objetivos y funcionamiento de la entidad (lo que pone en desventaja al personal externo), de la tecnología y del panorama siempre cambiante de las amenazas. La cualificación en este caso se basa también en certificaciones, pero las que existen todavía no tienen el mismo prestigio y reconocimiento que en otras áreas de actividad. La independencia respecto a quienes tengan responsabilidades en el desarrollo de soluciones y la prestación de servicios tecnológicos es un factor clave para la credibilidad y confianza en los dictámenes de estos profesionales.

PRIVACIDAD

El Reglamento Europeo de Protección de Datos de la Unión Europea, que será exigible a partir del 25 de mayo de 2018, establece la figura del Delegado de Protección de Datos (versión devaluada del "Data Privacy Officer" del original en inglés: un delegado no necesariamente tiene la responsabilidad y autoridad que se le presumen a un "officer"). No obstante la denominación y cómo acreditar la competencia necesaria, el Art. 38 despeja dudas sobre la posición de esta figura, que deberá rendir cuentas directamente al más alto nivel jerárquico del responsable o encargado del tratamiento, quienes a su vez deberán garantizar su independencia.

SEGURIDAD DE LA INFORMACIÓN

La (ciber)seguridad es un asunto que figura en las agendas políticas. Proteger la información, las infraestructuras tecnológicas y los servicios que dependen de ambas exige una preparación

específica y dedicación continua. Este es un campo en expansión en el que aparecen nuevas titulaciones y certificaciones que añadir a las ya consagradas (CISM, CISSP, etc). Ninguna entidad puede bastarse a si misma para satisfacer sus necesidades en esta materia. Al margen de las colaboraciones y servicios que pueda contratar, resulta imprescindible dotarse de una capacidad propia en este terreno que como mínimo coordine y gobierne la actividad de los agentes externos. Esta capacidad debe tener respaldo y autoridad suficientes para actuar en todos los ámbitos relevantes, que no se limitan a la provisión de servicios tecnológicos, y no estar en una posición subordinada a quienes tengan responsabilidades directas sobre esas infraestructuras y servicios.

SEGURIDAD FÍSICA

Aunque las fronteras entre seguridad física y lógica son cada vez más difusas, hay algunos asuntos que reciben un tratamiento diferenciado. Así, a lo largo de 2017 está previsto que algunos centros sanitarios sean declarados infraestructuras críticas. Este hecho traerá consigo una serie de obligaciones relativas a los planes de protección, así como la de dotarse de un Director de Seguridad. Actualmente sólo pueden serlo quienes hayan obtenido la correspondiente titulación que expide el Ministerio del Interior, o en su defecto una titulación universitaria específica. Esta nueva posición deberá tener un reflejo en los organigramas.

> ***La intervención de los responsables de las administraciones públicas es imprescindible y determinante para hacer frente a los retos transformación digital y la seguridad de la información. Las administraciones sanitarias lejos de ser una excepción son todo lo contrario, dada la importancia de la información que manejan y los derechos fundamentales afectados***

CUMPLIMIENTO LEGAL

Cómo actuar para lograr los objetivos funcionales cumpliendo los requisitos legales pertinentes requiere a veces la participación activa de los profesionales del derecho. Mientras que los servicios jurídicos de algunas comunidades autónomas intervienen de este modo en la búsqueda de soluciones, en otras autonomías la normativa que regula el funcionamiento de dichos servicios limita su actividad a la emisión de informes y a la defensa en juicio. En estas últimas esta participación reactiva no satisface las necesidades de asesoramiento legal de las administraciones y merma su eficiencia.

Las anteriores consideraciones pretenden demostrar que la intervención de los máximos responsables de las administraciones públicas es imprescindible y determinante para hacer frente a los retos que plantean la transformación digital, la seguridad de la información y el cumplimiento de la normativa legal sobre esas materias. Las administraciones sanitarias lejos de ser una excepción son todo lo contrario, dada la importancia de la información que manejan y los derechos fundamentales afectados. Una célebre frase de Benjamin Franklin resume perfectamente la situación: *By failing to prepare, you are preparing to fail.*

1. La Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, y su reglamento de desarrollo, el Real Decreto 1720/2007, hasta el 25/05/2018. A partir de esa fecha entrará plenamente en vigor el Reglamento (UE) 2016/276 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.
2. Véase el RD 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, y las normas técnicas del CCN-CERT que lo complementan. A estas referencias habría que añadir también las relacionadas con la protección de infraestructuras críticas.
3. Véanse las normas de la serie ISO/IEC 27000.
4. CISA: Certified Information Systems Auditor. Véase http://www.isaca.org

XIV Foro de Seguridad y Portección de Datos en Salud

La reutilización de la información de salud, según el nuevo RGPD de la UE

Los pasados 22 y 23 de febrero, la Sociedad Española de Informática de la Salud, con la colaboración de la Consejería de Salud de la Junta de Andalucía, además de la Agencia Española de Protección de Datos, la Agencia Vasca y la Catalana y el Consejo de Transparencia y Protección de Datos de Andalucía celebró el XIV Foro de Seguridad y Protección de datos de Salud. El encuentro tuvo lugar en Sevilla, en el Salón de Actos del Hospital Universitario Virgen del Rocío.

La asistencia a este XIV Foro fue muy superior a ediciones anteriores. Siempre estuvo presente entre todos los asistentes la ausencia y el recuerdo de nuestro querido Emilio Aced.
El foro se centró en el análisis de los retos que para la privacidad y la protección de datos personales se plantean ante la necesidad de reutilizar la información relativa a la salud, con fines de investigación, control de calidad, seguridad de los pacientes, etc. Estuvo estructurado en cinco sesiones, cuatro de las cuales tuvieron formato de debate.
Al igual que en años anteriores, antes del comienzo del foro y a puerta cerrada tuvo lugar la Reunión del Comité Técnico de Seguridad de la Información Sanitaria.

INAUGURACIÓN



La mesa inaugural estuvo formada por Aquilino Alonso Miranda, consejero de Salud de la Junta de Andalucía, Luciano Sáez Ayerra, presidente de la SEIS, Rosario Heras Carrasco, de la Agencia Española de Protección de Datos, Manuel Medina Guerrero, director del Consejo de Transparencia y Protección de Datos de Andalucía y Manuel Romero Gómez, director gerente del hospital.

Habló en primer lugar Manuel Romero quien manifestó el placer que suponía acoger a todos los presentes, a los que dio la bienvenida.

Luciano Sáez dio la bienvenida a todos y recordó que la SEIS ha contado con la colaboración de la Agencia Española de Protección de datos, la Autoridad Catalana de Protección de Datos, la

Agencia Vasca y el Consejo de Transparencia y Protección de Datos de Andalucía.
No faltó en el acto de bienvenida unas sentidas palabras en recuerdo de Emilio Aced, quien durante once años coordinó estas reuniones.
El presidente recordó que "La SEIS realiza diversas acciones y pone en marcha iniciativas para fomentar el desarrollo tecnológico con pleno derecho al respeto de las personas y a su privacidad". Así, en el 2004 se creó el Foro de Protección de Datos en Salud con el objetivo de disponer de un espacio de encuentro entre profesionales y autoridades y con el fin de transmitir conocimientos para conseguir un sistema sanitario de calidad y cuidando siempre los derechos de los ciudadanos. "Para cumplir esta misión se establecieron los siguientes objetivos: sensibilizar y concienciar a los directivos que para ofrecer una asistencia sanitaria de calidad es necesario definir políticas adecuadas para tratar los datos personales. Fomentar el establecimiento de canales que faciliten a las autoridades de protección de datos el conocimiento directo y las necesidades del sector sanitario. Potenciar el uso de las tecnologías de la información y de las telecomunicaciones".

Seguidamente, el consejero dio la palabra a Manuel Medina, quien consideró que no debería estar sentado en esta sala porque aún no han asumido la competencia en materia de protección de datos personales, a pesar que el Estatuto de Autonomía ya había atribuido directamente la competencia del control ejecutivo de protección de datos a la Comunidad Autónoma.

Por su parte Rosario Heras defendió que un foro que lleva tantos años de experiencia, quiere decir que los conocimientos que se están compartiendo son muy "interesantes". Dijo que ya que estos datos, "esta información que tratamos se ha recabado en un inicio para atender la salud de los pacientes, podemos decir que su finalidad era asistencial" y añade que "sin embargo, ahora se pretende hacer otro tipo de tratamiento con los datos personales por lo que es muy importante, para cada nuevo tratamiento de los datos, saber para qué fin se van a utilizar".
Actualmente, reflexionó Rosario Heras, se está planteando utilizar datos tanto para la salud pública como para la epidemiología e incluso para llegar a tener una atención más personalizada en la salud de los ciudadanos. "La agencia, hace unos meses, se ocupó de procedimientos y garantías de la anonimización de datos que serán tratados en este foro."

El consejero de Salud de la Junta de Andalucía, Aquilino Alonso Miranda, defendió que la SEIS se ha adelantado a los tiempos al tratar tan seriamente las TIC. Se va a abordar un tema de mucha utilidad como es la reutilización de los datos con diversos fines, "lo cual es muy importante para el Sistema Nacional de Salud, pero también es importante saber hasta dónde va a llegar esta actualización". En un repaso por el sistema de salud andaluz, el consejero recuerda que Andalucía tiene uno de los repositorios de datos clínicos más grandes del mundo. En la base datos poblacional hay más de 150 millones de registros que están preparados para su explotación. "Podemos hablar de una producción anual de más de 43 millones de hojas de seguimiento, 80 millones de citas, y 4,3 millones de pruebas analíticas".

PRIMERA SESIÓN

Soluciones tecnológicas existentes en el mercado para la seguridad y la reutilización de la información de salud

El moderador fue Juan Lucas Retamar, subdirector general de Tecnologías de la Información y Comunicaciones del Servicio Andaluz de Salud.

El primero en intervenir fue Álvaro Hornedo, abogado ICAM, CISA, CISM y auditor con capacidad de firma frente a la Dirección General de Ordenación del Juego. Su intervención se centró en la protección del dato y en los estudios de investigación biomédicos desde la perspectiva del reglamento europeo. Disociación, Codificación, Seudonimización y Reutilización. En definitiva, analizar todos los requisitos y medidas de seguridad que establece la Ley de Investigación Biomédica para el tra-



tamiento de todos los datos y toda la información que se deriva de un estudio de investigación y ver cómo se pueden encajar esos requisitos dentro de diferentes soluciones que ofrece la industria y ver qué nuevos requisitos establece el nuevo reglamento de la Ley de Protección de Datos.

Vidal Valdunciel, de Key Account Manager Corporation de Panda Security, disertó sobre ciberseguridad proactiva para los endpoint en el sector salud. Explicó que el dato es generalmente privado y desde luego, y en general, datos muy confidenciales, pero, sin embargo, para la prestación de servicios son datos que son compartidos por distintos actores, distintas entidades, tanto públicas como privadas. "De todos los sectores es donde más se comparte el dato, ya que está altamente afectado por las diferentes normativas y Directivas" explicó, al tiempo que añadió que "estamos ante un escenario con muchos retos".
Valdunciel explicó que en una encuesta a nivel europeo en la que no participó España se preguntaba a los responsables de la información sanitaria, cuáles eran los desafíos más importantes que veían dentro de los sistemas de información sanitarios y contestaron: disponibilidad del sistema ya que tienen que trabajar 24x7, la interoperabilidad (más importante en España), integridad del dato y seguridad de la red.
Los tres componentes que más afectan como tal a los datos son: el control de acceso, la seguridad en la red y la pérdida de datos, relacionada con lo anterior. "El end point o puesto de trabajo es una asignatura pendiente. Hay que proteger el puesto de trabajo evitando los ataques".

Regina Sastre Barriga, responsable de la Línea de Servicios de Protección de Datos Personales, Everis Aeroespacial, Defensa y Seguridad se centró en Privacy by design: enfoque por amenazas en el diseño de sistemas. "Hemos intentado aunar la parte técnica con la parte de seguridad para, a través de las herramientas tecnológicas, seguir el cumplimiento del reglamento. Seguimos con el concepto de datos de carácter personal cuando vayan a formar parte de un fichero o conjunto organizado de datos.
Uno de los riesgos que nos encontramos ahora son los datos sin clasificar". Confirmó Sastre que han elaborado cinco bloques de acción en los que atacar para cumplir con el reglamento: el primero sería el gobierno de la información, DPO; la responsabilidad activa; establecer todas las medidas técnicas y organizativas; gestionar las brechas de seguridad y tener en cuenta los derechos del interesado. "Hay que llevar a cabo análisis de riesgo y de impacto para ver qué medidas tenemos que implantar", aseguró e insistió en que "es muy importante establecer los procedimientos internos como qué información debe guardarse o qué tenemos que hacer con ella para informar a la Agencia Española". Define el Threat Modelling como un proceso de análisis de amenazas de un sistema o software y que incorpora la búsqueda de medidas para mitigarlas.

La cuarta intervención corrió a cargo de Manuel Borrás Borrás, IT Sales Consultant de T-Systems Iberia. Habló sobre Seguridad y Protección de Datos 360º. Para él la seguridad es el factor cla-

ve del negocio y es necesario que las instituciones se protejan de los ataques, compaginando requerimientos del negocio con el rigor requerido. "Desde nuestra óptica vemos 3 tipos de compañías: las que tienen una gran organización de seguridad con grandes recursos, las compañías que tienen un departamento de seguridad donde la seguridad de la infraestructura va por un lado y la seguridad de los datos por otro y todavía no se han enfrentado a la ciberseguridad y luego tenemos un gran grupo de compañías que suelen ser pequeñas en las que la seguridad queda restringida a lo que es la pura continuidad del negocio". La propuesta de Borrás, de 360º de seguridad, "la sustentamos en procesos y calidad, es decir, el cumplimiento de la ISO 27001 que nos da una base muy importante para crecer y tener un control sobre los datos".

En el marco de la primera mesa de debate, Juan Díaz, coordinador del Comité Técnico de Seguridad de la Información Sanitaria, presentó un resumen de las actividades del Comité Técnico de Seguridad de la Información de Salud. Este comité está compuesto por responsables y técnicos en seguridad de la información de los diferentes Servicios de Salud del Estado Español, para facilitar el mutuo conocimiento de los problemas a los que se enfrentan los departamentos de seguridad de la información sanitaria y las ventajas que proporciona el compartir información sobre las soluciones adoptadas.

Se llevó a cabo una reunión presencial del comité previo al Foro de Seguridad y Protección, donde se expusieron y comentaron diferentes proyectos abordados por los Servicios de Salud, se presentó el Plan de Seguridad del Servicio Gallego de Salud por Jorge Prado, la evaluación del estado de seguridad y riesgos de la infraestructura hospitalaria del Servicio Madrileño de Salud por José Manuel Laperal, los Planes de Auditoria del Servicio Canario de Salud por Juan Carlos Osorio, el plan de adecuación al Esquema Nacional de Seguridad por Marta Trigo y la Plataforma Centralizada de log del Servicio Balear de Salud por Miguel Ángel Benito, entre otras cuestiones.

También se discutieron aspectos candentes como la validez de los procedimientos de firma digital sobre los consentimientos informados, la autenticación del ciudadano ante los accesos de su historia clínica desde internet, la firma digital cualificada en la nube y los retos de las amenazas de la ciberseguridad que afectan a los Servicios de Salud.

SEGUNDA SESIÓN



Reutilización de la información de salud en el marco del RGPD de la UE

Manuel Medina Guerrero, director del Consejo de Transparencia y Protección de Datos de Andalucía, fue el moderador. Después de comentar algunos aspectos sobre el RGPD como que ha dejado cierto grado de maniobra a los legisladores nacionales en este ámbito, presentó a los debatientes. Calvo Medina, jefe de Área Informática de la Agencia Española de Protección de

Datos constató que la Agencia está muy preocupada por los procesos de anonimización que, en realidad, es un tratamiento de datos, por lo que los personales dejan de tener al carácter de datos personales para convertirse en algo distinto. "Hay que aplicar medidas que garanticen la confidencialidad y que gestione los riesgos.
Como tal tratamiento de datos está sujeto a lo que dice el reglamento, hay que hacer una evaluación de los datos que se van a anonimizar y qué objetivos se persiguen y durante cuánto tiempo van a estar anonimizados. También hay que tener en cuenta en los procesos de anonimización a los comités éticos".

Antonio Troncoso Reigada, catedrático de Derecho Constitucional en la Universidad de Cádiz y exdirector de la Agencia de Protección de Datos de la Comunidad de Madrid de 2001 a 2010, partió de la idea de que hay que poder favorecer la investigación, pero hay que hacerlo con garantías. El Reglamento Europeo va en la dirección de superar las legislaciones que dificultan la investigación.
"Hay que tener en cuenta quiénes son los investigadores", afirmó Troncoso que asegura que "tiene menos miedo a los investigadores públicos que a los privados que, aunque no les tiene miedo, sí mucho respeto". Paralelamente están las compañías aseguradoras, manejando información big data, "de las que tengo una información más nítida". Explicó que "el tratamiento big data aumenta, naturalmente, el nivel de riesgo. Unas veces el objetivo es la investigación y otras veces la finalidad es económica. Nunca hay que perder de vista los derechos de las personas que deben estar garantizados". Y consideró que el Reglamento permite la investigación.

Santiago Farré Tous, jefe de la Asesoría Jurídica de la Autoridad Catalana de Protección de Datos, sobre la noción de riesgo indicó que "en el reglamento europeo, el riesgo pasa a ser un elemento central del tratamiento. Ya no es solo un elemento a tener en cuenta para determinar las medidas de seguridad sino que pasa a ser una condición de la propia viabilidad del tratamiento. En el reglamento europeo aparecen dos conceptos que están muy estrechamente relacionados con lo que estamos comentando. Uno es "categoría especiales de datos", que determinan no solo una necesidad de habilitación específica para esas categorías, sino una serie de obligaciones como puede ser la de llevar un registro de actividad". Otro concepto, añadió, es el "tratamientos a gran escala".
Sobre el uso de datos de salud con fines de investigación científica afirmó que la ley debería prestar atención a medidas como la privacidad o protección de datos en el diseño.

Pedro Alberto González y González destacó el motivo por el cual se está hablando del reglamento. Según manifiesta, el reglamento era un obstáculo y era necesario disponer de un nuevo instrumento que no tuviera tantos obstáculos.
"En el proceso de elaboración del reglamento, que llevó cuatro años, se ha pasado por distintas formulaciones y durante todo este tiempo las partes interesadas han intervenido directamente en las distintas fases, tanto en la comisión europea como en el consejo". Con el nuevo reglamento, algunos de los derechos de las personas se han visto reforzados, mientras que otros han perdido, como es el caso del consentimiento.
"Con respecto a la reutilización no ha habido un gran cambio. Si se van a reutilizar datos que sean de carácter personal la anonimización es el paso previo que hay que utilizar.
Sería muy necesario entender, por los problemas que pudieran presentarse, qué se entiende por investigación científica", argumentó González. El hecho de que se haya introducido la pseudo anonimización como una medida, que en este caso contribuye a reforzar estas garantías que se exigen, especialmente para la investigación científica sí es algo bueno y además juegan varios elementos como es el hacer evaluaciones de impacto. "Es decir, el hecho de que haya evaluaciones de impacto sobre la privacidad, combinado con el análisis de riesgo, que de ahí se derivan, más las medidas que hay que adoptar para minimizar esos riesgos entre las cuales está la pseudo anonimización y que conduce a que las garantías sean mayores".
Como resumen, concluyó que el balance de cómo trata el reglamento a la investigación científica es que la permite ampliamente e introduce unas garantías adicionales que "nos llevan a una situación suficientemente balanceada".

TERCERA SESIÓN



Presentación de Casos prácticos

La tercera sesión del foro estuvo dedicada, como viene siendo habitual en las últimas ediciones, a la presentación de casos prácticos a partir de la experiencia de las autoridades de Protección de Datos durante el último año transcurrido. La mesa estuvo coordinada por Pedro Alberto González, responsable de Registro y Auditoría de Ficheros de la Agencia Vasca de Protección de Datos, y contó con la participación de juristas de las tres autoridades. La Agencia Española de Protección de Datos estuvo representada por Cristina Gómez Piqueras, coordinadora de Inspección del Sector Sanitario de la AEPD. Por parte de la Autoritat Catalana de Protecció de Dades intervino Carles San José i Amat, jefe del Área de Inspección en la APDCAT y, finalmente, en representación de la Agencia Vasca de Protección de Datos intervino Juana Vegas Fernández, letrada instructora de la Asesoría Jurídica de la AVPD-DBEB.

La sesión tuvo un desarrollo dinámico, presentando casos agrupados según la temática de fondo. Así, los principios considerados fueron la calidad, finalidad y legitimación de los tratamientos; la gestión del consentimiento; los accesos a la Historia Clínica por parte de los afectados y el ejercicio de los derechos de rectificación, cancelación y oposición; los accesos indebidos y el incumplimiento del deber de secreto por parte de los propios profesionales y, finalmente, cuestiones relativas a las medidas de seguridad de los datos de salud.

PRINCIPIO DE CALIDAD Y MINIMIZACIÓN DE DATOS

Se expusieron, en primer lugar, dos casos ya parcialmente tratados en ediciones anteriores, relacionados con la tramitación de sendos expedientes de responsabilidad patrimonial, en los cuales se había solicitado por el instructor e incorporado a dichos expedientes la totalidad de la historia clínica de los afectados. Por parte de la AVPD-DBEB se resolvió en su momento declarar una infracción del principio de calidad en ambos casos, por entender que los datos tratados excedían el principio de adecuación, pertinencia y minimización, y que se debió de realizar un juicio previo de ponderación, solicitando únicamente aquello que fuera imprescindible para poder resolver el asunto y que fuera relevante para el caso y no efectuar una petición genérica e indiscriminada de la historia clínica.

Ambas resoluciones fueron recurridas judicialmente por las autoridades sanitarias y resueltas contradictoriamente en primera instancia: en un caso se confirmó la resolución de la AVPD-DBEB, mientras que en el otro se estimó el recurso, anulándose la declaración de infracción. Ante tal discrepancia, ambas sentencias fueron, a su vez, respectivamente recurridas ante la Sala de lo Contencioso-Administrativo del Tribunal Superior de Justicia del País Vasco. Y en ambos casos se han visto confirmadas las resoluciones iniciales de la AVPD-DBEB, declarándose la infracción del principio de calidad por haber incorporado la

totalidad de la historia clínica a los expedientes de responsabilidad patrimonial sin haber efectuado un juicio previo de ponderación.
Por otra parte, se presentó también un caso relativo a determinados documentos de interconsulta, en los que se incluían datos relativos al diagnóstico o antecedentes personales del paciente, no relevantes para la gestión de las citas o el tratamiento. Se entendió que no resulta necesario que en los volantes, análisis de rutina o documento interconsulta, que van a ser vistos por personal no sanitario, conste de manera generalizada y como práctica habitual el diagnóstico del paciente. La inclusión generalizada y habitual del diagnóstico en dichos documentos no aporta nada al médico o personal sanitario que lo va a tratar, al constar ya en la historia clínica, especialmente cuando es electrónica, y, sin embargo, permite que dichos datos sobre la salud del paciente sean accedidos por personal no sanitario, para cuya labor no resulta necesario el conocimiento de dichos datos.

CALIDAD Y DESVÍO DE FINALIDAD

El principio de calidad restringe la utilización de los datos a finalidades "determinadas, explícitas y legítimas", no pudiendo usarse para finalidades distintas a aquellas para las que fueron recogidos. Se presentó por la AEPD, un caso en el que determinados datos, consistentes en determinadas grabaciones de sesiones terapéuticas, fueron utilizadas con posterioridad en actividades académicas de interés particular. Se declaró la infracción del principio de calidad, puesto que se habían tratado los datos para una finalidad diferente de aquella para la que fueron recogidos: la asistencia sanitaria, el tratamiento médico o la gestión de servicios sanitarios.
Asimismo, se presentó otro caso en el que un empleado de un establecimiento sanitario privado utilizó datos personales de una paciente para ponerse en contacto con ella, con una finalidad estrictamente particular. La AEPD declaró una infracción por parte del empleado, y no por parte del centro sanitario, por entender que aquel, al apropiarse de los datos, se convirtió en "responsable del tratamiento" y que había efectuado un tratamiento ilegítimo de los datos personales de la paciente.
También se expuso otro caso que, aunque pudiera parecer, en principio, similar, tuvo una diferente forma de resolución. En este caso, los datos de salud de una paciente fueron accedidos indebidamente por parte de determinado personal sanitario, y utilizados en su perjuicio dentro del contexto de un proceso de separación no amistosa. La APDCAT declaró una infracción al establecimiento sanitario, como responsable del tratamiento, por tratamiento ilícito de datos especialmente protegidos, pero con indicación de inicio de las actuaciones disciplinarias internas a que hubiese lugar.

CONSENTIMIENTO

Como regla general, la habilitación para el tratamiento de los datos de salud reside en la propia naturaleza de la prestación de asistencia sanitaria, la prevención, el diagnóstico y el tratamiento médicos, o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por personal sanitario sujeto al secreto profesional. Fuera de estos casos, solamente con el consentimiento expreso del afectado (o la existencia de una habilitación legal) podrán ser tratados los datos de salud.
El primer caso expuesto, en relación con el consentimiento, guarda una estrecha relación con el objeto principal de la presente edición del foro, es decir, la reutilización de la información de salud en el ámbito de la investigación: Un ciudadano que denunció la utilización de muestras biológicas, autorizadas para un estudio, pero posteriormente utilizadas, sin su consentimiento ni conocimiento, para otro estudio y para una tesis doctoral. La organización sanitaria afectada alega, en un primer momento, que el afectado prestó su consentimiento para ambos estudios. Sin embargo, no lo acredita ni documenta, mientras que el denunciante mantiene su negativa a haber prestado tal consentimiento (téngase en cuenta que corresponde al responsable del tratamiento la prueba de la existencia del consentimiento del afectado). Con posterioridad, alega que no hay una identificación indubitada del paciente y que los autores de la investigación no necesitaban la autorización del paciente, puesto que ya dio el consentimiento para el primer estudio. La AVPD declaró una infracción muy grave del principio

de consentimiento reforzado exigible en el caso de los datos especialmente protegidos, máxime cuando la Ley de Investigación Biomédica exige también consentimiento expreso y por escrito, no solo para la primera posible línea de investigación, sino también para las posteriores investigaciones relacionadas con la misma.

En el desarrollo de las sesiones quedó patente la reivindicación de muchos profesionales de la investigación científica con datos de salud de la necesidad de disponer de unos principios de legitimación no basados en el consentimiento. En cualquier caso, este es un punto en el cual en nuevo Reglamento General de Protección de Datos, que será aplicable a partir de mayo de 2018, aportará nuevos elementos de debate.

En otro orden de cosas, se presentó también un caso ciertamente curioso, relacionado con la inclusión de imágenes en los paquetes de tabaco como advertencias sobre los riesgos para la salud. La AEPD recibió la denuncia de un ciudadano que afirmaba haberse reconocido en una de dichas imágenes. Con posterioridad, se tuvo conocimiento por la prensa de que varias personas en toda Europa se habían identificado con la fotografía en cuestión. Tras la correspondiente investigación, se comprobó que la Comisión Europea había contratado con una empresa de publicidad la realización de las imágenes que se debían incluir en los paquetes de tabaco tras la aprobación de la Directiva 2014/40/UE, del Parlamento Europeo y del Consejo, relativa a productos del tabaco. Dicha Directiva establece la obligatoriedad de uso de una librería combinada de avisos de salud y fotografías. La librería está compuesta por un total de 42 fotografías realizadas por contratistas externos, habiéndose tomado medidas para asegurar el consentimiento y otros documentos legales para disponer de los derechos completos sobre las imágenes. Cualquier parecido con otras personas que no hayan dado su consentimiento, por desafortunado que sea, es puramente casual. En consecuencia, se archivaron las denuncias y se remitió la resolución a la Comisión Europea, para su conocimiento.

ACCESO A LA HC POR EL AFECTADO

El acceso a la historia clínica por parte del propio interesado es un derecho que, por regla general, no presenta grandes dudas en su aplicación. Sin embargo, hay casos específicos donde su aplicación puede ser problemática. Por ejemplo, en el caso de datos de menores con padres separados. En el caso presentado por la AVPD-DBEB, se trata de un acceso solicitado por uno de los padres a los detalles de la historia clínica de su hijo, mayor de 12 años, en tratamiento psicológico. La administración sanitaria entendió que el menor debía ser oído antes de conceder el acceso y, una vez informado, el menor denegó su conformidad a tal acceso. En consecuencia, la administración sanitaria valoró la opinión del menor y denegó el acceso detallado a la historia, entendiendo que ello podía poner en riesgo la salud del menor. No obstante, ofreció facilitar una información general sobre la situación clínica general y su evolución. Solicitada tutela de su derecho de acceso por el progenitor, la AVPD-DBEB consideró adecuada la denegación, puesto que se había efectuado una ponderación adecuada de los intereses en juego y se había resuelto motivadamente, primando el interés superior del menor.

Cuestión controvertida suele ser, también, el conocimiento por parte del titular de la historia clínica acerca de quienes hayan tenido acceso a la misma. En el caso presentado por la AEPD, se trataba no tanto del registro de accesos previsto como medida de seguridad exigible para los tratamientos de nivel alto, sino de un caso particularmente conflictivo: una paciente, al acudir a una cita que tenía concertada en un establecimiento sanitario, se encontró con que también había acudido su anterior pareja, la cual tenía decretada una orden de alejamiento. La paciente solicitó acceso a sus datos, en particular sobre quién había consultado sus citas. El establecimiento sanitario le denegó el acceso, alegando que se trataba de datos de terceros. La AEPD estimó la solicitud de tutela de su derecho, entendiendo que tenía un interés legítimo en defensa de sus intereses. Como consecuencia, se averiguó que su anterior pareja se había puesto en contacto telefónico, alegando la necesidad de acompañar a la paciente.

RECTIFICACIÓN DE DATOS DE SALUD

Las peticiones de rectificación de los datos de salud presentan también dificultades singula-

res, puesto que la determinación de cuándo los datos son "inexactos o incompletos" exige una valoración y ponderación facultativa, especialmente cuando la rectificación se refiere a datos relevantes para garantizar una asistencia sanitaria adecuada al paciente. En tales casos, la rectificación debe fundamentarse en el criterio expresado por los profesionales médicos que han intervenido en el proceso asistencial.

Como ejemplo de caso complejo, la APDCAT presentó un caso de petición de rectificación de informes médicos, elaborados con motivo de la prestación asistencial, así como de la rectificación de las manifestaciones efectuadas por un familiar al personal de urgencias, relativas a diagnósticos anteriores y a comportamientos del paciente. Respecto de la primera parte, la rectificación de informes médicos, la autoridad respetó el criterio de los profesionales médicos, pues la información controvertida formaba parte del contenido mínimo de la HC, que se configura como un instrumento destinado a garantizar una asistencia adecuada y en la cual se dejan constancia de todos los datos que, bajo criterio médico, permiten el conocimiento veraz y actualizado del estado de salud. Respecto de la segunda, las manifestaciones recogidas de un familiar, y a pesar de que el afectado aportó una declaración del familiar involucrado, donde se negaban buena parte de las afirmaciones que recogían los informes médicos, la autoridad también consideró que no procedía la rectificación solicitada. Consultados los profesionales de urgencias, se trataba de una transcripción literal de las manifestaciones del familiar, plenamente compatibles con el proceso que había conducido al episodio de urgencia.

MEDIDAS DE SEGURIDAD Y DEBER DE SECRETO

Uno de los puntos en los que se debe lograr un adecuado equilibrio, por parte de quienes diseñan los sistemas de control de acceso a las historias clínicas, es la ponderación entre las medidas de seguridad y la eficacia en las prestaciones asistenciales. Por ejemplo, se deben implantar controles de accesos que impidan los accesos indebidos, pero que, al mismo tiempo, permitan una cierta flexibilidad que no impida la asistencia en circunstancias fuera de lo habitual. Asimismo, las medidas de seguridad deben contribuir a asegurar el cumplimiento del deber de secreto, que afecta a todos los que intervengan en cualquier fase del tratamiento, pero que debe ser convenientemente reforzado, con una clara definición de funciones y obligaciones del personal, una adecuada difusión de las mismas y un conocimiento efectivo de las consecuencias de su incumplimiento.

Como ejemplo de lo anterior, se presentaros varios casos en los cuales se habían producido accesos indebidos por parte de empleados de organizaciones sanitarias, en diferentes circunstancias. Como criterio general, las autoridades de protección de datos valoraron a la hora de resolver el hecho de que se hubiesen adoptado medidas de seguridad para el control y registro de accesos, se hubiese supervisado tanto su cumplimiento como las excepciones al mismo, y, especialmente, que se hubiese actuado disciplinariamente en los casos de accesos indebidos.

También se presentaron casos en los que el deber de secreto se había quebrantado como consecuencia de circunstancias fortuitas o meros errores materiales. En tales casos, la clave para la declaración de infracción o el archivo de las actuaciones residió en la evitabilidad o no de los errores. En un caso de entrega de información cruzada a diferentes pacientes, se entendió que constituía un error evitable por parte del personal que imprimió y entregó los documentos, por falta de cuidado o atención suficiente. En cambio, en otro caso similar de envío de información a un correo electrónico, facilitado por el usuario, el cual contenía un error en un solo carácter, se decidió archivar la reclamación.

Finalmente, respecto de las medidas de seguridad, se expuso un caso singular, en cuanto a que se derivaba de la especial relación establecida entre franquiciadores y franquiciados de servicios relacionados con la salud. En algunos casos, los servicios prestados por el franquiciador pueden limitarse a facilitar una plataforma de comercialización de productos o servicios, pero en ocasiones también pueden gestionar una cartera de clientes compartida. En el primer caso, puede entenderse que el franquiciador se constituye en encargado de tratamiento del franquiciado, que será el responsable del trata-

miento. Pero en el segundo caso, si se comparte la cartera de clientes estaríamos en un caso de dos responsables de tratamiento, incluyendo todos los requisitos aplicables respecto de las cesiones de datos.
En lo que respecta a las medidas de seguridad exigibles al franquiciado, éste deberá adoptar sus propias medias de seguridad y, en su caso, deberá velar por que el encargado del tratamiento cumpla y aplique las medidas de seguridad indicadas en el correspondiente contrato, de forma tal que, en particular, se garantice en todo momento el acceso a la historia clínica de cada paciente por los profesionales que le asisten.

CUARTA SESIÓN



Estrategias y aplicaciones del análisis masivo de datos

Carles San José Amat moderó esta mesa debido a la imposibilidad de María Ángeles Barbará para llegar a Sevilla en el momento indicado.

Javier López siempre ha visto la investigación como algo del pasado ya que lo que hace es estudiar algo ocurrido anteriormente. "El 100% de la investigación se convierte en algo que utilizamos. Asocio la mentalidad que tenemos hoy con el concepto de big data. Si tenemos mayor capacidad computacional y somos capaces de trabajar mucho más rápido, con mucha información y muy variada, estaremos haciendo en tiempo real dedicación, es decir que la atención sanitaria estará totalmente relacionada con el proceso de investigación", aseguró. Bajo su punto de vista "ya no habrá esa línea de la que se hablaba ayer entre el uso de los datos para atención sanitaria y para investigación. Lo que debemos hacer es legislar pensando en el futuro, para actuar de forma proteccionista para algo que estamos dejando de hacer".
Los sistemas sanitarios, añadió López, "tenemos muchas necesidades que no están cubiertas. Por ello estamos enormemente interesados en el uso de los datos. Estamos convencidos de qué datos debe haber para cualquier uso, pero fundamentalmente nos estamos centrando en lo que se llama medicina personalizada y al mismo tiempo que seamos capaces de ofrecer un diagnóstico precoz". El sistema tiene minas de datos con los que "debemos de hacer cosas, según exigen los ciudadanos para que tengamos mejores herramientas terapéuticas".
Pensando en el concepto de abordaje de las enfermedades, "digamos que invertimos mu-

cho en recuperación de la enfermedad y quizás poco en promoción de la salud. Para mejorar todo esto es necesario que lleguemos a conocer mucha información que actualmente se encuentra fuera de los sistemas sanitarios. Aparece un reto importante que es cómo utilizar esa información con la que ya está a nuestra disposición", concluyó.

Ramón Román Viñas, responsable de Big Data y seguridad de la información AQUAS de la Agencia de Calidad y Evaluación Sanitaria de Cataluña, explicó que el Parlamento de Cataluña, para que se afronte este problema y se establezca el marco en el cual se pueda hacer el análisis de datos del conjunto del sistema de salud, puso en marcha un proyecto, que empezó en el año 2013 como una colaboración pública privada, siguiendo las directrices de la UE y pensando que de esta manera se podría conseguir un mayor rendimiento. En esta línea, las primeras acciones tenidas en cuenta fue hacer intervenir a la autoridad para participar en el diseño de este programa. "Se trabajó mucho con un ámbito muy restrictivo, mirándolo con mucho detalle, pensando que de esta manera se podría conseguir un mayor rendimiento, una mayor capacidad de inversión y una aceleración para ponerse en línea y empezar a tratar los datos de una forma más rápida". Por tanto, primer concepto, "seguridad en el diseño" que en el momento cero se vio que era un proceso muy ambicioso en el que habría participación privada. Este proyecto, añadió Román Viñas, se encargó a la agencia de calidad de evaluación ya que esta agencia comenzó evaluando tecnologías médicas y posteriormente se incorporó a la gestión operativa de los sistemas de información de salud y también tiene funciones de promoción de la investigación.
La agencia tiene un grado de independencia importante. "Se empezó a trabajar teniendo al principio un diálogo competitivo con empresas interesadas, que estudiaron el posible retorno que tendría la inversión. En paralelo, los diferentes grupos parlamentarios presentaron una moción en el parlamento de Cataluña en la cual se pide la suspensión de esta iniciativa, basándose en que no era correcto hacer ningún tipo de negocio con la información de los ciudadanos. La moción se aprobó por mayoría en el parlamento, suspendiéndose durante unos meses el desarrollo de este programa. Posteriormente, una nueva moción, permitió la continuidad del estudio que no se había llegado a interrumpir del todo.

Ángel Fernández Cruz, del Departamento de Arquitecturas y Tecnologías de Computadores de la E.T.S de Ingeniería Informática de la Universidad de Sevilla, dedicó su intervención a hablar de anonimización, mandato legal y reto (a la imaginación, tecnología y voluntad). Destacó que "el nuevo reglamento establece que, si a los datos personales se les hace un tratamiento ulterior, se puede utilizar para varios fines relacionados con la investigación científica. Se está quitando la limitación previa que había". Lo último del reglamento, avanza Fernández Cruz, es cómo está haciendo una llamada a la necesidad de utilizar big data en la investigación médica, cómo se pueden conseguir conocimientos de mucho valor ya que ahora se basan en una población mayor, con lo cual se obtienen muchas ventajas a la hora de explotar la información conseguida.
Otra cuestión importante, a juicio de Fernández Cruz, es que no hay un Santo Grial de la anonimización, aunque haya unas iniciativas que así lo vendan. La anonimización es distinta cada vez, ya que depende, no sólo de los datos que se van a anonimizar sino también de la función que se le quiere dar a esos datos y su propio contenido.
Las técnicas de anonimización se basan en dos principios del marco teórico. La diferencia que existe es que uno no distorsiona los datos. Los datos finales son ciertos, mientras que la aleatorización consiste en meter pequeños cambios en la información de forma que se mejore la resistencia a la reidentificación, concluyó.

Ramón Miralles López, coordinador de Auditoría y Seguridad de la Información de la Autoridad Catalana de Protección de Datos incidió en que "hay que advertir que el reglamento, como tal, ha de ser neutro, tecnológicamente hablando y con perdurabilidad en el tiempo, ya que el actual ha costado muchísimo conseguirlo".

Un concepto del reglamento es el tratamiento a gran escala que se aproxima un poco al mundo del big data, tratamiento masivo, etcétera. "Dentro de esta característica de gran escala, se considera que pudiéramos considerarlo de alto riesgo, al tratar mucha información y de muchas personas. Esto ya nos pone alerta, cuando pensamos en los derechos y libertades que pueden afectar a las personas con cuyos datos vamos a trabajar. Ello nos obliga a plantear al reglamento mayores cautelas, que nos permitan reducir los riesgos con los que contamos. Para ello disponemos de medidas de carácter técnico y organizativo. Entre las medidas están las tantas veces mencionada pseudo anonimización", explicó Miralles López.

Insistió en profundizar en la protección de los datos de carácter personal y su transformación, lo cual va dirigido a desvincular los datos personales de manera que no sea posible identificar a quien pertenecen. "No hay que perder de vista una cuestión y es que el origen son datos personales que luego han sido transformados para llevar a cabo un tratamiento de datos personales. Tengamos presente que si realizamos una reidentificación no autorizada estaríamos ante una violación de la seguridad de los datos".

Una manera de abordar la cuestión sería el "ciclo de desvinculación de datos personales", que debería iniciarse con un diseño del método de desvinculación. Seguidamente habría que aplicar el método diseñado. La tercera fase será verificar, antes de liberar la información que el riesgo está dentro de los márgenes previstos y que, además, la información tenga utilidad. La última fase del ciclo sería revisar, en cada caso, a fin de comprobar que el diseño inicial sigue siendo apto.

QUINTA SESIÓN



El Papel de los Comités de ética de Investigación en la reutilización de la Información de Salud

La sesión fue moderada por **Margarita Uría Etxebarria,** directora de la Agencia Vasca de Protección de Datos.

Matilde Vera Rodríguez, subdirectora de Asuntos Jurídicos del Servicio Andaluz de Salud y Vocal del Comité Autonómico de Ética de la Investigación, disertó sobre los Comités de Ética y, en su caso, del Comité de Ética de Investigación Biomédica. Se preguntó ¿qué papel juega en este mundo proceloso?. "Los comités de ética, en mi opinión, van a desempeñar un papel imprescindible, como guardianes de los derechos de los pacientes. Hay un reglamento de la UE del 6 de abril del 2014 que contempla los ensayos clínicos con medicamentos. La nor-

mativa estatal se adecua con un decreto que regula los ensayos con medicamentos de uso humano y que es el decreto 1090/15 de 4 de diciembre".
También se preguntó Vera Rodríguez ¿qué es un comité de ética?, ¿por quién está formado? y ¿cuál es su papel? "son órganos colegiados de varios integrantes donde la procedencia de sus miembros es muy diversa. Intervienen médicos de muchas especialidades, personal de enfermería, al menos un abogado y una persona que va a representar a los ciudadanos". El componentes de los comités son independientes de los laboratorios. La función fundamental es estudiar el riesgo / beneficio que aporta un nuevo medicamento. No solo desde el punto de vista sanitario.
"Mi visión sobre el papel que ya están jugando los Comités de Ética es crucial porque es un facilitador para que efectivamente esa normativa se pueda cumplir desde muchos puntos de vista. El reglamento europeo contempla la privacidad por diseño, la privacidad por defecto, es decir, sitúa ya las garantías de la privacidad antes del diseño de dicho sistema", concluye Vera Rodríguez.

Felipe Aizpuru Barandiarán, coordinador de la Unidad de Apoyo a la Investigación y vocal del Comité Ético de Investigación Clínica. Hospital Universitario Araba, defendió que "al ser investigador soy un usuario puro y duro de la reutilización de los datos. Como miembro del CEI tengo que contar que el otro día me manda una carta un investigador diciendo que le gustaría tener un consentimiento genérico para que todo lo que hagamos se pueda utilizar para investigación. Le contesté que hablara con el presidente pero que pensaba que eso no se permite. Aquí vemos uno de los primeros problemas que nos encontramos con el CEI que es estudiar la idoneidad de los investigadores".
"En medicina, el 25 o 30 % de las decisiones únicamente están tomadas con certeza. Estamos muy acostumbrados a trabajar en incertidumbres y a tomar riesgos", apuntó Aizpuru Barandiarán. Como investigador, añadió, "primero pensamos qué información necesitamos, luego la recogemos, con frecuencia menos de la que necesitamos, la que creemos que verdaderamente necesitamos no es la que necesitaríamos. La procesamos, estudiamos lo que hemos obtenido, sacamos nuestras conclusiones, la publicamos y la compartimos y eventualmente la reutilizamos. Si queremos reutilizar datos de la asistencia para la investigación, debemos reformar el sistema mismo de información porque está diseñado para la asistencial. Cuando quieres investigar empiezan los problemas porque hay cosas estructuradas, otras que no lo están. Y no quiero llegar a big data. Algunas hipótesis pueden ser peligrosas. Otra alternativa es el consentimiento abierto".

Amelia Marín Uranda, responsable de la Plataforma Española de Medicamentos Innovadores Farmaindustria, distingue dos momentos: los datos ya almacenados en bases de datos, en registros que tengamos, de las investigaciones que se vayan a realizar presentes y futuros. Hay que dar una seguridad jurídica a los investigadores que están reutilizando los datos y el reglamento "nos permite hablar de esos segundos usos". Explicó que todo esto hay que hacerlo con unas garantías fundamentales y en esto hay que mencionar a los comités de ética.
Ya hay proyectos de reutilización de datos en consorcios internacionales, algunos ideados por científicos españoles.
"Actualmente se está trabajando con los comités de ética para conseguir unos consentimientos más amplios, precisamente para que el paciente tenga la oportunidad de decir si quiere o no que su muestra sea almacenada y se pueda dejar en futuras investigaciones. Estamos en un momento importante a nivel jurídico y de investigación y de cómo investigamos dentro de unos años dependerá de lo que se decida. Pensad que dependerá de buscar las garantías adecuadas para seguir haciendo la mejor investigación posible". Concluyó Marín Uranda.

Dolores Jiménez Hernández, neuróloga investigadora y vicepresidenta del Comité de Ética de la Investigación de Sevilla, fue la siguiente en intervenir y aseguró que "el médico tiene un grado de desconocimiento muy importante de la protección de datos. Se pone un párrafo al final de los proyectos de investigación que viene a decir

que este proyecto está dentro y utiliza la LOPD. Los médicos aprendemos la LOPD cuando hacemos investigación o bien cuando nos acreditamos, pero normalmente desconocemos que es la LOPD".
En cuanto al marco normativo "recibí recientemente una disposición en la que hace ver cómo se ha de comportar el residente y el estudiante dentro de nuestros hospitales, ya que con el plan Bolonia manejan los datos y los utilizan con o sin privilegio. Los estudiantes lo firman y el hospital y la comisión de docencia se quedan con ambas copias, para saber que están haciendo buen uso de la legislación vigente".
Para terminar, mencionó la preocupación de los Comités por los cambios que se han presentado: "estamos en un momento clave para que nos preocupemos por la correcta utilización de datos, no solo en la investigación sino también en la asistencia".

CLAUSURA



El acto de clausura estuvo presidido por **Ramón González Carvajal,** secretario general de Investigación, Desarrollo e Innovación de Salud de la Junta de Andalucía. Le acompañaron **Manuel Romero Gómez**, director Gerente del Hospital Virgen del Rocío de Sevilla y **Juan Díaz García,** coordinador general del Foro de Seguridad y Protección de Datos de Salud.

Manuel Romero confirmó que se ha tratado un tema "candente" y que se ha votado en contra del acceso de los farmacéuticos de la comunidad a la historia de salud digital del paciente. "Hay que tener en cuenta que se anteponen, en este tema que estamos tratando, dos derechos fundamentales. En primer lugar, el derecho a la intimidad de los pacientes y en segundo lugar el derecho a la formación", explicó Romero y añadió que "a estas alturas tendrán todos unos posicionamientos mucho más claros, pero tenemos que encontrar ese punto de convergencia para garantizar todos los derechos y no conculquemos ninguno de ellos".
Muchas gracias a todos".

Ramón González demandó que se aclare el significado de lo que se denomina interés público. "La ley tiene una parte en la que, leyéndola, buscó lo que más le preocupa. Primero, ¿quién es el responsable de los datos? y en segundo lugar, ¿quién es el responsable cuando se ceden a terceros". Si el tercero falla en el uso, mantenimiento... de los datos, el responsable es el responsable, es decir el que cede los datos a un tercero". Todas estas cuestiones hay que regularlas con seguridad jurídica.


VII Reunión del Foro de Interoperabilidad en Salud
Siguenos en twitter:
@SEISeSalud
#interoperabilidad
" La Interoperabilidad, en la Transformación Digital para la Atención Integrada y la Continuidad de los Cuidados Socio-Sanitarios"
Organiza
SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD
Con la colaboración de
Junta de Castilla y León
Sacyl
SALAMANCA
Días 26 y 27 de abril de 2017
Facultad de Biología de la Universidad de Salamanca
Salón de Actos del Decanato (Edificio de Áulas)
C/Donantes de Sangre s/n
37007 Salamanca
COLABORADORES TECNOLÓGICOS
Atos
connectis
FUJITSU
gmv
Ibermática
indra
INFORMÁTICA El Corte Inglés
intel
InterSystems
SIEMENS Healthineers
PHILIPS
T-Systems

VII REUNIÓN DEL FORO DE INTEROPERABILIDAD EN SALUD

" La Interoperabilidad, en la Transformación Digital para la Atención Integrada y la Continuidad de los Cuidados Socio-Sanitarios"

SALAMANCA • DÍAS 26 Y 27 DE ABRIL DE 2017

Facultad de Biología de la Universidad de Salamanca Salón de Actos del Decanato (Edificio de Áulas) C/Donantes de Sangre s/n • 37007 Salamanca

OBJETIVO

La VII Reunión del Foro de Interoperabilidad en Salud se celebra este año en Salamanca los días 26 y 27 de Abril con el objetivo de abordar el tema de "La Interoperabilidad como factor crítico en la Trasformación Digital para la Atención Integrada y la Continuidad de los Cuidados".

Existe una visión general compartida sobre la necesidad de profundizar en la transformación digital de los sistemas de salud entre otros motivos para abordar el reto de la mejora de la atención a la cronicidad y la dependencia en el exigente contexto social y económico actual. En esa línea se puede observar un movimiento creciente para la implementación de modelos de atención integral cuya característica clave es la continuidad en la provisión de los cuidados de atención sanitaria y socio-sanitaria de una forma coordinada y comprensiva centrados en la persona. Esto supone la adquisición, procesado y uso compartido de información y conocimiento allí donde y cuando sea necesario de forma usable y segura a lo largo de los procesos de atención que involucran una amplia variedad de actores institucionales y de profesionales así como los propios pacientes, su familia y cuidadores informales. Ello requiere la interoperabilidad de una amplia variedad de sistemas de información dispersos y bajo distintas jurisdicciones, con requerimientos particularmente especiales de interoperabilidad semántica y organizativa.

Para cumplir con el objetivo planteado, la Organización de la VII Reunión del Foro de Interoperabilidad ha elaborado un Programa que sirva para compartir visiones, intercambiar experiencias y contrastar soluciones sobre las cuestiones de interoperabilidad asociadas a la trasformación digital para la mejora de la calidad y la eficiencia de la atención integral a pacientes crónicos y mayores dependientes. Para ello, en el Programa se incluyen sesiones dedicadas específicamente a:

- Debatir sobre las necesidades, enfoques y alcance de los requisitos de interoperabilidad en las info-estructuras digitales de soporte a la atención integral y la continuidad asistencial en los espacios de atención sanitaria y socio-sanitaria
- Conocer el estado de situación en el desarrollo de normas relevantes para la implementación de las soluciones de interoperabilidad (ISO, CEN, HL7, IHE)
- Saber de las actividades de investigación e innovación en herramientas y soluciones basadas en estándares para sistemas y plataformas interoperables
- Identificar las soluciones tecnológicas y experiencias de casos prácticos por desarrolladores y proveedores tecnológicos
- Conocer las estrategias, planes y proyectos desde las Administraciones y las organizaciones sanitarias y socio-sanitarias implicadas la transformación digital para la mejora de la atención a la cronicidad y la dependencia.

Para desarrollar los contenidos anteriores y estimular los debates se cuenta con un elenco de expertos y representantes de primera línea de los distintos actores implicados en el tema incluyendo autoridades, tecnólogos, investigadores, profesionales sanitarios y socio-sanitarios así como gestores de alto nivel. La asistencia a la VII Reunión del Foro de Interoperabilidad ofrece la oportunidad de conocer contrastar y debatir sobre el tema planteado dentro de un marco profesional estimulante y el entorno único y sugerente de la ciudad de Salamanca.

PROGRAMA VII REUNIÓN DEL FORO DE INTEROPERABILIDAD EN SALUD

MIÉRCOLES, 26 DE ABRIL DE 2017

16:00 - 16:30 Recogida de Documentación
16:30 - 17:00 Inauguración Oficial
Preside:
- Sr. D. Antonio María Sáez Aguado, Consejero de Sanidad. Junta de Castilla y León

Participan
- Sr. D. Luciano Sáez Ayerra, Presidente Sociedad Española de Informática de la Salud
- Sra. Dª Cristina Granados Ulecia, Gerente Complejo Asistencial Universitario de Salamanca

17:00 - 18:15 PRIMERA SESIÓN
«Monográfico "Sistema de conceptos para dar soporte a la continuidad asistencial (UNE-EN ISO 13940)"»
Moderador
- Sr. D. Adolfo Muñoz Carrero, Secretario CTN 139. Aenor. Coordinador General. VII Foro de Interoperabilidad en Salud

Ponente
- Sr. D. Pablo Serrano Balazote, Director de Planificación.Hospital Universitario 12 de Octubre

18:15 - 18:30 Pausa

18:30 - 20:00 Segunda Sesión Debate
«Necesidades y enfoques para la Interoperabilidad en las info-estructuras para la atención integral»
Moderador
- Sr. D. Rafael Sánchez Herrero, Director General de Investigación Innovación e Infraestructuras Consejería de Sanidad de la Junta de Castilla y León

Ponentes
- Sr. D. Gregorio Gómez Soriano, Representante Sociedad Española de Informática de la Salud
- Sr. D. Siro Lleras Muñoz, Jefe de Servicio de Coordinación Asistencial Sociosanitaria y Salud Mental Gerencia Regional de Salud. Junta Castilla y León
- Sr. D. Santiago Thovar Bermejo, Subdirector de Sistemas de Información. Servicio Extremeño de Salud
- Sr. D. Roberto Molero de las Heras, Sales Account Manager. InterSystems Iberia
- Sr. D. José Juan Moratilla Villaverde, Business Line Manager Digital Health Services. Siemens-healthineers
- Sr. D. Miguel Ángel Montero Martínez Director de Sanidad y Servicios Sociales Informática El Corte Inglés

21:00 Cocktail

JUEVES, 27 DE ABRIL DE 2017

9:00 - 10:30 Tercera Sesión
«Actividades de investigación e innovación en herramientas y soluciones de interoperabilidad»
Moderador
- Sr. D. José Luis Monteagudo Peña, Vicepresidente de Formación, Investigación e Innovación. Sociedad Española de Informática de la Salud

Ponentes
- *«Proyecto PITES TIISS»*
  Sr. D. Mario Pascual Carrasco, Unidad de Investigación en Telemedicina y e-Salud Instituto de Salud Carlos III
- *«Modelos de dominio HL7 mediante soluciones guiadas por modelos»*
  Sra. Dª Alicia Martínez García, Investigadora Universidad de Sevilla
- «*Financiación a la innovación tecnológica y subvenciones para proyectos de I+D»*
  Sra. Dª Carmen Alonso Martín, Asesora Dirección de Promoción y Cooperación. Centro de

Desarrollo Tecnológico Industrial. CDTI

- *«Diseño y desarrollo de un Sistema de Información para la gestión de datos sobre el cáncer de mama»*
  Sra. Dª Verónica Burriel Coll, Investigadora del Centro de Investigación PROS Universidad Politécnica de Valencia

10:30 - 11:00 Pausa Café

11:00 - 12:30 CUARTA SESIÓN

«Soluciones tecnológicas y experiencia de casos prácticos»

Moderador

- Sr. D. José Manuel Morales Pastora, Jefe de Servicio de Tecnologías de la Información y Comunicaciones Hospital Universitario Río Hortega

Ponentes

- *«Healthcare Content Management»*
  Sr. D. Pablo Camba, Director de Sanidad. T-Systems Iberia
- *«El valor de las Open APIs y FHIR en el ecosistema de servicios de Salud Digital»*
  Sr. D. Francisco Novillo, Consultor de Implantación. Orion Health
- *«Los retos actuales de la interoperabilidad en la sanidad»*
  Sr. D. Pedro Javier Jiménez Expósito, Consultor de Sanidad. Fujitsu

12:30 - 14:00 QUINTA SESIÓN

«Proyectos y planes de las Administraciones»

Moderadora

- Sra. Dª Susana García Dacal, Directora General de Infraestructuras y Tecnologías de la Información Gerencia Regional de Salud. Junta de Castilla y León. Presidenta del Comité Organizador Local

Ponentes

- Sr. D. Nicolás Francisco González López, Subdirección de Informática y Sistemas de Información. Servicio Vasco de Salud. Osakidetza
- Sr. D. Carlos Gallego Pérez, Responsable Oficina Standarts i Interoperabilitat. TicSalut
- Sra. Dª Carmen Ferrer Ripollés, Subdirectora de Sistemas de Información para la Salud. Consejería de Sanidad Universal y Salud Pública de Valencia
- Sr. D. Juan Fernando Muñoz Montalvo, Subdirector General de Tecnologías de la Información. Ministerio de Sanidad, Servicios Sociales e Igualdad

14:00 - 14:30 CLAUSURA

- Sr. D. Rafael López Iglesias. Director Gerente Gerencia Regional de Salud. Junta de Castilla y León
- Sr. D. Juan Fernando Muñoz Montalvo, Subdirector General de Tecnologías de la Información Ministerio de Sanidad, Servicios Sociales e Igualdad
- Sr. D. Adolfo Muñoz Carrero

Coordinador General VII Reunión Foro de Interoperabilidad en Salud

SECRETARÍA TÉCNICA

CEFIC, SL
Enrique Larreta, 5 - bajo izqda. 28036 Madrid
E-mail: secretaria.tecnica@cefic.es
Tel.: 91 388 94 78
www.seis.es

ENTIDADES COLABORADORAS

FUJITSU
INFORMÁTICA El Corte Inglés
InterSystems Health | Business | Government
IRE
ORION HEALTH THINKING SOFTWARE FOR LIFE
SIEMENS Healthineers
T-Systems

XXIV JORNADAS NACIONALES DE INNOVACIÓN Y SALUD EN ANDALUCÍA

Lema: ¿Quo Vadis,Sistemas de Soporte a la Decisión Clínica: ELIGES o ELIGEN?

MÁLAGA 7, 8 Y 9 DE JUNIO DE 2017

Toda Decisión Clínica aspira a ser segura para el enfermo, para el profesional y para la Institución responsable de la asistencia. Los Sistemas de Soporte a las DecisionesClínicas (CDSS), pretenden contribuir a ello considerando interacciones entre antecedentes personales, condiciones de salud, hallazgos clínicos,pruebas diagnósticas y medidas terapéuticas.Los CDSSpermiten, por ejemplo, minimizar reacciones alérgicas, interacciones nocivas, exposición excesiva a radiaciones, el riesgo de desarrollar resistencia a antimicrobianos, etc. Tambiénposibilitan el alinear a cada profesional con la mejor práctica, según la evidencia disponible y ajustándose a la decisión del enfermoen el contexto que hace posible esa terapia. Con ello se consigue, entre otros efectos, contribuir a la reducción de la variabilidad inadecuada en tiempo real, en el propio ejercicio de la práctica cotidiana. En su versión más avanzada y ambiciosa, los CDSS, además,aspiran a generar nuevas evidencias en tiempo real, creando círculos virtuosos de mejora continua tanto en el saber curar y cuidar, como en la gestión eficiente de los recursos sanitarios.

Consideramos que esta es la línea más importante que debemos consolidar durante los próximos años en el desarrollo de los sistemas de información para la salud y por ello, desde la SEIS queremos dedicar varias ediciones de las Jornadas de Innovación en Salud, que tienen lugar en Andalucía, a profundizar en ello.

Con frecuencia se dice de las decisiones de los humanos: "No decidir es decidir", "razones desconocidas apoyaron aquella decisión", "por inercia o por incuria aquello estaba descontextualizado". En esta primera edición dedicada a los CDSS abordamos el dilema "ELIGES o ELIGEN" para afirmar el compromiso con unas decisiones clínicas autónomas y responsables, apoyadas en fundamentos explícitos.

El objetivo general de las XXIV Jornadas es llevar a cabo una reflexión conjunta sobre las posibilidades y el estado del arte del soporte a las decisiones clínicas, revisando los aspectos conceptuales, los retos a los que se enfrenta, experiencias y proyectos reales, así como generar documentación útil para la construcción de proyectos en la vida real. Dado que este tema tiene un alto contenido clínico, nos proponemos también involucrar, mediante su participación activa,a otras asociaciones de profesionales sanitarios.

Se han definido 15 espacios que serán dirigidos por sendas "parejas" integradas cada una de ellas por un "Responsable institucional" y un "Socio colaborador"siguiendo el modelo habitual de las Jornadas. Once serán plenarios, de 30 minutos de duración cada uno, y cuatro serán talleres monográficos de 4 horas.

La sesión inicial constará de cuatro conferencias:

1. Sistemas de Soporte a la Decisión Clínica ¿Quo Vadis?
2. Con los pies en la tierra…
3. Aspectos regulatorios de los CDSS
4. Tecnologías del Lenguaje aplicadas a Sanidad en la Agenda Digital de España

En la mañana del jueves 8 de junio se desarrollarán los 4 talleres paralelos:

1. Prescripción en Atención Primaria
2. Resistencia a los antibióticos
3. De la imagen médica al tratamiento
4. El poder del enfermo en la Decisión Clínica

En la tarde del jueves 8 de junio se desarrollarán 4 Casos de Éxito:

1. Harmony: Estado actual megaproyecto europeo
2. Transición de Pacientes Críticos de la UCI a planta
3. Procesamiento del lenguaje natural
4. Nuevos instrumentos para la Gestión de Personas en Organizaciones Sanitarias

Durante el viernes 9 de junio se desarrollará un taller coordinado y dinamizado por antiguos alumnos del Master SEIS y gestores sobre "Barreras para la incorporación deSistemas de Soporte a la Decisión Clínica al SNS".

Las Jornadas culminarán con una mesa debate final. Se elaborarán encuestas para interactuar con los asistentes y obtener respuestas en tiempo real. Se formularán en un espacio de colaboración al que se accederá con smartphones. La organización irá mostrando a todos los participantes las respuestas que se vayan obteniendo en directo y hará elaboraciones más complejas en momentos ulteriores.

XXII PREMIOS NACIONALES DE INFORMÁTICA Y SALUD 2016

EL PASADO 19 DE ENERO TUVO LUGAR LA ENTREGA ANUAL DE LOS XXII PREMIOS NACIONALES DE INFORMÁTICA Y SALUD, CORRESPONDIENTES A 2016 Y AUSPICIADOS POR LA SEIS. COMO VIENE SIENDO HABITUAL, EL ACTO SE CELEBRÓ EN EL SALÓN DE ACTOS DE LA FACULTAD DE MEDICINA DE LA UNIVERSIDAD AUTÓNOMA DE MADRID.



El acto fue presentado por **Zaida Sampedro Préstamo**, vicepresidente de la SEIS, que dirigió unas palabras de bienvenida:

"Bienvenidos todos a este acto de entrega de los premios nacionales de Informática de la Salud que hoy alcanzan su vigesimosegunda edición.

Antes de comenzar la ceremonia de entrega, quiero dar las gracias a todos y, en particular a **Elena Andradas Aragonés,** directora general de Salud Pública, Calidad e Innovación del Ministerio de Sanidad, Servicios Sociales e Igualdad; **Mar España Martí,** directora de la Agencia Española de Protección de Datos; **Juan Antonio Vargas Núñez,** decano de la Facultad de Medicina de la UAM, que generosamente nos ofrece su hospitalidad y hace posible que hoy estemos reunidos en este magnífico entorno académico y



científico; **Mª José Marzal,** directora de ComputerWorld; **Juan Pablo Ramírez,** redactor Jefe de La Gaceta Médica y **José Ramón Zárate**, subdi-

rector de Correo Farmacéutico y Diario Médico, por su participación en este acto que inicia las actividades de la Sociedad Español de Informática de la Salud cada año".

Tras la intervención de **Juan Antonio Vargas**, **Luciano Sáez** y **Elena Andradas**, Zaida Sampedro procedió a la lectura del Acta del Jurado de los XXII Premios Nacionales.

Constituido el jurado de la Vigesimosegunda Edición de los Premios Nacionales de Informática y Salud correspondientes al año 2016, formado por







los miembros de la Junta Directiva de la Sociedad Española de Informática de la Salud, decide la concesión de los siguientes premios:

USO DE LAS TECNOLOGÍAS

1. Premio Nacional de Informática y Salud 2016, a la Entidad Pública o Privada que ha destacado en la implantación y uso de las Tecnologías de la Información y la Comunicación en el ámbito sanitario: Hospital Universitario Central de Asturias, por ser un centro de referencia en el uso de las TIC, ya que con dos años de andadura es un centro equipado con las últimas tecnologías. Es un centro dotado de una historia clínica electrónica centrada en la persona y que comparte toda la información de forma transversal en cualquier punto del hospital. Además permite incorporar el conocimiento a la toma de decisiones y así aplicar los últimos avances en la práctica clínica. Asocia los episodios clínicos de cada paciente con todo tipo de pruebas, intervenciones quirúrgicas, medicación, altas, exploraciones, etc. y facilita la transformación de la práctica clínica para un mejor cuidado de la salud de las personas.

El premio fue entregado por **José Ramón Zárate**, subdirector de Correo Farmacéutico y Diario Médico y recogido por **Luis Hevia Panizo**, gerente del Área VI de Asturias.

ESFUERZO TECNOLÓGICO

2. Premio Nacional de Informática y Salud 2016, a la Organización que ha realizado un mayor esfuerzo tecnológico para desarrollar soluciones en el sector sanitario: CERNER, por su contribución a la mejora sistémica de la atención sanitaria mediante el desarrollo de soluciones que favore-

cen la continuidad asistencial y que, sirviéndose de las últimas tecnologías, permiten identificar, analizar e intervenir de forma proactiva y coordinada en la gestión de la salud de las personas. Con una inversión anual en I+D de más de 600 M€, Cerner es considerada por Forbes como una de las 35 empresas más innovadoras del mundo. En España, está presente en más de 200 centros sanitarios. Las soluciones de HCE de Cerner cubren el 22% de las camas del SNS y alrededor del 30% de la población española. Cerner cuenta también con un nivel de referencias sin igual en el sector, incluyendo: 1 hospital HIMSS 7/Davies Award y 5 hospitales HIMSS.

Entregó el Premio **María José Marzal,** directora de ComputerWorld y lo recogió **Juan Fernández,** director general de Cerner España.

TRAYECTORIA PROFESIONAL

3. Premio Nacional de Informática y Salud 2016, al profesional que, por su trayectoria y dedicación, ha colaborado especialmente en la implantación de la Informática en el entorno sanitario, A Título Póstumo: D. Emilio Aced Félez, por toda su carrera profesional y especialmente por su aportación a la Protección de Datos en Sanidad y a la Sociedad Española de Informática de la Salud en sus últimos años.

Llegado este punto, Zaida Sampedro, en su nombre y en el de la Junta Directiva, pronunció unas sentidas palabras muy emotivas: "Emilio, nuestro querido Emilio, sentimos una gran tristeza con tu partida, aún no podemos creer que no estés físicamente con nosotros. El año pasado no pudiste asistir a esta cita anual, por compromisos profesionales. Luciano, nuestro presidente, me pidió que te sustituyera y lo hice con mucho gusto. Este año las circunstancias son otras... Para mí es un honor estar hoy aquí en tu nombre. Los que le hemos conocido coincidimos en que era discreto, conciliador, responsable, comprometido, sereno, un magnífico compañero y entrañable amigo. Al pensar en el binomio Salud y Protección de datos, nuestra mente evoca el recuerdo de Emilio, destacando además que fue un entusiasta colaborador de la SEIS. Tenemos que agradecerle su generosidad al haber compartido su conocimiento con todos nosotros, su dedicación, su entrega y la aportación de gran valor con su trabajo continuo. Para su mujer, Esmeralda; su hijo, Emilio; familiares, amigos y compañeros ha sido una suerte haber tenido la oportunidad de conocerle y que haya formado parte de nuestras vidas. Estamos orgullosos de él, de sus logros, algunos de ellos nos los deja en herencia. Podemos asegurar que ha sido un muy buen profesional y mejor persona. Emilio, sigues y seguirás estando en nuestros corazones".

El premio fue entregado por **Mar España Martí,** directora de la Agencia Española de Protección de Datos y Luciano Sáez Ayerra, presidente de la SEIS. El galardón fue recogido por **Dª Esmeralda Fuentes Lázaro,** su viuda.



IMPLANTACIÓN DE LAS TIC

4. Premio Nacional de Informática y Salud 2016, al trabajo realizado para difundir la implantación de las Tecnologías de la Información y la Comunicación en Salud: SANITAS, por su importante desarrollo TIC con la creación de BLUA, el nuevo seguro digital que integra la calidad asistencial que presta Sanitas a todos sus asegurados con las más innovadoras tecnologías de la información.

BLUA comprende de forma sencilla para el asegurado la posibilidad de hacer uso de la video consulta para hasta 13 especialidades (incluyendo Urgencias), pudiendo de esta manera elegirse el canal más conveniente para la visita médica. Los profesionales que ofrecen video-consulta son profesionales del cuadro médico habitual del paciente. Sanitas ha hecho un importante desarrollo TIC, maximizando la interoperabilidad de todos sus sistemas. El flujo de trabajo incluye la posibilidad



de acceder al área para pedir citas para video-consulta en las 13 especialidades desde la app del móvil o desde la Web, acceder a la misma, obtener los informes y prescripciones (tanto médicas como farmacológicas) resultantes y hacer un seguimiento de toda esa información en la Carpeta Personal de Salud privada del cliente (Mi Sanitas),
Entregó el galardón **Juan Pablo Ramírez,** redactor jefe de La Gaceta Médica, que fue recogido por **Loida Sánchez López de Carrión,** responsable BLUA en Marketing y Transformación Digital y **Jesús Jerónimo,** de Sanitas Seguros IT Business Partner.

MENCIÓN HONORÍFICA

Además se concedió una **Mención Honorífica de Informática y Salud 2016, al trabajo realizado para difundir la implantación de las Tecnologías de la Información y la Comunicación en Salud a** TICBioMed, por el impulso de la innovación en Salud para aportar a organizaciones sanitarias y empresas tecnológicas, mejorando la calidad de vida de ciudadanos y pacientes.
TICBioMed es una asociación que impulsa la innovación en salud para aportar valor a organizaciones sanitarias y empresas tecnológicas y mejorar la calidad de vida de pacientes y ciudadanos. Apoyan a empresas tecnológicas que ofrezcan soluciones viables en el entorno de la salud digital e impulsan la cooperación entre entidades del entorno sanitario.
Entregó el premio **Juan Pablo Ramírez,** redactor jefe de La Gaceta Médica y fue recogido por **Aquilino García Martos,** presidente de TICBioMed.

INNOVACIÓN EN PROYECTOS TIC

5. Premio Nacional de Informática y Salud 2016, al esfuerzo institucional o personal de investigación o innovación en Proyectos para la utilización de las Tecnologías de la Información y la Comunicación en Salud: Consejería de Sanidad del Gobierno de Castilla-La Mancha, por la creación, junto con el Servicio de Salud de Castilla-La Mancha, de las Redes de Expertos y Profesionales de diferentes ámbitos, utilizando herramientas tecnológicas que suponen un cambio en el modelo de gestión y participación, ya que otorga a profesionales y pacientes una labor participativa en la toma de decisiones basadas en el conocimiento, en la experiencia profesional, y mediante la innovación.
El premio fue entregado por **Elena Andradas Aragonés,** directora general de Salud Pública,





Calidad e Innovación del Ministerio de Sanidad, Servicios Sociales e Igualdad y fue recogido por **Regina Leal,** directora gerente del Servicio de Salud de Castilla-La Mancha.

APORTACIÓN SEIS

6. Premio Nacional de Informática y Salud 2016, a la mejor aportación presentada en las actividades de la SEIS durante los últimos 12 meses: Indizen Technologies, por la creación de una gran gama de soluciones y servicios innovadores mediante los cuales clasifican, estandarizan, analizan y hacen interoperable la información clínica.

Indizen está apoyando la transición a la CIE-10-ES con servicios y soluciones tecnológicas avanzadas, para mejorar la productividad de los codificadores y codificadoras, la calidad de los datos y la automatización de los procesos de codificación. Trabajan con un gran número de organizaciones tanto del sector público como del privado para facilitarles la transición a CIE-10-ES.

A nivel nacional, están ayudando al Ministerio de Sanidad, Servicios Sociales e Igualdad en el desarrollo del portal eCIEMaps.

Entregó el premio **María José Marzal,** Directora de Computer World, que fue recogido por **Enrique Mota López**, socio director de Indizen Technologies.





PREMIO ESPECIAL

El Premio Especial Informática y Salud 2016 fue para el Instituto para el Desarrollo e Integración de la Sanidad (IDIS), por la labor destacada que están realizando en materia de innovación mediante las TIC, potenciando la interoperabilidad en el ámbito de la Sanidad Privada y el desarrollo la plataforma mi e-salud para que el ciudadano pueda acceder a su información de salud a través de la red.

Entregó el galardón **Juan Antonio Vargas Núñez,** decano de la Facultad de medicina de la UAM, y fue recogido por **Adolfo Fernández–Valmayor,** presidente del Instituto para el Desarrollo e Integración de la Sanidad.

En el momento de la entrega todos los premiados pronunciaron unas breves palabras de agradecimiento. Seguidamente comenzó el concierto anual, al término del cual se ofreció a los asistentes una copa de vino español.

USO INTELIGENTE DE DATOS PARA UNA GESTIÓN PROACTIVA DE LA SALUD DE LA POBLACIÓN

Dr. Ernest Sarrias
Director Médico de Cerner España

A medida que la prestación de la asistencia sanitaria se desplaza hacia un modelo basado en la creación de valor, crece la necesidad de soluciones eficaces para gestionar la salud de la población. El envejecimiento de ésta y el aumento de la esperanza de vida, aumentan la presión sobre el gasto sanitario. Por ende, debemos apostar por un uso inteligente de la información, utilizando el* Big Data *para generar modelos predictivos y nuevos algoritmos que nos permitan dar respuestas personalizadas a cada persona.

La gestión de la cronicidad exige estrategias basadas en la interoperabilidad, con sistemas de información altamente eficientes que optimicen los recursos existentes. Cerner ofrece la plataforma *HealtheIntent*, que se ha implantado en 109 clientes a nivel global y, a día de hoy, integra los datos de más de 360 fuentes para una población de 88 millones de personas. *HealtheIntent* permite agregar, transformar y estandarizar datos provenientes de diferentes fuentes y sistemas, tanto clínicos como transaccionales, a lo largo de todo el continuo social y sanitario. Con ello se asegura que en todos los puntos del continuo asistencial se dispone de la información pertinente y oportuna para una atención segura, de calidad, efectiva y eficiente, centrada en la persona y sus preferencias, necesidades sanitarias y sociales.

El caso de Advocate Health Care y su Programa de Integración Clínica es un buen ejemplo de lo mucho que puede hacer la tecnología Big Data para mejorar la salud de las comunidades. Con sede en Illinois (EE.UU.), Advocate cuenta con más de 250 centros asistenciales, incluyendo 11 hospitales y un equipo de más de 5.000 médicos. En 2014, la organización trabajó con Cerner para identificar sectores de población en riesgo de desarrollar una enfermedad crónica y anticiparse a ello. Entre los resultados del programa, destaca la mejora en el tratamiento de pacientes asmáticos: la ratio de control de esta patología en hospitales de la Advocate Health Care llega al 76,5% mientras que la media de los Estados Unidos se queda en el 50%[1].

En nuestro entorno, donde hace décadas donde tenemos desplegado este modelo centrado en la gestión de la salud poblacional (que incluye la promoción de la salud, la prevención, y la rehabilitación, no solo la asistencia), las tecnologías de la información son la palanca que permitirá asegurar la sostenibilidad del sistema.

1. Fuente: Informe Anual 2016 de Advocate Health Care http://www.advocatemediacenter.com/2016/valuereport/performance.html

PROTECCIÓN DE
DATOS EN SALUD

Coordina: **Juan Diaz**

El Análisis de Impacto de la Privacidad, un reto para las organizaciones Sanitarias

El Reglamento General de Protección de Datos UE 2016/679 recoge varias novedades a la hora de abordar las estrategias de seguridad que aplican a la información y en concreto a los tratamientos de información especial como la "Salud".

El nuevo marco permite una aplicación flexible de medidas de seguridad en función de los requerimientos de cada tipo de tratamiento de datos, adecuando proporcionalmente las salvaguardas en función de los riesgos detectados. Las organizaciones sanitarias tendrán que realizar un análisis de riesgo de los tratamientos que realizan (PIA Privacy Impact Analysis) para determinar qué medidas tienen que aplicar y cómo hacerlo.

Puede definirse como una metodología para evaluar el impacto en la privacidad de un proyecto, política, programa, servicio, producto o cualquier iniciativa que implique el tratamiento de datos personales y, tras haber consultado con todas las partes implicadas, tomar las medidas necesarias para evitar o minimizar los impactos negativos. Una evaluación de impacto en la privacidad es un proceso que debería comenzar en las etapas más iníciales que sea posible, cuando todavía hay oportunidades de influir en el resultado del proyecto.

Una PIA o una Evaluación de Impacto en la Protección de los Datos Personales (EIPD) es un ejercicio de análisis de los riesgos que un determinado sistema de información o servicio puede entrañar para el derecho fundamental a la protección de datos de los afectados y, tras ese análisis, afrontar la gestión eficaz de los riesgos identificados mediante la adopción de las medidas necesarias para eliminarlos o mitigarlos.

Permite identificar los posibles riesgos y corregirlos anticipadamente, evitando los costes derivados de descubrirlos a posteriori, cuando el servicio está en funcionamiento o, lo que es peor, cuando la lesión de los derechos se ha producido. En estos casos no solo se incurre en costes económicos, sino también de imagen para la organización cuya reputación se ve afectada.

En las organizaciones sanitarias residen don aspectos claves que nos obligan a realizar dicho análisis de impacto, uno es la naturaleza de los datos que se tratan y otro es el tratamiento masivo de ellos que hacemos.

El tener de cada sistema de información los flujos de información que se producen, los riesgos derivados de los propios datos, los riesgos de las herramientas que lo soportan, las medias de seguridad implementadas y el marco normativo específico constituyen la base del informe del análisis de impacto. En dicho informe estarán cuantificados los riesgos identificados, las recomendaciones, las propuestas para eliminarlos o mitigarlos y deberá ser notificado a la dirección de la organización.

Una vez priorizadas las acciones que deben llevarse a cabo, se asignaran los recursos necesarios para su ejecución y del responsable de implantarlas. Revisando la efectividad de las medidas y verificando si se han creado nuevos riesgos o se han detectado otros que habían pasado desapercibidos. Estableciendo un proceso de mejora continua sobre la seguridad de la información de salud.

Es un tema complejo que requieres un esfuerzo de las organizaciones y debemos realizarlo para todos nuestros sistemas de información de salud antes de la entrada definitiva del nuevo reglamento de protección de datos UE 2016/679 el próximo 25 de Mayo de 2018.

FORO DE
GOBERNANZA

Coordina: **Martín Begoña**

La Transformación Digital y el Gobierno TI (2)

La transformación digital nos obliga a redefinir en el Gobierno TI, entre otros, los siguientes componentes: el catálogo de servicios TI, el modelo de sourcing y el modelo de relación con el usuario.

El nuevo paradigma empresarial al que se camina, en el que las Tecnologías de la Información se configuran como principal catalizador, hace que su gobierno necesite evolucionar de forma muy sensible.
El catálogo de servicios debe experimentar importantes cambios. Las nuevas tecnologías hacen que se tengan que redefinir los servicios existentes. La incidencia del cloud en los servicios de infraestructuras es evidente, ofreciendo la posibilidad de transformación de inversiones en costes, facilitando los crecimientos e introduciendo nuevos parámetros de gestión.
Se deben valorar los costes, los riesgos, la legislación, etc., para optar por las ventajas que ofrecen los servicios cloud. Aparecen nuevos elementos (dispositivos, sensores, ...), que es preciso integrar. Los datos y la importancia de su análisis, obligan a configurar nuevas herramientas y servicios.
En el ámbito de los servicios AM (Applications Management), hay que priorizar los proyectos y analizar los perfiles que se precisan. Los servicios en general deberán estar totalmente sincronizados con las necesidades del negocio y proveerse con la velocidad y requerimientos que éste precisa para aprovechar las oportunidades que ofrece el nuevo escenario de transformación digital.
En la redefinición del catálogo de servicios se evidencia la necesaria evolución del modelo de sourcing. Los servicios cloud, ya sea cloud privada o pública, darán el paso de la propiedad de las infraestructuras a servicios de alquiler, proporcionados por un proveedor, que posibilita la disposición de las infraestructuras al momento. En los servicios AM, habrá que valorar la disponibilidad, o en su caso la incorporación, de expertos en las nuevas tecnologías o la subcontratación de proyectos y/o profesionales; la capacidad de profesionales con conocimientos avanzados en las nuevas tecnologías será el criterio fundamental para adoptar las decisiones adecuadas.
La especial incidencia que tiene la transformación digital en el negocio, hace que el modelo de relación con el usuario deba experimentar importantes cambios. Los profesionales de marketing y de tecnología deben trabajar juntos para crear y ejecutar la hoja de ruta única de la agenda digital de la empresa. El diseño de la estrategia de transformación digital se debe realizar sumando la visión de negocio y la tecnológica; y en la ejecución deben existir un diálogo y un contraste constantes para garantizar el éxito y la proyección de futuro de los proyectos.
Por otra parte veremos en un capítulo posterior las aportaciones del Gobierno TI en el desarrollo de las competencias digitales de los profesionales que integran la organización; cómo desde el Gobierno TI se debe participar en el desarrollo de los profesionales en el nuevo escenario digital.
En el contexto del nuevo Gobierno TI, y dentro de la sopa de letras que existe en TI y en la gestión empresarial, aparece un nuevo acrónimo, CDO (Chief Digital Officer). El CDO es el "jefe de la transformación digital", que debe gestionar una de las dos velocidades del Gobierno TI, la de la transformación digital. La organización deberá decidir si el actual CIO puede ser el CDO o si debe sumarse un responsable TI, que asuma el papel de Chief Digital Officer, líder de la transformación digital.
Como señala McKinsey, en su artículo 'Transformer in chief': The new chief digital officer", la verdadera medida del éxito del CDO, es cuando este rol se convierte en innecesario, pero también es verdad, que su verdadera naturaleza ha funcionado con éxito.

FORO DE
TELEMEDICINA

Coordina: **Óscar Moreno**

Usar el teléfono móvil para analizar el aliento y detectar enfermedades

Un proyecto financiado por la UE ha desarrollado un módulo llamado Sniffphone para los teléfonos móviles y que es capaz de analizar el aliento del usuario para detectar hasta diecisiete enfermedades diferentes.



Añadir sensores a los teléfonos móviles se ha convertido en toda una tendencia, y los modelos más innovadores logran detectar cambios en cosas tan dispares como la temperatura, la humedad, los gestos manuales o la luz. A pesar de que ya se han comercializado dispositivos portátiles para detectar el nivel de alcohol en la sangre y mostrarlo en el móvil, el uso y aprovechamiento de la tecnología del análisis del aliento aportaría un grado más en la evolución de los teléfonos móviles, abriendo un nuevo campo de desarrollo de aplicaciones.

En un estudio publicado en la revista ACS Nano en diciembre pasado se presentaba la tecnología «Na-Nose» la cual, integrada en un dispositivo, detecta los patrones químicos de los compuestos orgánicos volátiles que exhalan los pacientes. Este nuevo estudio, aparte de demostrar por primera vez que se puede establecer un vínculo entre enfermedades específicas y estos patrones químicos, pone de manifiesto que el Na-Nose usa nanopartículas de oro y nanotubos de carbono para diagnosticar hasta diecisiete enfermedades distintas, entre ellas algunos cánceres en fases tempranas.

Las finas capas de nanopartículas de oro o monotubos de carbono de la matriz de sensores están revestidas de ligandos orgánicos. El funcionamiento se basa en que cuando los compuestos exhalados se fijan a los ligandos, se produce un cambio en la resistencia eléctrica entre las nanopartículas o los nanotubos. La señal resultante se envía a un ordenador que emplea un programa de reconocimiento de patrones para determinar si concuerda con la de una enfermedad concreta.

El dispositivo está preparado para reconocer veintitrés dolencias, después de que fuese probado con ocho mil pacientes para enseñar al programa a distinguir entre una enfermedad y posibles factores de confusión como la contaminación, la edad, el sexo, una enfermedad subyacente y la zona geográfica. El año pasado, ya demostraron que, en un ensayo a ciegas, esta herramienta logró detectar cáncer gástrico en pacientes con una precisión de entre el 92 % y el 94 %. Ahora bien, con este nuevo estudio han dado un paso adelante al utilizar Na-Nose para detectar y distinguir entre 17 enfermedades distintas en el aliento de 1 404 personas de 5 países diferentes.

El siguiente paso consiste en miniaturizar el dispositivo para poder incorporarlo a los teléfonos móviles de aquí a agosto de 2018, gracias a la financiación recibida por el proyecto SNIFFPHONE en el marco del programa Horizonte 2020. «Aspiramos a detectar las enfermedades en una fase temprana para poder incrementar el índice de supervivencia», comenta Hosssan Haick, el ingeniero inventor del sistema.

El proyecto Sniffphone está coordinado en Israel y tiene un presupuesto total de casi 6M€ dentro de la convocatoria ICT-2014-1, de la Acción de Innovación e Investigación (RIA) del Horizonte 2020.

Más información:
- *CORDIS - http://cordis.europa.eu/news/home_en.html*
- *SNIFFPHONE - https://www.sniffphone.eu/*

FORO DE
INTEROPERABILIDAD

Coordina: **Adolfo Muñoz Carrero**

UNE –EN ISO13940 – Cuestiones sanitarias

Continuamos con la exposición de los conceptos definidos por la norma UNE-EN ISO13940 que se comenzó en el número anterior. Se recuerda que no se pretende describir completamente los conceptos y sus relaciones, para lo que es recomendable acudir a la Norma que ya está disponible, sino dar unas nociones básicas sobre el significado de los conceptos y cómo usarlos.

En **negrita** se escribe el concepto que se define con la definición normalizada subrayada. En itálica otros conceptos también definidos por la Norma.

- **Cuestión sanitaria:** representación de una cuestión relacionada con la salud de un *sujeto de la asistencia* y/o la provisión de asistencia sanitaria a dicho *sujeto de la asistencia* tal y como viene identificado por uno o varios actores sanitarios.
- **Tema de salud:** representación de un tema relacionado con la salud de un *sujeto de la asistencia* tal y como viene representado por uno o varios *actores sanitarios*.
- **Condición de salud:** aspectos del *estado de salud* observados o potencialmente observables en un momento dado.
  - Puede ser *condición observada, problema de salud o condición potencial de salud.*
- **Condición observada:** *condición de salud* observada por un *actor sanitario.*
  - Puede ser *condición valorada profesionalmente o condición resultante*
- **Problema de salud:** *condición de salud* considerada como un problema por un actor sanitario.
- **Condición de salud potencial:** *condición de salud* actual o posible en el futuro descrita por un *actor sanitario*.
  - Puede ser *condición de riesgo, condición considerada, condición pronóstico o condición objetivo*
- **Condición valorada profesionalmente:** *condición observada* valorada por un *profesional sanitario* en relación al origen, curso, la gravedad o el impacto del *estado de salud.*
- **Condición resultante:** *condición observada* que representa el *estado de salud de salida.*
- **Condición considerada:** *condición de salud potencial* considerada por un *actor sanitario* sobre la base de una o más *condiciones observadas.*
- **Diagnóstico de trabajo:** *condición considerada* que uno o más profesionales sanitarios han determinado que es la más consistente a la vista de las *condiciones observadas que se conocen en ese momento.*
- **Condición excluida:** *condición considerada* que uno o más *actores sanitarios* han determinado que no es consistente con las *condiciones observadas conocidas.*
- **Condición objetivo:** *condición de salud potencial* que representa los *objetivos de salud y/o las metas sanitarias.*
- **Condición pronóstico:** *condición de salud potencial* que representa el curso esperado de un *estado de salud* según la valoración de profesionales sanitarios.
- **Condición de riesgo:** *condición de salud potencial* que representa un futuro no pretendido de un *estado de salud.*
- **Estado de salud:** funciones físicas y mentales, estructura corporal, factores personales, actividad, participación y factores del entorno que componen la salud de un *sujeto de la asistencia.*
- **Estado de salud de entrada:** *estado de salud* al inicio del *proceso sanitario.*
- **Estado de salud de salida:** *estado de salud* al finalizar el *proceso sanitario.*
- **Necesidad de salud:** déficit en el *estado de salud* actual comparado con un *estado de salud* deseado en el futuro.
- **Serie de salud**: asociación definida entre *cuestiones sanitarias* determinada por uno o varios *actores sanitarios*.
- **Interés del proceso clínico:** *serie de salud* que comprende todas las *cuestiones sanitarias* relacionadas con un *proceso clínico* específico.
- **Lista de problemas de salud:** *serie de salud* que enlaza un conjunto de *problemas de salud.*
- **Evolución de la condición de salud:** *serie de salud* que muestra la evolución de las *condiciones de salud* durante el *proceso sanitario* comenzando con la *condición de salud* que represente el *estado de salud de entrada.*

SECTOR
ENFERMERÍA

Coordina: **Azucena Santillán**

Soluciones tecnológicas para las personas con TEA

En el marco de la Jornada de Enfermería para la entrega de la "I Edición de los Premios de Investigación en Enfermería" del Hospital Gregorio Marañón se expusieron varios trabajos de innovación tecnológica que han visto la luz (o están en vías de verla) gracias al trabajo de los enfermeros que los han impulsado y de las instituciones que los han apoyado.



Uno de estos trabajos expuestos y que más recorrido tiene es el portal "Doctor TEA" (www.doctortea.org), creado por La Fundación Orange y el Hospital General Universitario Gregorio Marañón (a través de su Fundación para la Investigación Biomédica). Esta página web trata de facilitar las visitas médicas de las personas con trastorno del espectro autista (TEA), familiarizándose con el entorno médico a través de un recorrido por distintos espacios, profesionales y procedimientos médicos, que se explican con viñetas, videos y animaciones. Además, cuenta también con una sección de juegos para hacer más fácil y divertida esta familiarización con el entorno hospitalario.

Doctor Tea pretende, por un lado, facilitar las visitas médicas de las personas con autismo proporcionando información sobre las prácticas médicas más frecuentes para que las puedan entender y anticipar, y, por otro lado, trata de proporcionar información a los médicos sobre las características de estos pacientes, así como consejos prácticos a las familias.

En la web también se ofrece la presentación de varios profesionales como enfermeros, psicólogos, oftalmólogos, neurólogos… la visualización de los instrumentos más comunes en las pruebas médicas (electroencefalograma, resonancia magnética, análisis de sangre…) e incluso una sección de juegos que permitan un acercamiento más lúdico a la información de los elementos hospitalarios ("encuentra las diferencias", "colorea", "une los puntos"…).

Se ha accedido a la web desde más de 70 países diferentes, siendo los 10 con más visitas: España, Argentina, Rusia, Estados Unidos, México, Chile, China, Perú, Venezuela y Francia.

Otros resultados cualitativos incluyen el interés de instituciones extranjeras para traducir los materiales a diferentes idiomas y la invitación a múltiples foros científicos, asociaciones de familiares y asociaciones profesionales para presentar el proyecto.

Cabe destacar que Doctor TEA es una herramienta gratuita de acceso abierto con la que colaboran otros hospitales como el Hospital Universitario de Burgos, Hospital Puerta de Hierro, Hospital de Villalba, Hospital Clic de Barcelona o el Hospital de Manises entre otros. Desde el propio Doctor TEA se anima a otros hospitales a que se sumen al proyecto.

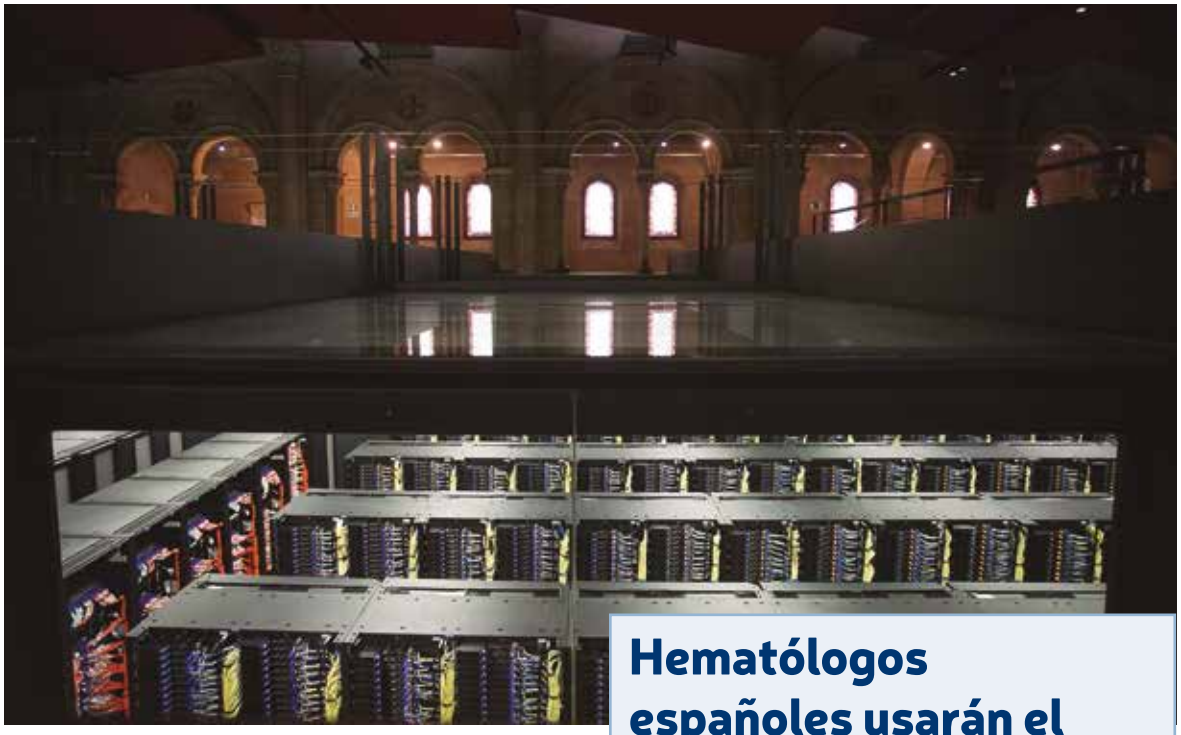
REFERENCIAS

Boada, L., & Parellada, M. (2016). Ir al médico sin miedo: www.doctortea. org para la habituación al entorno médico de pacientes con autismo. Revista de Psiquiatría y Salud Mental.

INFORMÁTICA
MÉDICA

Coordina: **José Sacristán**

El superordenador español entra al taller para salvar más vidas



AHORA EL MARENOSTRUM ESTÁ ANTE UN RETO MAYOR.

Está tratando datos de 3.000 tumores de veinte tipos distintos. El Barcelona Supercomputing Center es uno de los ocho centros de investigación de todo el mundo que forma parte de PanCancer, un proyecto de big data que analiza mutaciones a gran escala para conocer más la enfermedad. La aplicación de este conocimiento a los hospitales "no es inmediata", asegura Torrents. Sin embargo, añade que trabajar codo a codo con los centro sanitarios es clave y, en ese sentido, el BSC lo está haciendo con el Clínic y el Vall d'Hebron de Barcelona.

Más información: http://elpais.com/elpais/2017/03/13/talento_digital/1489425002_979125.html

Hematólogos españoles usarán el Big Data para dibujar el mapa europeo de los tumores hematológicos

Los hematólogos Jesús María Hernández Rivas y Guillermo Sanz Santillan liderarán en coordinación con el Instituto de Investigación Biomédica de Salamanca (IBSAL) el proyecto 'Harmony'. Este proyecto europeo ha sido aprobado por la Iniciativa de Medicamentos Innovadores, y servirá para dibujar el mapa europeo de los tumores hematológicos mediante el Big Data.

http://www.phmk.es/hematologos-espanoles-usaran-big-data-dibujar-mapa-europeo-tumores-hematologicos/

SECTOR
FARMACIA

Jose Manuel Simarro
Responsable de Sistemas de Información en la AEMPS

Coordina: **Alberto Gómez Lafón**

Modelización de información farmacéutica: Modelo relacional de datos Europeo RDM y Estándares ISO IDMP (Identification of Medicinal Product)

Los modelos de información farmacéutica definen y relacionan elementos de información entre sí, siendo referencia para que sistemas independientes entiendan, interpreten y utilicen la información de la misma manera y puedan intercambiar la información entre ellos.

ISO ha desarrollado cinco normas denominadas series IDMP para la modelización de la información farmacéutica, han sido desarrolladas en respuesta a la necesidad mundial de especificaciones internacionales armonizadas. Juntas proporcionan la base para la identificación exhaustiva de medicamentos. Estas cinco normas son:

- ISO/DIS 11615 Health Informatics - Estándar para la Identificación de Medicamentos. Identificador MPID.
- ISO/DIS 11616 Health Informatics - Estándar para la Identificación de Productos Medicinales. Identificador PhPID.
- ISO/DIS 11238 Health Informatics - Estándar para la Identificación de Principios Activos
- ISO/DIS 11239 Health Informatics - Estándar para la Identificación Formas Farmacéuticas, Dosis, Unidades de Presentación, Rutas de Administración y dispositivos y materiales de acondicionamiento
- ISO/DIS 11240 Health Informatics - Estándar para la Identificación de Unidades de Medida

Estos estándares definen una jerarquía de conceptos en cuya raíz aparece el medicamento (Medicinal Product) identificado por un código denominado MPID (Medicinal Product Identifier), un medicamento está compuesto por Productos Farmacéuticos (Pharmaceutical Products) identificados por códigos PhPID. Un medicamento puede relacionarse con uno o más productos farmacéuticos, por ejemplo un kit que contiene capsulas de 500 mg y una crema al 10% o un kit con polvos y disolvente administrable después de la reconstitución según se especifique en el resumen de las características del producto son medicamentos compuestos por dos productos farmacéuticos.

Los productos farmacéuticos vienen especificados por los principios activos que contienen, sus respectivas dosis, sus formas farmacéuticas, vías de administración y los dispositivos incluidos en ellos (por ejemplo una malla para promover crecimiento de tejido celular que viniese incluida en un producto farmacéutico). Estos son los atributos identificativos de un producto farmacéutico (pharmaceutical product).

Los principios activos (substances) son quizás el concepto más relevante y complejo de la especificación IDMP. En el modelo de datos los principios activos son parte de los productos farmacéuticos, esto es un producto farmacéutico puede tener una o varias sustancias activas. El estándar distingue entre sustancia (substance) y sustancia especificada (specified substance) estas últimas son un subconjunto de las primeras. Una sustancia es cualquier materia que tiene una existencia discreta, cuyo origen puede ser biológico, mineral o químico. Las sustancias se clasifican en sales, solventes, ácidos, bases, y sustancias compuestas de ingredientes simples o sintetizados. Las sustancias especificadas son un subconjunto que incorpora información más detallada recogiendo en el modelo información sobre productos intermedios, información de fabricación y propiedades físicas y biológicas. El estándar ISO/DIS 11238 define un modelo de datos adecuado y consensuado internacionalmente para recoger todas estas informaciones que caracterizan a los principios activos.

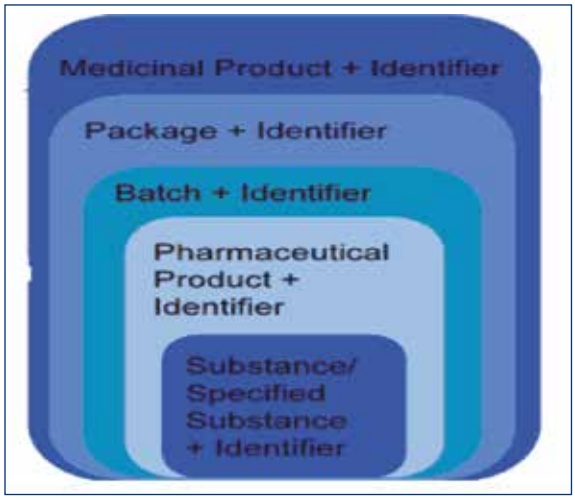
Los últimos dos estándares definen conceptos que sirven para caracterizar a los medicamentos y productos farmacéuticos, conceptos tales como forma farmacéutica (cápsulas, comprimidos, ...), dosis, rutas de administración (administración oral, administración rectal, ...) y finalmente unidades de medida.

Especial interés tiene la introducción de identificadores que hace el estándar ISO/DIS 11615 y su vinculación con el concepto de medicamento, lo relevante de estos códigos es validez internacional y su vocación para ser utilizados de forma universal en el mundo regulatorio dejando abierta la puerta a su uso en el mundo de los servicios de salud (Sistemas de prescripción, historia clínica digital, etc…

Estos identificadores se asocian ateniendo a la siguiente lógica:

- Identificación de medicamento: el identificador MPID identifica a un medicamento (sustancias activas, forma, dosis, vías y marca comercial), por ejemplo el fármaco – Amoxicilina XXX cápsulas, administración oral, 250 mg -, tendría el identificador, país-V-00-0XYZ1-20Z0 (valor ficticio). El código equivalente en nuestro sistema nacional de salud sería el número de registro.
- Identificación de presentación (Identificación del medicamento dada en el punto anterior añadiendo el nº de formas que contiene el paquete ej 20 cápsulas); El código equivalente en nuestro sistema nacional de salud sería el Código Nacional de la presentación. El estándar establece un identificador PCID, que permite la discriminación de presentaciones de un medicamento, pe:
- Amoxicilina XXX cápsulas, administración oral, 250 mg. Número de autorización para 250 mg cápsulas (nivel del producto) país-V-00-0XYZ1-20Z0; número de autorización (nivel de presentación) país-V-00-0XYZ1-20Z0-0001 para 20 capsulas y país-V-00-0XYZ1-20Z0-0002 para 30 cápsulas.
- Fármaco A - uso subcutáneo - suspensión inyectable - 40 IU/ml -Frasco (vidrio) - 10ml (1,4 mg/ml) - 1 frasco. Identificador → país-V-00-1YX00-0003;
- Fármaco A - uso subcutáneo - suspensión inyectable - 100 UI/ml - Frasco (vidrio) - 10 ml (3,5 mg/ml) - 1 frasco. Identificador → país-V-00-1YX00-0003.
- Identificador de lote del medicamento (BAID_1): Identificador que asocia un medicamento con un nº de lote. (MPID + Batch Sequence Number).
- Identificador de lote de la presentación (BAID_2): Identificador que asocia una presentación con un nº de lote. (PCID+ Batch Sequence Number)

Los atributos del medicamento asociados a estos identificadores son:



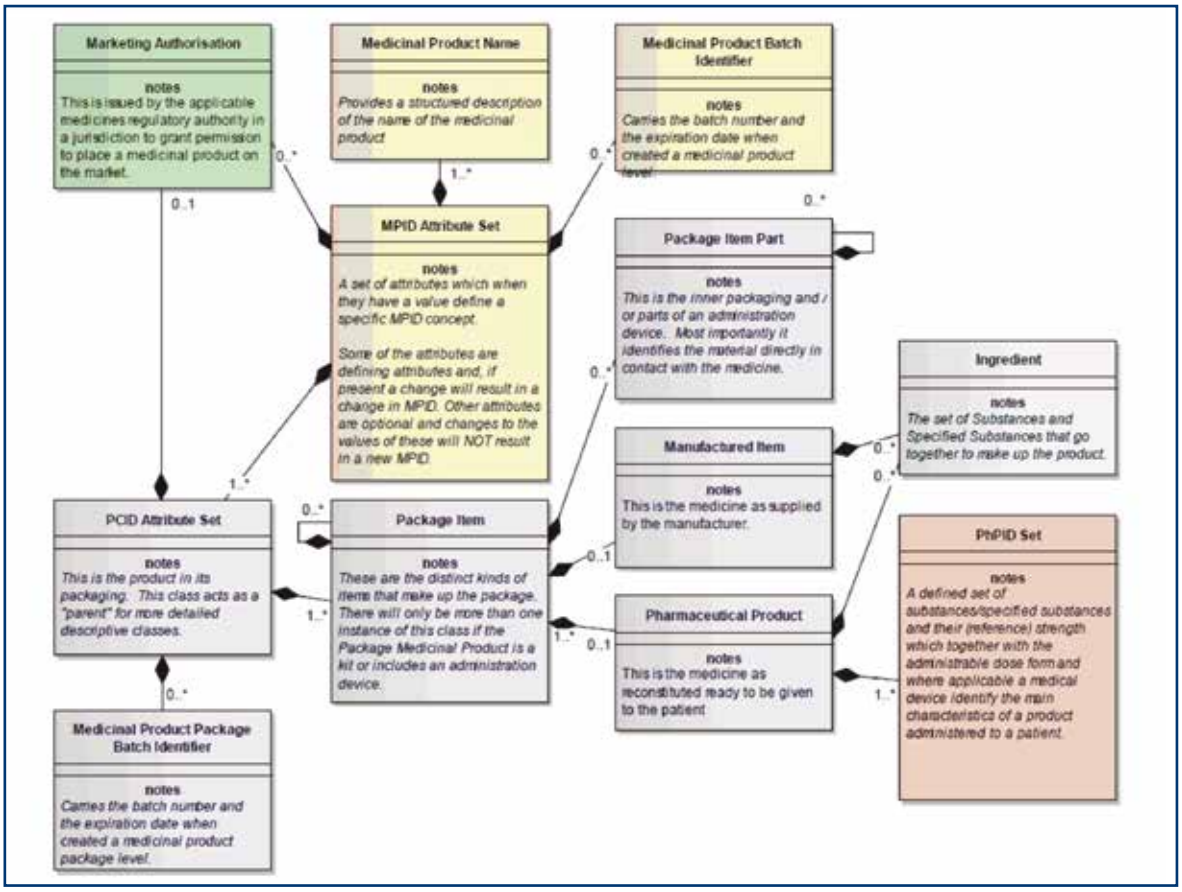
Jerarquía de Identificadores

- Nombre del medicamento.
- Estado administrativo.
- Términos de la autorización de comercialización.
- Titular de la autorización.
- Fabricantes de producto terminado y sustancias.
- Autoridad Reguladora que emitió autorización de comercialización.
- composición cuantitativa y cualitativa.
- Dosis, forma farmacéutica, ruta de administración.
- Dispositivos que forman parte del medicamento.
- Indicaciones autorizadas.
- Clasificación del producto.
- Descripción de la presentación (envase, dispositivos de administración, materiales, cierres y tamaños)

El cambio de uno de estos atributos a nivel regulatorio implicaría la asignación de nuevos identificadores. La norma también define los conceptos necesarios para asociar MPID y PCID con los números de autorización asignados por una autoridad regulatoria de medicamentos de una jurisdicción dada. Tal asociación deberá utilizar los siguientes dos principios:

A) El MPID será asociado con el número de autorización de comercialización de medicamentos (por ejemplo el MPID pais-15.2YZ será asociado con la autorización número país-055-0957 para el medicamento B - comprimidos recubiertos con película - 250 mg, con presentaciones de 50 y 100 comprimidos).

B) el PCID será asociado con el número de autorización de comercialización aplicable para una presentación específica (e.g. PCID país-0787-2550-05 será asociada a 0XYZ1-20Z0-05 para Amoxicilina 250 mg 20 cápsulas).



Modelo de datos de alto nivel definido por el estándar ISO ISO/DIS 11615

Finalmente también fija los conceptos necesarios para la asociación entre identificadores de medicamentos y los números de códigos de artículo™ (GTIN). El código GTIN en el área de salud es el sistema de codificación más extendido aunque no único, usado para identificar elementos que son comercializados a través de una cadena de suministro (p. ej. productos farmacéuticos y productos sanitarios). El número Global de artículo comercial (GTIN) sirve identificar cualquiera de estos elementos y recuperar información predefinida del mismo como precio, ordenado o facturado u otro dato de interés en cualquier punto en cualquier cadena de suministro. La recuperación se realizaría a través de una consulta a una Base de Datos y a partir del identificador GTIN. Los valores GTIN pueden ser 8, 12, 13 o 14 dígitos de longitud. El Grupo de usuarios de salud GS1 defiende el uso de la normalización global para facilitar el cumplimiento de normas seguridad y lucha contra medicamentos falsificados en todos los países. Sin embargo las normas nacionales, federales o locales tienen prevalencia sobre cualquier estándar de GS1.

Las características básicas definidas en un código GTIN de un elemento comercializado son:

- Nombre del producto y marca del producto y descripción del producto
- Composición (ingredientes activos) y Dosis
- Cantidad neta (peso, volumen u otra dimensión afecta comercio)
- Configuración de embalaje
- Forma Farmacéutica
- Para las agrupaciones, el número de sus elementos unitarios y su subdivisión en unidades empaquetadas, materiales de acondicionamiento.

Además de la identificación del producto (GTIN), el código de barras, incluye el número de lote y la fecha de caducidad. La norma define también los conceptos necesarios para asociar PCID y BAID_2 (Identificador del nº de lote de la presentación) con el GTIN pertinente. Tal asociación deberá utilizar los siguientes dos principios:

A) el PCID siempre será asociado con el GTIN aplicable del medicamento.

B) El lote número, la fecha de caducidad y el GTIN, identifican a un BAID_2.

NOTICIAS DEL SECTOR

Coordina: **Diego Sáez**

- **InterSystems anuncia** su acuerdo con MCG Health, proveedor de soluciones de atención sanitaria. MCG Health utilizará InterSystems HealthShare® como plataforma de interoperabilidad para compartir las pautas de atención sanitaria básica basadas en el análisis de los datos con los planes de salud y sus proveedores. La nueva solución de MCG, basada en cloud, Care Net, desarrollada sobre HealthShare, conectará a los pagadores y proveedores para que los procesos de atención sean más eficientes.

- **ViDAL Vademecum** se consolida en Chile como actor de referencia en terminología de medicamentos. El sistema de información farmacológica de ViDAL Vademecum que se utiliza en el 80% de los Servicios de Salud Chilenos incorpora la terminología SnomedCT en su versión TFC - Terminología Farmacéutica Chilena - y permitirá a los sistemas de información tanto hospitalarios como de Atención Primaria mejorar su interoperabilidad semántica así como vincular información clínica estructurada con información administrativa de los medicamentos.

- **El Grupo Hospitalario HLA** ha decidido invertir para mejorar la seguridad en el uso de los medicamentos y los procesos relacionados con la información del medicamento. Tich Consulting del grupo HLA se encarga de desarrollar e implementar el sistema de gestión clínica Green Cube® utilizado en toda la red de ASISA y donde se integra la solución de información de medicamentos de ViDAL Vademecum.

- **SIA ha sido seleccionada por Asepeyo**, Mutua Colaboradora con la Seguridad Social nº 151 para implementar una solución destinada a la gestión de sus cuentas privilegiadas (Privileged Account Manager - PAM). Dotará a Asepeyo de una solución para establecer controles robustos en el uso de las cuentas privilegiadas y de sus credenciales, y reducir los riesgos asociados.

- **Fraternidad-Muprespa** contrata una solución VNA-PACS (Vendor Neutral Archive – PACS) como corazón digital de su nuevo hospital en Paseo de la Habana (Madrid). El nuevo hospital, cuya apertura se realizará en 2018 y está especializado en cirugía traumatológica, ha licitado de acuerdo a la Ley de Contratos del Sector Público y ha contratado la solución VUE de Carestream. Este PACS permitirá centralizar toda la información clínica, tanto del servicio de diagnóstico por la imagen como de los quirófanos integrados; éstos estarán dotados de capacidad de procesamiento de imágenes y vídeos procedentes de los sistemas de endoscopia, cámara quirúrgica y cámaras ambientes.

- **GFI consolida su Business Unit de Salud.** En 2006 Gfi ya adquirió Savac Consultores y el pasado año 2016 con la adquisición de EFRON Consulting, Gfi ha consolidado su Unidad de Salud. Esta unidad dirigida por Alicia Abad está conformada por un equipo de más de 230 consultores y un volumen de negocio de 11 millones de euros y cuenta con una amplia cartera de clientes de la sanidad pública y privada, a los que provee de soluciones propias y a medida. Entre sus soluciones cabe destacar GESCOT®, Savac Pharma y Savac HIS/mira.

- **El Gobierno de Castilla-La Mancha** ha completado la implantación del programa de teledermatología (DERCAM) en un total de 113 centros de salud de la Comunidad Autónoma, además de estar disponible actualmente en el conjunto de la red hospitalaria regional, generando ya 12.867 consultas desde su inicio en 2007. Este procedimiento permite hacer un diagnóstico dermatológico a distancia, sin que existan diferencias en la fiabilidad diagnóstica al compararse con las consultas convencionales de presencia.

- **SESCAM:** El Hospital Nacional de Parapléjicos ha organizado el lunes, 3 de abril, el seminario ´Tecnologías innovadoras en discapacidad, nuevos métodos de comunicación , Acto dirigido a profesionales que trabajan en este ámbito y en el que dieron a conocer un sistema alternativo de comunicación que se maneja a través de la tecnología Irisbond, la cual permite controlar el ´softwaré de un ordenador a través de la mirada.

- **El Área del medicamento del Servicio Cátalan de Salut CATSALUD** modificará su estructura a partir de abril. Armonización farmacoterapéutica, prestaciones farmaceúticas y acceso al medicamento y acción territorial del medicamento serán los tres grandes ámbitos que sufrirán cambios para dar continuidad a la estructura actual existente y reforzar la proximidad en el territorio.

XXIV Jornadas Nacionales de Innovación y Salud en Andalucía

¿Quo Vadis, Sistemas de Soporte a la Decisión Clínica: ELIGES o ELIGEN?

Organiza

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

Con la colaboración de

JUNTA DE ANDALUCIA
CONSEJERÍA DE SALUD

MÁLAGA

7, 8 y 9 de junio 2017

HOTEL MELIÁ SOL PRÍNCIPE
Paseo Colorado, 26
29620 Torremolinos

COLABORADORES TECNOLÓGICOS

Atos · connectis · FUJITSU · gmv · Ibermática · indra · INFORMÁTICA El Corte Inglés · intel · InterSystems · SIEMENS Healthineers · PHILIPS · T-Systems