NÚMERO
134

I+S

ABRIL
2019

REVISTA DE LA SOCIEDAD ESPAÑOLA DE INFORMÁTICA Y SALUD

ESPECIAL

UN NUEVO MARCO EN LA CIBERSEGURIDAD Y LA 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** UN NUEVO MARCO EN LA CIBERSEGURIDAD Y LA PROTECCIÓN DE DATOS

7 Principales Novedades de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales desde la Perspectiva Sanitaria

12 Gestión de Identidades del Ib-Salut Caso práctico: Solicitud de Certificados Electrónicos Centralizados a través del Portal de Autoservicio

17 La Ciberseguridad, un Remedio Sanitario

21 Experiencia en la Implantación de un Sistema de Gestión de Seguridad de la Información basado en ISO 27000: Sistema Sanitario Público de Galicia

24 Evaluación de Impacto en la Protección de Datos. Paralelismos

27 Situación del Delegado de Protección Datos en el SNS

32 La Salud del Negocio en Situaciones de Crisis

34 Implantando una Solución NAC (Network Access Control) en una Organización Sanitaria

37 Retos a la Hora de Proteger la Ciberseguridad de los Hospitales Conectados

41 **ACTIVIDADES DE LA SEIS**

41 Foro para la Gobernanza de las TIC en Salud

48 XVI Foro de Seguridad y Protección de Datos de Salud

57 XXIV Premios Nacionales de la Informática de la Salud 2018

61 XXVI Jornadas Nacionales de Innovación y Salud en Andalucía

64 VIII Reunión de la Plataforma Tecnológica para la Innovación en Salud

64 **FOROS Y SECTORES**

66 Foro de Protección de Datos en Salud

67 Foro de Interoperabilidad

68 Foro de Gobernanza

70 Foro de Salud Conectada

71 Sector de Informática Médica

72 Sector de Enfermería

73 Sector de Farmacia

74 **AGENDA**

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

I.C.P. INGENIEROS, SA

COLEGIO OFICIAL DE FARMACÉUTICOS DE CÁCERES

COLEGIO OFICIAL DE FARMACÉUTIOS DE BADAJOZ

IDCSALUD

MUTUA UNIVERSAL

MUTUAL CYCLOPS-CENTRE DOCUMENTACIÓ

EMERGRAF, SL - CREACIONES GRÁFICAS

HOSPITAL CLINIC. SISTEMAS DE INFORMACIÓN

COLABORADORES TECNOLÓGICOS

Atos

FUJITSU

HUAWEI

Ibermática

INFORMÁTICA El Corte Inglés

Microsoft

minsait An Indra company

PHILIPS

SIEMENS Healthineers

La Seguridad y la Protección de Datos de Salud

Dedicamos este número a un tema crucial para nuestro sector: la seguridad y la protección de datos de salud. Este tema, si bien siempre ha tenido un tratamiento específico por parte de la Sociedad Española de Informática de la Salud, consideramos que es de total actualidad revisar la situación generada ante la entrada en vigor en mayo de 2018 del Reglamento Europeo y de la nueva Ley de Protección de Datos Personales y Garantía de los Derechos Digitales, de diciembre de 2018.

Nos encontramos en el sector Salud con un nuevo escenario normativo, al que tenemos que adaptarnos, pero que resuelve o clarifica, en gran medida, muchos problemas que nos estábamos encontrando, esencialmente para la utilización de datos de salud y para otros fines para los que fueron obtenidos específicamente.

Por otra parte, surge la figura del Delegado de Protección de Datos, para cuya cobertura o designación, se están produciendo diferentes soluciones organizativas según la CC AA en la que se trate.

Desde la SEIS y a través de su Foro de Seguridad y Protección de Datos, en concreto con el Comité de Seguridad de la Información de Salud, se están analizando las repercusiones de esta nueva normativa, tanto desde el punto de vista de las organizaciones, como de los profesionales sanitarios y de los pacientes. Así mismo, se están realizando propuestas al sector, con el fin de solucionar de la forma más homogénea posible la toma de medidas, tanto tecnológicas como organizativas, para garantizar el cumplimiento de la nueva ley y, a su vez, facilitar el trabajo de las organizaciones sanitarias, los profesionales sanitarios e investigadores de nuestro sector.

La permanente colaboración de la Agencia Española de Protección de Datos para facilitar soluciones a los problemas que vamos detectando ha sido vital para que, lejos de encontrarnos en una situación de mayor dificultad, se vayan resolviendo muchos de los problemas que habían surgido.

También hay que destacar el importante papel que está realizando el Comité Técnico de Seguridad de la Información de Salud, como canal de comunicación, de compartición de experiencias y realización de propuestas al Sistema Nacional de Salud, provenientes de los responsables de seguridad y protección de datos de sus organizaciones.

Un nuevo marco en la **Ciberseguridad y la Protección de Datos**

Juan Díaz
Coordinador del Especial

LAS ORGANIZACIONES SANITARIAS SE ENFRENTA ANTE NUEVOS RETOS, CAMBIOS ORGANIZATIVOS Y FUNCIONALES QUE AFECTAN A LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL Y LA SEGURIDAD DE LA INFORMACIÓN SANITARIA.



La consolidación del reglamento Europeo de Protección de Datos, la transposición de la directiva Nis, las obligaciones que afectan a las administraciones públicas en el marco del Esquema Nacional de Seguridad y el Plan Nacional de Infraestructuras Críticas ente otras normativas nos afectan en el día a día de la Asistencia Sanitaria.

Recogemos diferentes artículos de análisis de situación y estrategias de implantación del Reglamento General de Protección de Datos, así aspectos de implantación de medidas de seguridad, estándares y análisis de situación de la infraestructuras y equipamiento electromédico.

Igualmente recogemos la visión más avanzada de los proveedores de soluciones tecnologías que ayudan a mejorar las medidas de seguridad y privacidad de las organizaciones sanitarias.

Esperamos que sean de interés ya que recogen algunas iniciativas desde las diferentes Comunidades Autónomas que abordan medidas de protección de la información para mejorar la confianza en nuestras organizaciones sanitarias.

Principales Novedades de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales desde la Perspectiva Sanitaria

Vicente Lomas Hernández.
Jefe de Servicio de Coordinación Jurídica. Responsable de Seguridad. Servicio de Salud de Castilla-La Mancha. (Sescam)

LA LEY ORGÁNICA 3/2018 DE 5 DE DICIEMBRE DE PROTECCIÓN DE DATOS PERSONALES Y GARANTÍA DE LOS DERECHOS DIGITALES (EN ADELANTE LOPDGDD), REPRESENTA ENTRE OTRAS MUCHAS COSAS, Y POR LO QUE AL SECTOR SANITARIO SE REFIERE, LA OPORTUNIDAD PERDIDA DE HABER CONSEGUIDO PARA LOS DATOS SANITARIOS LA TAN DESEADA COMO NECESARIA REGULACIÓN LEGAL PROPIA Y ESPECÍFICA. EN EFECTO, COMO ES SABIDO LA LOPDGDD OBJETO DE COMENTARIO SIGUE LA SENDA DE LA DEROGADA LOPD Y PROYECTA SU ÁMBITO DE APLICACIÓN SOBRE EL CONJUNTO DE LOS DATOS PERSONALES, SI BIEN CON ALGUNAS REFERENCIAS AISLADAS A SANIDAD EN SU DISPOSICIÓN ADICIONAL DECIMOSÉPTIMA Y LA DISPOSICIÓN FINAL NOVENA, QUE INEVITABLEMENTE HAY QUE COMPLETAR CON LA LECTURA DEL REGLAMENTO UE 2016/679 DE 27 DE ABRIL.

Un buen ejemplo del carácter complementario/subsidiario de la Ley respecto del Reglamento de la UE se advierte, por ejemplo, en la ausencia de una definición legal de *"dato sanitario"* que, en cambio, sí nos lo proporciona la referida disposición comunitaria en su artículo 4, distinguiendo entre: a) datos genéticos, b) datos biométricos, y c) datos relativos a la salud.

No obstante el artículo 12.5 de la LOPDGDD parece contemplar la primacía de los regímenes especiales que, en materia de protección de datos de carácter personal, pueden establecerse por otras leyes, como bien podría ser el caso de las leyes sanitarias enumeradas en el apartado primero de la disposición adicional decimoséptima. En concreto, dicho precepto legal establece *"cuando las leyes aplicables a determinados tratamientos establezcan un régimen especial que afecte al ejercicio de los derechos previstos en el capítulo tercero del Reglamento 2016/ 679, se estará a lo dispuesto en aquellas"*.

Veamos muy brevemente desde una perspectiva sanitaria los aspectos más relevantes del marco normativo actual en materia de protección de datos, destacando todos aquellos en los que puedan existir diferencias con la legislación sectorial, o bien adquieran especial interés para el ámbito sanitario.

I. TRATAMIENTO DE DATOS DE PERSONAS FALLECIDAS

La LOPDGDD, al igual que el Reglamento comunitario, excluye de su ámbito de aplicación el tratamiento de datos personales de personas fallecidas (art. 2.2.b). Sin embargo el legislador nacional, en su artículo 3, ha querido regular el acceso a los datos personales del fallecido por parte de aquellas personas vinculadas a éste por razones familiares o de hecho, así como sus herederos.

Desde el punto de vista de la legislación sanitaria, el art. 18.4 de la Ley 41/2002 de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica, distingue en cuanto al régimen jurídico de acceso a la historia clínica del paciente fallecido según si la petición de acceso la protagoniza un familiar, o si ésta la formula un tercero.

En el primer caso hay que entender que las personas vinculadas al paciente por razones familiares (considerando como tales al cónyuge, ascendientes y descendientes y hermanos si nos ajustamos a lo dispuesto en el art. 4 de la LO 1/82) o de hecho, pueden acceder a la historia clínica salvo que el fallecido se hubiera opuesto y así se acredite, y en todo caso siendo de aplicación las mismas limitaciones que regirían para el propio paciente si estuviese vivo, a saber: a) la intimidad de terceras personas, b) anotaciones subjetivas, y c) el conocido "*privilegio terapéutico*" de los profesionales sanitarios.

II. LOS DEBERES DE CONFIDENCIALIDAD Y SECRETO PROFESIONAL

La LOPDGDD establece que el tratamiento de los datos personales, incluidos los datos de carácter sanitario, están sometidos al deber de confidencialidad por parte tanto de los responsables y encargados del tratamiento, como de todas las personas que intervengan en cualquier fase de éste (artículo 5.1). Estamos ante un deber que se complementa, a su vez, con los deberes de secreto profesional a los que alude el apartado segundo del referido precepto legal, y que deberán interpretarse de conformidad con su normativa vigente.

> ***En el ámbito sanitario la relevancia del deber de secreto profesional resulta más que evidente; pensemos por un momento en las obligaciones deontológicas que en este sentido deben asumir todos los profesionales sanitarios, o en las graves responsabilidades penales a las que se enfrenta***

En el ámbito sanitario la relevancia del deber de secreto profesional resulta más que evidente; pensemos por un momento en las obligaciones deontológicas que en este sentido deben asumir todos los profesionales sanitarios, o en las graves responsabilidades penales a las que se enfrenta este colectivo por incurrir en la comisión de un delito de descubrimiento y revelación de secreto tipificado en los artículos 197 y siguientes del Código Penal, en los supuestos de accesos indebidos a la historia clínica, o revelación de secreto a terceros.

Precisamente el Reglamento, en su artículo 9.2. h), cuando alude al tratamiento de datos para fines de medicina preventiva o laboral, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario, o gestión de sistemas y servicios de asistencia sanitaria, establece claramente la obligación de que dicho tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional o bajo su responsabilidad, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros.

III. DELIMITACIÓN DE BASES JURÍDICAS PARA EL TRATAMIENTO DE DATOS DE SALUD POR LAS ADMINISTRACIONES PÚBLICAS

Por lo que respecta a la delimitación de las bases jurídicas necesarias para legitimar el tratamiento de los datos sanitarios, cabría destacar la regulación recogida en los artículos 8 y 9 de la LOPDGDD. El primero de ellos por cuánto viene a perfilar con mayor claridad el alcance de las bases jurídicas recogidas en el artículo 6.1 del Reglamento con proyección en el ámbito de las Administraciones Públicas, en concreto: a) el tratamiento de datos para el cumplimiento de una misión realizada en interés público, y b) el

ejercicio de poderes públicos conferidos al responsable del tratamiento.

En ambos casos la LOPDGDD deja bien claro que podremos estar ante un tratamiento de datos fundado en cualquiera de los supuestos anteriormente citados, siempre que "*derive de una competencia atribuida por una norma con rango de ley*". Precisamente esta misma exigencia también se predica respecto de los tratamientos de datos en los supuestos previstos en las letras g), h) e i) del artículo 9.2 del Reglamento, que de forma resumida se identificarían con los supuestos de tratamientos de datos por razones de salud. En este sentido el artículo 9.2 -pero ahora de la LOPDGDD -, no deja lugar a dudas cuando establece, respecto del tratamiento de este tipo de datos, que deberán estar amparados en una norma con rango de ley.

En definitiva, la reserva de ley para el tratamiento legítimo de datos personales de carácter sanitario resulta indiscutible, lo que a su vez comporta que la vigencia de buena parte de las abundantes previsiones reglamentarias existentes en esta materia queden en entredicho.

IV. CONSENTIMIENTO DE LOS MENORES DE EDAD

Otro aspecto especialmente delicado en el ámbito sanitario, y sobre el que se pronuncia la LOPDGDD objeto de comentario, es el relativo al tratamiento de datos personales de los menores de edad. La Ley en su artículo 7 fija en 14 años la mayoría de edad en relación con la protección de datos de carácter personal, de modo que el tratamiento de los datos personales de un menor de edad únicamente podrá fundarse en su consentimiento cuando sea mayor de 14 años. A su vez el artículo 12.6 del referido texto legal, establece que "*en cualquier caso los titulares de la patria potestad podrán ejercitar en nombre y representación de los menores de 14 años, los derechos de acceso, rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles*".

La pregunta obligada que habría que plantearse sería si, a la luz de la actual regulación en materia de protección de datos de carácter personal, un paciente menor de edad con 14 o más años cumplidos, podría oponerse a que sus padres puedan acceder al contenido de su historia clínica sin su consentimiento, teniendo en cuenta la existencia en la legislación sanitaria de la figura conocida como "menor maduro". Sobre este respecto, el Informe 339/2015 de la Agencia Española de Protección de Datos, sobre acceso a la historia clínica de los menores entre 16 y 18 años, concluía afirmando que si bien el menor de edad mayor de catorce años podrá, en general, ejercitar por sí solo el derecho de acceso a la historia clínica, en cambio no podría oponerse a que sus padres, titulares de la patria potestad, pueden acceder igualmente a los datos del menor de edad para el cumplimiento de las obligaciones previstas en el Código Civil. Una afirmación discutible.

V. EJERCICIO DE DERECHOS

La LOPDGDD establece que todas las actuaciones que se hayan de llevar a cabo por el responsable del tratamiento para atender las solicitudes de ejercicio de derechos serán gratuitas, con las salvedades previstas en los apartados 3 y 4 del artículo 13 de la Ley, a saber: a) peticiones repetitivas reiteradas en el plazo de 6 meses sin causa legítima para ello, y b) elección por el interesado de un medio distinto al ofrecido que suponga un coste desproporcionado.

La traslación al ámbito sanitario de esta previsión legal, supondrá la imposibilidad de exigir al paciente contraprestación económica alguna por la obtención de copia de su historia clínica, más allá de las excepciones a las que me he referido anteriormente.

Por lo que respecta a los restantes derechos, el Reglamento establece en relación con el "*derecho de supresión*", que éste no podrá ser ejercido cuando el tratamiento sea necesario, entre otros casos, por razones de interés público en el ámbito de la salud. Queda clara, por tanto, la inexistencia del derecho de cancelación de los datos sanitarios.

Estrechamente relacionado con el derecho de supresión, el artículo 21 del Reglamento regula el "*derecho de oposición*" al tratamiento de da-

tos personales sobre la base del interés público o el ejercicio de potestades públicas, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses los derechos y las libertades del interesado. Ahora bien, en este otro caso no queda tan claro que los mismos límites que impiden el ejercicio del derecho de cancelación, puedan regir respecto del derecho de oposición al tratamiento de datos sanitarios.

Particularmente confuso resulta el "*derecho a la portabilidad*" (art. 20) de los datos en el ámbito sanitario. Hay que tener en cuenta que conforme al Reglamento comunitario este derecho está ligado a la concurrencia de alguno de los siguientes requisitos: a) que el tratamiento esté basado en el consentimiento o en un contrato, y b) que el tratamiento se efectúe por medios automatizados. Téngase en cuenta que el tratamiento de datos sanitarios en el ámbito de la sanidad pública, no pivota sobre la base jurídica del consentimiento del interesado, sino que se apoyaría sobre el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, bases jurídicas que como ya ha quedado expuesto, hunden sus raíces en la Ley.

VI. RELACIONES ENTRE EL RESPONSABLE DEL TRATAMIENTO Y EL ENCARGADO DEL TRATAMIENTO

A diferencia de la derogada Ley Orgánica del año 1999, la LOPDGDD no aborda en profundidad las relaciones entre el responsable y el encargado del tratamiento, por lo que habrá que acudir nuevamente al Reglamento comunitario para conocer los términos en los que se han de articular las comunicaciones de datos entre ambas figuras. Este constituye, sin duda, un aspecto especialmente importante debido a que en el ámbito sanitario suele ser relativamente frecuente el recurso a la figura de la "*externalización*" para la prestación de servicios sanitarios, ya sea a través de la formalización de contratos en el marco de la Ley de Contratos del Sector Público, o bien a través de figuras afines como los convenios singulares de vinculación. En todo caso la disposición adicional segunda de la LOPDGDD, establece que "*En los casos en los que un tercero preste un servicio en régimen de concesión, encomienda de gestión o contrato, las medidas de seguridad se corresponderán con las de la Administración pública de origen y se ajustarán al Esquema Nacional de Seguridad*".

VII. RESPONSABILIDAD PROACTIVA Y LA CREACIÓN DE LA FIGURA DEL DELEGADO DE PROTECCIÓN DE DATOS (DPD)

La LOPDGDD incorpora dos nuevas obligaciones que deben asumir tanto los responsables como los encargados del tratamiento también en el ámbito sanitario:

- La adopción de medidas técnicas y organizativas apropiadas para garantizar y acreditar que el tratamiento de los datos personales se efectúa conforme al Reglamento comunitario y la Ley Orgánica.

Estamos ante una obligación de gran importancia en el entorno sanitario por cuánto uno de los supuestos que mayores riesgos presenta para el tratamiento de la información, son todas aquellas situaciones de pérdida de confidencialidad de datos sujetos al secreto profesional, supuestos en los que se lleve a cabo el tratamiento de datos de grupos de afectados en situación de especial vulnerabilidad ,y en particular de menores de edad y personas con discapacidad, y cuando se produzca un tratamiento masivo que implique a un gran número de afectados o conlleve la recogida de una gran cantidad de datos personales. (art. 28.2 de la LOPDGDD).

- La designación de un DPD en los supuestos previstos en el artículo 37.1.

La LOPDGDD establece que los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes, deben designar un delegado de protección de datos. Se trata, por tanto, de una obligación clara y contundente de modo que resultaría jurídicamente cuestionable la implantación de un único delegado de protección de datos para todos los sectores de actividad administrativa de una Comunidad Autónoma, incluido el sector sanitario, como vienen haciendo algunas Administraciones Públicas.

En todo caso parece innegable que: a) la singulari-

dad de los datos de salud, b) la complejidad organizativa del servicio de salud, y c) el volumen de información que tratan las Instituciones Sanitarias, son argumentos más que suficientes para apostar por la existencia de un DPD propio para sanidad.

VIII. TRATAMIENTOS DE LOS DATOS DE SALUD

Finalizar este brevísimo repaso de la Ley con la regulación que del tratamiento de este tipo de datos se hace en la extensa disposición adicional decimoséptima en relación, a su vez, con la disposición final novena del citado texto legal.

El apartado 2 de la referida disposición adicional analiza de forma monográfica el tratamiento de estos datos con fines de investigación en salud, estableciendo como regla general, que el tratamiento de datos con estas finalidades exige que el interesado haya otorgado su consentimiento. En todo caso, para llevar a cabo un tratamiento con fines de investigación en salud pública, el legislador obliga a realizar una evaluación de impacto que determine los riesgos derivados del tratamiento, someter la investigación científica a normas de calidad, y adoptar medidas dirigidas a garantizar que los investigadores no accedan a datos de identificación.

A partir de este escenario, la citada disposición adicional distingue entre:

a. Tratamiento de datos sanitarios por autoridades sanitarias con competencias en vigilancia de la salud pública.
b. Reutilización de datos personales con fines de investigación.
c. Seudonimización de datos personales con fines de investigación en salud.

Respecto a la disposición final novena ésta modifica el apartado 3 del artículo 16 de la Ley 41/2002 de 14 de noviembre. Conforme a esta nueva redacción, el acceso a la historia clínica con fines judiciales, epidemiológicos, de salud pública, de investigación, o de docencia, obliga a preservar los datos de identificación personal del paciente separados de los datos de carácter clínico asistencial, de manera que, como regla general, queda asegurado el anonimato salvo que el propio paciente haya dado su consentimiento para no separarlos.

> ***La LOPDGDD establece que los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes, deben designar un delegado de protección de datos***

Sin embargo, tras establecer la importancia de la disociación, el párrafo segundo de este mismo apartado añade que se exceptúan los supuestos de investigación previstos en el apartado 2 de la disposición adicional decimoséptima de la Ley Orgánica. Esta excepción resulta difícilmente comprensible por cuánto el apartado 2 de la referida disposición adicional incluye un supuesto específico para la seudonimización de datos personales que vayan a ser tratados con fines de investigación en salud. Así pues la Ley parece incurrir en cierta contradicción.

IX. CONCLUSIÓN

Se ha malogrado una buena ocasión para haber regulado de forma independiente la protección de los datos sanitarios tal y como ya propusiera, entre otros muchos, la Sociedad Española de Salud Pública y Administración Sanitaria (SESPAS). La citada sociedad científica en su informe elaborado a tal efecto, afirmaba "*es ineludible la necesidad de disponer de una ley específica sobre protección de datos personales relativos a la salud; ley que, por ende, se enmarcaría en la normativa del sector sanitario. Hoy es opinión generalizada que lo más operativo es elaborar una ley estatal para la protección de los datos personales de salud, que complemente el RGPD y sustituya a las disposiciones contenidas en la todavía vigente Ley Orgánica de Protección de Datos, en la Ley Básica de Autonomía del Paciente, y en el resto de legislación sanitaria estatal*".

Tan solo nos queda confiar en que los gestores y las autoridades de protección de datos sean conscientes de la singularidad que reviste el dato sanitario, y sepan obrar en consecuencia.

Gestión de Identidades del Ib-Salut **Caso práctico:** Solicitud de certificados electrónicos centralizados a través del portal de autoservicio

Miguel Ángel Benito Tovar[1]; Ignacio Amoeiro Bosch[2]; Rubén Fernández Nicolau[3]
1. Jefe de Servicio de Seguridad de la Información del Servicio de Salud de las Illes Balears
2. Team Leader en SIA
3. Senior Security Consultant en SIA

PALABRAS CLAVE

Gestión de Identidades, Firma centralizada, Esquema Nacional de Seguridad, Seguridad de la información.

INTRODUCCIÓN

El Servicio de Salud de las Illes Balears, en lo sucesivo Servicio de Salud, cuenta con más de 15.500 profesionales y más de 1.500 colabores externos que diariamente acceden a sistemas de información los cuales en su mayoría contienen datos de salud y por ende sobre los que hay que garantizar el mayor nivel de seguridad y privacidad atendiendo a lo establecido por el Reglamento 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 así como por la reciente Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Con el fin de garantizar la correcta privacidad de los datos de los pacientes del Servicio de Salud y garantizar la seguridad de los sistemas de información, se hace necesaria la implantación de medidas de seguridad organizativas, operacionales y técnicas.

En este sentido, entre las medidas operacionales establecidas en el Anexo II del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad se enmarcan, entre otras, las relativas al control de accesos e identificación de los profesionales que acceden a los sistemas de información.

Es por ello, que el Servicio de Salud de las Illes Balears cuenta desde el año 2007 con un sistema de gestión de identidades y accesos el cual se ha renovado completamente en el año 2018 coincidiendo también con la puesta en marcha de la emisión de certificados electrónicos centralizados de empleado público.

Asimismo, la necesidad de garantizar la correcta gestión de la solicitud, emisión, activación y revocación de los certificados electrónicos centralizados en un entorno tan complejo como es el sanitario y con la especial singularidad de la insularidad en el caso de las Illes Balears, hace necesaria la implantación de procedimientos y circuitos que faciliten las tareas de todos los actores involucrados en las distintas fases del ciclo de vida de un certificado electrónico claro está cumpliendo con la legislación vigente en materia de firma electrónica entre la que cabe destacar la Ley 59/2003, de 19 de diciembre, de firma electrónica así como por el Reglamento (UE) n ° 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 , relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

Para facilitar la citada gestión de los certificados, por parte de la Subdirección de Tecnología y Sistemas de Información, en lo sucesivo STSI, se

procedió a integrar la solicitud, emisión, activación y revocación de los certificados electrónicos con el sistema de gestión de identidades del Organismo quedando por lo tanto enlazado el ciclo de vida de la identidad del certificado con la propia del profesional.

OBJETIVOS DEL PROYECTO DE GESTIÓN DE IDENTIDADES

Dentro de la estrategia definida por el Servicio de Salud y la STSI para la implantación y evolución del proyecto de gestión de identidades se encuentran enmarcados los siguientes objetivos:

- Dotar a los profesionales del Servicio de Salud de una única credencial para el acceso a todos sistemas de información a los que necesitan tener acceso según su rol en el Organismo.
- Garantizar que los profesionales puedan acceder a los sistemas de información desde el mismo momento de su contratación.
- Revocar automáticamente los permisos de accesos a los sistemas de cuando éstos abandonan el organismo o cuando desaparece la necesidad que motivó el otorgamiento de los permisos.
- Proporcionar a los profesionales de una herramienta sencilla e intuitiva (portal de auto servicio) a través de la cual puedan solicitar el acceso a sistemas que no tengan concedidos por reglas de negocio según su perfil.
- Disponer de un mecanismo sencillo y rápido para la generación de una nueva contraseña en caso de olvido o bloqueo.
- Incluir en el ciclo de vida de identidad de los profesionales la gestión del certificado electrónico centralizado.
- Disponer de la trazabilidad de las autorizaciones de accesos a los sistemas de información.
- Auditar los permisos de accesos a los sistemas de información.
- Simplificar las labores de los departamentos de recursos humanos, informática y del Centro de Atención al Usuario (CAU).
- Generación de informes y cuadros de mando de seguimiento para la Dirección.
- Dar cumplimiento a los requerimientos de seguridad establecidos por el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad y el Reglamento General de Protección de Datos (RGPD).

MEDIOS DISPONIBLES

Para la implantación, administración y evolución del sistema de gestión de identidades, el Servicio de Salud cuenta con:

- Una oficina técnica de gestión de identidades formada por:
    - Un responsable del proyecto por parte del Servicio de Salud.
    - 2 profesionales externos (Grupo SIA) especialistas en materia de gestión de identidades y seguridad de la información.
- Pool de especialistas en remoto para la ejecución de desarrollos de seguridad.
- Licencias corporativas de la solución Oracle Identity Governance Suite 11g.
- Curso on-line sobre la gestión de identidades para los operadores y profesionales del Ib-Salut
- Curso on-line para los departamentos de recursos humanos sobre la gestión de las solicitudes de los certificados electrónicos centralizados
- Curso on-line para los profesionales sobre la solicitud y activación del certificado electrónico centralizado



FIGURA 1. Curso on-line para operadores y usuarios

SOLUCIÓN TECNOLÓGICA SELECCIONADA

La solución seleccionada para el proyecto de gestión de identidades del Servicio de Salud ha sido Oracle Identity Governance. Entre las principales características por las que se optó por la citada solución caben destacar:

- Servicio de autoservicio y solicitud de acceso.
- Gestión avanzada del ciclo de vida de roles.
- Certificación de identidad simplificada.
- Gestión de cuentas privilegiadas.
- Monitoreo e informes de auditoría.

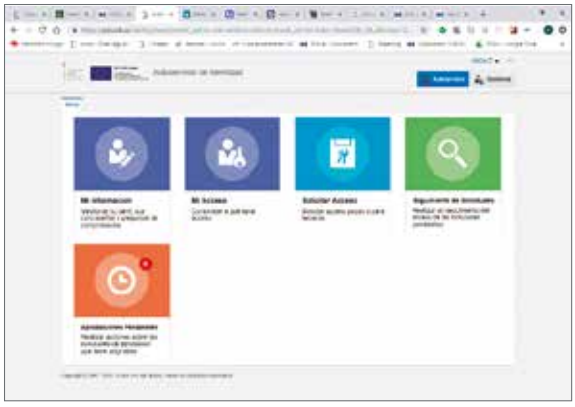


Figura 2. Pantalla principal del usuario



Figura 3. Pantalla principal de operadores

PORTAL AUTO SERVICIO PARA EL PROFESIONAL

Tal como se expuso anteriormente, uno de los principales objetivos del proyecto de gestión de identidades es el referente a proporcionar a los profesionales una herramienta sencilla e intuitiva.

A tal efecto, el Servicio de Salud ha puesto en marcha el Portal de Autoservicio mediante el cual los profesionales tienen la posibilidad de solicitar de una manera sencilla e intuitiva el acceso a sistemas de información que no tengan concedidos por reglas de negocio según su perfil. Entre los principales objetivos del Portal de Autoservicio se enmarcan los siguientes:

- Dotar a los profesionales de un único portal/procedimiento para la solicitud de permisos.
- Evitar desplazamientos de los profesionales.
- Simplificar la tarea de aprobación de las solicitudes por parte del responsable del profesional y de los responsables de los sistemas de Información.
- Asignación automática de los permisos tras la aprobación de los responsables.
- Disponer de trazabilidad de todas las autorizaciones de permisos de acceso

En aras de facilitar la búsqueda de los sistemas de información o recursos sobre los cuales se quiere solicitar acceso, además del buscador propio del Portal Autoservicio, se ha realizado una clasificación de todos los sistemas/recursos solicitables atendiendo a la siguiente tipología:

- Accesos Remotos (Citrix y VPN).
- Aplicaciones sanitarias.
- Aplicaciones de gestión.
- Unidades de red.
- Otros recursos.
- Certificado Electrónico Centralizado.

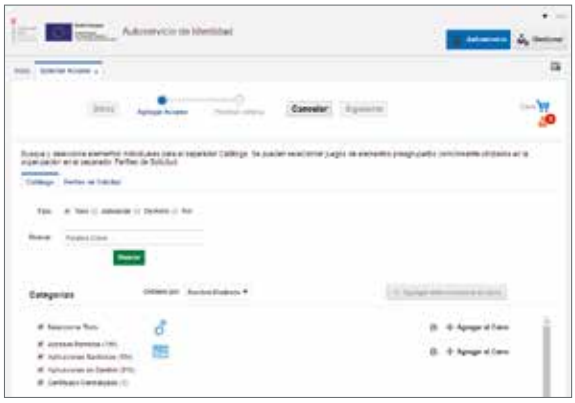


Figura 4. Portal Autoservicio



Figura 5. Ejemplo aplicaciones solicitables

INTEGRACIÓN DE LA GESTIÓN DE IDENTIDADES CON EL SERVICIO DE FIRMA CENTRALIZADA

Con motivo de la puesta en marcha del servicio de firma centralizada, el pasado mes de noviembre, se procedió a llevar a cabo la integración de la solución de gestión de identidades con la Autoridad de Certificación de la empresa SIA.

El objetivo principal de esta integración es incluir el recurso de certificado electrónico centralizado se incluya dentro del ciclo de vida de la identidad del profesional

Es por lo anterior, que a través de esta integración se gestiona la:

- Solicitud del certificado por parte del profesional desde el portal Autoservicio.
- Aprobación/Rechazo de la solicitud por parte del área de RRHH desde la propia solución de gestión de identidades.
- Revocación automática del certificado centralizado cuando el profesional causa baja en el Servicio de Salud o se modifica alguno de los datos mediante los cuales se generó el certificado (DNI, nombre, apellidos y cargo).

Entre los **beneficios** que ha supuesto para el Servicio de Salud esta integración caben destacar:

- Disminución del tiempo necesario para la emisión de los certificados. En la actualidad el tiempo medio dedicado en total para la solicitud, aprobación y activación del certificado centralizado es de 5 minutos en contra de los más de 25 minutos (sin contar desplazamientos) que suponía la emisión de certificados en tarjeta.
- Los profesionales pueden solicitar el certificado centralizado desde su propio puesto de trabajo evitando de esta manera los desplazamientos.
- Se procede a la revocación de los certificados de empleado público de manera automática una vez que los profesionales causan bajan en el Servicio de Salud.
- Se dispone en todo momento de la trazabilidad de los certificados emitidos y revocados.

RESULTADOS

Desde un punto de vista cualitativo, como consecuencia de la implantación del sistema de gestión de identidades, en el Servicio de Salud:

- Se gestionan las identidades y contraseñas de más de 15.500 profesionales y más de 1.500 colabores externos repartidos entre 10 centros de atención especializada y 159 centros de atención Primaria.
- Más de 14.000 profesionales cuentan con las preguntas/respuestas de desafío introducidas como método para la recuperación de las contraseñas.
- Se ha integrado el sistema de gestión de identidades con el sistema IVR (Respuesta de Voz Interactiva) corporativo para la recuperación de la contraseña a través de SMS por parte de aquellos profesionales que tengan informado el número de su teléfono móvil en su identidad (en la actualidad 6.750 profesionales).
- Se encuentra integrado con más de 50 sistemas entre los que cabe destacar el sistema de recursos humanos, la emisión de certificados electrónicos, el sistema de historia de salud corporativa, el sistema de historia clínica del hospital Son Espases así como el sistema de laboratorio corporativo.
- Se gestiona la sincronización de más de 400 cambios de contraseñas diarios.



Figura 6. Principales logros

- Diariamente se gestionan más de 150 altas, bajas y modificaciones de identidades de usuarios.
- Desde el mes de octubre, fecha en la que se puso en marcha el nuevo sistema de gestión de identidades, se han gestionado más de 800 solicitudes de acceso a aplicaciones a través del portal de autoservicio del profesional y alrededor de 2.000 solicitudes de certificados electrónicos centralizados de empleado público.
- Se ha disminuido en 20 minutos el proceso de registro y emisión de los certificados de empleado público.
- A través del siguiente gráfico se resaltan igualmente los principales logros obtenidos desde un punto de vista cualitativo:

CONCLUSIONES

Debido al elevado número de profesionales que forman parte de un Servicio de Salud, el alto nivel de rotación de los mismos así como el elevado número de sistemas de información a los que los profesionales necesita tener acceso, hace necesario contar con soluciones tecnológicas que ayuden a automatizar las altas y bajas de los permisos de accesos a los sistemas de información a los cuales necesitan tener acceso los profesionales desde el momento de su incorporación con el fin de garantizar la correcta atención de los pacientes que acuden a los centros del Servicio de Salud.

Entre las soluciones tecnológicas sin duda los sistemas de gestión de identidades vienen a satisfacer las necesidades anteriormente mencionadas así como a los imperativos legales existentes en materia de seguridad

REFERENCIAS

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

[2] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. https://www.boe.es/buscar/doc.php?id=-BOE-A-2018-16673

[3] 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) https://www.boe.es/doue/2016/119/L00001-00088.pdf

[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] Oracle Identity Governance Suite. https://www.oracle.com/technetwork/middleware/id-mgmt/overview/11gr2ps2-idg-datasheet-2293567.pdf.

La Ciberseguridad, un Remedio Sanitario

Juan Díaz García
Responsable de la Unidad de Gestión de Riesgos Digitales del Servicio Andaluz de Salud.

EL MODELO SANITARIO DE NUESTRA SOCIEDAD SE BASA EN UN MARCO DE "SALUD INTEGRAL" CON UNA HISTORIA CLÍNICA COMPARTIDA POR LOS DIFERENTES ACTORES SANITARIOS Y ACCESIBLE POR EL CIUDADANO. ACTUALMENTE SE DEMANDA UN ACCESO CONTINUO A LA PRESTACIÓN / ASISTENCIA SANITARIA INCLUSO DESDE EL MÓVIL MEDIANTE APP SANITARIAS, BUSCANDO UNA ATENCIÓN EFICAZ E INMEDIATA QUE REQUIERE UN ALTO NIVEL DE INTEGRACIÓN DE SISTEMAS DE INFORMACIÓN MUY COMPLEJOS.



Esto implica que los sistemas y tecnologías necesarios en la asistencia sanitaria estén conectados, pero con un riesgo inherente de la propia conectividad que podría traicionar la seguridad de los pacientes, sometiéndolos a riesgos innecesarios y obligándolos a pagar costes personales inaceptables.

Según un informe publicado en el Journal of the American Medical Association, los incidentes de seguridad en la atención médica han aumentado significativamente desde 2010, más del 80 por ciento han sufrido ataques de secuestro de información o han tenido brechas de fuga de información.

Debemos velar por asegurar y proteger los sistemas de información de los incidentes de ciberseguridad, ya sean intencionados o no. Los casos reales de robo de identidad, rescate y piratería informática dirigida al sector sanitario demuestran que nuestros datos de atención médica son vulnerables. Los datos pueden utilizarse para fines malintencionados como el fraude, el robo de identidad, las interrupciones en la cadena de suministros, el robo de investigación, la manipulación de existencias o la extorsión, llegando a veces a interrumpir la propia en la atención al paciente.

Existen nuevos riesgos y múltiples circunstancias que facilitan la ocurrencia de ciberataques que pueden ser debidos a las siguientes causas: La mayoría de hospitales y servicio de salud no dispone de personal especializado en seguridad de la información a tiempo completo. Gran parte de los sistemas de información se basan en plataformas antiguas, no están soportadas y sus sistemas operativos son vulnerables. Los sistemas de información están diseñados para dar respuesta a problemas locales con un diseño e implementación poco seguro, lo que impide que responden adecuadamente a modelos integrados e hiperconectados que se demanda. Las vulnerabilidades de los sistemas informáticos afectan directamente a la asistencia sanitaria, bloqueando su funcionamiento o ralentizando hospitales completos. Incapacidad de la tecnología médica de estar actualizada, los equipos y los programas se quedan sin mantenimiento o no pueden actualizarse por falta de compatibilidad con los nuevos sistemas operativos.



> ***La mayoría de hospitales y servicio de salud no dispone de personal especializado en seguridad de la información a tiempo completo. Gran parte de los sistemas de información se basan en plataformas antiguas, no están soportadas y sus sistemas operativos son vulnerables***

Esto ocurre en el sector de la salud, que es complejo e incluye organizaciones de salud muy grandes, hospitales privados, servicios diagnósticos, aseguradoras, instituciones de investigación, desarrolladores de dispositivos médicos y compañías de software sanitario. Estos deben adaptarse continuamente a nuevas demandas sociales, a la limitación de los recursos disponibles para su consecución, un marco normativo complejo y con nuevos requerimientos en la protección de los datos y privacidad. Obligándolos a una mayor responsabilidad para asegurar sus sistemas de información, dispositivos médicos y datos de los pacientes.

Cada vez se requieren nuevas prestaciones sanitarias, servicios más eficientes con costes limitados o menguantes y una política restrictiva en los recursos humanos especializados. Incrementando la demanda y complejidad de los sistemas de información y tecnológicos implicados.

Esto incrementa las situaciones de riesgos y muchas organizaciones sanitarias no pueden permitirse el lujo de retener personal interno de seguridad de la información, encargando los temas de ciberseguridad como secundarios al día a día del personal de las Tecnologías de la Información y Comunicaciones. Estas organizaciones a menudo carecen de la infraestructura necesaria para identificar y rastrear las amenazas, la capacidad de analizar y de actuar sobre esa información. Ya que carecen de experiencia necesaria para hacer

frente a las amenazas actuales y emergentes de la ciberseguridad, siendo posible que estas organizaciones no sepan que han experimentado un ataque hasta mucho después de que éste haya ocurrido.

Nos encontramos frecuentemente con numerosos sistemas de información heredados no soportados y no se pueden reemplazar fácilmente (hardware, software y sistemas operativos) con un gran número de vulnerabilidades y pocas contramedidas modernas. El sector sanitario tendrá que reducir drásticamente el uso de equipamiento y productos heredados, sin mantenimiento, no respaldados y no actualizables, debiendo reducir de manera más eficaz el riesgo en los productos futuros mediante estrategias sólidas de diseño y desarrollo.

Se producen nuevos tipo ataques y vulnerabilidades de los sistemas que produce una creciente superficie de ataque de hoy en día, el cambiante panorama de amenazas, las regulaciones inconstantes y los desafíos sistémicos exigen un enfoque dedicado e innovador para proteger los dispositivos médicos conectados. Los recientes incidentes de ransomware han comprometido a los Sistemas de Información interrumpiendo la atención sanitaria a los pacientes, demostrando así lo vulnerable que son.

Existe una baja percepción de riesgos de los profesionales sanitarios y de los propios proveedores de los sistemas, que creen que las infraestructuras, los dispositivos y los sistemas de información funcionan eficientemente y con escasos riesgos.

Algunos incidentes recientes de gravedad, como los ataques de ransomware y las violaciones de la privacidad a gran escala, han demostrado que esta suposición de seguridad es falsa y ha brindado una oportunidad para aumentar la educación y la concienciación sobre los beneficios de la ciberseguridad en el sector sanitario. Demostrando la importancia de las protecciones en ciberseguridad para la supervivencia del sector sanitario, incluyendo cómo la mitigación de riesgos puede ahorrar dinero y proteger contra el daño a la reputación a largo plazo. Sin que suponga una ralentización del imparable y necesario proceso de digitalización de los hospitales.

> ***Priorizar la ciberseguridad dentro de las organizaciones sanitarias requiere cambios culturales y una mayor comunicación hacia y desde el liderazgo, así como cambios en la forma en que los proveedores desempeñan sus funciones en el entorno clínico***

Priorizar la ciberseguridad dentro de las organizaciones sanitarias requiere cambios culturales y una mayor comunicación hacia y desde el liderazgo, así como cambios en la forma en que los proveedores desempeñan sus funciones en el entorno clínico. La ciberseguridad en los Sistemas Sanitarios es un elemento clave para asegurar la asistencia que requiriere un soporte inmediato y continuo.

A modo de ejemplo describimos unas líneas de mejora recogidas del informe "REPORT ON IMPROVING CYBERSECURITY IN THE HEALTH CARE INDUSTRY, June 2017":

1. Definir y racionalizar el liderazgo, la gobernanza y las expectativas en materia de ciberseguridad del sector sanitario.
2. Aumentar la seguridad y resiliencia de los dispositivos médicos y las tecnologías de la información de la salud.
3. Desarrollar la estrategia desde las direcciones sanitarias para priorizar y garantizar la concienciación sobre la ciberseguridad y las capacidades técnicas de su personal.
4. Aumentar la preparación del sector salud a través de una mayor concienciación y educación en ciberseguridad.
5. Identificar mecanismos para proteger los esfuerzos de investigación y desarrollo y la propiedad intelectual ante los ataques o la difusión indebida.
6. Mejorar el intercambio de información so-

bre amenazas, debilidades y mitigaciones entre las diferentes administraciones y proveedores de servicio y tecnologías.

Todo esto se debe hacer horizontalmente en los sistemas de salud para que llegue a todo tipo de estructuras sanitarias, recogiendo mejoras en los aspectos organizativos, técnicos, humanos y cumplimiento normativo.

Entre los aspectos organizativos uno de los hitos es la publicación de la Política de la Seguridad de la Información que ayude definir roles y responsabilidades, ayude a la alineación interna de las partes interesadas, permita identificar y asumir los riesgos, así como aprobar, controlar los planes de seguridad de la organización y asegurar los recursos necesarios para su correcta ejecución. Permitiendo la consecución de objetivos de la organización, de la privacidad de los pacientes y la seguridad de los datos.



> ***Los recursos humanos son cruciales y deben existir profesionales propios especializados en ciberseguridad que actúen como Responsables de Seguridad de la Información, con una función diferenciada se las Responsables de los Sistemas Informáticos***

Entre los aspectos técnicos, la ciberseguridad requiere la dotación de infraestructura especializada y herramientas para el análisis de eventos y su correlación. Que deben analizar no solo las comunicaciones y redes sino todo tipo de equipamiento presente en las organizaciones sanitarias, incluido el electromédico, sistemas de control industrial y los nuevos dispositivos bajo el paraguas de IOT.

Los recursos humanos son cruciales y deben existir profesionales propios especializados en ciberseguridad que actúen como Responsables de Seguridad de la Información, con una función diferenciada se las Responsables de los Sistemas Informáticos. Ya que la función de seguridad es proponer y verificar que las medidas de seguridad se aplican correctamente por los responsables técnicos (Responsables de Sistemas, Comunicaciones, Bases de Datos, Desarrollo, etc).

2018 ha sido un año con grandes novedades en el cumplimiento normativo, la entrada en vigor del Reglamento General de Protección de Datos, la puesta en marcha de la directiva europea NIS de notificación de ciberincidentes y la aplicación obligatoria del Esquema Nacional de Seguridad (ENS) para que las Administraciones Públicas y sus proveedores de servicios. La aplicación de buenas prácticas y estándares internacionales son también pilares fundamentales, como las certificaciones en ISO 27000 o las certificaciones de equipamiento electromédico como la UL2900, aprobada por la FDA.

Podemos concluir que la aplicación satisfactoria de estas recomendaciones requerirá recursos y coordinación adecuados en los sectores público y privado. El objetivo debe ser situar la ciberseguridad en el primer plano de las agendas de los ejecutivos del sector. Desafortunadamente, muchas veces reaccionamos a eventos catastróficos y carecemos de continuidad y visión estratégica, cuando la seguridad de la información debe ser parte de la agenda de la Transformación Digital de los sistemas sanitarios.

Estas medidas organizativas, técnicas, humanas y normativas aumentarán la seguridad y la confianza de las organizaciones, redes y dispositivos médicos presentes en el sector sanitario. Repercutiendo en una asistencia sanitaria segura y valorada positivamente por los usuarios.

Experiencia en la implantación de un Sistema de Gestión de Seguridad de la Información basado en ISO 27000: **Sistema Sanitario Público de Galicia**

Jorge Prado Casal, Benigno Rosón Calvo, Eva Marcos Doldán, Paulo Bueno Capeáns
Subdirección General Sistemas y T.I., Secretaría General Técnica
Consellería de Sanidade – Xunta de Galicia



MOTIVACIÓN

Históricamente, las características principales de los sistemas y tecnologías de la información en el Sistema Sanitario Público de Galicia son la integración, el uso de plataformas comunes y la estandarización.

Dada alto nivel de integración existente, uno de los pilares sobre los que se asientan dichos sistemas y tecnologías de la información es la optimización de la gestión de la seguridad de la información. Y la mejor manera de dar presencia a este pilar es mediante la adopción de metodologías reconocidas y certificables, que den confianza a todos los actores implicados.

EVALUACIÓN DE ALTERNATIVAS

Antes de abordar este proceso, y teniendo en cuenta el coste de la implantación de una metodología de gestión de la seguridad, procedimos a ponderar las ventajas que podría reportarle a nuestra organización.

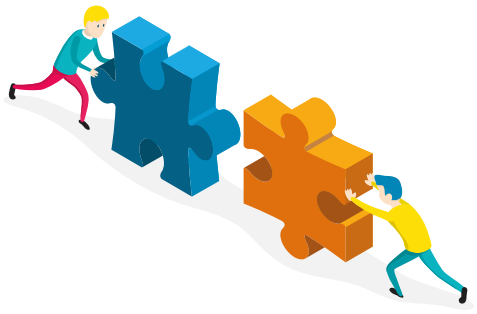
En primer lugar, estimamos el posible coste de no gestionar la seguridad. Es una opción totalmente inaceptable desde cualquier perspectiva que se contemple: estratégica, económica, social, política, legal y moral. Además, las consecuencias de una negligencia absoluta en la gestión de la seguridad en cualquiera de las dimensiones citadas alcanzarían un nivel de gravedad difícil de cuantificar, con consecuencias inasumibles para las personas e instituciones implicadas, pudiendo llegar a generarse conflictos sociales graves.

Habiendo descartado de raíz la posibilidad de no gestionar de una manera previsible y organizada la seguridad de la información, el siguiente paso fue estudiar las metodologías existentes para escoger aquella que mejor se adapta a nuestra casuística.

En el año 2001 comenzamos a implantar los procesos de la biblioteca ITIL para la gestión del servicio TIC, por lo que, entre otros procesos, se evaluaron los relativos a la seguridad de la información, ponderándolos con la alternativa que en aquellos momentos constituía el estándar ISO 17799.

Tras un estudio detallado, estimamos que el estándar ISO presentaba una hoja de ruta más consistente y que resultaba más sencillo de explicar al conjunto de la organización. Otras de las ventajas que ofrecía era la individualización del proceso formativo, que resulta específico para el marco de la seguridad de la información, mientras que en el caso de ITIL estaba embebida en un conjunto normativo global.

Ambas alternativas compartían la misma carencia: la ausencia de un marco de auditoría y certificación externa. Este requisito resulta de especial interés en un modelo de gestión distribuida de sistemas fuertemente integrados, donde el aseguramiento de la calidad constituye un elemento básico para conocer el nivel de madurez de procesos, evaluar la habilidad en el desempeño, identificar oportunidades y deficiencias y ofrecer garantías a todos los actores implicados en el funcionamiento de las TIC sobre la eficacia de los controles.



> ***Nuestra experiencia en la gestión del SGSI en base a las normas de la serie ISO 27000 es muy favorable. Traslada confianza tanto al conjunto de la organización como a los distintos actores que interaccionan con ella a través de los sistemas y tecnologías de la información***

PRIMEROS PASOS

Dada esta carencia, optamos por implantar un sistema de gestión de la calidad basado en la norma ISO 9000 en la que se incluyeron como procesos estratégicos aquellos obtenidos de ITIL e ISO 17799. Este sistema de gestión de la calidad fue certificado por primera vez el año 2006 y fuimos ampliando su ámbito de aplicación de manera progresiva y continuada. En estos momentos abarca a todas las unidades de sistemas y tecnologías de la información a lo largo de la Consellería de Sanidad y el Servicio Gallego de Salud.

EVOLUCIÓN DE LAS NORMAS

Posteriormente, a partir de ITIL se desarrollaron las normas de la serie ISO 20000 y a partir del estándar ISO 17799 se crearon las de la serie ISO 27000, que ya permiten una certificación autónoma.

De hecho, los movimientos en el ámbito de las normativas de gestión de la seguridad de la información se produjeron de una forma continuada, partiendo de la creación en el año 2005 de la

norma ISO 27001 y de la segunda versión de ISO 17799, que en julio de 2007 cambió su número de referencia a ISO/IEC 27002:2005, donde origen al amplio conjunto de normas que hoy conocemos como series ISO/IEC 27000

PUESTA EN MARCHA DEL SGSI

En el año 2007 decidimos abordar la implantación de ISO 27000 de manera específica, y como elemento integrante de nuestro sistema de gestión de la calidad, buscando desde el primer momento el mayor alcance posible y una visión global de toda la información gestionada por el sistema sanitario público de Galicia.

El primer paso fue la formación al personal de la organización en los fundamentos básicos de la norma.

A continuación se realizó un análisis detallado de la situación de partida, que finalizó en el año 2009, momento en el cual se comenzó el proceso formal de adaptación de nuestro sistema de gestión de la seguridad de la información (SGSI) a las normas de la serie ISO 27000.

Escogimos la metodología MAGERIT para realizar el análisis y gestión de riesgos de Sistemas de la Información, utilizando la herramienta PILAR para implementarla.

Tras una serie de auditorías internas, nuestro SGSI fue certificado por primera vez a finales de 2015.

ALCANCE

En estos momentos estamos gestionando todas las actividades de desarrollo o adquisición de sistemas de información, así como su implantación, explotación y/o administración; cubriendo las 185 aplicaciones y proyectos incluidos en el Catálogo corporativos de Aplicaciones (CATAP) de la Conselleria de Sanidade y Servicio Galego de Saúde (SERGAS). El sistema cubre también los servicios de gestión de la plataforma hardware y red de telecomunicaciones, correo electrónico y todo el servicio de gestión del soporte a los elementos indicados.

Se incluyen dentro del ámbito cubierto por la certificación en estos momentos a 6 edificios administrativos, a la totalidad de los 458 centros de salud, y a los centros hospitalarios de 4 de las 7 gerencias de gestión integrada. En esos centros trabajan 20.000 empleados públicos.

EVALUACIÓN DE LA GESTIÓN DEL SGSI

Nuestra experiencia en la gestión del SGSI en base a las normas de la serie ISO 27000 es muy favorable. Traslada confianza tanto al conjunto de la organización como a los distintos actores que interaccionan con ella a través de los sistemas y tecnologías de la información, nos ayuda a ordenar la gestión de los riesgos digitales, permitiendo además manejarlos de una manera previsible. También nos facilita llevar una contabilidad efectiva de la situación de dichos riesgos a través de la implantación de medidas y controles. Además, el SGSI implantado nos permitido verificar el cumplimiento del marco legal al estar incluido dentro de su ámbito de aplicación.

Como el alcance de ISO 27000 es muy amplio y no está restringido al ámbito puramente técnico, y dada la facilidad para aplicarla a organizaciones de todo tipo y tamaño, se han convertido en una referencia para gran parte de los marcos de tratamiento de datos, incluso legales. Eso nos ha deparado ventajas que inicialmente eran imposibles de prever, por ejemplo:

- Cuando abordamos la implantación del Esquema nacional de Seguridad (ENS), el hecho de que sea un esquema inspirado en la familia de estándares ISO 27000 nos ha facilitado la verificación de las medidas establecidas, permitiendo que con un nivel de esfuerzo muy contenido podamos generar esta confianza exigida legalmente en el uso de los medios electrónicos.
- En esa misma línea, el SGSI implantado nos ha facilitado incluso la adopción de la nueva normativa de protección de datos, tanto el Reglamento General de Protección de Datos como la Ley Orgánica 2/2018, ya que nos hemos basado en la gestión de riesgos ya existente en nuestro SGSI para abordar los riesgos inherentes a los tratamientos de datos de carácter personal que realizamos.

De cara al futuro inmediato, pretendemos incluir durante este año 2019 a los hospitales restantes en el alcance de la certificación ISO 27001 y abordar la certificación formal en ENS.

Evaluación de Impacto en la Protección de Datos
Paralelismos

Rafael Marín Jiménez
Unidad de Gestión de Riesgos Digitales. Servicio Andaluz de Salud.

MUCHO SE HA ESCRITO SOBRE ESTE TEMA, INCLUSO ANTES DE LA ENTRADA EN VIGOR DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS DE LA UE 2016/679 (RGPD); EN ESTA OCASIÓN NOS PLANTEAMOS LLEVAR A CABO UNA ORDENACIÓN DE MODO SIMÉTRICA DE ALGUNOS DE SUS ELEMENTOS FRENTE A SIMILARES MARCOS DE REFERENCIA CON OBJETIVOS BIEN DISTINTOS. NO CABE DUDA QUE LA EVALUACIÓN DE IMPACTO NO HA NACIDO DE LA MANO DE LA PROTECCIÓN DE DATOS Y POR TANTO PARECE RECOMENDABLE INDAGAR EN SU APLICACIÓN EN OTROS ÁMBITOS COMO PUEDA SER EL RELATIVO A LAS CUESTIONES DE GÉNERO O A LA SALUD PÚBLICA, SIEMPRE DESDE EL MÁXIMO RESPECTO.

En todos los casos, se trata de una medida regulada legalmente aunque con distintos niveles de desarrollo o madurez. Mientras que la Evaluación de Impacto en la Protección de Datos (EIPD) viene impuesta por el RGPD, en varios considerandos pero principalmente en el artículo 35; la Evaluación del Impacto de Género (EIG) ha sido el fruto de la evolución de un conjunto de Directivas europeas[1] que han desembocado a nivel nacional en la *Ley Orgánica 3/2007, de 22 de marzo, para la igualdad efectiva de mujeres y hombres,* haciéndose patente principalmente en su artículo 19; y la Evaluación de Impacto en Salud (EIS) procedente de la *Ley 33/2011, de 4 de octubre, General de Salud Pública,* preceptuada en el capítulo VII del Título II.

Para el caso andaluz, además podemos avanzar aún más en el desarrollo normativo; siendo así que para la EIG contamos con la *Ley 12/2007, de 26 de noviembre, para la Promoción de la Igualdad de Género en Andalucía* y con el *Decreto 17/2012, de 7 de febrero, por el que se regula la elaboración del Informe de Evaluación del Impacto de Género.* Igualmente para la EIS contamos con la *Ley 16/2011, de 23 de diciembre, de Salud Pública de Andalucía* y con el *Decreto 169/2014, de 9 de diciembre, por el que se establece el procedimiento de la Evaluación del Impacto en la Salud de la Comunidad Autónoma de Andalucía.*

La meta que persigue la evaluación de impacto es determinar el grado de afección en los derechos de las personas físicas desde aproximaciones objetivas diferentes; en un caso desde la óptica de la protección de los datos personales, en otro desde la equiparación oportunidades entre géneros y en el tercero a través de la defensa de la salud pública. Baste con observar las siguientes definiciones para percatarse de las similitudes más allá del bien protegido:

- El EIPD es una herramienta que permite evaluar de manera anticipada cuáles son los potenciales riesgos a los que están expuestos los datos personales en función de las actividades de tratamiento que se llevan a cabo con los mismos.
- La EIG es una evaluación previa de los resultados y efectos que determinadas disposiciones o planes de especial relevancia puedan tener sobre mujeres y hombres, así como la incidencia de sus

[1] Directiva 2002/73/CE, de reforma de la Directiva 76/207/CEE, relativa a la aplicación del principio de igualdad de trato entre hombres y mujeres en lo que se refiere al acceso al empleo, a la formación y a la promoción profesionales, y a las condiciones de trabajo. Directiva 2004/113/CE, sobre aplicación del principio de igualdad de trato entre hombres y mujeres en el acceso a bienes y servicios y su suministro. Directiva 2006/54/CE del Parlamento Europeo y del Consejo, de 5 de julio de 2006 , relativa a la aplicación del principio de igualdad de oportunidades e igualdad de trato entre hombres y mujeres en asuntos de empleo y ocupación.



resultados en relación con la igualdad de oportunidades entre ambos sexos.

- La EIS es una combinación de procedimientos, métodos y herramientas mediante las que una política, programa o proyecto puede ser evaluado en función de sus potenciales efectos en la salud de la población y de su distribución en dicha población.

Atendidos los criterios que hacen obligatoria la realización de una evaluación de impacto en cada caso, si analizamos el grado de vinculación que la misma supone para la organización, podemos apreciar las consideraciones. El reglamento europeo y guías que desarrollan la EIPD mencionan que su resultado debe **tenerse en cuenta, necesariamente,** a la hora de tomar las decisiones o medidas[2] relacionadas con el cumplimiento de lo previsto en el RGPD y la toma de decisión de la viabilidad o no de llevar a cabo el tratamiento de los datos. La ley nacional que regula la EIG no precisa la consideración que ha de mostrarse a los resultados del informe, y dado que no llegó a desarrollarse reglamentariamente como requiere su disposición transitoria décima, tampoco es posible recurrir a dicho desarrollo; la norma andaluza detalla[3] algunos aspectos de la EIG sin informar tampoco de su carácter, siendo el Decreto[4] que desarrolla la norma andaluza quien otorga el carácter **preceptivo** al informe de evaluación del impacto de género que acompañará al acuerdo de iniciación del procedimiento de elaboración de una disposición. Y la ley nacional que regula la EIS tan sólo contempla[5] que sus resultados se integrarán en el sistema de información de salud pública y en la Red de Vigilancia de la Salud Pública, sin explicitar su carácter; en cambio la norma andaluza es mucho más prolija, determinando[6] los casos en los que la misma tiene un carácter exclusivamente **preceptivo** (artículo 56.1.a) y aquellos en los que además es **vinculante** (artículos 56.1.b, c y d).

Enlazando el precedente análisis sobre el carácter de la evaluación de impacto con el siguiente elemento comparado, las responsabilidades sobre la misma, en relación a la normativa de protección de datos resulta oportuno recordar las recomendaciones hechas por el Grupo de Trabajo del artículo 29, ahora Comité Europeo de Protección de Datos, respecto de las principales cuestiones sobre las que el responsable del tratamiento debe buscar el asesoramiento del DPD:

- *Si debe llevarse a cabo o no una evaluación de impacto relativa a la protección de datos.*
- *Qué metodología debe seguirse al llevar a cabo una evaluación de impacto.*
- *Si debe realizarse la evaluación de impacto en la propia organización o subcontratarse.*
- *Qué salvaguardias (incluidas medidas técnicas y organizativas) deben aplicarse para mitigar*

[2] RGPD, considerando 84
[3] Ley 12/2007, de 26 de noviembre, para la promoción de la igualdad de género en Andalucía. Artículo 6.
[4] Decreto 17/2012, de 7 de febrero, por el que se regula la elaboración del Informe de Evaluación del Impacto de Género. Artículo 4.2.
[5] Ley 33/2011, de 4 de octubre, General de Salud Pública. Artículo 35
[6] Ley 16/2011, de 23 de diciembre, de Salud Pública de Andalucía. Artículo 58

cualquier riesgo para los derechos e intereses de los interesados.

- *Si la evaluación de impacto relativa a la protección de datos se ha llevado a cabo correctamente o no y si sus conclusiones (si seguir adelante o no con el tratamiento y qué salvaguardias aplicar) son conformes con el RGPD.*
- El Grupo de Trabajo continuaba diciendo que *si el responsable no está de acuerdo con el asesoramiento ofrecido por el DPD, la documentación de la evaluación de impacto debe justificar específicamente por escrito por qué no se ha tenido en cuenta el consejo.*

Como ya hemos adelantado, otro elemento relevante en el que fijar la atención, quizás el más importante, es el que tiene que ver con los agentes sobre los que recae la responsabilidad de intervenir en la elaboración de la evaluación de impacto. La EIPD es una herramienta con carácter preventivo que debe realizar el **responsable del tratamiento,** considerando que el artículo 35.2 del RGPD relega al **delegado de protección de datos,** en su caso, a ofrecer asesoramiento al primero para su adecuada ejecución; mismo papel se otorga al **encargado del tratamiento**, si lo hubiese. Si acudimos a la guía[7] de la AEPD encontramos una interesante matriz de asignación de responsabilidades respecto de cada una de las seis fases en las que estructura el EIPD, de ella resulta oportuno traer a colación dos aspectos aún no mencionados; el primero es que el delegado de protección de datos no sólo debe ser consultado sino que también debe ser informado sobre la realización de cada fase; el segundo es la necesaria consulta a **otros agentes** en según qué fases, como es el caso de los miembros de las áreas de seguridad, riesgos, asesoría jurídica, etc. El decreto andaluz que regula la elaboración del informe de la EIG dispone en su artículo 4 que éste debe ser elaborado por el **centro directivo competente** para la iniciación del procedimiento de elaboración de la disposición, mientras deja la función de asesoramiento a la **Unidades de Igualdad de Género**[8] permitiéndoles formular observaciones a los informes y valorar su contenido. Conforme al decreto andaluz, el informe derivado de la EIS es responsabilidad de la **autoridad competente en materia de salud pública**, que será fruto de la evaluación del documento de valoración de impacto en salud (VIS) previamente emitido por **las personas, entidades o administraciones promotoras** de instrumentos de planeamiento; tales promotores podrán obtener de la mencionada autoridad información sobre el alcance, amplitud y grado de especificación con el que debe realizarse la valoración del impacto en la salud.

Profundizando un poco más en el paralelismo sobre las responsabilidades, es posible comparar las mencionadas Unidades de Igualdad de Género con las **Unidades de Seguridad TIC**[9] que se constituyen en la administración andaluza. En ambos casos tienen un alcance al menos a nivel de Consejería, competencias transversales a la misma en la medida que afecten a su finalidad de creación y funciones específicas de asesoramiento, impulso, seguimiento, sensibilización,..., respecto de dicha finalidad. Parece sensato suponer que si la Unidad de Igualdad de Género tiene como primer cometido reflejado en el artículo 4.a de su decreto de creación la función de *"asesorar a los órganos competentes de la Consejería en la elaboración del informe de evaluación del impacto por razón de género, previsto en el artículo 6 de la Ley 12/2007, de 26 de noviembre"*; éste mismo cometido respecto de la seguridad de la información, debiera formar parte de la futura actualización del decreto de creación de las Unidades de Seguridad TIC, las cuales podrían evolucionar hacia Unidades de Ciberseguridad, o mejor aún a **Unidades de Seguridad de la Información**. Esta propuesta es perfectamente viable en la medida que tal Unidad forme parte de la estructura de soporte del DPD como órgano competente de la Consejería.

Existen varios elementos más sobre los que procedería continuar el paralelismo entre las distintas evaluaciones de impacto, tal es el caso de la oportunidad de su ejecución en lo que al momento temporal se refiere, del contenido mínimo que debe incluir, etc. Sin embargo, lo expuesto hasta el momento es suficiente para sustentar la idea que da título al artículo; y no menos importante, pone de manifiesto importantes conclusiones respecto de las responsabilidades de los distintos agentes intervinientes en la EIPD.

[7] Guía práctica para las Evaluaciones de Impacto en la Protección de los datos sujetas al RGPD

[8] Decreto 275/2010, de 27 de abril, por el que se regulan las Unidades de Igualdad de Género en la Administración de la Junta de Andalucía

[9] Decreto 1/2011, de 11 de enero, por el que se establece la política de seguridad de las tecnologías de la información y comunicaciones en la Administración de la Junta de Andalucía; modificado por el Decreto 70/2017, de 6 de junio

Situación del **Delegado de Protección Datos** en el SNS

Elvira Alonso Suero, Elena Díaz García
Servicio de Salud de Principado de Asturias

LA FIGURA DEL DELEGADO DE PROTECCIÓN DE DATOS (EN ADELANTE, DPD), SE ENCONTRABA EXPRESAMENTE RECONOCIDA EN EL ARTÍCULO 18 DE LA DIRECTIVA 95/46/CE DEL PARLAMENTO EUROPEO Y DEL CONSEJO, DE 24 DE OCTUBRE DE 1995, RELATIVA A LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES Y A LA LIBRE CIRCULACIÓN DE ESOS DATOS. EN LA PRÁCTICA EL PRECEPTO OBLIGABA A LOS ESTADOS MIEMBROS A ESCOGER, EN LA TRANSPOSICIÓN DE LA DIRECTIVA, ENTRE UN SISTEMA DE NOTIFICACIÓN DE FICHEROS A LA AUTORIDAD DE CONTROL, POR LO QUE SE DECANTÓ ESPAÑA (ARTÍCULO 26 LOPD 15/1999), O A CONTAR CON UN PROFESIONAL DEDICADO A LA MATERIA. ESTE PROFESIONAL DEBÍA: HACER APLICAR EN EL ÁMBITO INTERNO LA NORMATIVA EN MATERIA DE PROTECCIÓN DE DATOS Y LLEVAR UN REGISTRO D E LOS TRATAMIENTOS EFECTUADOS POR EL RESPONSABLE.

Como es sabido la Directiva se ha visto derogada por 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 (en adelante, RGPD), que, en lo que respecta al DPD, lo considera en su artículo 35, de designación obligatoria entre otros supuestos, y, en lo que aquí nos interesa, como reza el apartado a), cuando "el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial". De manera que como administraciones públicas, y en el caso de los Servicios de Salud, entidades u organismos públicos, estaríamos obligados a contar con un DPD. En el ámbito sanitario debemos tener en cuenta además el apartado c) que obliga a la designación de esta figura, "cuando las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categoría especiales de datos con arreglo al artículo 9 o de datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10". Siendo así, que en los Servicios de Salud se tratan obviamente datos relativos a la salud y datos genéticos, ambas categorías incluidas en el artículo 9.

En este sentido, el Grupo del Artículo 29, a través del documento "Directrices sobre los delegados de la protección de datos", ha precisado lo siguiente sobre el supuesto de obligatoriedad en las Administraciones públicas:

El RGPD no define que se considera como "autoridad u organismo público" por lo que tal noción debe determinarse de conformidad con la legislación de cada país, que si bien se entienden incluidas las autoridades nacionales, regionales y locales, también pueden ser incluidos otros organismos regidos por el derecho público. Respecto a las organizaciones privadas que participen a través de las diferentes modalidades de contratación de la gestión de los servicios público, si bien no sería obligatorio la designación del delegado de protección de datos, se recomienda como buena práctica su nombramiento, cubriendo su actividad no sólo los tratamientos relacionadas con esa gestión pública sino también los que no lo estén.

En este sentido, nuestra Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Per-

sonales y garantía de los derechos digitales (en adelante, LOPDGDD), amplía los supuestos de designación obligatoria, y en lo que al ámbito sanitario se refiere establece en el apartado f) del art 34, que, el responsable y encargado del tratamiento, deberán designar un DPD, en todo caso cuando se trate de las siguientes entidades, entre otras: "los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes. Se exceptúan los profesionales de la salud que, aun estando legalmente obligados al mantenimiento de historias clínicas de los pacientes, ejerzan su actividad a título individual". Lo anterior nos lleva a preguntarnos si todos los Hospitales deben contar con un DPD, o si el DPD único para toda la administración, incluida la sanitaria, o específico de la administración sanitaria, debe de encargarse de esas funciones en relación con todos los hospitales de la red sanitaria pública ubicados en su territorio. Así como de velar de que tanto contratistas como concesionarios de servicios públicos sanitarios, cumplan con sus obligaciones en materia de protección de datos y se protejan los derechos y libertades de los interesados en un ámbito especialmente sensible como el sanitario.

En el documento "El impacto del Reglamento General de Protección de Datos, sobre la actividad de las Administraciones públicas", la AEPD considera como uno de los impactos sobre las citadas Administraciones precisamente la necesidad de designar un Delegado de Protección de Datos: "El RGPD prevé que todas las "autoridades u organismos públicos" nombrarán un DPD. También establece cuáles habrán de ser los criterios para su designación (cualidades profesionales y conocimientos en derecho y práctica de la protección de datos), su posición en la organización y sus funciones. Prevé, igualmente, que en el caso de las autoridades u organismos públicos puedan nombrarse un único DPD para varios de ellos, teniendo en cuenta su tamaño y estructura organizativa.

Las previsiones del RGPD relativas al DPD se contienen en los artículos 37 a 39, que establecen un mínimo estatuto jurídico de la figura, que propicia, como veremos mas adelante que cada administración haya optado dentro de los parámetros legales, por muy diferentes formas de organización e incluso perfiles profesionales, al exigirse únicamente "conocimientos especializados en derecho y la práctica en materia de protección de datos". La LOPDGDD, contempla la figura en los artículos 35 a 37, añadiendo a las previsiones del Reglamento, otros supuestos de designación obligatoria, así como su intervención en los procedimientos de reclamación ante las autoridades de protección de datos.

De manera que en virtud de la regulación, muchas son las decisiones que quedan en manos de cada administración y/o organismo, lo que va a suponer una falta de uniformidad en la configuración de la figura en cada Comunidad Autónoma, y en cada administración, Así, deberán determinarse las unidades en que se va a integrar el DPD dentro de cada administración y/o organismo, su posición en la estructura administrativa y los mecanismos para asegurar que los DPD designados reúnen los requisitos de cualificación y competencia establecidos por el RGPD.

Es acorde con el RGPD designar un único Delegado para, por ejemplo, un ministerio, consejería, ayuntamiento, o administración de una Comunidad Autónoma, como también lo sería designar uno por cada Consejería por ejemplo.

Lo que no parece aconsejable que ese único Delegado actúe respecto de grandes unidades u órganos con entidad y tareas claramente diferenciadas (como ocurre por ejemplo con los Servicios de Salud autonómicos), como veremos se ha considerado necesario en muchos Servicios de Salud el nombramiento específico para este ámbito. Parece claro también que dadas las funciones del Delegado de Protección de Datos, su adscripción dentro de la estructura de la organización deba hacerse a órganos o unidades con competencias y funciones trasversales. El nivel del puesto de trabajo debe ser el adecuado para poder relacionarse con la dirección del órgano u organismo en el que desempeñe sus funciones, y lo lógico sería proceder a su creación en la relación de puestos de trabajo, aunque en la práctica no es esto lo que ha ocurrido, dado que en muchos casos los nombramientos se han acumulado a los de los puestos de trabajo que desempeñaba su titular, compaginando, a duras penas, las funciones propias de su puesto y las "añadidas" de DPD.



El RGPD prevé que el Delegado pueda desarrollar su actividad, a tiempo completo o parcial, y también que podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios. En los casos en que se haya optado por dotar un puesto especifico en las relaciones de puestos de trabajo, el desempeño es a tiempo completo y por personal propio de las administraciones. Cuando se "acumulan" las funciones a los puestos de los titulares, el desempeño es lógicamente a tiempo parcial, situación no idónea.

Otro límite a los nombramientos, lo constituye el hecho de que el Delegado al actuar como asesor y supervisor interno, determina que ese puesto no puede ser ocupado por personas que, a la vez, tengan tareas que impliquen decisiones sobre la existencia de tratamientos de datos o sobre el modo en que van a ser tratados los datos, de ahí que hayan quedado excluidos los responsables de tecnologías de la información, o de seguridad de la información).El RGPD posibilita que se externalicen las funciones de Delegado, en la práctica se ha contratado externamente alguna de estas.

Con tales mimbres, brevemente expuestos, se ha revisado la situación en las distintas comunidades autónomas para tener una visión de cómo se ha cumplido la normativa en relación con los nombramientos del delegado de protección de datos en cada una de ellas.

Comprobándose que existen, básicamente, cinco modelos de diferentes:

- Único delegado de protección de datos para toda la administración de la Comunidad Autónoma.
- Un delegado de protección de datos exclusivo para sanidad.
- Nombramiento de delegado de protección de datos en la figura colegiada de un Comité Delegado de protección de datos.
- Nombramiento de un delegado de protección de datos con el apoyo de un Comité de Seguridad.
- Nombramientos de DPDs por cada Consejería y Organismo Autónomo.

En cuanto a las formulas utilizadas para realizar los nombramientos:

- Por Resolución, de la Consejería o del Servicio de Salud correspondiente.
- Nombramiento en formulario de comunicación de Delegado de Protección de Datos (DPD) a la Agencia Española de Protección de Datos (AEPD).

- Acuerdo de Consejo Gobierno.
- Decreto de Consejo de Gobierno.

Es claro que la especialización de los DPD en el sector sanidad, no ha sido la solución adoptada por todas las CCAA, puesto que las hay que han nombrado un único DPD para toda la administración autonómica. Entendemos que la solución más adecuada y más acorde con la norma sería el nombramiento específico de un DPD para sanidad, que este coordinado, en su caso, con los DPDs del resto de la administración autonómica (sanidad, educación y justicia).

La justificación a esta especialización en la figura del DPD, vendría dada por la complejidad de las estructuras de las organizaciones sanitarias, con una estructura periférica constituida por centros de salud y hospitales que en ocasiones se encuentran dispersos geográficamente. Por los distintos orígenes los datos (buzones de sugerencias, formularios de historia clínica, dispositivos, pruebas diagnosticas...) hacen que los formatos de almacenamiento sean múltiples y específicos. Así como por la importante normativa específica, propia del sector sanitario, que es necesario manejar e interpretar conjuntamente con la propia de la protección de datos.

Esta especificidad ya viene recogida en el artículo 9 LPDGDD, donde se establece que el tratamiento de los datos de salud, deberá estar amparados en una norma con rango de ley, que podrá establecer requisitos adicionales relativos a su seguridad y confidencialidad. Y, en particular, la norma podrá amparar el tratamiento de datos en el ámbito de la salud, cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria.

> ***"Salvo excepciones, ha intentado cumplirse con el RGPD a "coste 0"... Los delegados únicos deben abordar la problemática específica de sectores como Sanidad o Educación que claramente demandan contar con un delegado propio con conocimientos de la normativa sectorial, además de la propia de protección de datos***

Con la situación descrita en las CCAA, se publica en abril de 2019 el Informe de la Agencia Española de Protección de Datos, 2995/2019, donde se plantean diversas cuestiones relativas a la figura del Delegado de Protección de Datos, planteadas por la Generalitat Valenciana y que hacen referencia, entre otras, a cuestiones abordadas en el presente escrito, en particular:

1. Sobre la validez de nombrar un DPD único para centros educativos, sanitarios y comités de ética de la investigación, que ha sido como se ha visto el modelo adoptado por muchas CCAA. Al respecto la AEPD considera que el art 34 LOPDGDD, amplia el espectro de sujetos "responsables" obligados a la designación de un DPD, exigiendo un nombramiento que debe reputarse específico y diferenciado, en el supuesto de los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes. De manera que no considera válido el modelo de DPD único para centros educativos, sanitarios y comités de ética de investigación, lo que cabe preguntarse ahora es si el modelo adoptado por algunas CCAA de un DPD específico para el ámbito sanitario sirve para cubrir esa exigencia o si es necesario el nombramiento de un DPD para cada centro sanitario. Entendemos que el DPD específico para sanidad cumpliría esta previsión lo que valida la opción de las CCAA que han optado por dicho modelo.
2. En relación con los equipos de soporte o apoyo al DPD, se consultó a la AEPD si sería extensible a los miembros de tal equipo cuanto se prevé para el DPO en cuestiones tales como el acceso a datos personales y a procesos de tratamiento (art 36.3 LOPDGDD), capacidad inspectora (ART 36.1) o régimen sancionador (art 70). Respondiendo la Agencia que tales actividades corresponden siempre al propio DPD, y no al personal adscrito a su "soporte", en particular la función inspectora. Y que su existencia no exime al DPD de ninguna de sus obligaciones.

La necesidad de que existan profesionales garantes de la privacidad y del derecho a la protección de datos, hoy DPD, se evidencia en:

1. Que el derecho a la protección de datos es un derecho fundamental, declarado como tal por el Tribunal Constitucional.
2. El papel de estos profesionales es esencial para el respeto de este derecho y además incorpora valores positivos que benefician a las organizaciones (responsabilidad proactiva, compliance).
3. Dicha figura debe consolidarse y regularse adecuadamente, convirtiéndola en un perfil reconocido y sólido. En términos de las conclusiones de la reunión celebrada en Valencia con los delegados de protección de datos autonómicos, sería conveniente la elaboración de un estatuto jurídico del DPD.
4. El papel del asociacionismo y la coordinación entre distintas figuras en este ámbito es esencial, dada la diversidad de fórmulas que se han adoptado como se ha señalado, para aprovechar la experiencia de otros y buscar soluciones uniformes y conjuntas, a fin de cuentas estamos ante un único sistema nacional de salud, y la protección de datos sanitarios no debería ser mejor ni peor, más o menos intensa según la Comunidad Autónoma de que se trate.
5. Los retos para el futuro de la privacidad en el ámbito sanitario son muchos y muy complejos, siendo imprescindible el papel del DPD para hacerles frente.

Las importantes tareas y responsabilidades que deben asumir los DPDs, también en el ámbito de las administraciones, casan mal con la aparente poca importancia o atención que desde estas se les ha prestado. Salvo excepciones, ha intentado cumplirse con el RGPD a "coste 0", sin dotación de puestos específicos, ni presupuesto adicional alguno. Los delegados únicos deben abordar, además de los temas generales, la problemática específica de sectores como sanidad o educación que claramente demandan contar con un delegado propio con conocimientos de la normativa sectorial, además de la propia de protección de datos. A esto hay que añadir la interpretación que la AEPD ha dado de la previsón del art 34 LOPDGDD, que exigiría un nombramiento específico. En las administraciones hay departamentos muy desarrollados en materia de protección de datos y otros que no lo están en absoluto, debiendo el DPO aglutinar el conocimiento e intentar que todos se desarrollen por igual. La ausencia de una regulación sobre la forma de realizar los nombramientos hace que la situación sea muy dispar entre las CAAA, así únicamente Euskadi cuenta con un nombramiento de alto cargo, como DPD, por 6 años; en otros casos como Navarra estamos ante un puesto de libre designación pero que no cuenta con una unidad como tal; otros se acumulan a los puestos principales; algunos cuentan con Comités de apoyo (Asturias) y en otras Comunidades se crean Unidades de protección de datos (Aragón). Esta circunstancia va a propiciar diferentes ritmos e intensidades a la hora de cumplir con el RGPD, por cada Comunidad Autónoma, dependiendo de la estructura de la que cada una se haya dotado para afrontar dicho reto y del nivel de implicación de sus responsables con la materia. El reciente informe de la AEPD 002995/2019 viene a arrojar algo de luz sobre estas cuestiones organizativas, lo que contribuirá a uniformizar determinados aspectos relacionados con los DPDs autonómicos.

BIBLIOGRAFÍA

Reglamento General de Protección de Datos https://www.boe.es/doue/2016/119/L00001-00088.pdf

Corrección de errores del 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)

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales. https://www.boe.es/eli/es/lo/2018/12/05/3

Directrices sobre los delegados de la protección de datos, https://ec.europa.eu/newsroom/art29.

El impacto del Reglamento General de Protección de Datos, sobre la actividad de las Administraciones públicas, AEPD, https://www.aepd.es/media/docs/impacto-rgpd-en-aapp.pdf.

El rol del DPO, https://secure.edps.europa.eu/EDPSWEB/webday/site/mysite/shared/Documents/EDPS/Publications/Papers/PositionP/05-11-28DPOpaperEN.pdf Informe 2995/2019 de la AEPD sobre la figura del Delegado de Protección de Datos.

La Salud del Negocio en Situaciones de Crisis

Jesús Martín Romero
Manager de Continuidad de Negocio en SIA.

EN LA ACTUALIDAD, TODAS LAS ORGANIZACIONES DEL SECTOR PÚBLICO Y PRIVADO ESTÁN EXPUESTAS A AMENAZAS DE DIFERENTES ÁMBITOS, COMO PUEDEN SER EVENTOS DE ORIGEN NATURAL, INDUSTRIAL, HUMANO O TECNOLÓGICO. ESTAS AMENAZAS PUEDEN MATERIALIZARSE Y ORIGINAR SITUACIONES DE CRISIS PARA LAS QUE DEBEMOS ESTAR PREPARADOS YA QUE AFECTAN DIRECTAMENTE A LA OPERATIVA NORMAL Y A LA SEGURIDAD DE LAS PERSONAS.



En este tipo de situaciones, la preparación de las personas involucradas y la dotación de los medios necesarios para tener capacidades de respuesta inmediata son vitales para sobrellevarlas con éxito. Durante las situaciones de crisis, la seguridad de las personas, los activos de las organizaciones, la imagen y los servicios que se prestan están expuestos, y es por ello que, durante su transcurso, cada segundo cuenta.

Una mala gestión, tanto de los recursos como de las comunicaciones, especialmente en el sector sanitario, puede acabar con consecuencias nefastas; sin contar con las pérdidas económicas asociadas, de infraestructuras críticas, como son hospitales y atención primaria, o el daño a la imagen reputacional de los profesionales de la sanidad.

La capacidad de reacción tiene mucho que ver con el análisis previo, la puesta en marcha de mecanismos preventivos, la planificación de actividades a realizar y los canales de comunicación que cada día tienen mayor peso debido a la importancia de los medios de comunicación y las redes sociales.

PREPARACIÓN Y RESPUESTA

Uno de los aspectos más importantes son el estudio previo de escenarios de riesgos natura-

PLANES DE EMERGENCIA	PLANES DE RECOLOCACIÓN	PLANES DE COMUNICACIÓN	PLANES TECNOLÓGICOS
Conjunto de actividades de evacuación y gestión de emergencias (contacto con autoridades, responsables de emergencia por localización, etc.).	Actividades requeridas para la recolocación del personal crítico en localizaciones alternativas y/o ubicaciones de emergencia, etc.	Actividades para la gestión global de notificaciones internas y/o externas dirigidas a personal, medios de comunicación, organismos oficiales, proveedores y clientes.	Actividades de recuperación de los sistemas afectados durante una crisis, orden de recuperación infraestructuras tecnológicas, información crítica (historiales médicos, información estadística, estudios de análisis…).

les, tecnológicos, de personas, infraestructuras, proveedores y actualmente las ciberamenazas. Igualmente y para conocer dónde centrar todos los esfuerzos, es necesario el estudio de los impactos económicos, legales y de reputación que puede causar la materialización de cualquier amenaza.

Estar preparados y responder a eventos críticos implica el desarrollo de planes y entrenamiento de los mismos, poniendo a prueba capacidades para cada una de las fases de una crisis, desde la alerta temprana hasta la resolución.

Los equipos de emergencia tienen el papel fundamental de realizar las acciones previas de comunicación de una posible situación de crisis, donde todos los equipos involucrados en la respuesta y recuperación, deben contar con todos los medios necesarios para llevar a cabo las acciones definidas previamente en diferentes planes.

En SIA contamos con un equipo experto en resiliencia y continuidad de negocio con amplia experiencia en diversos sectores y establecemos las bases para asegurar la preparación de las personas y equipos de gestión de crisis y así estar preparados ante cualquier situación adversa.

A lo largo de los años, SIA ha firmado acuerdos de colaboración con las mayores firmas de gestión de continuidad de negocio y gestión de comunicación de eventos críticos. Recientemente ha cerrado con Everbridge, compañía líder mundial en soluciones integradas para la gestión de eventos críticos, un acuerdo que garantiza que las organizaciones empresariales, gubernamentales y de atención médica estén preparadas para responder rápidamente, e incluso evitar, interrupciones repentinas e inesperadas de su actividad.

La solución conjunta de SIA y Everbridge permite a los equipos de respuesta y comunicación notificar de manera fluida y eficiente en los momentos de crisis, ayudando a reducir los tiempos de interrupción y respuesta además de aumentar la seguridad de las personas e infraestructuras.

CONCLUSIONES

Todas las organizaciones necesitan una estrategia de recuperación para sus servicios, equipos de respuesta definidos, grupos de actuación frente a emergencias e infraestructura que las apoye. Todos los roles, funciones e intercomunicación de los integrantes de los equipos y grupos necesitan estar entrenados y preparados en las actuaciones durante una crisis y para las actividades posteriores como parte de la evaluación y la mejora continua.

SIA y su nuevo partner Everbridge ofrecen todas estas capacidades, junto a su background de conocimiento para dar apoyo y prepararlos a enfrentarse a estas complejas situaciones y dar respuesta a los retos que proponen las nuevas legislaciones de protección de datos, historias clínicas, Banca, Seguros y sector Servicios.

Implantando una solución NAC (Network Access Control) en una organización sanitaria

EL PROCESO DE TRANSFORMACIÓN DIGITAL DE LAS ORGANIZACIONES SANITARIAS LLEVA APAREJADO UN AUMENTO EXPONENCIAL DEL NÚMERO DE DISPOSITIVOS CONECTADOS A LA RED. ESTOS DISPOSITIVOS, DE ÍNDOLE HETEROGÉNEO, REPRESENTAN TODAS LAS CASUÍSTICAS IMAGINABLES: DESDE TERMINALES WINDOWS PLATAFORMADOS CONFORME A ESTÁNDARES DE SEGURIDAD A EQUIPAMIENTO IOT -CÁMARAS, LECTORES DE ACCESOS- QUE EN MUCHOS CASOS NO VAN A PERMITIR UN BASTIONADO SUFICIENTE, PASANDO POR DISPOSITIVOS MÉDICOS BASADOS EN ARQUITECTURAS WINDOWS OBSOLETAS, SIN NINGÚN TIPO DE PROTECCIÓN.

Por si fuera poco, las redes sanitarias suelen estar físicamente dispersas, con equipos de acceso distribuidos entre edificios, con diferentes salas, consultorios, quirófanos... dificultando el control físico de qué y quién se conecta en cada puerto e incrementando el riesgo de brechas de seguridad:

- Un intruso podría usar la conexión de un equipo no controlado (por ejemplo, una cámara) para conseguir acceder a la red.
- Un técnico o un usuario podría, involuntariamente, conectar un equipo que no estuviera suficientemente securizado, añadiendo un vector de compromiso sobre el que el administrador de seguridad no tiene visibilidad ni control.

Para gestionar este tipo de entornos es necesario implantar soluciones de Control de Acceso a Red (Network Access Control, en adelante, NAC) que permitan a las organizaciones sanitarias:

1. Ganar visibilidad de los dispositivos conectados, perfilándolos en función de sus características y disponer de un inventario en tiempo real e histórico.
2. Decidir, en cada conexión, si el dispositivo que intenta acceder está autorizado y cumple los estándares de seguridad definidos por la organización, controlando dinámicamente a qué recursos de red tiene acceso.
3. Mejorar la respuesta ante incidencias (Respuesta)



Fortinet, fabricante líder mundial de soluciones de seguridad de infraestructuras, integra en su arquitectura Security Fabric una solución de Control de Acceso a Red denominada FortiNAC, que opera en entornos multifabricante y con un número ilimitado de dispositivos. FortiNAC proporciona control de acceso a la red, visibilidad



> ***Para facilitar el análisis forense de problemas, FortiNAC está garantizando la trazabilidad de las conexiones de los dispositivos, guardando históricos que permiten recuperar en qué momento se conectó un determinado dispositivo a la red, las acciones asociadas***

mejorada y capacidades de respuesta automatizadas, extendiendo la protección integrada y automatizada de Security Fabric a entornos multifabricante.

El Hospital Universitario y Politécnico de La Fe de Valencia ha implantado esta solución para resolver la problemática de acceso a su red.

En palabras de Juan Carlos Casanova, Responsable de Comunicaciones y Sistemas del Hospital La Fe, "En el momento de la puesta en marcha de la red del hospital y con cerca de 9000 dispositivos concurrentes a los que facilitar la conectividad en las diferentes VLANs, el uso de FortiNAC tuvo una importancia decisiva. Mediante la aplicación de reglas de perfilado fue posible realizar un despliegue rápido de dichos dispositivos y que éste se realizara de manera segura. Actualmente en el día a día de la administración de una red hospitalaria tan heterogénea como la nuestra, en cuanto a los dispositivos de todo tipo que se conectan, FortiNAC nos permite realizar el control de acceso a red de manera centralizada y eficiente".

Gracias a FortiNAC, el Hopiral de La Fe ha podido inventariar el parque de dispositivos conectados a la red, estableciendo controles que aseguran que todos los dispositivos son autorizados y los usuarios están autenticados, asegurando que están sujetos a una política contextual que define quién, qué, cuándo y dónde se permite el acceso, garantizando que solo las personas y los dispositivos adecuados puedan conectarse y acceder a determinadas aplicaciones, infraestructura y activos.

Para facilitar el análisis forense de problemas, FortiNAC está garantizando la trazabilidad de las conexiones de los dispositivos, guardando históricos que permiten recuperar en qué momento se conectó un determinado dispositivo a la red, las acciones asociadas (se le denegó el acceso, se le permitió acceder y a qué vlan se le asoció, quién registró ese dispositivo en la red, el grado de cumplimiento de políticas de seguridad…) y cuánto tiempo estuvo conectado.

FortiNAC colabora con los elementos de red, tanto cableada como inalámbrica: La red notificará de nuevos eventos de conexión y desconexión, y FortiNAC obtendrá información tanto de los propios elementos de red como del propio dispositivo, para crear un perfil preciso de qué tipo de elemento es y determinar si su acceso a red está validado. En función del resultado, procederá a ubicar al dispositivo en la VLAN que corresponda, e incluso informará a los elementos de seguridad para asociarle una política determinada, asegurando el control de los flujos horizontales y verticales para garantizar que ese dispositivo (o usuario) no va a poder acceder a información sensible cuando no le corresponde y no va a suponer una amenaza para red. Adicionalmente, si no está validado, notificará a los administradores del descubrimiento para que, o bien se dé por bueno su validación y se



permita su acceso, o en caso contrario se tomen las medidas oportunas.

Tras la conexión, FortiNAC realiza una evaluación continua de cada dispositivo. Si en un momento dado deja de cumplir cualquiera de los condicionantes que permitieron su acceso, será puesto en cuarentena inmediatamente, alertando a los administradores.

Como valor añadido, FortiNAC está ayudando a cumplir las políticas de parcheo de dispositivos y de versiones de firmware de la organización. Además, proporciona un entorno de validación y control de usuarios temporales: Bien usuarios invitados (visitantes, asistentes a congresos...) a los que se les ofrece un servicio de cortesía o a empleados temporales y externos que tienen que acceder a la red temporalmente.

> ***FortiNAC es una solución potente y versátil que da respuesta a los retos a los que se enfrentan diariamente los administradores de red y seguridad de las redes sanitarias***

La solución de control de acceso evolucionará para integrar las capacidades de detección de amenazas de los firewalls de nueva generación del Hospital, también del fabricante Fortinet, con la solución FortiNAC. De esta forma, los dispositivos de seguridad se encargarán de la detección y triage de amenazas asociadas a los dispositivos conectados, y colaborarán con el Security Fabric y FortiNAC para automatizar su contención en apenas segundos, donde un proceso manual puede llevar días o semanas, realizando además las notificaciones pertinentes. Con esta funcionalidad la colaboración entre NOC y SOC se estrecha y se automatiza.

FortiNAC es una solución potente y versátil que da respuesta a los retos a los que se enfrentan diariamente los administradores de red y seguridad de las redes sanitarias, ofreciendo una arquitectura de control de acceso, de fácil administración, que se adapta a los diferentes escenarios a los que se puedan enfrentar (gestión de activos, BYOD -Bring your own device-, gestión de usuarios temporales...).

Retos a la Hora de Proteger la Ciberseguridad de los Hospitales Conectados

Raúl Guillén
Strategic Alliances & Partnerships Manager | Trend Micro Iberia

LA ESPERANZA DE VIDA A NIVEL MUNDIAL ESTÁ AUMENTANDO CONSTANTEMENTE Y GRAN PARTE DE ELLO PUEDE ATRIBUIRSE A LOS AVANCES EN LA MEDICINA Y LA TECNOLOGÍA SANITARIA. LA TECNOLOGÍA PERMITE A LOS MÉDICOS IDENTIFICAR ENFERMEDADES Y TRATAR A LOS PACIENTES DE FORMA RÁPIDA Y EFICAZ. UN PACIENTE EN UN HOSPITAL MODERNO SUELE SER TRATADO POR UN PEQUEÑO EQUIPO DE MÉDICOS Y ENFERMERAS QUE SE OCUPAN DE DIFERENTES ASPECTOS DE LA ATENCIÓN DEL PACIENTE. ESTE SISTEMA ESTÁ DISEÑADO PARA ASEGURAR QUE EL PACIENTE RECIBA EL MEJOR TRATAMIENTO POSIBLE DE LA MANERA MÁS EFICAZ. ESTA ATENCIÓN COOPERATIVA AL PACIENTE ES POSIBLE GRACIAS A LOS AVANCES EN LA TECNOLOGÍA MÉDICA Y A LA RÁPIDA TRANSFERENCIA DE DATOS.



La tecnología está en el corazón de cualquier hospital moderno y el Sistema de Información Hospitalaria (HIS) es la columna vertebral que hace posible esta transferencia de datos y que gestiona toda la información de la operativa de un hospital, desde los aspectos médicos (diagnóstico, tratamiento, admisiones/altas, soporte vital, etc.), hasta los legales, administrativos, financieros, registros, etc. Por lo tanto, es importante reconocer que cada aplicación y cada dispositivo que se ejecuta en la red representa un posible punto de entrada para un ciberataque contra el hospital. Claramente, esta conexión también hace que los hospitales modernos, que

cuentan con mucha tecnología, sean objetivos lucrativos para los ciberdelincuentes. Por un lado, dada la naturaleza crítica de los hospitales, los ciberdelincuentes rápidamente se han dado cuenta de que si pueden comprometer con éxito el entorno tecnológico del hospital utilizando ataques de ransomware (secuestro de información y solicitud del pago de un rescate), entonces hay una alta probabilidad de que los hospitales afectados paguen. Más allá de los programas de ransomware, los hospitales son también un tesoro de información personal identificable (PII), que incluso contiene datos financieros, que pueden monetizarse en el mercado clandestino de la Deep Web.

Por su parte, los avances en cloud, Internet de las Cosas (IoT) y los sistemas de TI digitales han ayudado notablemente a las entidades sanitarias a mejorar en gran medida la calidad de la atención ofrecida a los pacientes. Los registros de salud electrónicos son la base de una red de atención al paciente cada vez más compleja, personalizada y eficiente, pero la posibilidad de que se produzca un robo de datos confidenciales o interrupciones operativas, también ha aumentado. Según un informe elaborado por Trend Micro en colaboración con HITRUST (Health Information Trust Alliance) en el que se han analizado todos los elementos médicos conectados en un hospital -bases de datos, aplicativos, consolas de administración y, por supuesto, equipamiento médico, así como la cadena de suministro- con el fin de estudiar en profundidad todos los vectores de ataque; se revela que podría haber al menos hasta 80.000 sistemas expuestos en hospitales de todo el mundo. El mayor hallazgo es que también existe una desconexión o brecha preocupante entre la percepción actual y la realidad.

Atendiendo a este análisis de ciberamenazas contra hospitales se han identificado tres grandes áreas de exposición con un alto riesgo y que, además, son un objetivo claro para los cibercriminales.

- Operativa del hospital, donde se incluye todo lo relacionado con la operativa de explotación diaria del personal del hospital (cuadrantes de trabajo, sistemas de pago, control de edificios BMS, sistemas neumáticos de transporte, sistemas de inventario, nóminas, administración, etcétera).
- Datos médicos y de carácter personal, tanto de los pacientes (datos médicos, datos de diagnóstico, tratamiento, seguros médicos (muy importante en la sanidad privada), investigación y tratamientos de prueba (propiedad intelectual), etc. como los datos de los propios empleados y personal médico.
- Salud pública, que es todo lo relacionado con el equipamiento médico tanto en lo relacionado con el diagnóstico como con el tratamiento o monitorización de los mismos, también el sistema de gestión hospitalaria HIS.

Ante este escenario, los equipos de TI de los hospitales deben comprender mejor y mitigar estos nuevos ciberriesgos, especialmente aquellos introducidos por la cadena de suministro. La atención médica ya tiene todos los peligros asociados a cualquier otra empresa, pero la atención médica también tiene la seguridad más importante para el paciente. Y cada vez se pone más en riesgo la seguridad con la mayor introducción de sistemas IoT en el cuidado de la salud.

PERCEPCIÓN VS REALIDAD

Si se tienen en cuenta los ataques recibidos en multitud de hospitales en todo el mundo podemos afirmar que no hay un standard de ciberseguridad que proteja al sector sanitario ante ataques como el que recibió el sistema sanitario británico en mayo de 2017, basado en el ransomware WannaCry. Se estima que este ataque provocó que unas 19.000 citas y operaciones se cancelaran solo en el Reino Unido y afectó al menos a 80 de los 244 hospitales del país, a 603 centros de atención primaria junto con otras organizaciones del servicio nacional de salud (NHS), provocando un colapso del sistema sanitario durante varios días.

Pero tal y como se apunta anteriormente, el ransomware es solo una de las muchas amenazas a las que se enfrentan los hospitales modernos. Colectivamente ponen en riesgo operaciones en el hospital, la privacidad del paciente y, lo más importante, la salud del paciente. Desafortunadamente, el bombardeo de WannaCry no parece haber promovido la reevaluación de los esfuer-

zos de ciberseguridad entre las entidades sanitarias en todo el mundo.

En el corazón del desafío está la cuestión de los dispositivos y sistemas expuestos, que incluyen imágenes médicas, protocolos, bases de datos, controladores industriales y software de sistemas de atención médica. Trend Micro ha descubierto que en podría haber entre 50.000 y 80.000 sistemas expuestos dentro de hospitales/clínicas en todo el mundo. Esta exposición podría poner a los hospitales en riesgo de sufrir ataques DDoS, malware y robo de datos. Utilizando el modelo de evaluación de amenazas DREAD, el estudio pone de manifiesto que los ataques DDoS son la amenaza general más seria para las entidades sanitarias, seguidos del ransomware. Esto se debe a que los ataques son bastante fáciles de ejecutar y no requieren conocimientos especializados sobre los dispositivos o sistemas que se aprovechan.

Si analizamos por qué los hospitales tenían poca ciberseguridad, encontramos entre otras razones las siguientes:

- El objetivo principal de un centro de salud es atender al paciente y es ahí donde se destinan la mayor parte de los recursos, dejando solo el presupuesto básico y esencial disponible para el gasto en ciberseguridad.
- Los equipos informáticos del hospital y el equipamiento de diagnóstico tienen muchos usuarios, por ejemplo, médicos, enfermeras y técnicos, que rotan regularmente dentro del hospital. Esto hace que sea muy difícil incorporar estrictas políticas de ciberseguridad y procedimientos de autenticación, especialmente si esas políticas impiden las operaciones diarias.
- El equipo de diagnóstico es extremadamente costoso y los hospitales no pueden permitirse tener sus dispositivos médicos inactivos durante períodos prolongados por mantenimiento. En algunos casos, la modificación de la configuración del dispositivo médico o la actualización del sistema operativo (SO) integrado anularán la certificación, la garantía y la cobertura de seguro del dispositivo, por lo que los dispositivos médicos permanecen intactos.
- Precisamente, porque el, equipamiento de diagnóstico es costoso, no se reemplaza con frecuencia (incluso pueden pasar décadas) siempre que funcione correctamente. Es posible que estos dispositivos y sistemas ya no tengan soporte o que sean muy caros de reemplazar. ¿Por qué cambiar algo si no está roto?
- Los fabricantes de equipamiento de diagnóstico son los responsables de garantizar que sus equipos cumplan con las pautas de HITRUST CSF® para dispositivos médicos. Dado que el CSF se actualiza periódicamente, es posible que los dispositivos médicos más antiguos que aún se utilizan en los hospitales no cumplan con los requisitos.
- No todos los hospitales tienen un equipo de respuesta dedicado a ciberseguridad. En la mayoría de los hospitales, el personal de TI tiene una doble función: investigar y mitigar los incidentes de un ciberataque, así como proporcionar servicios generales de TI al hospital. Esta configuración tiene el inconveniente crítico de distribuir recursos para ambas funciones.

EL RIESGO DE LA CADENA DE SUMINISTRO

Otra área de riesgo que el informe ha descubierto en las TI de atención sanitaria está relacionada con la cadena de suministro. Por hacernos una idea, alrededor del 30% de todas las brechas comunicadas al Departamento de Salud y Servicios Humanos de EE.UU. (HHS) en 2016 se debieron a brechas de partners de negocio y proveedores externos… y el porcentaje no disminuye. Esta es un área que aún no recibe la atención que merece. Desde proveedores cloud hasta fabricantes y revendedores de IoT, desarrolladores de salud móviles y más, la compleja red de proveedores hospitalarios interconectados representa una superficie de ataque en crecimiento.

Los huecos aparecen inevitablemente cuando algunos terceros no toman la ciberseguridad tan en serio como el propio hospital. El firmware del dispositivo, las aplicaciones móviles de mHealth, el código fuente comprometido, phishing de los empleados del partner, e incluso las amenazas internas son todos riesgos muy reales. Sin una adecuada segmentación de red y un control de los empleados de la cadena de suministro, los equipos de TI del hospital se exponen a da-

ños financieros y de reputación junto al riesgo de cumplimiento normativo.

Las amenazas de la cadena de suministro, igualmente, hacen referencia a riesgos potenciales asociados con los proveedores de bienes y servicios en organizaciones de salud, donde un infractor puede filtrar información confidencial o sensible, introducir una función o diseño no deseado, interrumpir las operaciones diarias, manipular datos, instalar software malicioso e introducir dispositivos falsos y perjudicar a la continuidad del negocio. El sector sanitario es más que nunca el sector más dependiente de los sistemas basados en la nube, los proveedores de servicios externos y los proveedores de la cadena de suministro. Con esto en mente, se han examinado los diferentes puntos de entrada que pueden hacer que una red sea susceptible a un ataque de la cadena de suministro, y los diferentes tipos de ataques que pueden ser perpetrados por los ciberdelincuentes.

Después de identificar los riesgos de exposición y de la cadena de suministro, el equipo de investigación de Trend Micro realizó un ejercicio de modelado de amenazas DREAD en redes de atención médica para comprender dónde, entre varias amenazas, se encuentra el mayor riesgo.

Mediante esta investigación, se ha procurado dotar a los equipos de seguridad TI médicos con una perspectiva más amplia sobre los tipos de amenazas contra las que deberían defender sus redes. Lo que es más importante, se ha proporcionado un conjunto de indicaciones prácticas, técnicas y no técnicas, para abordar los riesgos de la exposición y la cadena de suministro, ya que los proveedores de terceros tienen credenciales que incluyen inicios de sesión, contraseñas y distintivos de acceso que pueden verse comprometidos. Estos proveedores también pueden almacenar registros físicos, dispositivos médicos y equipos de oficina. Los hospitales deben ser abastecidos por una cadena de suministro sólida y robusta para garantizar un servicio ininterrumpido a los pacientes y, por tanto, proteger la cadena de suministro del hospital contra los ciberataques se convierte en una necesidad crítica.

DEFENSA DE TI PARA HOSPITALES

La buena noticia es que, siguiendo unas mejores prácticas y metodologías de eficacia ya probada, los CIO y CISO de los hospitales pueden trabajar para mitigar muchos de los riesgos destacados en el informe. La simple configuración incorrecta, por ejemplo, es la causa número uno de los dispositivos expuestos. El Instituto Nacional de Estándares y Tecnología (NIST) ofrece un marco útil para la gestión del riesgo de la cadena de suministro (SCRM).

El enfoque debe ser asumir que en algún momento los sistemas se verán comprometidos y que deben tomarse medidas rápidas para responder.

De acuerdo con la investigación, los responsables de TI de los hospitales deberían edentificar rápidamente y responder a las brechas de seguridad en curso, contener la brecha de seguridad y detener la pérdida de datos confidenciales, prevenir anticipadamente ataques asegurando todas las avenidas explotables y aplicar las lecciones aprendidas para fortalecer aún más las defensas y prevenir incidentes repetidos.

En la práctica, esto significa aplicar tecnologías como el cifrado, para los PII sensibles; escaneo de vulnerabilidades; segmentación de red; IPS/IDS; detección de brechas; antimalware y por último, aunque no por ello menos importante, gestión de parches virtual, pues las tecnologías como Virtual Patching permiten identificar aquellas vulnerabilidades que no han sido parcheadas de forma tradicional en un sistema y sus aplicaciones, aplicando medidas de protección activas que bloqueen los intentos de dichos ataques remotos. De esta manera se protegen los sistemas de forma transparente y sin impacto para el usuario o el servicio asociado.

*__Nota__. *Para obtener más información sobre de las ciberamenazas a las que se enfrentan los hospitales y cómo equilibrar las operaciones de TI eficientes con la seguridad de la red, consulte el informe de Trend Micro* ***Protegiendo los Hospitales Conectados.***

FORO PARA LA GOBERNANZA DE LAS TIC EN SALUD

"Nuevos retos en la era digital"

LA SEIS CELEBRÓ EN PALMA DE MALLORCA EL FORO DE GOBERNANZA. EL ACTO TUVO LUGAR EN EL HOTEL PALMA BELLVER LOS DÍAS 21 Y 22 DE NOVIEMBRE.

ACTO INAUGURAL



Estuvo presidido por Patricia Gómez i Picard, consejera de Salud del Gobierno de las Islas Baleares, a la que acompañaron Luciano Sáez Ayerra, presidente de la SEIS, y Juan Fernando Muñoz, subdirector general de Tecnologías de la Información del Ministerio de Sanidad, Consumo y Bienestar Social.

Sáez dio las gracias a la consejera porque este Foro se celebraba en Palma de Mallorca y a Juan Fernando Muñoz le agradeció su participación en el mismo. "Sus múltiples conocimientos son clave para la aplicación de las TIC en nuestro sector", señaló. Tuvo palabras de agradecimiento también para el coordinador del Foro, Martín Begoña, por su esfuerzo y lamentó que no hubiera podido llegar a tiempo y al Comité Ejecutivo del Foro, al Comité Local coordinado por Antònia Salvá y a Sebastiá Matas y Miguel Ángel Benito, delegado de la SEIS en esta Comunidad. Después de los agradecimientos explicó a los asistentes la historia de este Foro de Gobernanza, que representa un espacio en el que anualmente se analizan las preocupaciones más relevantes de los responsables de los sistemas del SNS. También explicó como estaba estructurado el programa y agradeció a todos, incluyendo a las empresas, por su ayuda para que pudieran realizar esta jornada de trabajo.

Nota: *Como ya hemos dicho en números anteriores de I+S, la gran cantidad de información que produce la SEIS es imposible resumirla adecuadamente en cada uno de nuestros números. Pedimos por ello disculpas a los lectores y advertimos, como es habitual, que el contenido completo de nuestras actividades pueden encontrarlo en la web de la Sociedad. www. seis.es*

Juan Fernando Muñoz felicitó a todos los que hicieron posible este Foro: "Martín, coordinador general de este Foro, y responsable de tecnología de Osakidetza, está en estos momentos en el Ministerio del interior, tratando temas de la gobernanza que es tan necesaria para la cooperación. Tenemos un elemento muy importante que son las llamadas estructuras críticas. Y hay que gobernar esas infraestructuras críticas porque todos somos interdependientes. Para poder gobernar esa situación, foros como este son absolutamente imprescindibles". Explicó que se habían establecido tres ámbitos: uno es la tecnología sanitaria, otro, las redes de cooperación, hoy centradas básicamente en enfermedades raras y muchos otros elementos y el tercer ámbito eran las tecnologías aplicadas a la sanidad.

"De este Foro esperamos poder sacar unas conclusiones que nos permitan ir un poco más allá en aquellos retos que nos ha planteado la comisión", puntualizó.

Patricia Gómez i Picard agradeció que se hubiera elegido Baleares para celebrar este Foro y esperó que no fuera la última vez. "A veces tengo un sentimiento agridulce debido a que Baleares fue pionera en los sistemas de información, en un momento dado de la historia. En el 2002, el hospital Son Llàtzer fue el primer hospital sin papeles, en el 2004 empezamos a trabajar con la historia clínica de primaria, en el 2007 ya se unieron más hospitales a trabajar con esa historia clínica y también fuimos la primera Comunidad Autónoma que trabajó con la receta electrónica. Todo esto culminó en el 2008 con una historia de salud. Luego vino una época de desinversión. En el 2015 hubo una apuesta muy clara por el avance. Creo que vamos a tener ocasión de que comparen lo que tenemos en relación con otros".

Nombró algunos de los hitos y algunas de las cosas que tenían pendientes, sacadas de su programa para el periodo 2015-2019. "Empezamos por un sistema de información poblacional único con los principales datos administrativos. La renovación en los sistemas de información en atención primaria es un reto. La implantación de la firma en la nube para la prescripción farmacéutica estará en breve. A finales de noviembre se podrá extender a todos los profesionales. La prescripción enfermera, con la que ya estamos a punto de poder entrar en el sistema de receta electrónica, se paró y lo hemos retomado e intentamos poder concluirlo. La radiología en red y el proyecto Sofía que trata de un sistema de información que para mí, como profesional, admiro y consulto muy frecuentemente, para conocer, de las consultas realizadas, cuáles son los resultados en salud, etc. También están trabajando en conseguir una historia clínica integrada, centrada en el paciente y armonizada. "

Antònia Salvà Fiol, subdirectora de Tecnología y

CONFERENCIA

Sistemas de Información, del Servicio de Salud de las Islas Baleares, presentó a Benjami Villoslada Gil, director general del Departamento Tecnológico de la Comunidad Autónoma de las Islas Baleares, que fue la persona que pronunció la conferencia inaugural de estas jornadas.

La conferencia se tituló "El Caos Existe". Habló de los orígenes humanistas de la tecnología digital y puso el proyecto de genoma humano como ejemplo de colaboración entre sanidad y tecnología digital. Citó a Douglas Engelbart que en los años 60 inauguró el Augmentation Research Center y manifiestó que el caos existe y ha estado siempre a nuestro alrededor.



SESIÓN DEBATE 1. "GOBERNANZA BASADA EN DATOS"



Jossue Sallent Ribes, director general de la Fundación TIC en Salud fue el moderador de la mesa. Indicó que nos encontramos con una cantidad ingente de todo tipo de datos y preguntó a los contertulios sobre cómo se está utilizando la información que tienen los servicios de salud y sobre si realmente éramos conscientes de ese poder, de cómo está organizado el papel de data oficcer. "¿Lo tienen o no vuestras organizaciones?, ¿Qué planteamientos estáis haciendo al respecto?", inquirió.

Posteriormente presentó a todos los que iban a formar parte de este debate:

Ruiz, responsable de la Innovación y Continuidad Asistencial de la Fundación Rioja Salud, de la Consejería de Sanidad y Consumo de La Rioja, Benigno Rosón Calvo, subdirector general de Sistemas y Tecnologías de la Información del Servicio Gallego de Salud, Luis Javier Bonilla, General Manager Iberia de Orios Health, Iñaki del Rio, director del Instituto de Innovación i3B, Marisa Felipe Gil, Industry General Manager, South Europa, Healthcare & Life Sciences. DXC, Javier Jarauta Sánchez, director de consultoría del grupo SIA y Biel Frontera Borrueco, gerente de la Fundación Balear de Innovación y Tecnología. Ruiz pidió a todos que contestaran brevemente a la pregunta formulada: ¿Cómo están utilizando la información las organizaciones que dan servicios de salud?

Habló en primer lugar Javier Jarauta que opinó que no se podía utilizar una inteligencia artificial genérica y que había que ver qué preguntas se hacían, de qué datos disponíamos y qué respuestas podíamos dar.

Por su parte Lola Ruiz, comentó que la gobernanza de las TIC está vinculada a la gobernanza de la gestión.

Luis Javier Bonilla, destacó que en España había tendencia a crear el puesto y luego su función.

Por su lado, Marisa Felipe Gil mostró su acuerdo con Bonilla y añadió que había muchos datos pero había que tener en cuenta la fragmentación. Mientras, Benigno Rosón explicó que "si tenemos la estrategia de lo que queremos hacer con nuestros datos, efectivamente tiene que ser una estrategia de gobernanza y al final aplicarlos a nivel de detalle y asegurarse de que lo que se ha definido como estrategia, se esté cumpliendo.".

Biel Frontera, citó a John Snow, padre de la epidemiología así como Florence Nightingale, la madre de la enfermería moderna, quienes ya en 1850 ayudaron a tomar decisiones basadas en sus datos.

Iñaki del Río señaló que en su empresa las áreas

de operación eran más sensibles al dato y las áreas de gestión eran más sensibles al trámite.

El moderador intervino para comentar que "siguiendo lo que ha dicho **Javier,** al final están los datos que son neutros y otra cosa es cómo los utilizamos, es decir los algoritmos de toma de decisiones".

Bonilla apuntó que "nuestro negocio como gestores de datos, es dar respuesta a esta enorme variación que tienen en la práctica asistencial", mientras **Lola** opinó que "estamos hablando de gobernanza de las TIC, gobernanza del dato, gobernanza de la información y parece que todo va de lo mismo".

Posteriormente, Marisa Felipe añadió que el retorno era la clave y **Jarauta** señaló que "el cambio de paradigma de lo que estamos hablando es que yo no necesito millones de datos para una toma de decisiones y para gobernar un sistema sanitario. Solo necesito x datos y muy concretos".

El moderador preguntó si tenía sentido que las plantillas de los centros médicos fueran flexibles. En este sentido, Benigno Rosón insistió en que quería hablar "del gobierno de datos en un sistema que genera información que todos hemos implantado con mejor o peor fortuna".

Bonilla señaló que "cuando hablamos del gobierno de los datos hay un problema de interoperabilidad que tiene un peligro y es que cuando tienes un dato malo y utilizamos sistemas muy interoperables se expande inmediatamente."

Después, con escaso tiempo como suele suceder, hubo alguna pregunta interesante de los asistentes, en la que intervino **Guillermo Vázquez** comentando que los ponentes no habían contestado bien al título de la mesa porque el título era Gobernanza basada en datos.

SESIÓN DEBATE 2. "LA AMENAZA DEL INTERNET DE LAS COSAS"



Pilar Barba Arranz, directora del CGIPC, del servicio Aragonés de Salud, fue la moderadora a la que acompañaban, **José Manuel Laperal**, responsable del Área de Seguridad (CISO) del Servicio Madrileño de Salud, **Alez Etxeberria Aranburu**, director general de la Sociedad de Informática del Gobierno Vasco- EJIE, **Carmen Ferrer Ripollés,** subdirectora de Sistemas de Información para la Salud de la Consejería de Sanidad Universal y Salud Pública de Valencia, **Carlos Hernando**, responsable del Área de Technology Consulting de Accenture Health, **Luis Miguel Garrido**, Manager Major Accounts. Fortinet y **Miguel Ángel Montero Martínez**, director de Sanidad y Servicios Sociales de Informática de El Corte Inglés.

Pilar Barba Arranz dio a cada ponente 5 minutos para que explicaran su posicionamiento con respecto el tema de la mesa.

Luis Miguel Garrido destacó los miles de millones de dispositivos que había, muchos de los cuales se encontraban en el ambiente hospitalario, lo que dificultaba la seguridad.

Sin embargo, aseguró Carmen Ferrer, que los que utilizaban este tipo de dispositivos, en el ambiente sanitario, lo hacían para mejorar la calidad de vida. También puso énfasis en las cuestiones relacionadas con la seguridad y con la integridad de la información.

Miguel Ángel Montero señaló que lo digital afectaba a la relación con el paciente y merecía la pena ser cuidadosos y opinó que habría que hablar de medical things.

Por su parte, Carlos Hernando destacó que se podría mejorar el día a día del paciente y también mejorar su gestión. Además, Alex Exchevarria explicó la visión que se intentaba afrontar desde el Gobierno Vasco que era conseguir compartir infraestructuras y redes.

Pilar Barba, la moderadora, pidió a los ponentes abrir más el tema y debatir como gestionar los aparatos. En este sentido, Carmen Ferrer comentó un proyecto que era utilizar IoT para los parches de diabéticos que suben información a la nube.

Laperal explicó que al tener tantos dispositivos íbamos a tener muchísimos datos de los cuales podía salir información del paciente más importante que la contenida en su propia anamnesis.

Según Miguel Ángel Montero había cosas que se podían mejorar dentro de un hospital que era un sitio grande y caótico y citó múltiples aplicaciones basadas en IoT.

Pilar Barba preguntó a los debatientes si consideraban que había que guardar todos los datos o agruparlos según su interés mientras que

Carlos Garrido opinó que debería haber lo que él denominaba Ingeniero Científico de datos.

SESIÓN DEBATE 3. "NUEVOS RETOS PARA LA TRANSFORMACIÓN DIGITAL"



El moderador fue José Antonio Alonso Arranz, director general de Sistemas de Información Sanitaria, del Servicio Madrileño de Salud. Participaron en el debate José Luis del Val Román, catedrático de la Facultad de Ingeniería de la Universidad de Deusto, José Luis Monteagudo Peña, director del Master de Sistemas y Tecnologías de la Información y las Comunicaciones

para la Salud, Santiago Thovar Bermejo, subdirector de Sistemas de Información del Servicio extremeño de Salud, Manuel Escudero Sánchez, subdirector general de Tecnologías de la Información del Servicio Murciano de Salud, Ángel Blanco Rubio, director corporativo de Organización, Procesos Tic y Digital QuironSalud, Carlos Córdoba, asesor del Departamento de Ciberseguridad del Centro Criptológico Nacional y Alexandre Bento, Comercial Sales Manager de VMWare Iberia.

El moderador empezó el debate dando 4 minutos a cada ponente para que expresasen una primera opinión sobre el tema.

Ángel Blanco destacó que "estamos en un verdadero cambio social y nuestra profesión desaparece. Empiezan profesiones nuevas". Por su parte, Carlos Córdoba señaló que "antes en cada lugar teníamos un responsable de seguridad, un responsable de la información, ahora aparece la figura del delegado de protección de datos. Todo esto hay que armonizarlo".

Santiago Thovar explicó que "hace algunos años éramos nosotros los que intentábamos dinamizar a la organización para decir que se modernizara. Hoy somos nosotros los que no somos capaces de responder al ritmo que nos exigen." Durante su intervención Alexandre Bento insistió en que hay que adaptar la enseñanza a la situación actual. En su opinión la educación era la base.

Manuel Escudero, señaló "que la educación debe alinearse con el mercado. Evoluciona más rápido la necesidad que la capacidad de las instituciones para cambiar."

José Luis del Val admitió que estaba encantado al oír decir que el negocio más importante era el suyo, es decir, el de la formación, mientras que José Luis Monteagudo mencióno la dificultad, complejidad y compromiso.

> ***"Antes en cada lugar teníamos un responsable de seguridad, un responsable de la información, ahora aparece la figura del delegado de protección de datos. Todo esto hay que armonizarlo"***

Después de haber dado todos los participantes una primera opinión, José Antonio Alonso, inició el debate preguntando si era necesario crear nuevos perfiles.

Ángel Blanco puntualizó que no y que había que hablar de talento y de iniciativa. Por su parte, Carlos Córdoba habló de la gestión mixta y de la búsqueda de talento aunque era difícil encontrarlo en ciberseguridad, mientras que Monteagudo se resistió a pensar que debían inventar otros.

El moderador, volviendo al desarrollo de las competencias, preguntó cómo pensaban que se podían medir y como podían abordar el desarrollo de las mismas.

Ángel Blanco opinó que el liderazgo no era incompatible con la estructura. "Pienso que la estructura como la seguridad la puedes utilizar para avanzar o para justificarte".

En esta ocasión, Monteagudo intervino para decir que las organizaciones sanitarias eran muy complejas y eran organizaciones de aprendizaje.

Thovar destacó que la gestión de recursos humanos era lo más complicado. "Tenemos que aprender a aprender, porque estamos en un continuo cambio".

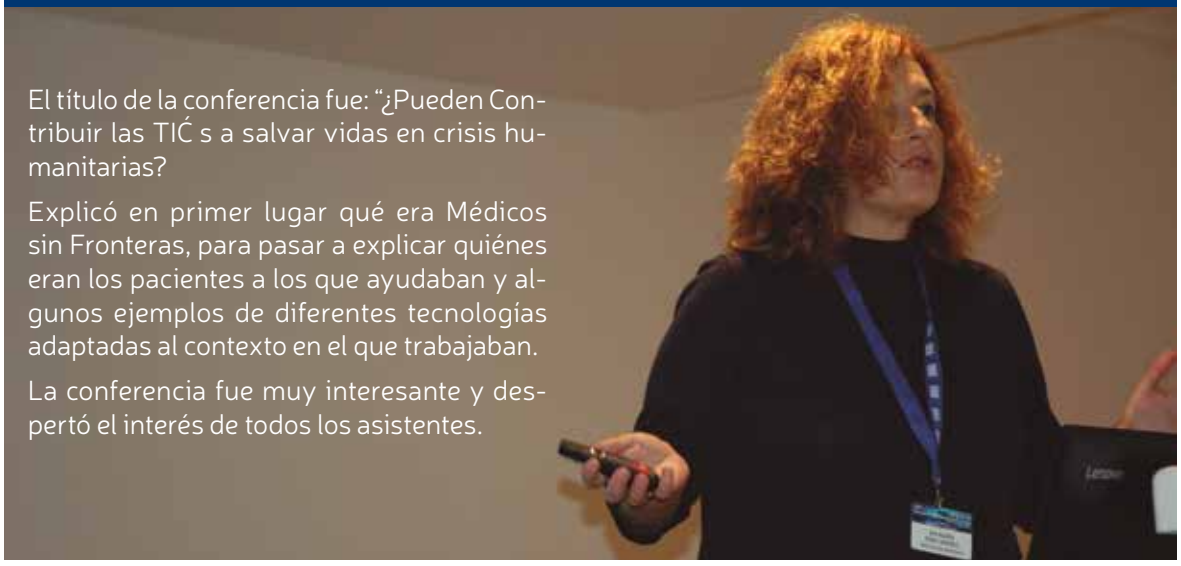
José Antonio Alonso preguntó qué se podía hacer para recuperar el interés y la demanda para que asistan mujeres. Por su parte, Thovar, señaló que el trabajo lo hacían mejor las mujeres.

Monteagudo, quiso llevar la contraria y subrayó que había muchos factores y elementos sociales que solían escaparse. "Falta una cultura general. En ingeniería no parece que las mujeres estén muy inclinadas", indicó.

Por su lado, Espinosa opinó que la preparación que reciben nuestros hijos no era suficiente para abordar una carrera técnica.

Juan Fernando Muñoz Montalvo, presentó a Milagros Font Jiménez, delegada de Médicos sin Fronteras en la Comunidad Valenciana, Cataluña, Baleares y Región de Murcia.

SEGUNDA CONFERENCIA



El título de la conferencia fue: "¿Pueden Contribuir las TIĆ s a salvar vidas en crisis humanitarias?

Explicó en primer lugar qué era Médicos sin Fronteras, para pasar a explicar quiénes eran los pacientes a los que ayudaban y algunos ejemplos de diferentes tecnologías adaptadas al contexto en el que trabajaban.

La conferencia fue muy interesante y despertó el interés de todos los asistentes.

ACTO DE CLAUSURA



Estuvo presidido por **Juli Fuster Culebras**, director general del Servicio de Salud de las Islas Baleares, al que acompañaron **Martín Begoña Oleaga**, coordinador general de la VIII Reunión del Foro para la Gobernanza de las TIC en Salud y **Antonia Salvà Fiol**, subdirectora de Tecnología y sistemas de Información, del Servicio de Salud de las Islas Baleares.

Martín Begoña recordó la magnífica conferencia de Benjamín Villoslada Gil y mencionó las tres sesiones de debate que compusieron la VIII Reunión. Igualmente felicitó a Milagros Font por su conferencia.

Antonia Salvà tuvo palabras de agradecimiento para todos los Comités que habían intervenido y dio la enhorabuena a todos los ponentes y moderadores. También apuntó que la mesa que más le había gustado era la tercera: "Nuevos roles de profesionales para la transformación digital".

Juli Fuster dio las gracias a todos los que hicieron posible este acto. "Cuando Antonia nos planteó este evento nos volcamos, porque pensamos que estaba dentro de la línea de avance" y declaró que la reunión quedaba clausurada.

XVI FORO DE SEGURIDAD Y PROTECCIÓN DE DATOS DE SALUD

EL HOSPITAL RÍO ORTEGA DE VALLADOLID ACOGIÓ LOS DÍAS 6 Y 7 DE FEBRERO, EL XVI FORO DE SEGURIDAD Y PROTECCIÓN DE DATOS DE SALUD DE LA SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD, CON EL TÍTULO "SEGURIDAD Y PROTECCIÓN DE DATOS EN EL TRATAMIENTO DE DATOS DE SALUD A GRAN ESCALA".

ACTO INAUGURAL



El foro estuvo presidido por Antonio María Sáez Aguado, consejero de Sanidad de Castilla y León. En primer lugar, Luciano Sáez dio la palabra a José Miguel García Vela, gerente del Hospital quien agradeció que la SEIS celebrara este acto en el Río Ortega. En su intervención apuntó que la protección de datos se ha realizado siempre en el hospital y confió en que la SEIS siguiera adelante con este tema porque era de máxima actualidad.

A continuación, Luciano Sáez, presidente de la SEIS, pronunció unas palabras agradeciendo, en primer lugar, al hospital y a la Consejería el apoyo que habían prestado a la SEIS para la celebración del foro. Igualmente valoró la ayuda de la Agencia Vasca y la Autoridad Catalana de protección de datos, y muy especialmente de la Agencia Española. También incluyó en este capítulo de agradecimientos al Consejo de Transparencia y Protección de datos de Andalucía.

Agradeció al Consejero su presencia en la inauguración así como a Mar España, directora General de la Agencia Española, lo cual demostraba su sensibilidad y la importancia que otorgaba al Foro. También destacó la presencia de Margarita Uría, directora de la Agencia Vasca, de Santiago

Nota: *Como ya hemos dicho en números anteriores de I+S, la gran cantidad de información que produce la SEIS es imposible de resumir adecuadamente en cada uno de nuestros números. El contenido completo de nuestras actividades pueden encontrarlo en la web de la Sociedad: www. seis.es*

Farré que representó a la autoridad catalana de Protección de Datos y de Manuel Medina Guerrero, presidente del Consejo de Transparencia y Protección de Datos de Andalucía. Igualmente dio las gracias al gerente del Hospital.

Explicó que la SEIS creó en el año 2004 el Foro de Protección de Datos con la idea de disponer de un espacio de encuentro desde el cual poder defender los derechos de las personas y sobre todo de los ciudadanos y con el fin de compartir experiencias y conocimiento para asegurar una atención sanitaria de calidad.

También señaló que había que potenciar el uso de las tecnologías de la información y comunicaciones para proteger, entre otras cosas, la seguridad que era un concepto vital para la implantación de los sistemas de información en salud.

Después tuvo palabras de agradecimiento para Juan Díaz, coordinador del Comité Técnico de Seguridad de la Información de Salud y a todos sus miembros provenientes de todas las CCAA.

Esta edición se centró en un tema de máxima actualidad como era el tratamiento de los datos de salud a gran escala. En este sentido alabó la implicación de las empresas que con su conocimiento y patrocinio habían ayudado a celebrar el Foro, agradecimiento que hizo extensivo a todos los que de una u otra manera habían colaborado con su esfuerzo en la organización de este acto y a todos los asistentes.

A continuación, Manuel Medina Calvo intervino para, en primer lugar, hacer una breve reseña de la historia del Consejo de Transparencia y Protección de Datos en Andalucía, indicando que "hemos sido testigos de cómo se iba regulando y consolidando el marco normativo de la regulación de los datos en el ámbito de la salud. Tenemos ya un marco jurídico consolidado y estable". Agradeció la invitación y esperó que el Foro fuera fructífero para todos los presentes.

Santiago Farré agradeció a la SEIS que un año más invitaran a la Autoridad Catalana de Protección de Datos. "Huelga decir que la seguridad de los datos de salud para nosotros tiene una enorme importancia. La seguridad de la información es un elemento esencial. Una no adecuada identificación de los riesgos de las medidas de seguridad que debemos aplicar puede impedir la viabilidad del propio tratamiento. Hay que gestionar los riesgos lo que implica analizar muchas variables", puntualizó.

Margarita Uría Etxebarría, dio las gracias a los diferentes comités que habían intervenido y habían hecho posible un Foro que estaba totalmente consolidado. "La Agencia Vasca está presente no sólo en esta inauguración sino también en las diferentes mesas que se van a celebrar". Asimismo consideró que el contenido de las jornadas era muy interesante y esperó que se pudieran obtener importantes conclusiones en todos los debates. Hizo comparaciones interesantes entre el Foro del pasado año y el actual y agradeció de nuevo a la SEIS la organización de estas Jornadas.

Mar España, directora de la Agencia Española de Protección de Datos, ofreció una interesante exposición que, por su interés, calidad y extensión, resulta imposible resumir sin citar todos los puntos importantes que mencionó durante su intervención. La ponencia completa puede encontrarse en la web de la SEIS.

En primer lugar, manifestó el absoluto respeto y admiración a los profesionales de la salud porque con una absoluta profesionalidad y vocación de servicio dedicaban todo su trabajo y entusiasmo a la asistencia a los pacientes para que nuestra salud fuera lo mejor posible. Destacó también las implicaciones del marco normativo de este nuevo reglamento de carácter europeo y habló de salud y privacidad, que eran dos conceptos muy interdependientes que afectaban a los profesionales del sistema sanitario español, uno de los mejores a nivel mundial.

En este punto recordó que, de forma tradicional, la Sociedad Española de Informática de la Salud tuvo el reconocimiento y la colaboración de la Agencia por su intensa actividad en la promoción y difusión del derecho a la protección de datos en el sector sanitario, en el que se estaba llevando a cabo una actividad pionera al producirse cambios normativos sobre este derecho.

La Directora explicó el plan estratégico de la Agencia Española de Protección de Datos, que desde el 2015 incluía acciones sobre la sanidad y servicios sociales. Recientemente se inspeccio-

nó un centro del Imserso, otro de una CCAA, y un centro de personas de avanzada edad con alzheimer, dentro del Plan General de Inspección.

Respecto a la historia clínica comentó que era necesario en algunos casos y con absoluta garantía, tener que consultar la información contenida en ellas, por lo que en foros de seguridad y protección de datos como el actual se podían plantear y resolver problemas, dudas y se podía llegar a unas conclusiones. Estas podían estar relacionadas con el intercambio de determinados datos, del acceso a determinada información para que desde la Agencia pudieran valorarlo y en su caso incorporarlo a los proyectos relacionados que se están desarrollando, para ayudar y facilitar el cumplimiento con las mejores garantías.

Sobre la ley orgánica, aprobada en diciembre, se explicó que tenía varias disposiciones que regulaban el ámbito de la salud, destacando el punto décimo séptimo que era precisamente el que tenía que ver con la legitimación del uso de datos por interés público.

La Directora, más adelante, hizo referencia a algunas otras disposiciones desarrolladas en la ley e hizo un llamamiento a la responsabilidad ACTIVA que implicaría que los servicios de salud debían establecer su registro de actividades de tratamiento, que sustituían a la obligación de comunicar los ficheros a la Agencia; realizar un análisis de riesgo tanto para la seguridad de los datos como para los derechos de los ciudadanos; implantar medidas de seguridad adecuadas y establecer procedimientos de notificación de brechas de seguridad; llevar a cabo evaluaciones de impacto en la protección de datos personales y designar un delegado de protección de datos.

También destacó la principal actuación en el ámbito de salud, que fue la conclusión del Plan de Inspección Sectorial de hospitales públicos y la presentación de sus conclusiones a las comunidades autónomas en colaboración con el Ministerio de Sanidad, Servicios Sociales e Igualdad. Esta inspección teníaun carácter preventivo e incluía un conjunto de recomendaciones así como un decálogo dirigido al personal sanitario y administrativo con el fin de mejorar la seguridad en los centros sanitarios. Esta colaboración con el Ministerio sirvió también para facilitar información a los responsables de servicios sanitarios sobre las implicaciones del Reglamento General de Protección de Datos.

Antonio María Sáez Aguado tomó la palabra para dar a todos la bienvenida a Valladolid y al Hospital Río Ortega y señaló que abordar en este foro la importancia de los temas que van a ser tratados estaba fuera de toda duda. "Los servicios autonómicos de salud y en general el servicio nacional de salud no estaban bien preparados para la aplicación del reglamento y cuando alguien dice que hay un nuevo reglamento que va a entrar en vigor, muchos pensaron que habría que esperar a que llegara creyendo que no era algo tan próximo. Los días anteriores al 25 de mayo hubo una serie de nombramientos masivos de los delegados de protección de datos porque ya era imprescindible y, a partir de ahí, el conjunto del sector público y el del privado nos hemos involucrado en esta tarea compleja, sobre todo en el sector sanitario que acumula tantos datos. Por eso me parece especialmente importante que se hable de seguridad y tratamiento de los datos de salud porque es el sector que tiene más datos concentrados. La Agencia Tributaria y el sector bancario también disponen de muchos datos pero son limitados", subrayó.

Continuó su intervención explicando que "en un debate que se produjo en la tramitación de la Ley Orgánica, algunos investigadores consideraron que el texto del proyecto de ley que se había presentado era más restrictivo que el reglamento y ponía en peligro, por consiguiente, el análisis de los datos en la medida en que se interpretaba que pudiera necesitarse un consentimiento expreso para el tratamiento de los datos, lo cual impedía la utilización masiva de esta información porque masivamente existían esos conocimientos informados. En este aspecto citó el proyecto Harmoni que cuenta con 53 entidades y múltiples sociedades científicas, fundamentalmente de hematólogos. Es un proyecto que tiene previsto albergar datos de 80.000 pacientes que han sido diagnosticados de algún tipo de cáncer. En este mismo hospital se están ya desarrollando otros proyectos".

También citó los conceptos principales que iban a ser tratados en el Foro y que tenían una enorme relevancia: "Creo que, en general, el personal sanitario todavía no es consciente de que tienen una información que no conforma una idea suficientemente avanzada de lo que representa la confidencialidad y de las consecuencias de determinadas actuaciones". Finalmente reiteró la felicitación y el agradecimiento a la SEIS por volver una vez más a este hospital y declaró inaugurado el XVI Foro de Seguridad y Protección de datos de salud".

La mesa estuvo moderada por Susana García Dacal, directora general de Infraestructuras y Tecnologías de la Información del Servicio de Salud de Castilla y León.

PRIMERA MESA REDONDA



"Soluciones de seguridad ante el tratamiento de datos de salud"

Los ponentes fueron Ramsés Gallego, Strategist & Evangelist, Office of the CTO. Symantec, con la intervención: "No es Transformación Digital. ¡Es Innovación Radical!" Fue una ponencia excelente en la que citó a Dick Cheney: "Todo está yendo a la Innovación Digital. Freedom is not free".

Jaime Solar Pedrola, Senior Manager de Accenture Security, participó con: "Nuevas tendencias tecnológicas para la protección de datos" y destacó: "En Sanidad es donde se tratan datos sensibles y críticos, necesarios para predecir enfermedades, monitorizar a los pacientes, descubrir nuevos fármacos, seguimiento del paciente en tiempo real e historial médico on line avanzado".

Oscar Riaño de Antonio, Responsable del CERT de GMV, habló sobre: "Incident Response: ¿estamos preparados?, donde señaló que "un centro tiene 4 pilares básicos: prevención, detección, respuestas y post incidente (análisis forense)".

Zulayka Vera Uruena, líder del Área de Consultoría de Seguridad de la Información y Punto Focal de GDPR para España y Portugal. IBM Security, intervino con :"Ciberataques: Una nueva pandemia", de la que subrayó: "El ciberataque es una nueva pandemia. Robar datos de salud es el doble de rentable que robar datos bancarios". Juan Cornago Baratech, Senior Manager de las áreas de GRC y Resiliencia. SIA, participó con "La certificación de las medidas de seguridad en la Sanidad Pública". Hizo su presentación desde un punto de vista innovador, comentando los antecedentes de la estrategia de la seguridad nacional de 2013 y citó la Ley Pic de protección de infraestructuras críticas.

Por último, Alfredo Díaz, Responsable de Ciberseguridad. Oesia, participó con: "Oficinas de Seguridad en el sector Salud", quien dio un enfoque estratégico para seguridad y explicó cómo funcionaban sus oficinas de seguridad.

SEGUNDA SESIÓN DE DEBATE



"El ciudadano y el tratamiento masivo de sus datos de salud"

La sesión fue moderada por Santiago Farré Tous, jefe de la Asesoría Jurídica de la Autoridad Catalana de Protección de Datos.

Los ponentes fueron Teresa Garrote Sastre, médico de admisión CA de Zamora, quien puntualizó que ignoraba lo que representaría el tratamiento masivo de los datos, un hito importante que va a marcar la relación del médico con el paciente, que debía estar informado y, por tanto, tener acceso a los datos.

El ponente Josep Ma Busquets i Font, secretario de la Comité de Bioética de Catalunya, destacó que "estamos trabajando en este tema pero también deberíamos hacerlo en los comités de ética asistencial" y admitió la gran cantidad de autorizaciones que tiene que firmar el paciente.

José Luis Almudí Alegre, presidente del Colegio de Médicos de Valladolid, puntualizó que acudía como médico de atención primaria y no como presidente del Colegio de Médicos. "El ser médicó de primaria me da una perspectiva de conjunto de toda la información y los datos de salud que giran alrededor de los pacientes. Dispongo de datos no solo de su salud, sino también de su entorno y de su familia y también de su relación con otros proveedores como puede ser el hospital. También de todas las interacciones que tiene ese paciente con la mensajería instantánea, con las APP, etc. En general recibimos a nuestros pacientes muy bien informados aunque en algunos casos, pocos, no es así", explicó.

TERCERA SESIÓN DE DEBATE

"La Seguridad y Confidencialidad ante el tratamiento de datos de salud a gran escala"

El moderador fue José Luis Falcón Pliego, jefe del Gabinete de Publicidad Activa y delegado de protección de datos del Consejo de Transparencia y Protección de datos en Andalucía.

Actuó como ponente Juan Díaz García, coordinador del Comité Técnico de Seguridad de la Información de Salud, quien subrayó que "la sesión del Comité Técnico en la que participan los Responsables de Seguridad de las diferentes Comunidades Autónomas y Organismos



relacionadas con la Seguridad y Protección de Datos, entre los puntos tratados, se plantea cómo afrontar la problemática de la gestión de Incidentes, los encargados de Tratamiento en Salud, así como los códigos de conducta y el valor de las certificaciones para proveedores en el marco del ENS".

Por su parte, Jorge Prado Casal, jefe de Servicio de Soporte e Implantación del Servicio Gallego de Salud, hizo una puntualización interesante: "hablamos de seguridad y de confidencialidad cuando la seguridad son tres cosas, la confidencialidad la integridad y la disponibilidad". También destacó aspectos generales de la seguridad en el marco de la salud y habló de tres retos actuales: "el que se presenta cuando los usuarios nos piden sus datos. Otro sería las capacidades de relación de análisis de datos y la movilización de los datos".

Por su parte, Javier Candau, jefe del Departamento de Ciberseguridad CCN preguntó a los asistentes cuántos de ellos tenían teléfonos amber. Se interesó después por cuántos tenían iphone, para posteriormente, después de ver que la mayoría de los asistentes estaban en Facebook o en otras redes sociales, decirles que no podían quejarse de que los datos no tuvieran la suficiente protección cuando se estaban prodigando. Durante la intervención, la agencia vasca preguntó si podían fiarse de los informáticos, un tema sobre el que el delegado de protección de datos y los compañeros de mesa aludieron a la confidencialidad, integridad y disponibilidad, sin olvidar la trazabilidad y la autenticidad. Puntualizó también que "los servicios de salud tienen que darle al ciudadano la confianza suficiente".

Juan Carlos Muria, subdirector del S2 Grupo, quiso dar un enfoque de arriba abajo y habló primero de los factores determinantes de la salud. Destacó que en la asistencia sanitaria impacta mucho más la genética. "Hablamos de big data y de tratamiento masivo de pacientes pero eso es solo la punta del iceberg, por otro lado si se trabaja con inteligencia artificial habría que utilizar datos de otras fuentes. Todo esto, al final compagina muy bien con las funciones de la práctica clínica y también la reglamentación y gestión. La pregunta es, ¿nos basta la historia clínica del paciente? Tendremos que incorporar algunos datos. En los últimos años se utiliza un término que proviene del mundo militar: "VUCA", que es un entorno volátil, "incierto (uncertainty) complejidad (complexity) y ambiguo".

Muria también recordó lo difícil e importante que era el uso de los datos de los pacientes porque "cuando se habla de la seguridad de los datos realmente se está hablando de la seguridad del paciente", matizó. Posteriormente tuvo lugar un interesante coloquio entre ponentes y asistentes.

CUARTA SESIÓN DE DEBATE



Casos prácticos:
"la experiencia de las autoridades de protección de datos"

Moderó la sesión Pedro Alberto González González, responsable del Registro y Auditoría de Ficheros de la Agencia Vasca de Protección de Datos. Esta mesa fue la más entretenida porque los ponentes explicaban casos reales que se habían presentado en las agencias que intervinieron y que fueron hábilmente presentados por el moderador.

Actuaron como ponentes, Juana Mª Vegas Fernández, letrada de la Asesoría Jurídica de la Agencia Vasca de Protección de Datos, que habló del principio de minimización e hizo comentarios sobre el derecho de cancelación.

Por su parte, Carles San José i Amat, jefe del Área de Inspección de la Autoridad Catalana de Protección de Datos, intervino para comentar el derecho de acceso y detalló un caso a propósito del derecho de cancelación. Posteriormente, habló sobre las medidas de seguridad.

Cristina Gómez Piqueras, inspectora - instructora de la Subdirección General de Inspección de Datos de la Agencia Española de Protección de Datos, comentó el caso de una mujer operada por un traumatólogo que pidió grabar la intervención con fines didácticos. Después de unos meses, la enferma solicitó ver la grabación pero el médico argumentó que era privada, mientras la Agencia puntualizó que no.

Los tres ponentes relataron casos problemáticos y la forma en que se resolvieron. Finalmente, Pedro Alberto González, intervino en el tema del acceso a la historia clínica de personas que no están relacionadas con los pacientes, lo que dio lugar a que se expusieran casos de gran interés.

QUINTA SESIÓN DE DEBATE

"La figura del DPD en las organizaciones sanitarias"

Moderó el debate Rosario Heras Carrasco, responsable de la Unidad de Evaluación y Estudios Tecnológicos de la Agencia Española de Protección de Datos.

Participaron los ponentes, José Ignacio Sánchez Brezmes, delegado de Protección de Datos de la Gerencia Regional de Salud de Castilla y León, quien comenzó a explicar las funciones del DPD y dar su opinión sobre la base de su propia experiencia. También planteó la cuestión sobre si en el conjunto de las administraciones públicas el sector sanitario debía tener DPD. "Es importante tratar de lo que dice el art. 9 en cuanto a la categoría de los datos ya que se piensa que dentro de la categoría



de especiales los datos de salud son los más especiales", aclaró.

Por su parte, Núria Alberich Margalef, responsable del Área de Protección de Datos y DPO Consorci de Salut i Social de Catalunya, comentó que el 2019 "plantea que se estudie cuál es la situación actual de la ley implantada". Presentó las características que debe tener el DPD y enumeró tres puntos que consideraba importantes: revisar el registro, revisar el protocolo de acceso de los trabajadores y revisar el protocolo de archivo.

Vicente Andreu Navarro, delegado de Protección de Datos de la Generalitat Valenciana explicó como estaba diseñada la delegación de la protección de datos en la Comunidad Valenciana y las ventajas que tenía el modelo que han implantado, con un equipo que se empezó a crear en junio y actualmente está conformado por 5 personas.

SEXTA SESIÓN DE DEBATE



"La figura del DPD en las organizaciones sanitarias"

Moderó la sesión Ana Aperribai Ulacia, responsable de la Asesoría Jurídica de la Agencia Vasca de Protección de Datos. La ponente, Cristina Dietrich Plaza, responsable de Proyectos Normativos y Estudios Jurídicos de la Autoridad Catalana de Protección de Datos, explicó que "tuvimos recientemente una consulta de un centro hospitalario sobre la relación con el monitor de un ensayo clínico. Partiendo de la base de que el hospital es el responsable de la historia clínica, en este caso pensamos que tanto el hospital como el promotor tenían responsabilidad en este tratamiento de datos que tiene que ver con la realización del ensayo clínico, ya sean

datos propiamente de la historia clínica propia o de la autonomía del paciente".

Por su lado, **Andrés Calvo Medina**, jefe de Área de Informática de la Agencia Española de Protección de Datos señaló que "si nos vamos al año 1995, cuando aparece la directiva, para saber si una persona es identificable, hay que promocionar el conjunto de medios razonables utilizados para llevar a cabo el objetivo de identificar a la persona".

Roberto Bilbao Urquiola, director científico de Biobanco Vasco detalló que "en el biobanco se encargan de gestionar todas las muestras y datos asociados que se recogen en Osakidetza. Desde 2004 hasta hoy hemos ido pasando por las diferentes normativas que nos han ido afectando y que han ido cambiando la manera de trabajar con muestras. Hace unos años contactan con nosotros desde Europa para comunicarnos que hay una convocatoria europea del horizonte 2020 sobre proyectos de big data y salud pública. Se aceptó la propuesta y promovimos el proyecto dentro del País Vasco. Nos presentamos y nos lo dieron. Básicamente este proyecto pretende crear una plataforma con bases de datos y software para el análisis de los mismos y obtener información para beneficiar a los pacientes en 5 países europeos. En el país vasco nos interesamos por la obesidad infantil".

José María Lacalle, responsable de los sistemas en la nube de la AEMPS, explicó que "quizás, en nuestro caso, lo más importante sea conseguir el consentimiento del interesado. Tomando como base el reglamento los hemos agrupado en cuatro áreas principales. La seguridad, que es el punto que más nos interesa, la contemplamos desde el inicio implantando sistemas seguros". Para terminar habló de BIFAP es una base de datos informatizada de registros médicos de Atención Primaria para la realización de estudios fármaco epidemiológicos, perteneciente a la AEMPS.

Por otro lado, **Amelia Martín Uranga**, responsable de la Plataforma Tecnológica Española de Medicamentos Innovadores Farmaindustria, intervino destacando que "hay un elemento que ha sucedido en estos días y en este informe del comité europeo de protección de datos que habla específicamente sobre la interrelación entre el reglamento de protección de datos y el reglamento de ensayos clínicos. Creo que ha aclarado mucho el panorama sobre el que se ha escrito en los últimos años", e insistió en que el consentimiento es clave en el ámbito de los ensayos clínicos.

CLAUSURA



Estuvo presidida por **Rafael López Iglesias** quien estuvo acompañado por **José Miguel García Vela**, gerente del Hospital Río Hortega, **André Calvo Medina**, de la Agencia Española de Protección de datos y **Juan Díaz**, coordinador General del Foro.

Todos pronunciaron unas breves palabras con las que avalaron el éxito alcanzado en este Foro, tanto por la calidad de las intervenciones como por los temas tratados. En su intervención, Juan Díaz hizo un breve resumen de todas las mesas y Rafael López Iglesias clausuró el acto.

XXIV PREMIOS NACIONALES DE LA INFORMÁTICA DE LA SALUD 2018



EL PASADO 17 DE ENERO TUVO LUGAR EL ACTO DE ENTREGA DE LA VIGÉSIMO CUARTA EDICIÓN DE LOS PREMIOS NACIONALES DE INFORMÁTICA DE LA SALUD. COMO VIENE SIENDO HABITUAL, 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 Estrategia Digital de la SEIS, que se dirigió a los asistentes dando la bienvenida a todos y agradeciendo su asistencia. En especial se dirigió a Pilar Aparicio Azcárraga, directora general de Salud Pública, Calidad e Innovación del Ministerio de Sanidad, Consumo y Bienestar Social; Juan Antonio Vargas Núñez, decano de la Facultad de Medicina de la Universidad Autónoma de Madrid, que generosamente nos ofrece su hospitalidad y hace posible que hoy estemos reunidos, un año más, en este magnífico entorno académico y científico; Javier Ortega García, vicerrector de Innovación, Transferencia y Tecnología de la Universidad Autónoma de Ma-



drid; José Ramón Zárate Covo, subdirector de Diario Médico/Correo Farmacéutico; Javier Olave Lusarreta, vicepresidente de la Asociación de la Prensa de Madrid y María José Marzal, directora de ComputerWorld, por su participación en este Acto que inicia las actividades de la Sociedad Española de Informática de la Salud cada año."

Seguidamente Zaida Sampedro dio paso a Pilar Aparicio Azcárraga, Juan Antonio Vargas Núñez y Luciano Sáez Ayerra.

En primer lugar Juan Antonio Vargas, pronunció unas palabras destacando que este año era muy importante para la Facultad, ya que cumplía 50 años desde su fundación y que, como institución, se sentía muy honrada de poder albergar, un año más, la entrega de premios de la SEIS.

Luciano Sáez dió "la bienvenida a todos y agradeció la presencia de autoridades y directivos del sistema sanitario, de la Universidad y presidentes y representantes de asociaciones profesionales, científicas y empresariales. A lo largo de su intervención destacó que "Es de gran importancia, para la innovación en nuestro sector, la labor de difusión de las tic en salud" y también señaló la necesidad de "promover el cambio cultural que los profesionales del ámbito sanitario deben asumir con el fin de incorporar a la práctica diaria la innovación tecnológica".

Pasó a enumerar los logros alcanzados durante 2018 y las acciones que se realizarán durante 2019. Añadió que por su importancia debo resaltar el convenio marco de colaboración con el Ministerio de Sanidad, Consumo y Bienestar Social firmado este pasado año con el objetivo general de analizar, impulsar y evaluar la transformación digital en el ámbito de la salud." Manifestó, en nombre de la SEIS, "nuestro agradecimiento y compromiso con el Ministerio para colaborar en todo aquello que consideren podamos ser de utilidad."

Señaló que la SEIS contara con "Observatorio que permita presentar la situación y evolución de la innovación en el SNS; por ello ofrecemos anualmente desde 2012 el índice SEIS, trabajo que realizamos conjuntamente con los responsables de sistemas de las 17 CC AA y del Ministerio de Sanidad y red.es, y que nos permite conocer la situación real de la inversión en sistemas de información. En estos momentos se está elaborando el índice correspondiente al 2018, del que esperamos poder ofrecer sus resultados en el próximo congreso nacional de informática de la salud en el mes de marzo."

Seguidamente intervino Pilar Aparicio que, después de un amplio capítulo de agradecimientos, comentó que "La informática es una disciplina indispensable para los directivos de las organizaciones sanitarias, pero también para los pacientes y usuarios constituyendo una de las principales fortalezas de los nuevos sistemas de gestión sanitaria.

"Somos plenamente conscientes de todas estas necesidades en el Ministerio de Sanidad donde valoramos continuamente el apoyo que hemos recibido de la Sociedad Española de Informática de la salud para el desarrollo de las TIC en los sistemas sanitarios públicos españoles. No podemos olvidar que la sanidad pública sigue siendo un ámbito de actividad clara y como nos ha comentado recientemente Luciano Sáez, para la SEIS y para todos sus asociados. Nuestro Ministerio con el concurso y la cooperación de los servicios de salud de las CC AA, que es un claro exponente de la apuesta por la innovación que el desarrollo informático que ha conseguido hacer realidad la interoperabilidad de datos dentro del sistema nacional de salud. Interoperabilidad que es soportada tecnológicamente por el Ministerio desde donde coordinamos todo lo que sea más necesario y útil como la historia clínica digital y la receta electrónica", dijo.

Acto seguido Zaida Sampedro dio lectura al acta del Jurado, citando a todos los premiados así como los merecimientos para recibir el premio.

La Mención Honorífica de Informática y Salud 2018, a la Organización que ha realizado un mayor esfuerzo tecnológico para desarrollar soluciones en el sector sanitario.

Otorgado a Grupo Hospitalario HLA, por su apuesta decidida por la innovación tecnológica y la eficiencia en el uso de las TIC al servicio de la salud, con repercusión en aspectos como la reducción del coste, el incremento de la productividad o la mejora del rendimiento y garantía de seguridad. Recogió el premio el Dr. Benito García-Legaz, director médico de HLA Grupo Hospitalario. Fue entregado por Mª José Marzal, directora. ComputerWorld.

1. Premio Nacional de Informática y Salud 2018, a la Entidad Pública o Privada que ha destacado en proyectos de transformación digital en el ámbito sanitario.

Otorgado a la Dirección General de Investigación, Innovación, Tecnología y Calidad. Conselleria de Sanidad Universal y Salud Pública de la Generalitat Valenciana, por su contribución a la mejora de la atención sanitaria mediante el desarrollo de acciones en ejes estratégicos como la seguridad de la información, el uso racional del medicamento o la integración de la información de salud. Recogió el premio Ana Mª Ávila Peñalver, directora general de Investigación, Innovación, Tecnología y Calidad, con competencia, entre otras, en la gestión de las TIC en el ámbito de la salud, tanto en los servicios centrales como en los diferentes centros sanitarios. Fue entregado por Pilar Aparicio Azcárraga.

2. Premio Nacional de Informática y Salud 2018, a la Organización que ha realizado un mayor esfuerzo tecnológico para desarrollar soluciones en el sector sanitario.

Otorgado a HM Hospitales, por la transformación digital experimentada en sus procesos asistenciales gracias a la APP de HM Hospitales, que ha revolucionado la atención con los pacientes, siendo uno de los primeros grupos hospitalarios de Europa en proporcionar a sus clientes el tiempo de espera en Urgencia por especialidad en todos sus centros de Madrid y algunos del resto de España vía APP, y el único a nivel mundial en el desarrollo del proceso "He llegado" que permite la geo-localización del paciente para su identificación en la llegada a una cita médica. Recogió el premioJuan Abarca Cidón, presidente y director general de HM Hospitales, licenciado en Medicina, especialidad en Medicina Familiar y Comunitaria, Licenciado en Derecho. Además, presidente y consejero delegado de PROMEDE (Profesionales de la Medicina y el Derecho). Miembro de la Comisión Permanente del Consejo Asesor de Sanidad. También es fundador de la Fundación Idis y vicepresidente de la Asociación Española de Derecho Sanitario. Entregó el premio José Ramón Zárate Covo.

3. Premio Nacional de Informática y Salud 2018, al Profesional que, por su trayectoria y dedicación, ha colaborado especialmente en promover la transformación digital en el entorno sanitario.







Otorgado a Jesús Óscar Díaz González, por su trayectoria profesional de más de 25 años, donde destacó como gran gestor y defensor de lo público. Trabajador incansable y riguroso, siempre buscando maximizar la rentabilidad de las TIC para mejorar la prestación sanitaria.

Recogió el premio Brezo Rubín (esposa de Jesús Óscar Díaz González) que fue entregado por Luciano Sáez Ayerra.

4. Premio Nacional de Informática y Salud 2018, al Trabajo realizado para difundir la implantación de las Tecnologías de la Información y la Comunicación en Salud.

Otorgado al Proyecto Harmony, por su contribución en el uso adecuado de la mejor y más avanzada tecnología de la información para tratar las leucemias, siendo muy destacable su continua









presencia en diferentes foros compartiendo los logros y dificultades en las diferentes fases del proyecto. Recogió el premio **Jesús María Hernández Rivas**, que le fue entregado por **Juan Antonio Vargas Núñez**

5. Premio Nacional de Informática y Salud 2018, 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.

Otorgado a Víctor Maojo García, por su trayectoria investigadora en Informática Biomédica y de la Salud y su reconocimiento internacional, siendo uno de los científicos de este ámbito más conocido y reconocido a nivel mundial. Recogió el premio **Víctor Maojo García**, que le fue entregado por **Javier Ortega García**.

6. Premio Nacional de Informática y Salud 2018, a la mejor Aportación presentada en las actividades de la SEIS durante los últimos 12 meses.

Otorgado a Historia Clínica Digital para dispositivos móviles del Servicio Canario de la Salud, por el desarrollo de una aplicación *responsive* con TypeScript, JavaScript que puede ser compilada para cualquier dispositivo móvil, lo que permite acceder desde cualquier dispositivo a la Historia Clínica del paciente. Recogió el premio **Teresa Salamanca Barquín**, Médico especialista en Medicina Familiar y Comunitaria. Adscrita a la Dirección General de Programas Asistenciales del Servicio Canario de la Salud en la coordinación de la Historia Clínica Digital de Atención Primaria y del Sistema Nacional de Salud. Fue entregado por **Javier Olave Lusarreta**.

Premio Especial Informática y Salud 2018.

Otorgado al Servicio Murciano de Salud, por el desarrollo de una estrategia de Salud Digital que ha aportado a los pacientes y a los profesionales nuevas formas de relacionarse, y soluciones innovadoras, que han supuesto una auténtica mejora en la asistencia sanitaria prestada en la Región de Murcia. Recogió el premio **Asensio López Santiago**. director Gerente del Servicio Murciano de Salud. Fue entregado por **Pilar Aparicio Azcárraga**.

Tras la misma, dio comienzo el ya tradicional Concierto de Música de Cámara a cargo de los profesores **Rafael Domínguez** (Violonchelo) y **Antonio Palmer** (Piano). A la finalización del mismo se sirvió, como es habitual, un Vino Español.

XXVI JORNADAS NACIONALES DE INNOVACIÓN Y SALUD EN ANDALUCÍA

"Historia Digital de Salud que Aprende"



INTRODUCCIÓN

Estas jornadas ocurrirán unas semanas después de la mayoría de las elecciones autonómicas, cuando se están formando casi todos los nuevos gobiernos regionales de nuestro Estado. La Transformación Digital que precisa el Sistema Nacional de Salud se está produciendo con demasiada lentitud. Se habla mucho de su necesidad, están en curso iniciativas parciales y dispersas, pero está sin definir una estrategia coherente que aglutine acciones e
intereses convergentes de usuarios, gobernantes y proveedores para encontrar soluciones de masa crítica viables a corto y medio plazo. En este contexto, desde la SEIS, consideramos que ante el reto "Historia Digital de Salud que Aprende" se pueden aglutinar proyectos concretos, de pequeña y gran magnitud, para todos y cada uno de esos nuevos planes de Buen Gobierno y así generar una acción sinérgica de
singularidad. El resultado será un incremento sustancial de la eficiencia interna del Sistema, a la vez que se mejora la calidad y el confort de los servicios de salud y se hace una aportación sin precedentes al saber en salud. Esta Trasformación Digital permitirá un profundo rediseño de procesos que reemplace comportamientos obsoletos y onerosos, facilitará la Equidad en el acceso a servicios, y acortará los ciclos que generan nuevo conocimiento para prevenir, predecir, curar y cuidar.

En servicios de salud llegar tarde o abordar lo complejo ignorando lo relevante equivale a dañar o morir. Esto aplica a cada caso, a las pautas de diagnóstico tratamiento, a las carteras de servicios, a la financiación solidaria del gasto generado ahora por "urgencia vital", y al diseño y construcción de infraestructuras.

En nuestro medio se impone construir el futuro inmediato concebido desde una "visión digital" en su esencia. No se trata de "digitalizar lo obsoleto". Otros sectores de nuestra sociedad ya lo han hecho y en el Sistema Nacional de Salud ya hay demasiada experiencia de este tipo. El desarrollo actual de las Tecnologías Digitales de Información y Conocimiento puede
incrementar la rapidez para encontrar la solución adecuada y solidaria a cada problema, en cada circunstancia, en fracciones de tiempo casi
inimaginables. Con los sistemas de aprendizaje actuales se puede identificar un error de con-

cepto mucho antes de dañar a cientos o miles de personas; y se pueden diseñar sistemas dinámicos de oferta de servicios con flujos variables muy ajustados a necesidades cambiantes. Con la creatividad y capacidad investigadora disponible es posible identificar relaciones incluso causas de enfermar desconocidas y generar nuevas soluciones plausibles.

Urgidos por esta necesidad, desde la SEIS convocamos a un encuentro entre múltiples actores durante tres días para hacer un ejercicio de 'inteligencia colectiva pragmática' abocado a producir algo imposible de obtener desde perspectivas individuales, parciales o limitadas. Aplicando metodologías creativas y participativas, visiones multidimensionales y en clima de cooperación, queremos identificar soluciones concretas para ponerlas a disposición de quienes inician nuevos ciclos cuatrienales de gobierno.

Entre las señas de identidad de las Jornadas Nacionales de Innovación y Salud que ocurren en Andalucía está su carácter de laboratorio vivo, de entorno para la investigación de métodos de trabajo inéditos o poco aplicados a este sector, a la vez que intentan obtener "algo imposible de conseguir por la mera adición de todos sus componentes". La propuesta para esta XXVI edición incluye múltiples novedades para favorecer la mejor interacción entre personas, imaginaciones, voliciones, retos y capacidades tecnológicas y humanas con sentido pragmático y de la oportunidad.

Todos Vds. están invitados a participar en ellas, por cualquiera de los canales habilitados.

Para este año, son especialmente relevantes los siguientes términos:

Aprendizaje, Interacción, retorno, retroalimentación, resultado mensurable, digitalización, reproductibilidad, pertinencia, elección, ponderación, priorización, síntesis, oportunidad, relación significativa, causalidad, asociación, temporalidad, estímulo, inhibición, inteligencia colectiva, inferencia, coherencia, evidencia …

La propuesta que se está elaborando, incluye mejoras para esta edición 2019 en los siguientes aspectos:

- Elección de contenidos para tratar con mayor intensidad durante las Jornadas.
- Vinculación e incorporación de nuevos actores clave para la dinamización y productividad del encuentro. Al menos estarán los perfiles: usuario activo, clínico, proveedores de diagnóstico y tratamiento, proveedores TIC, Gobernanza, …
- Métodos de trabajo y variedad de oportunidades para incrementar la creatividad y favorecer la interacción entre personas.
- Amplificación electiva de los resultados obtenidos: la organización transmitirá los resultados construidos entre todos a los supuestos responsables de su ejecución

Y las siguientes novedades:

a. Énfasis en los "retornos": devolver a los asistentes en tiempo real aquello que ellos mismos aportan por diferentes canales de comunicación (hall, resultados de encuestas, puestas en común, etc.)
b. Trabajaremos con metodologías de trabajo idóneas para la creatividad colectiva.
c. Coincidiremos actores muy relevantes para aplicar la tecnología digital: clínicos, proveedores de dispositivos electrónicos, de medicamentos, juristas, etc.
d. Plantearemos retos multidisciplinares enfocados a resultados tangibles a corto y medio plazo.
e. Compartiremos entregables útiles para nuestra vuelta a la actividad cotidiana.
f. Generaremos red de contactos que "ha resuelto un problema común en clima de colaboración".

OBJETIVOS

Lema: "Historia Digital de Salud que Aprende".

Propósitos:

1. Favorecer la accesibilidad equitativa de cualquier persona al servicio necesario y pertinente de salud, en cualquier lugar, en cualquier momento.
2. Crear tipologías de proyectos concretos aplicables en la diversidad de cada CCAA confluyentes en un marco común de interoperabilidad real de eventos de salud, transacciones económicas y de contribución a nuevo conocimiento científico sobre el prevenir, predecir, curar, cuidar y enfermar.
3. Avanzar en la fase de ideación previa a la defi-

nición de concursos públicos para orquestar la próxima Trasformación Digital de las Historias de Salud actuales: Idear nuevas formas de Compra y financiación de nuevas soluciones digitales diagnósticas y terapéuticas basadas en resultados de la vida real con datos del mundo real (RWD)

4. Fortalecer lazos entre actores clave para incrementar su mutua cooperación.
5. Mejorar y acortar los ciclos de creación de nuevo conocimiento biomédico y de la Salud basado en datos reales.
6 Mejorar los retornos de inversión y los precios de adquisición de soluciones tecnológicas digitales.

Los ámbitos objeto de incorporar a la discusión son los siguientes:

1. Diseño HDS:
   a) Estructuración del Lenguaje
   b) Compartir información entre niveles asistenciales
   c) Soporte a procesos asistenciales, Ayuda a la Decisión (diagnóstico y tratamiento), Normalización decisiones
2. Uso adecuado HDS:
   a) Capacitación inicial, buen /mal uso ordinario, accesos,
   b) Enriquecimiento: lenguaje natural, hablado, codificado,
   libre, efectos adversos…
   c) 'Ensayos clínicos dinámicos' (mejor opción en función de la retroalimentación resultados en tiempo real)
   d) Lecturas agregadas, evaluaciones, preguntas, retornos de resultados, identificación de relaciones significativas…
   e) Problemas, incidencias, Centros Atención a Usuarios,
3. Infraestructura tecnológica:
   a) Arquitecturas
   b) Integración "M2M" – "IoT" –
   c) Integración niveles asistenciales, entre CCAA y Estado, entre Estados…
4. Empoderamiento y gobierno de usuarios:
   a) Control accesos y usos
   b) Enfermo activo ("ensayo clínico continuo")
   c) …
5. Usos para Gestión Sanitaria
   a) Capacidades, rendimientos, gestión flujos actividad y agendas
   b) Contratos riesgo compartido sobre resultados basados en RWD.
   c) Remuneración e incentivación profesionales
   d) Cuadro de Mando Integral
6. Salud Pública y Vigilancia Epidemiológica Activa
   a) Enfermedades Trasmisibles, inmunizaciones…
   b) E. no transmisibles
   c) Antibióticos
   d) Vigilancia Farmacológica

Esta lista sigue abierta hasta que hagamos una elección para llevar cada asunto a cada espacio del cronograma.

MIÉRCOLES, 5 DE JUNIO DE 2019

16.00 - 16.30 Registro de Participantes

16.30 - 17.00 Inauguración

17.00 - 17.30 Presentación Jornadas y Encuesta A "Momento O"

17.30 - 18.30 Plenario 1

"Nuestra reciente experiencia unificando la Historia de Salud"

18.30 - 18.45 Requisitos para la HDSqA

18.45 - 19.00 Descanso

19.00 - 20.00 Plenario 2

20.00 - 20.30 Presentación Talleres

21.30 Cena de Bienvenida

JUEVES, 6 DE JUNIO DE 2019

09.30 - 14.00 Talleres Paralelos

11.30 - 12.00 Pausa - Café

13.45 - 16.30 Almuerzo

16.30 - 18.00 Plenario 3

18.00 - 18.30 Descanso

18.30 - 19.30 Puesta en común de talleres

21.30 Copa de Vino Español

VIERNES, 7 DE JUNIO DE 2019

09.30 - 11.30 Plenario 4

11.30 - 12.00 Pausa - Café

12.00 - 13.00 Puesta en común

13.00 - 13.30 Clausura

PROGRAMA PRELIMINAR

VIII REUNIÓN DE LA PLATAFORMA TECNOLÓGICA PARA LA INNOVACIÓN EN SALUD

"Tecnologías que transforman la organización y su relación con los proveedores, ¿de la compra de tecnología a la de servicios?"



INTRODUCCIÓN Y OBJETIVOS

En el contexto actual de cambio continuo de la sociedad, motivado por unainclusióndelatecnologíaenlavidadiaria,unprotagonismocadavez más claro de los individuos y una redefinición constante de los valores personales y colectivos, estamos obligados a reinventarnos cada día y a considerar la innovación como un motor de cambio y transformación continua que tenemos que incluir en nuestras organizaciones para hacerlas, no solo sostenibles, sino auténticas generadoras de conocimiento yriqueza.

Con esta realidad y sabiendo que nos movemos en un entorno multidisciplinar,multisectorialynosiempreconlasestructurascolaborativas más adecuadas, la Plataforma Tecnológica de Innovación en Salud de la SEIS, trabaja para poner en sintonía a ciudadanos, profesionales de la salud, organizaciones sanitarias públicas y privadas, investigadores, centros tecnológicos y empresas para desarrollar soluciones innovadoras, que se adecuen totalmente a las necesidades reales de los ciudadanos y del SNS, al mismo tiempo, gracias a la movilización coordinada de la investigación y la empresa lograr la generación deriqueza.

Esta VIII Reunión de la Plataforma Tecnológica de Innovación en Salud se celebra en Logroño los días 21 y 22 de mayo con el lema "Tecnologías que transforman la organización y su relación con losproveedores,

¿de la compra de tecnología a la de servicios?" y seorienta especialmente al análisis y promoción de proyectos innovadores surgidos de la convergencia del conocimiento clínico y/o del modelo de negocio y las Tecnologías de la información, buscando sinergias entre todos los actores y los agentes financiadores.

En esta edición se hará foco especialmente en todo lo relacionado con el diagnóstico automático de Imagen Radiológica, implantes gestionables, Big-data, Inteligencia Artificial e Internet de las cosas, analizando su capacidadtransformadoradelmodeloasistencialylaposiblereorientación del modelo de negocio y relación con los proveedores de tecnología médica yTIC.

Seguiremos con la experiencia iniciada en las anteriores Reuniones de incubadoradeproyectoslideradosporclínicos,priorizandoaquellosque tenganelcarácterdemulticéntricosymulticomunitariosomultinacionales.

Los principales objetivos de esta iniciativa son:

- El desarrollo de una cultura de innovación continua ensalud.
- Conocer y evaluar los avances que nos ofrece la industria y las TIC, con capacidad transformadora del sistemasanitario.
- Identificarprofesionalestractoresparaquelideren ideasy proyectos.
- Preparar el sistema para los nuevos modelos organizativos que surgiránconlairrupcióndelamedicinapersonalizadayelcambio de estrategia en el manejo de patologíacrónica.
- Potenciarlaculturacolaborativayasociativaentretodoslos participantesparaeldesarrollodeproyectosinnovadores.
- Redefinir el papel del ciudadano en el sectorsanitario.
- Activar fuentes de financiación para la innovación enSalud.

MARTES, 21 DE MAYO

16.00 - 16.30 Registro de Participantes
16.30 - 16.45 Inauguración Oficial
16.45 - 18.15 Primera Sesión
"Modelos y Estrategias para la Innovación"
18.15 - 18.30 Pausa
18.30 - 20.00 Segunda Sesión
"Barreras y Soluciones para la Innovación en Salud"
21.30 Cena

MIÉRCOLES, 22 DEMAYO

09.00 - 09.30 Comunicaciones
09.30 - 11.00 Tercera Sesión
"Diagnóstico Radiológico Automático"
09.30 - 11.00 Sesión Especial Cerrada-
11.00 - 11.30 Café
11.30 - 13.30 Cuarta Sesión
"Implantes Gestionables"
13.30 - 14.00 Conclusión y cierre

MARTES, 21 DE MAYO

16.00 - 16.30 Registro de Participantes
16.30 - 16.45 Inauguración Oficial

MARTES, 21 DE MAYO

16.45 - 18.15 Primera Sesión
"Modelos y Estrategias para la Innovación"
Modera
Sr. D. Javier Aparicio Soria
Director Gerente CIBIR
Ponentes
"Estrategia para la promoción de la Innovación en La Rioja"
Sr. D. Juan Carlos Oliva Pérez
Director de Innovación Sanitaria Rioja Salud
18.15 - 18.30 Pausa

MARTES, 21 DE MAYO

18.30 - 20.00 Segunda Sesión
"Barreras y Soluciones para la Innovación en Salud"
21.30 Cena - LaGrajera

MIÉRCOLES, 22 DE MAYO

09.00 - 09.30 Comunicaciones
09.30 - 13.30 Sesión Especial Cerrada-Sala x
"Proyecto Realidad VIrtual La Rioja"
09.30 - 11.00 Tercera Sesión
"Diagnóstico Radiológico Automático"
11.00 - 11.30 Pausa - Café

MIÉRCOLES, 22 DE MAYO

11.30 - 13.30 Cuarta Sesión
"Implantes Gestionables"
"Lasnuevastecnologíasaplicadasalámbitoasistencial:Impresión 3D y RealidadVirtual"

MIÉRCOLES, 22 DE MAYO

13.30 - 14.00 Conclusión y cierre

PROGRAMA PRELIMINAR

SEGURIDAD Y PROTECCIÓN DE **DATOS**

Coordina: **Juan Díaz**

Implantación de la Figura del **Delegado de Protección de Datos** en el Sistema Nacional de Salud

POSICIONAMIENTO DEL COMITÉ TÉCNICO DE SEGURIDAD Y PROTECCIÓN DE DATOS DE SALUD DE LA SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

Juan Díaz García
Coordinador del Comité de Seguridad y Protección de Datos de Salud

La importancia que reviste la novedosa figura del "delegado de protección de datos" se acrecienta en el ámbito sanitario tal y como se pone de manifiesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, al establecer en su artículo 34 que en todo caso se deberá designar un delegado cuando se trate de "Los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes". Asimismo, en la Disposición adicional decimoséptima de dicha norma se indica que "En el plazo máximo de un año desde la entrada en vigor de esta ley, los comités de ética de la investigación, en el ámbito de la salud, biomédico o del medicamento, deberán integrar entre sus miembros un delegado de protección de datos o, en su defecto, un experto con conocimientos suficientes del Reglamento (UE) 2016/679 cuando se ocupen de actividades de investigación que comporten el tratamiento de datos personales o de datos seudonimizados o anonimizados".

La obligación de nombrar un delegado de protección de datos es competencia del responsable del tratamiento, que es "la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento". En caso de los servicios públicos de salud, el responsable del tratamiento suele ser la autoridad que asume la representación legal del organismo público correspondiente.

La mayoría de las comunidades autónomas han optado por nombrar un delegado de protección de datos para su servicio de salud, reconociendo así el ingente volumen de trabajo, la necesaria especialización en la normativa sectorial y el también necesario conocimiento del sector sanitario para ejercer eficazmente las funciones de asesoramiento y supervisión, particularmente de los análisis de riesgos y evaluaciones de impacto en la protección de datos en los tratamientos con finalidad asistencial o investigadora.

Otras comunidades autónomas han optado, en el ejercicio legítimo de su potestad organizativa, por la designación de un único delegado de protección de datos para toda la administración regional, lo que no deja de sorprender a tenor de las previsiones legales anteriormente transcritas.

En virtud de las razones expuestas, consideramos imprescindible la designación de al menos un delegado de protección de datos ESPECIALIZADO y específico para sanidad, diferenciado del delegado/s que para los restantes sectores de actividad (educación, justicia, administración general...) puedan designar las distintas administraciones autonómicas.

FORO DE
INTEROPERABILIDAD

Coordina: **Adolfo Muñoz**

España avanza en su **Modelo de Interoperabilidad** para el SNS

Recientemente se han destacado en los medios varias noticias sobre el modelo de interoperabilidad del SNS que se está desarrollando desde el Ministerio de Sanidad, Consumo y Bienestar Social:

Por un lado, en enero se publicó[1] que Cataluña se incorporaba al proyecto de historia clínica digital del Sistema Nacional de Salud (HCDSNS). De momento, esta inclusión es sólo como emisor (es decir, desde el resto de España se pueden consultar los resúmenes de historia de los habitantes de Cataluña) aunque la incorporación como receptor (que en Cataluña se puedan consultar los informes producidos en el resto del SNS) se alcanzará en los próximos meses. Esto supone llegar a un 94,64% de cobertura en el proyecto HCDSNS de la población atendida por el SNS. Con este paso se completa el mapa de participación de todas las autonomías en el proyecto, lo que significará un avance en la cohesión del país, contribuyendo a mejorar la calidad de la atención sanitaria, la seguridad clínica y la continuidad asistencial. Además, este proyecto se encuentra conectado con otras iniciativas de la Unión Europea para el intercambio de información clínica entre los Estados Miembros.

En este sentido, España participa en el proyecto eHDSI[2] (eHealth Digital Service Infrastructure – Infraestructura Digital de eSalud), en el que el MSCBS se ha comprometido, junto con 14 comunidades autónomas, a proveer el servicio de intercambio de historias clínicas resumidas en 2020. El proyecto eHDSI, perteneciente al instrumento CEF (Connecting Europe Facility – Servicios para Conectar Europa) ha elegido 2 casos de uso para su implementación: la prescripción y dispensación electrónica y la historia clínica resumida. El despliegue del proyecto se está haciendo en 4 oleadas, comenzando con Portugal, Croacia, Chipre, la República Checa y Finlandia en 2018. España se incorporará en 2020 para el caso de la historia clínica resumida, como ya se ha dicho, y en 2021 en la prescripción y dispensación electrónica.

Por último, también se ha publicado recientemente[3] que el proyecto de receta electrónica está a punto de completarse con la inclusión de la Comunidad de Madrid, que está siendo certificada en estos días, tras cumplir con todos los requisitos técnicos. Con esta inclusión, cualquier ciudadano podrá retirar los medicamentos que tenga prescritos en cualquier farmacia de todo el territorio nacional. Este proyecto ha sido posible, en parte, gracias a la interoperabilidad de la tarjeta sanitaria, ya que, independientemente de su diseño y de la Comunidad en que haya sido emitida, es válida en cualquier punto del SNS o en cualquier farmacia española. Esta interoperabilidad se basa en un sistema común de identificación personal, centralizado en el propio Ministerio, que recoge información de todas las tarjetas en la Base de Datos de Población Protegida del SNS, asignando a cada persona un identificador único.

1. https://www.mscbs.gob.es/gabinete/notasPrensa.do?id=4479
2. https://ec.europa.eu/cefdigital/wiki/display/EHOPERATIONS/eHDSI+Mission
3. https://www.mscbs.gob.es/gabinete/notasPrensa.do?id=4531

FORO DE
GOBERNANZA

Coordina: **Martín Begoña**

Cómo viajar en la **TRANSFORMACIÓN DIGITAL (2)**

Pilar Ruiz Ayuso
Consultora en Transformación Digital e Inteligencia Artificial

Haciendo una breve sinopsis del artículo anterior, comento la importancia del establecimiento de ciertas medidas de forma temprana para poder realizar una transformación digital ágil y eficiente.

Se dividen en dos líneas de trabajo:

1. Línea Estratégico Empresarial: Se centra en el desarrollo de la estrategia Digital de la compañía, donde cobra especial relevancia el papel del CIO, a la hora de identificación de necesidades y en la coordinación de todos los cambios necesarios a realizar y que van a impactar en cada una de las áreas de la compañía, flujos de trabajo y cadena de suministro. Dicha línea responde a las preguntas "WHAT" y "WHY"
2. Línea Sistémico Tecnológica: Se centra en aportar valor a las empresas en el desarrollo de sus proyectos generados a través de la Línea Estratégica Empresarial, a partir del conocimiento y expertise tecnológico. Dicha línea de trabajo responde a la pregunta de "HOW" y se traccionan mediante una serie de Ejes Tecnológicos que ayudarán a acometer desde la tecnología, los proyectos de Transformación Digital definidos y son: Disruptivo, Datadriven y Omniubicuo.

En este y posteriores artículos, ampliaremos la Línea de Trabajo Sistémico Tecnológica porque doy por supuesto que la mayor parte de las empresas actualmente tienen definida su propia estrategia empresarial y por este motivo, es más interesante desglosar detalladamente cómo a través de la tecnología, se cubren los requisitos de los proyectos empresariales de Transformación Digital previamente definidos.

Datadriven, el empoderamiento del dato, clave para alcanzar la Transformación Digital

Comienzo hablando del eje tractor que está más relacionado con el empoderamiento del dato, y que cobra especial relevancia en la cuarta revolución tecnológica que estamos viviendo con la digitalización, que sería el Eje Datadriven.

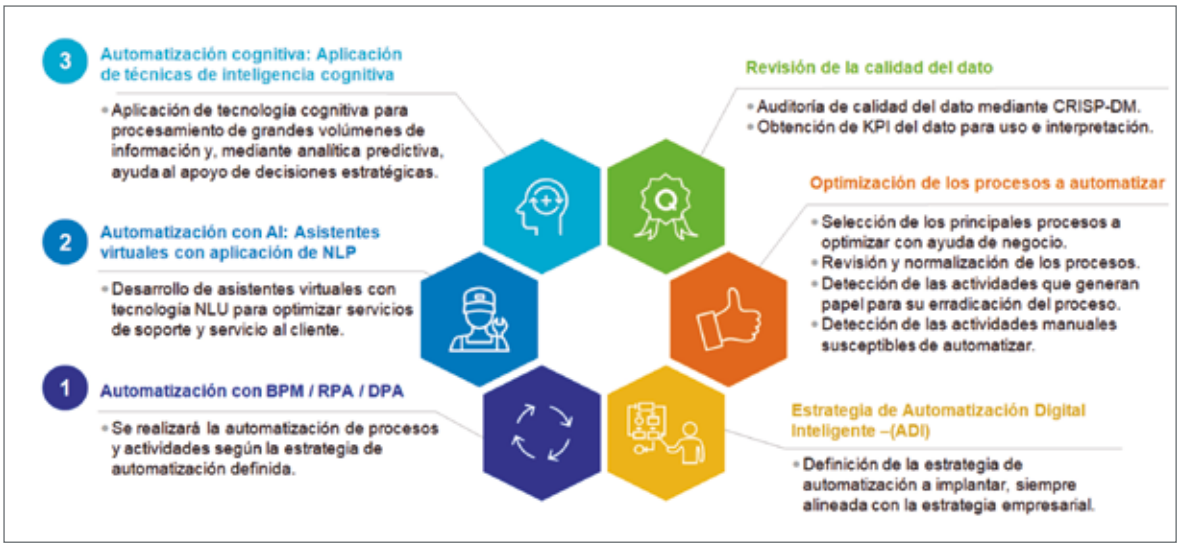
Actualmente el recurso más valioso del mundo ya no es el petróleo, sino los datos, por su potencial generador de ventajas competitivas y por su alcance, que nos permite ampliar el conocimiento de nuestros mercados.

Si hago una analogía entre el petróleo y los datos, igual que el petróleo, sin un refinado previo no sirve para su uso, igual pasa con los datos, en esta era digital, nos enfrentamos ante una creciente complejidad de desafíos en torno a la generación, uso y explotación de datos, con fronteras borrosas entre sectores y múltiples problemáticas regulatorios y legislativos.

Según el estudio de EMC sobre el universo digital, creado en colaboración con IDC, cuantifica el volumen de datos que produciremos en 2020, que será en torno a 40 zettabyte o más de 5 terabytes por persona. Para que nos hagamos una idea 1 zettabyte equivale a 1.000 millones de terabytes. Si se guardara toda esta información en discos Blu-Ray, su peso equivaldría a 424 portaaviones de la clase Nimitz de las Fuerzas Armadas de los EEUU.

Ha habido un crecimiento exponencial en los últimos tres años debido a una mayor actividad en el consumo de servicios a través de dispositivos informáticos y móviles, internet y crecimiento de datos generados por máquinas o sensores (IoT).

A continuación, expongo varios ejemplos del



porqué se hace necesario el tratamiento del dato visto desde varios sectores:

- Sector Energético, el desarrollo de energías renovables, las redes inteligentes, la instalación de sensores y contadores a lo largo del sistema eléctrico (plantas, líneas de tensión, empresas, hogares,...), demandan nuevas capacidades y marcos regulatorios cada vez más apoyados en la generación e intercambio de datos masivos.
- Sector Salud, la introducción de la medicina digital permitirá que a través de la salud móvil, los historiales clínicos electrónicos, la codificación automática de la información clínica y atención virtualizada, se generen cada vez mayores volúmenes de información, con potencial de mejorar los procesos de diagnóstico, la medicina preventiva, la efectividad de medicamentos y controles epidemiológicos.

Hay que partir de un Marco de Trabajo que nos ayude a trabajar las áreas más relevantes que impactan en el dato, para hacer uso seguro y eficiente de la información que generamos con nuestros procesos y actividades empresariales y sacar el máximo partido de éstos.

Trabajar la Gobernanza del dato a través del Marco de Trabajo ADI (Automatización Digital Inteligente)

El Marco de Trabajo denominado ADI (Automatización Digital Inteligente) es un desarrollo propio, que indica diferentes áreas a tratar, que explicaré brevemente a continuación y ahondaré en próximas entregas, incluyendo ejemplos específicos de casos de éxito obtenidos y que cubren problemáticas cubiertas en diferentes clientes del sector salud.

El Marco de Trabajo ADI se divide en 6 áreas específicas de trabajo y son las siguientes:

1. Revisión de la Calidad del Dato con Metodología basada en el Estándar Internacional de Minería de Datos CRISP-DM.
2. Optimización de los procesos (enfocado al dato) haciendo uso de sw de process mining.
3. Consultoría estratégica de implantación de Nivel de Automatización Digital Inteligente adecuado para la evolución del negocio empresarial.

Dentro de los niveles de automatización inteligente hay:

4. Nivel 1: Desarrollo de proyectos que manejan procesos que hacen uso de cierta lógico tipo plataformas BPM (Business Process Management), software de automatización de tareas RPA (Robot Process Automation), y uso del DPA (Digital Process Automation) que engloba la aplicación de software de OCR inteligente y oficina "paperless".
5. Nivel 2: Desarrollo de chatbots con uso de tecnología de inteligencia artificial NLP (Natural Lenguage Processing).
6. Nivel 3: Desarrollo de proyectos con Analitica Avanzada haciendo uso de tecnología cognitiva con Modelos Supervisados y No Supervisados.

FORO DE
SALUD CONECTADA

Coordina: **Óscar Moreno**

Robots para realizar **cirugía de la columna vertebral** con mayor precisión



Actualmente se está desarrollando un proyecto de investigación del que forman parte mecanismos robóticos que son capaces de perforar la columna vertebral del paciente con elevada precisión.

El proyecto, dirigido por la Universidad de Nottingham Trent, consiste en dos brazos robóticos que perforan semi-autónomamente las vértebras de un paciente de forma individual.

Los brazos, conocidos como robot de referencia y robot de instrumental, trabajan juntos para asegurar la columna vertebral de los pacientes y perforan tan solo 0,1 mm. El robot de referencia está sujeto a una vértebra y se mueve con ella para seguir los movimientos naturales del paciente. Instantáneamente transmite información sobre este movimiento a un ordenador, lo que permite que el robot de instrumental se ajuste automáticamente para que permanezca sobre su ruta ya predeterminada.

Esta tecnología permite trabajar con niveles de precisión inalcanzables para las manos humanas.

También se utilizará la realidad aumentada para brindar a los cirujanos información visual en directo durante la cirugía, permitiéndoles monitorear con exactitud las incisiones que se están realizando.

Los orificios perforados en las vértebras se utilizan para insertar tornillos pediculares que están unidos a varillas y que permiten a los cirujanos mover las vértebras individualmente y realinear la columna vertebral.

La investigación está siendo dirigida por el profesor Philip Breedon, del Grupo de Investigación de Diseño Médico junto con el profesor David Brown ambos de la Escuela de Ciencia y Tecnología de la Universidad de Nottingham Trent.

El profesor Breedon comentó: "Los cirujanos que realizan operaciones para corregir afecciones de la columna vertebral, como la escoliosis o la cifosis y que cambian la vida de los pacientes, deben garantizar niveles de precisión exactos para evitar causar lesiones innecesarias y potencialmente graves.

"Esta tecnología promete ofrecer mayores niveles de precisión que nunca antes se habían alcanzado, o incluso humanamente posibles, para mejorar la seguridad y la eficiencia de los procedimientos que necesitan las personas con afecciones vertebrales graves".

La cirugía se utiliza para corregir la columna vertebral de los pacientes con afecciones como la escoliosis.

El profesor Bronek Boszczyk, jefe de cirugía de columna en el Benedictus Krankenhaus Tutzing en Alemania y profesor visitante en la universidad, dijo que el proyecto era un "ejemplo brillante de robótica que puede incrementar y mejorar las operaciones". "Es de suma importancia que los procedimientos espinales se realicen con total precisión para minimizar los riesgos sustanciales para un paciente". "Es un ejemplo brillante de cómo la robótica puede aumentar y mejorar la forma en que se realizan las operaciones intrusivas, mejorando la seguridad del paciente y garantizando la eficiencia del proceso", dijo.

Más información:

- Digital Health - https://www.digitalhealth.net/news/
- Video demostrador - https://youtu.be/jejkkf5k15c
- Nottingham Trent University - https://www.ntu.ac.uk/about-us/news

INFORMÁTICA MÉDICA

Coordina: **José Sacristán**

La inteligencia artificial ya puede diagnosticar dolencias infantiles con la precisión de un pediatra

Un equipo internacional desarrolla una máquina capaz de analizar las condiciones de salud de miles de niños gracias al potencial del aprendizaje automático.
Los autores del artículo, publicado en Nature Medicine, explican que la disponibilidad de información médica ha crecido exponencialmente en los últimos años, lo que complica la toma de decisiones por parte de los médicos. La capacidad de la inteligencia artificial de analizar grandes cantidades de datos puede ayudar a reducir esta carga y facilitar la valoración adecuada de cada caso clínico, aseguran.

https://elpais.com/tecnologia/2019/02/11/actualidad/1549882554_285280.html


EL PAÍS TECNOLOGÍA

La inteligencia artificial ya puede diagnosticar dolencias infantiles con la precisión de un pediatra

Un equipo internacional desarrolla una máquina capaz de analizar las condiciones de salud de miles de niños gracias al potencial del aprendizaje automático



Requisitos para el uso de IA (Inteligencia Artificial) en sector público

Precisión, transparencia, control del sesgo y estabilidad son algunos de los factores a tener en cuenta entre las administraciones gubernamentales al trabajar con inteligencia artificial.

La inteligencia artificial se está popularizando de forma generalizada, aplicándose a través de sus diversas ramas en distintos verticales y sectores. Según un estudio de la firma Deloitte, las industrias manifiestan diferencias en el retorno en la inversión.
Sobre su aplicación en el sector público, la inteligencia artificial está ganando adeptos entre agencias gubernamentales para su empleo en tareas de control o para mejora de decisiones, como identificar patrones de evasión fiscal o ayudar a detectar casos sensibles en temas de servicios sociales. Además de la mejora para las responsabilidades del gobierno con la ciudadanía, el empleo de herramientas de IA ayudaría a conseguir mayor efectividad y a reducir los costes.

https://www.ciospain.es/aapp/requisitos-para-el-uso-de-ia-en-sector-publico

SECTOR
ENFERMERÍA

Coordina: **Inmaculada Moro**

Enfermería, TIC e innovación

XXII Congreso Nacional de Informática de la Salud



Soy Inmaculada Moro, enfermera y a partir de este momento coordinare esta sección en la revista de la SEIS.

Mi objetivo es que desde esta tribuna podamos contar experiencias de desarrollo entorno a las TIC, la tecnología y la innovación desde la perspectiva asistencial, y me gustaría que fuera una oportunidad para que diferentes profesionales de cualquier ámbito puedan difundir su conocimiento y experiencia.

Quiero también hacer una mención a Azucena Santillán, que hasta ahora ha conducido esta sección de manera extraordinaria, incorporando artículos con el conocimiento más actualizado y fiable y de interés general.

En esta ocasión, quiero la hacer un resumen de enfermería que se celebró en el pasado congreso de XXII Congreso Nacional de Informática de la Salud 2019. 5, 6 y 7 de Marzo de 2019 en Madrid. Bajo el tema, "Enfermería, TIC e innovación" celebramos una mesa debate que tuve el placer de moderar. Participaron profesionales con experiencia en innovación y desarrollo de las TIC en diferentes áreas asistenciales y de distintas CC AA.

Participaron:

- Montserrat Hernández, gerente adjunta de Procesos Asistenciales, Gerencia Asistencial de Atención Primaria del SERMAS, nos habló de los sistemas de información aplicados a los cuidados su papel en la continuidad asistencial y importancia de poner en valor los resultados en salud de los cuidados a través de indicadores específicos de cuidados .
- Verónica Ruiz Pereda, adjunta de Enfermería de la OSI Ezkerradea-Enkarterri Cruces de Osakidetza y líder del proyecto de movilidad que desarrolla apps clínicas para el uso a pie de cama, y nos hablo del impacto y de cómo había cambiado la forma de trabajar de las enfermeras en su organización tras la implantación de este sistema innovador
- Pedro Soriano, técnico de la Escuela Madrileña de Salud, y fundador de #FFpaciente nos contó su experiencia sobre el uso de las TIC las redes sociales como herramientas de empoderamiento para los pacientes.
- Faustino González, supervisor de una Unidad de Calidad e Innovación de HU Marques de Valdecilla abordo la digitalización de los hospitales y la implicación de la enfermería en ellos asi como la adecuación de las aplicaciones de cuidados a la realidad asistencial
- María del Cristo Gonzalez, Coordinadora autonómica de Estrategia Canaria de Cuidados. Responsable de la campaña Nursing Now, la enfermería frente al 2020, la innovación como herramienta de desarrollo profesional y objetivo de Nursing now

Durante el debate se puso en valor la importante aportación de la tecnología y de las TIC para el desarrollo de los cuidados, y como son una palanca de cambio para favorecer el avance de la profesión y su desarrollo,y que permita responder a las necesidades de salud actuales y futuras de la sociedad.

SECTOR
FARMACIA

Coordina: **Alberto Gómez Lafón**

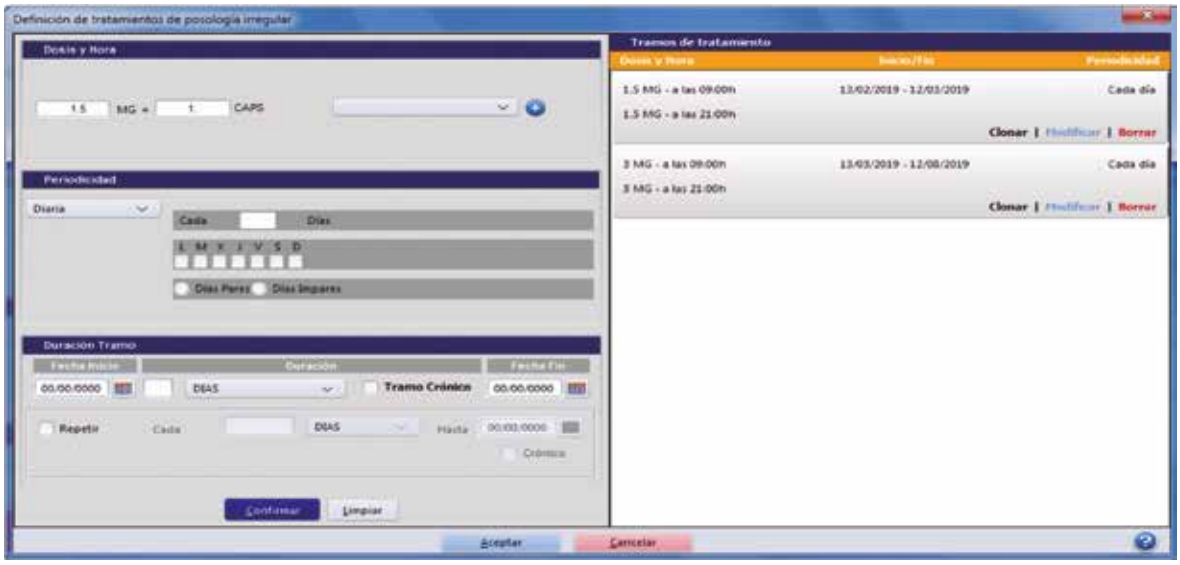
Herramientas de información para el paciente en **receta electrónica**

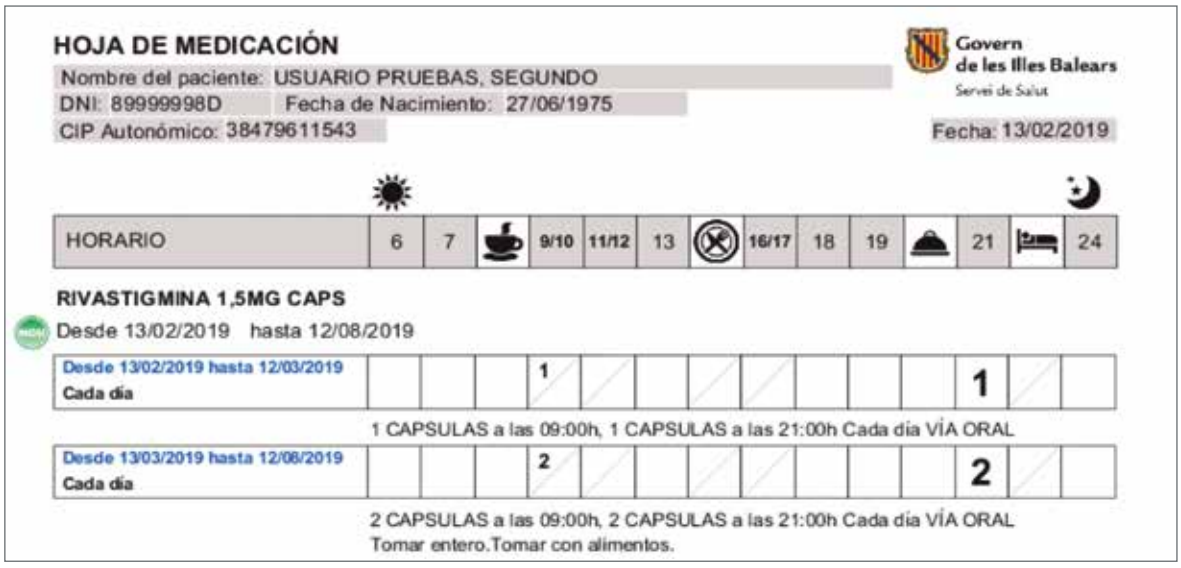
M. Fernández Tous y M. A. Boronat Moreiro
Servicio de Farmacia Servicios Centrales. Servei de Salut de les Illes Balears.

Receta Electrónica (RELE) es un sistema que integra la prescripción y dispensación de medicamentos y productos sanitarios en un proceso continuo y enteramente electrónico.

La automatización de estos procesos permite disponer de información, estructurada e integrable con otros sistemas, relativa al prescriptor, al paciente y al tratamiento prescrito. Una de las consecuencias de la implantación de RELE es poder diseñar herramientas que registren de manera precisa la información sobre la pauta posológica (dosis, periodicidad o frecuencia de administración y duración) de los tratamientos prescritos mostrando dicha información en soportes adaptados a las preferencias y necesidades de cada usuario.

La mayoría de tratamientos en el ámbito comunitario se prescriben con pauta regular, entendida como aquella en la que el paciente toma la misma dosis en la misma hora de toma de manera invariable durante el tiempo indicado. No obstante hay medicamentos, especialmente los de dispensación hospitalaria, que requieren de pautas posológicas complejas en las que la dosis y hora de toma no se mantienen constantes a lo largo del tratamiento. Así, podemos encontrar esquemas de tratamiento con dosis distintas según hora de toma, con periodos de inducción y mantenimiento con dosis diferentes, con ciclos de tratamiento y períodos de descanso, etc. Estas casuísticas han hecho necesario desarrollar una herramienta en RELE que permita la prescripción de pautas irregulares, entendidas como aquellas en las que la dosis y la frecuencia pueden variar durante el período de tratamiento prescrito, permitiendo el cálculo automático de la cantidad total de dosis de medicamento necesaria para cubrir el trata-





HOJA DE MEDICACIÓN

Govern de les Illes Balears
Servei de Salut

Nombre del paciente: USUARIO PRUEBAS, SEGUNDO
DNI: 89999998D Fecha de Nacimiento: 27/06/1975
CIP Autonómico: 38479611543
Fecha: 13/02/2019

HORARIO	6	7	9/10	11/12	13	16/17	18	19	21	24
RIVASTIGMINA 1,5MG CAPS										
Desde 13/02/2019 hasta 12/08/2019										
Desde 13/02/2019 hasta 12/03/2019 Cada día			1						1	
1 CAPSULAS a las 09:00h, 1 CAPSULAS a las 21:00h Cada día VÍA ORAL										
Desde 13/03/2019 hasta 12/08/2019 Cada día			2						2	
2 CAPSULAS a las 09:00h, 2 CAPSULAS a las 21:00h Cada día VÍA ORAL Tomar entero.Tomar con alimentos.										

miento y ajustando los diferentes formatos de envases a dispensar de manera automática.

Esta herramienta de posología irregular está disponible a través de un acceso ubicado en la propia ventana de prescripción que utiliza el prescriptor cuando pretende prescribir un nuevo tratamiento o modificar uno ya prescrito con anterioridad.

El disponer de todos los datos estructurados relativos al tratamiento prescrito permite generar herramientas o documentos que recojan esa información en soporte electrónico o papel destinados al paciente, como es la hoja de medicación o las etiquetas de posología. La hoja de medicación es un documento destinado al paciente que recoge información sobre el tratamiento completo. Muestra una gradilla horaria con el medicamento o producto sanitario prescrito, la fecha de inicio y finalización del tratamiento, el detalle de la posología (si esta es irregular se especifican las horas de toma de cada periodo de tratamiento así como los períodos de descansos si los hubiera). También se muestra información acerca de la vía de administración y consejos de administración que el profesional considere necesario anotar. La información se muestra de forma gráfica y entendible para el paciente. La hoja de medicación puede emitirse en soporte papel desde el módulo de prescripción o dispensación de RELE en cualquier momento y por cualquier profesional que atienda al paciente, bien sea el médico, el farmacéutico o el enfermero. Asimismo, el paciente puede consultar esta hoja de medicación a través del portal de salud corporativo de Servicio de Salud de las Islas Baleares, al que accede cuando quiere consultar sus datos de salud.

Del mismo modo, RELE permite emitir etiquetas de Posología que recogen la información sobre la pauta posológica para poder adherirlas a los envases de los medicamentos dispensados en la farmacia comunitaria o en el servicio de farmacia hospitalario.

En conclusión, la implantación de RELE permite disponer de información estructurada de los tratamientos prescritos e incorporar herramientas que registran de manera exacta las pautas de tratamiento, garantizando veracidad en la historia farmacoterapéutica del paciente, seguridad en el proceso de atención al paciente y eficiencia en la cantidad de medicamento a dispensar para cubrir el plan de tratamiento prescrito. Asimismo, RELE permite incorporar elementos de información para el paciente como la hoja de medicación y las etiquetas de posología, que mejoran el conocimiento de los pacientes sobre los tratamientos prescritos y su cumplimiento terapéutico.

BIBLIOGRAFÍA

http://www.receptaelectronicabalears.es/WebAjudaRELE/FuncionamientoPosologiaIrregular.html

NOTICIAS DEL SECTOR

Coordina: **Diego Sáez**

Orion Health ha cerrado un importante acuerdo en Abu Dhabi para desarrollar la primera plataforma HIE (Healthcare Information Exchange) en Oriente Medio. El acuerdo es con Abu Dhabi Health Data Services, una nueva compañía de proyectos establecida como parte del Departamento de Salud, e Injazat Data Systems. El HIE se conocerá como "Malaffi" y, en última instancia, conectará a 2,000 proveedores públicos y privados de atención sanitaria en todo Abu Dhabi.

IBM presenta IBM Q SystemOne, el primer ordenador cuántico para uso comercial. IBM anuncia un nuevo proyecto que ha dado vida a la computadora cuántica más sofisticada hasta la fecha, esto gracias a sus 50 qubits, o bits cuánticos, que nos abren un mundo de posibilidades hacia una nueva y potente forma de procesar la información.

La inteligencia artificial ya puede diagnosticar dolencias infantiles con la precisión de un pediatra. Un equipo internacional desarrolla una máquina capaz de analizar las condiciones de salud de miles de niños gracias al potencial del aprendizaje automático. Los autores del artículo, publicado en Nature Medicine, explican que la disponibilidad de información médica ha crecido exponencialmente en los últimos años, lo que complica la toma de decisiones por parte de los médicos.

Requisitos para el uso de IA (linteligenciaArtificial) en sector público. Precisión, transparencia, control del sesgo y estabilidad son algunos de los factores a tener en cuenta entre las administraciones gubernamentales al trabajar con inteligencia artificial. Sobre su aplicación en el sector público, la inteligencia artificial está ganando adeptos entre agencias gubernamentales para su empleo en tareas de control o para mejora de decisiones, como identificar patrones de evasión fiscal o ayudar a detectar casos sensibles en temas de servicios sociales.

TICH Consulting ha ganado la licitación de la compañía saudí Hosna Medical Care Company y la consultora belga Aralis, para implantar su historia clínica de gestión sanitaria integral, Green Cube, en dos empresas sanitarias asentadas en la ciudad de Riad, capital de provincia y de Arabia Saudí.

AGENDA 2019

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

VIII REUNIÓN DE LA PLATAFORMA TECNOLÓGICA PARA LA INNOVACIÓN EN SALUD
Fecha: 21 y 22 mayo · **Lugar:** La Rioja

XXVI JORNADAS NACIONALES DE INNOVACIÓN Y SALUD EN ANDALUCÍA
Fecha: 5, 6 y 7 junio · **Lugar:** Málaga

IX FORO PARA LA GOBERNANZA DE LAS TIC EN SALUD
Fecha: 2 y 3 octubre ·**Lugar:** Toledo

XVII REUNIÓN DE SALUD CONECTADA
Fecha: 20 y 21 noviembre · **Lugar:** Las Palmas

V MÁSTER EN DIRECCIÓN DE SISTEMAS Y TICS PARA LA SALUD
Fecha: noviembre 2018-octubre 2019 · **Lugar:** Madrid

XXVI Jornadas Nacionales de Innovación y Salud en Andalucía

Siguenos en twitter:
#JISA2019

"Historia Digital de Salud que Aprende"

Organiza

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

Con la colaboración de

JUNTA DE ANDALUCIA
CONSEJERIA DE SALUD



"NGC2237 #Nebulosa de la Roseta. 2019 desde la Tierra. Imagen cedida por Adolfo Muñoz Carreto"

MÁLAGA 5 ,6 y 7 junio 2019

HOTEL SOL GUADALMAR
Calle Moby Dick, 2, 29004 Málaga

COLABORADORES TECNOLÓGICOS

Atos · FUJITSU · HUAWEI · Ibermática · INFORMÁTICA El Corte Inglés · Microsoft · minsait An Indra company · PHILIPS · SIEMENS Healthineers