NÚMERO
127

I+S

FEBRERO
2018

REVISTA DE LA SOCIEDAD ESPAÑOLA DE INFORMÁTICA Y SALUD

ESPECIAL

IMPACTO DEL NUEVO REGLAMENTO DE PROTECCIÓN DE DATOS EN EL ÁMBITO SANITARIO



"40 AÑOS TRABAJANDO POR LA INNOVACIÓN TIC EN SALUD"

ENTIDADES ASOCIADAS

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

accenture

ESTEVE

PLEXUS

AGFA HealthCare

indra

Redytel

ASCENDO CONSULTING

INFOLOGIC-SALUD Avancemos juntos

Roche

Bilbomática

indizen Technology & Business Confluence

SAVAC

gfi

Carestream

InterSystems Health | Business | Government

sia

Cerner

Microsoft

Tich Consulting

connectis

medmesafe

GRUPO TRC

EY Building a better working world

ORION HEALTH THINKING SOFTWARE FOR LIFE

VIDAL VADEMECUM Drug Information Systems CONSULT ESPAÑA

Dedalus HEALTHCARE SYSTEMS GROUP GLOBAL SERVICES

panda

vodafone

VORTAL Connecting business.

AÑO 2018 NÚMERO 127 **SUMARIO**

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** IMPACTO DEL NUEVO REGLAMENTO DE PROTECCIÓN DE DATOS EN EL ÁMBITO SANITARIO

6 Cuenta atrás hacia el 25 de mayo de 2018
8 MAR ESPAÑA: Directora de la Agencia Española de Protección de Datos
13 El Reglamento General de Protección de Datos y su aplicación en el ámbito sanitario
21 El Delegado de Protección de Datos
24 RGPD: Evaluaciones de impacto
28 Seguridad, Análisis de Riesgos y Auditorías en el RGPD
31 Guías y Herramientas de Apoyo para Adaptarse al RGPD
34 Resultados del Plan de Inspección Sectorial de Oficio de Hospitales Públicos
38 Tutelas y Denuncias Relevantes del Sector Sanitario
46 Elementos clave del RGPD: Inventario de tratamientos y Evaluación de impacto
48 El Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal
52 Nuevos retos normativos para el ámbito sanitario
56 RGPD, un Reglamento que Afecta q todas las Organizaciones, Públicas y Privadas, en Europa ¿Estamos Preparados?
58 Una "hoja de ruta" para la Adecuación de las Organizaciones Sanitarias Públicas al #RGPD
62 Ciberseguridad en salud: Un desafío inevitable

64 **ACTIVIDADES DE LA SEIS**

64 VII REUNIÓN DE LA PLATAFORMA TECNOLÓGICA
74 XXI CONGRESO NACIONAL DE INFORMÁTICA DE LA SALUD

77 **FOROS Y SECTORES**

77 Foro de Telemedicina
78 Foro de Interoperabilidad
79 Foro de Gobernanza
80 Sector de Enfermería
81 Sector de Informática Médica
82 Sector de Farmacia

86 **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

COLEGIO OFICIAL DE FARMACÉUTICOS DE CÁCERES

COLEGIO OFICIAL DE FARMACÉUTIOS DE BADAJOZ

IDCSALUD

MUTUA UNIVERSAL

MUTUAL CYCLOPS-CENTRE DOCUMENTACIÓ

EMERGRAF, S.L. CREACIONES GRÁFICAS

HOSPITAL CLINIC. SISTEMAS DE INFORMACIÓN

CONSEJO GENERAL DE COLEGIOS OFICIALES DE FARMACÉUTICOS

OSAKIDETZA - SERVICIO VASCO DE SALUD

COLABORADORES TECNOLÓGICOS

Atos

connectis

FUJITSU

gmv

Ibermática

indra

INFORMÁTICA El Corte Inglés

SIEMENS Healthineers

InterSystems Health | Business | Government

PHILIPS

Acciones para la transformación digital del sector salud

En este primer número del año, no podemos dejar de destacar algunos temas que impulsamos en 2017, enmarcados todos ellos en la transformación digital del sector salud, como la reutilización de la información de salud, interoperabilidad para la atención integrada y la continuidad de los cuidados sanitarios y sociales, sistemas de soporte a la decisión clínica, la necesidad de líderes digitales, herramientas de salud conectada y, en concreto, para la salud mental.

No podemos olvidar por su relevancia el Máster en Dirección de Sistemas y Tecnologías de la Información y la Comunicación para la Salud, ya en su IV edición.

Una función esencial que realiza nuestra Sociedad es disponer de un observatorio que permita presentar la situación y evolución de la innovación en nuestro sector; por ello ofrecemos anualmente desde 2012: el ÍNDICE SEIS, que nos permite conocer la situación real de la inversión en sistemas de información en el SNS. En estos momentos se está elaborando el ÍNDICE correspondiente a 2017, del que esperamos poder ofrecer sus resultados en el próximo Congreso Nacional de Informática de la Salud en el mes de marzo.

Iniciamos nuestro trabajo del año 2018, bajo el hilo conductor planificado para este cuatrienio: promover la innovación, incrementar la inversión, obtener indicadores de resultados de los proyectos TIC y destacar las oportunidades que la tecnología y la situación actual nos permiten. También exponer los frenos existentes y realizar acciones para superarlos. Estas acciones se podrán seguir a través de las redes sociales, de nuestra web seis.es y de nuestra revista I+S.

La SEIS es una Sociedad abierta a otras sociedades, asociaciones e instituciones, ya que nuestro interés es impulsar la innovación, avanzar en la transformación digital del sector salud y, para ello, es necesario contar con el esfuerzo de todos los profesionales y de todas las organizaciones que participan de nuestro escenario.

La cooperación es imprescindible en un sector complejo como el nuestro, donde todos nuestros servicios tienen un objetivo común: la salud del ciudadano.

En esta línea de colaboración, agradecemos al Ministerio de Sanidad, Servicios Sociales e Igualdad que haya contado con la SEIS para impulsar la transformación digital del Sistema Nacional de Salud: objetivo del Convenio Marco de Colaboración que acabamos de firmar.

Debemos destacar la importancia de este número de nuestra revista, en el que incorporamos un especial sobre los cambios normativos en materia de seguridad y protección de datos, para el que contamos con la especial colaboración de la Agencia Española de Protección de Datos, además de la Agencia Vasca y la industria. Desde aquí nuestro agradecimiento.

Por su relevancia para el sector salud, hemos hecho coincidir este número con la próxima reunión del Foro de Seguridad y Protección de Datos de Salud que tratará sobre las responsabilidades de las organizaciones sanitarias, ante el nuevo reglamento que entra en vigor en mayo próximo.

Cuenta atrás hacia el 25 de mayo de 2018

Juan Díaz, *Coordinador Especial Nuevo Reglamento de Protección de Datos*

FALTAN APENAS TRES MESES PARA LA APLICACIÓN COMPLETA DEL REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS, Y NOS ENCONTRAMOS ANTE DUDAS DE CÓMO NOS AFECTA A LAS ORGANIZACIONES SANITARIAS, A SUS PROFESIONALES O LOS RECURSOS NECESARIOS PARA SU CUMPLIMIENTO.

El abordaje del Reglamento Europeo de Protección de Datos (RGPD) debe ser multidisciplinar e implica tener una estrategia para su desarrollo en los diferentes tipos de estructuras sanitarias. Establecer estos criterios dependen no solo de las nuevas normas o encaje con las existentes, sino de situación histórica y procedimientos establecidos a lo largo de muchos años.

Actualmente los pacientes son cada vez más conscientes de su papel central en la asistencia sanitaria y su capacidad de autodeterminación de su información y los usos que se hagan de la misma. La confianza que demuestran sobre la organizaciones sanitarias no puede ser desatendida y requiere extremar los aspectos de privacidad y seguridad de su información.

Para las organizaciones supone este nuevo marco un reto de mejora continua, ya que se plantea un modelo de revisión flexible de las medidas técnicas y organizativas a los diferentes tipos de tratamientos de los datos. Así como demostrar mediante evidencias que se hace uso de la información de salud adecuadamente, para garantizar al paciente sus derechos y evitar posibles riesgos en el manejo de la misma.

Adecuarse a la mejores prácticas no es una tarea sencilla ya que concurren intereses de los diferentes actores que participan en las organizaciones sanitarias, desde el núcleo fundamental que es la asistencia sanitaria inmediata hasta el resto de actividades (gestión, docencia, investigación, salud pública, etc.) conforman un complejo entramado que hace que la salud de todos mejores y sea eficiente.

El RGPD refuerza las garantías en el tratamiento de la información, siendo un reto armonizar los aspectos funcionales y su marco regulatorio, ya que aparecen cuestiones a dilucidar como: Cuales serán los criterios objetivos para notificar los incidentes de seguridad, asumir el papel de corresponsable con los Encargados de Tratamiento y destinar recursos para la vigilancia continua de la pertinencia sus procedimientos y resultados; establecer los registros sistemáticos de las evidencias de cumplimiento y que requieren un esfuerzo de normalización, desarrollo y soporte.

Otros retos son la ejecución de la Evaluaciones de Impacto en paralelo con la evaluaciones de riesgos de la seguridad de la información, ya que la mayoría las organizaciones sanitarias son públicas y cuando las privadas prestan servicios también aplican el cumplimiento del Esquema Nacional de Seguridad. Así como la demostración de la aplicación de los principios de privacidad y seguridad desde el diseño o la dificultad de demostración de los consentimiento expresos no firmados de las voluntades de los pacientes, ante casos de oposiciones al tratamiento de sus datos, la presencia de alumnos o su acceso a las historias clínicas.

Por último no podemos olvidar su impacto sobre la investigación sanitaria, donde la granularidad del consentimiento será clave, la valoración de las finalidades compatibles, el uso de la minimización de los datos, la anonimización, la necesidad de evaluaciones de impacto de privacidad para ese tratamiento de investigación y las posibles cesiones de datos a terceros.

Para ayudar a aclarar ciertas incógnitas se plantea este monográfico, donde se recoge la visión de la Agencia Española de Protección de Datos con diferentes artículos y en concreto una entrevista con su Directora para el abordaje de los diferentes aspectos fundamentales del RGPD, también recogemos la visión de la Agencia Vasca de Protección de Datos para acometer ordenadamente estos nuevos retos. Esperamos que este número especial de I+S ayude a aclarar parte de las cuestiones que nos asaltan a todos.

Nextel S.A.
Ingeniería y Consultoría

GDPR

Te ayudamos a proteger tus datos para la adecuación a la nueva LOPD



Infórmate sobre nuestra sesión formativa

www.nextel.es/sesion_gdpr

MAR ESPAÑA

Directora de la Agencia Española de Protección de Datos

"Los ciudadanos van a ver ampliados sus derechos y reforzado el control sobre sus datos personales"

¿Qué novedades en materia de Protección de Datos nos trae este año 2018?

La aplicación del Reglamento General de Protección de Datos (RGPD) el 25 de mayo va a marcar un punto de inflexión de forma transversal. Va a tener una repercusión importante entre los ciudadanos, que van a ver ampliados sus derechos y reforzado el control sobre sus datos personales en un mundo en el que la tecnología adquiere cada vez más importancia. Pero, sin duda, también va a suponer un cambio de mentalidad para las empresas y los organismos públicos que tratan datos personales. El cambio fundamental del Reglamento para aquellos que tratan datos es la denominada responsabilidad activa, es decir, asumir la protección de datos desde el punto de vista preventivo para evitar que haya que actuar una vez que el daño a los ciudadanos ya se ha producido.

> ***La Agencia ha visitado prácticamente todas las Comunidades Autónomas para explicar en los institutos autonómicos de Administración Pública y las confederaciones de empresarios las implicaciones del Reglamento en la actividad del tejido empresarial y las diferentes administraciones.***

¿Qué preparativos han realizado ante estos cambios la Agencia Española de Protección de Datos?

La Agencia está intensificando sus esfuerzos en diferentes ámbitos para facilitar el conocimiento de los principios y requerimientos que impone el nuevo Reglamento General de Protección de Datos, tanto con la participación en foros sectoriales como con la elaboración de materiales de ayuda como guías, orientaciones y herramientas para empresas, administraciones públicas y ciudadanos.

En el ámbito público y privado, la Agencia ha visitado prácticamente todas las Comunidades Autónomas para explicar en los institutos autonómicos de Administración Pública y las confederaciones de empresarios las implicaciones del Reglamento en la actividad del tejido empresarial y las diferentes administraciones. Asimismo, hemos trabajado con la Federación Española de Municipios y Provincias (FEMP) y estamos trabajando con el Consejo General de los Colegios Profesionales de Secretarios, Interventores y Tesoreros de Administración local (COSITAL)



> ***El cambio fundamental del Reglamento para aquellos que tratan datos es la denominada responsabilidad activa, es decir, asumir la protección de datos desde el punto de vista preventivo para evitar que haya que actuar una vez que el daño a los ciudadanos ya se ha producido"***

con el objetivo de ofrecer formación que facilite la adaptación de las entidades locales al Reglamento, así como con el Instituto Nacional de Administración Pública (INAP), celebrando jornadas para explicar los cambios normativos y sus implicaciones.

También hemos presentado Facilita RGPD, un cuestionario online gratuito para empresas y profesionales que tratan datos de bajo riesgo y, con el que pueden obtener los documentos mínimos indispensables para facilitar el cumplimiento del Reglamento. Siguiendo esta línea y para aquellas organizaciones que no pueden utilizar Facilita por tratar datos de riesgo medio o alto, estamos ultimando el lanzamiento de una Guía de Análisis de Riesgos y la actualización de nuestra Guía de Evaluación de Impacto. Adicionalmente estamos trabajando con los Colegios profesionales para promover fórmulas flexibles y de economías de escala en cuanto a los Delegados de Protección de Datos (DPD). En este punto es importante incidir en la figura del DPD, cuya designación es obligatoria para organizaciones que traten datos a gran escala o datos sensibles así como para organismos públicos. En este contexto, la AEPD ha promovido su Esquema de certificación de DPD junto a ENAC, aportando seguridad y fiabilidad tanto a las personas que van a ejercer estos puestos como a las empresas y organismos que tienen que contar con sus servicios. Y aunque esta certificación no es obligatoria para poder ejercer como DPD, este Esquema ofrece una garantía para acreditar la cualificación y capacidad profesional de los Delegados de Protección de Datos.

En paralelo, se encuentra en tramitación parlamentaria el Proyecto de Ley Orgánica de Protección de Datos. La Agencia participó activamente como miembro de la Ponencia de la Comisión que preparó el borrador de Anteproyecto de Ley, aportando sus conocimientos técnicos como órgano especializado y con la experiencia práctica derivada de la aplicación de la normativa actual.

¿Qué acciones han realizado en el ámbito de la salud?

La principal actuación ha sido 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 tiene un carácter preventivo e incluye 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 ha servido, también, para facilitar información a los responsables de servicios sanitarios sobre las implicaciones del Reglamento General de Protección de Datos.

En el Plan Estratégico 2015-2019 tenemos previsto además una Guía para profesionales sanitarios y otra para pacientes.

Para mejorar la confidencialidad y privacidad de los datos de salud, ¿qué recomendaciones en realizaría para nuestras instituciones sanitarias?

Las principales recomendaciones del Plan para mejorar la confidencialidad y la privacidad de los datos de salud están relacionadas con la mejora de la información a los pacientes, el establecimiento de normas internas que obliguen a la confidencialidad de los datos, la mejora de los controles de acceso a la información clínica, especialmente para pacientes que no están asignados al facultativo, y la realización de auditorías de seguridad en el plazo máximo de dos años.

También se han detectado, en algunos casos "islas de información departamentales" en las que se instalan aplicaciones sin conocimiento del responsable de seguridad del centro y, por tanto, con deficientes medidas de seguridad que deben ser corregidas.

El principio de RESPONSABILIDAD ACTIVA implicará que los servicios de salud deban establecer su registro de actividades de tratamiento, que sustituye 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.

¿Cómo afectará el nuevo Reglamento Europeo de Protección de Datos a los prestadores de Salud?

El Reglamento afecta de forma significativa a los prestadores de servicios de salud. El RGPD establece un nuevo modelo de cumplimiento basado en los principios de responsabilidad proactiva, enfoque de riesgo y protección de datos desde el diseño y por defecto.

Este modelo contempla un abanico de medidas de cumplimiento que serán particularmente aplicables en los servicios de salud al tratarse masivamente datos especialmente protegidos.

¿El principio de Accountability o Responsabilidad Activa que cambios supone?

El principio de responsabilidad activa implicará que los servicios de salud deban establecer su registro de actividades de tratamiento, que sustituye 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. Asimismo deberán actualizar sus cláusulas informativas y revisar los contratos de prestación de servicios que tengan externalizados para adaptarlos al Reglamento General de Protección de Datos.

¿Cuál es el papel de los Directivos de las Organizaciones Sanitarias para impulsar y cumplir con el nuevo marco legal?

Los directivos de las organizaciones sanitarias tienen un papel esencial para impulsar el nuevo modelo de cumplimiento en materia de protección de datos. En particular, deberían designar al Delegado de Protección de Datos para que colabore con la organización en el proceso de adaptación al Reglamento, que será aplicable el 25 de mayo de este año.

La figura del DPD se caracteriza por su independencia, por lo que en su designación deben evitarse incompatibilidades y conflictos de intereses con las actividades de la organización implicadas en la aplicación del Reglamento.

Además, debe garantizarse su acceso directo a los niveles de dirección de la organización. Por otra parte, los directivos deben impulsar en colaboración con el DPD la formación de todo el personal en esta materia.

¿Cuáles son los retos de la figura del Delegado de Protección de Datos en el Sector Salud?

Dada la complejidad de los tratamientos de datos en el ámbito de la salud, que abarcan desde la asistencia clínica hasta las diversas modalidades de investigación sanitaria, el Delegado de Protección de Datos, además de un conocimiento detallado de la normativa de protección de datos y de la regulación sectorial sanitaria, debe tener una cualificación profesional sobre el conocimiento de las organizaciones sanitarias y capacidad para mantener una relación fluida con ellas.

En consecuencia, se debe facilitar su formación especializada en estos ámbitos y dotarle de recursos para que pueda desarrollar su función.

¿Cómo afectará el nuevo reglamento sobre los profesionales sanitarios?

Los profesionales sanitarios deben obtener información sobre el conjunto de garantías previstas en el Reglamento General de Protección de Datos, para lo que es preciso insistir en la necesidad de que se promocione la formación a estos profesionales a fin de que puedan contribuir a un adecuado cumplimiento de la normativa de protección de datos.

¿Cómo se verán afectados os tratamientos de datos para investigación por el nuevo reglamento?

> ***"La SEIS ha tenido tradicionalmente el reconocimiento y la colaboración de la Agencia por su intensa actividad de promoción y difusión del derecho a la protección de datos en el sector sanitario, llevando a cabo una actividad pionera cuando se han producido cambios normativos sobre este derecho"***

El Reglamento promueve el tratamiento de la información con fines de investigación con carácter general y, en particular, en el ámbito sanitario. No obstante, la investigación sanitaria es una actividad sobre la que existe un amplio abanico de regulaciones sectoriales como son, entre otras, la normativa sobre ensayos clínicos con medicamentos o la investigación biomédica, en la que se recogen garantías específicas para el tratamiento de datos personales que deberán ser interpretadas conforme a las previsiones del Reglamento. En estas modalidades de investigación jugarán un papel relevante los procesos de seudonimización y anonimización de la información, especialmente cuando se desarrollen con tecnologías de tratamientos masivos de datos como el Big Data.

Asimismo, debe tenerse en cuenta que los proyectos de investigación deberán ir acompañados de evaluaciones de impacto en la protección de datos personales.

¿Cómo valora desde la AEPD el papel que la Sociedad Española de Informática de la Salud está representando en la difusión y promoción de los derechos de los ciudadanos en materia de su información de salud?

La SEIS ha tenido tradicionalmente el reconocimiento y la colaboración de la Agencia por su intensa actividad de promoción y difusión del derecho a la protección de datos en el sector sanitario, llevando a cabo una actividad pionera cuando se han producido cambios normativos sobre este derecho, como está sucediendo en el momento presente con la aplicación el Reglamento General de Protección de Datos.



Global Factory, S.L. es una compañía de 'Consultoría' comprometida con la innovación, el desarrollo y la aplicación de nuevas soluciones en materia de seguridad, derecho y protección de datos.

Global Factory, cuenta con un equipo de profesionales cualificado, experimentado y dinámico, que combina equilibradamente las disciplinas técnica y jurídica.

R.G.P.D.

Adecuación al cumplimiento del RGPD
Delegado de Protección de Datos - DPO
Evaluaciones de impacto - Análisis de Riesgos
Registro de las actividades de tratamiento, ...

e-Learning - FORMACIÓN

Reglamento europeo de protección de datos RGPD
Protección de datos sanitarios
e-Administración, Firma electrónica
Software libre, Open data, ...

SERVICIOS JURÍDICOS

Derecho Digital
Informes Jurídicos TIC
Asesoramiento RGPD

CIBERSEGURIDAD

Protección
Concienciación
Reputación
Resiliencia

AUDITORÍA

Sistemas de Información
Protección de Datos
Esquema Nacional de Seguridad

Global Factory, S.L.
Nervión 3 5º Planta
48001 Bilbao
www.globalfactory.es
gfbilbao@globalfactory.es
94 661 27 74

DIGITALIZACIÓN
NÓMINAS
CALL CENTER

El Reglamento General de Protección de Datos y su aplicación en el ámbito sanitario

Rafael García
Agencia Española de Protección de Datos

EL RÉGIMEN DE PROTECCIÓN DE DATOS EN LA UNIÓN EUROPEA ESTÁ BASADO EN UNA NORMA QUE EN ESTOS MOMENTOS TIENE MÁS DE 20 AÑOS DE VIGENCIA: LA DIRECTIVA 95/46. DESDE SU APROBACIÓN HEMOS ASISTIDO A UN DESARROLLO EXPONENCIAL DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN Y UNA UNIVERSALIZACIÓN EN SU USO. ESTO ES ESPECIALMENTE CIERTO PARA TODOS LOS SERVICIOS ASOCIADOS A INTERNET.

El rápido avance tecnológico y sus consecuencias, unido a cambios en los modelos de actividad económica y también a modificaciones en el marco legislativo europeo derivadas del Tratado de Lisboa, condujeron a la revisión de esa norma central para adaptarla a las nuevas circunstancias.

La norma elegida para llevar a cabo esta adaptación es el Reglamento General de Protección de Datos 2016/679 (RGPD)[1].

La elección de un acto jurídico como es un reglamento supone, en sí misma, un primer factor a considerar a la hora de analizar los efectos de la nueva normativa sobre los ordenamientos nacionales. Los reglamentos son normas de directa aplicación, que despliegan sus efectos sobre el derecho interno de los Estados Miembross sin necesidad de normas nacionales de trasposición. Los reglamentos, desde su publicación y entrada en vigor, se convierten en norma aplicable directamente en toda la Unión como si de una norma nacional más se tratara, y con la particularidad de que sus disposiciones prevalecen sobre las normas de derecho interno que sean contrarias a ellos.

La decisión de utilizar un reglamento para reemplazar a la actual directiva tenía como objetivo lograr una mayor armonización, en realidad una unificación, del derecho europeo a la protección de datos. La experiencia de los años de vigencia de la Directiva del 95 enseñaba que a pesar de que existía un sustrato general común a todos los Estados Miembros, los desarrollos nacionales de la Directiva habían dado lugar también a discrepancias significativas en los diferentes sistemas nacionales, lo que ha conducido a niveles también diferentes de protección del derecho.

La adopción del RGPD pretende poner fin a esas discrepancias, sustituyendo las normas nacionales por una sola norma europea.

A ese fin debiera contribuir otra de las características propias de los reglamentos, que ofrecen posibilidades de desarrollo o aplicación normativa interna muy limitadas. Sólo cuando el Reglamento explícitamente prevé que los Estados puedan tomar medidas para complementar sus disposiciones o cuando esas medidas sean indispensables para permitir la aplicación del reglamento podrán esos Estados aprobar normas internas.

En el caso del RGPD, este rasgo característico de los reglamentos europeos se cumple, aunque con matices. El RGPD contiene un número

1. Debe señalarse que junto con el RGPD fue aprobada también una Directiva sobre tratamientos de datos en los ámbitos policial y judicial penal, la Directiva 2016/680. Sin embargo, y dada la especialidad de esta norma, no será mencionada a lo largo de esta presentación.

significativo de previsiones en que se remite al derecho nacional o que permiten a los Estados actuar normativamente en aplicación del Reglamento. Algunas de estas disposiciones afectan al ámbito sanitario, y posteriormente se hará una referencia más concreta a ellas.

En todo caso, es útil tener en cuenta que el RGPD será la pieza central de un marco normativo de protección de datos integrado por el propio Reglamento, normas nacionales generales de protección de datos (que en el caso español será la futura Ley Orgánica de Protección de Datos, actualmente en fase de tramitación parlamentaria) y normas nacionales sectoriales que incluyan previsiones en materia de protección de datos.

En el ámbito sanitario, objeto de detalladas regulaciones internas en la mayoría de los Estados Miembros, esta situación será especialmente evidente.

Más allá de los aspectos formales, el contenido del RGPD define un modelo de protección de datos basado en tres ejes fundamentales: refuerzo de los principios y derechos clásicos ya presentes en el diseño de la Directiva, cambio en el enfoque de las obligaciones de quienes tratan datos personales y consolidación del sistema de supervisión basado en autoridades administrativas independientes y especializadas.

En el terreno de los principios y derechos, el RGPD avanza un paso con respecto a la Directiva en la medida en que aborda el derecho a la protección de datos como tal derecho fundamental. En la Directiva, la regulación derivaba de la necesidad de evitar que las exigencias del derecho a la protección de datos se convirtieran en un obstáculo a la libre de circulación de personas, bienes, servicios y capitales que define lo que ahora conocemos como Mercado Interior.

Sin embargo, aparte de su reconocimiento en las constituciones de los Estados Miembros, el derecho a la protección de datos está incluido como tal en la Carta Europea de Derechos Fundamentales y en el Tratado de Lisboa. El RGPD, por tanto, se hace eco de esta nueva caracterización de la protección de datos y establece que su objeto es no sólo asegurar la libre circulación de los datos personales, sino también establecer reglas para garantizar ese derecho.

Ese enfoque de la protección de datos como un derecho fundamental tiene importantes consecuencias. La principal es, sin duda, que sus efectos se extienden a todos los ámbitos y no se limitan al de las relaciones de consumo, o se fraccionan en función del sector económico en que se proyecten.

El RGPD retoma en gran medida los mismos principios que han de presidir todo tratamiento de datos personales que ya enunciaba la Directiva. Principios como los de licitud, lealtad y transparencia, limitación de finalidad o minimización de datos que ya formaban el régimen de protección de datos en Europa se mantienen en el nuevo texto.

La principal novedad en este catálogo es la inclusión de un principio de "integridad y confidencialidad", según el cual los datos deben ser tratados de manera que se garantice una seguridad adecuada.

Por otro lado, se añade otro principio de "accountability" o "responsabilidad proactiva", que supone que los responsables de tratamiento asumen la responsabilidad por el cumplimiento de todos los demás principios recogidos en el Reglamento y deben ser capaces de demostrar que están en condiciones de hacerlo. Este principio se relaciona directamente con ese segundo eje respecto a las obligaciones de los responsables que ya se ha mencionado y sobre el que se volverá posteriormente.

El principio de licitud o legalidad de los tratamientos exige que todo tratamiento de datos se legitime en una base jurídica. El RGPD recoge las mismas seis bases jurídicas que ya se incluían en la Directiva: consentimiento del interesado, que el tratamiento sea necesario para la ejecución de un contrato, que sea necesario para atender un interés vital de interesado o de terceros, que sea necesario para cumplir una obligación legal impuesta al responsable, que sea necesario para satisfacer un interés público o para el ejercicio de poderes públicos o, finalmente, que sea necesario para satisfacer intereses legítimos del responsable o de terceros a los que se comuniquen los datos siempre que sobre esos intereses no prevalezcan los derechos, libertades o intereses de los afectados.

Como se indica, no hay aquí cambios sustanciales respecto de la Directiva, y, consecuentemente, tampoco debiera haberlos respecto a las disposiciones nacionales que la trasponen. Sin

embargo, lo cierto es que esas trasposiciones han implicado en ocasiones determinadas opciones a favor o en contra de alguna o algunas de las bases jurídicas, cuando todas ellas se presentan en pie de igualdad.

En el caso de España, nuestra vigente LOPD parece establecer una posición privilegiada para el consentimiento, dado que su artículo 6 señala que sólo serán válidos los tratamientos que cuenten con ese consentimiento y presenta otras opciones de un modo que podría considerarse como excepciones a este principio general. El RGPD zanja definitivamente estas diferentes interpretaciones. Todas las bases jurídicas tienen el mismo valor, y su uso dependerá de las circunstancias propias de cada tratamiento.

Dicho lo anterior, es también cierto que el RGPD concede una mayor atención a la base jurídica del consentimiento, sin duda porque es la que más directamente se relaciona con el ejercicio por parte de los afectados del control sobre sus datos personales.

En este punto, el Reglamento contiene una definición de consentimiento que puede suponer cambios en la legislación y en la práctica de algunos Estados Miembross, entre ellos España.

El RGPD exige que el consentimiento sea libre, informado, específico e inequívoco. Estos requisitos son los mismos que fija la Directiva. Pero el Reglamento añade que para considerar el consentimiento como inequívoco, debe prestarse mediante una declaración o mediante una "clara acción afirmativa" que indique que el interesado acepta el tratamiento de sus datos.

La referencia a la "clara acción afirmativa" implica que dejan de ser válidos los consentimientos fundados en la inacción o la falta de reacción de los interesados, algo que en determinadas circunstancias y bajo condiciones estrictas venía permitiendo hasta ahora nuestra normativa de protección de datos.

Por otra parte, el Reglamento se refiere específicamente al consentimiento en contextos determinados, y uno de ellos es el de la investigación científica. Según su Considerando 33, y dado que con frecuencia no es posible determinar totalmente la finalidad de un tratamiento con fines de investigación en el momento de recogida de los datos, debe permitirse que los interesados den su consentimiento para ámbitos de investigación científica que respeten las normas éticas reconocidas para la investigación científica. Al mismo tiempo, debe permitirse a los interesados limitar su consentimiento a determinadas áreas de investigación o partes de proyectos de investigación siempre que lo permita la finalidad perseguida.

Siguiendo con las bases jurídicas previstas por el RGPD, es interesante destacar que uno de los ámbitos en que se deja flexibilidad a los Estados Miembross para complementar sus previsiones es el de las condiciones de los tratamientos cuando se realicen en cumplimiento de una obligación legal para el responsable, en ejercicio de poderes públicos o para el logro de fines de interés público.

En todos estos casos, los Estados podrán introducir especificaciones a las condiciones generales de tratamiento establecidas por el Reglamento. Estas especificidades pueden incluir, como señala a título ilustrativo el Considerando 45 del RGPD, la determinación del responsable del tratamiento, el tipo de datos personales objeto de tratamiento, los interesados afectados, las entidades a las que se pueden comunicar los datos personales, las limitaciones de la finalidad, el plazo de conservación de los datos y otras medidas para garantizar un tratamiento lícito y leal.

El mismo Considerando menciona expresamente entre los fines de interés público los fines sanitarios como la salud pública, la protección social o la gestión de servicios sanitarios.

En relación con el principio de licitud, pero también con el de limitación de finalidad, el Reglamento mantiene el criterio de la Directiva en el sentido de considerar las finalidades de investigación científica, históricas y estadísticas como compatibles con las finalidades originarias a los efectos de tratamientos ulteriores. A esta lista se añaden como novedad las finalidades de archivística en interés público.

El Reglamento señala en su Considerando 50 que cuando los datos sean tratados para una nueva finalidad compatible, no se requerirá una base jurídica aparte, distinta de la que permitió la obtención inicial de los datos. Esta afirmación, sin embargo, parece que debe matizarse para los casos en que el tratamiento originario estuviera basado en el consentimiento o en obligaciones legales, ya que para esos supuestos el propio

Considerando contiene previsiones específicas que parecen descartar que el consentimiento inicial o la misma obligación puedan servir para tratamientos ulteriores.

El tratamiento de las "categorías especiales de datos", los conocidos como datos sensibles, sigue en el RGPD los mismos parámetros que establece la Directiva del 95, es decir, existe una prohibición genérica de tratar estos datos, que se levanta cuando sea aplicable alguna de las excepciones que el mismo Reglamento establece.

Existen, sin embargo, algunas novedades. La primera es que se amplía la lista de datos sensibles con dos nuevas categorías, los datos genéricos, considerados sensibles al margen de su vinculación con los datos de salud, y los datos biométricos que permitan la identificación unívoca de una persona física.

Además, el Reglamento establece claramente que la aplicación de las excepciones debe hacerse solo si se respeta el resto de sus disposiciones, mencionando específicamente las relativas a la licitud del tratamiento. Ello significa que en los casos en que una excepción no se remita en sí misma a una base jurídica legitimadora del tratamiento, como sucede, por ejemplo, cuando se autoriza a tratar los datos para cumplir las obligaciones legales del responsable como empleador según el derecho laboral de los Estados Miembros, el tratamiento deberá basarse en alguna de las bases previstas en su Artículo 6.1.

Finalmente, la lista de excepciones del Reglamento se amplía significativamente respecto a la contenida en la Directiva e incluye, en muchos casos remisiones a las condiciones que establezca el derecho nacional.

Así sucede con las excepciones contenidas en las letras g), h) e i) de su Artículo 9, en las que el tratamiento de los datos sensibles por razones de interés público esencial, para finalidades asistenciales y para finalidades de salud pública podrá llevarse a cabo en los términos que determinen el Derecho de la Unión o de los Estados Miembros, que deberá establecer medidas para proteger los derechos y libertades de los interesados.

De hecho, el apartado 4 del mismo artículo autoriza a los Estados Miembros a mantener o introducir condiciones adicionales, se entiende que a las previstas en el Reglamento, para el tratamiento de datos genéticos, biométricos o relativos a la salud.

La forma en que están configuradas estas excepciones es importante, ya que el RGPD renuncia a fijar de forma rígida o detallada las condiciones en que podrán tratarse los datos sensibles para estas finalidades, características en el ámbito sanitario. Será la legislación de los Estados la que deberá determinar, manteniendo la legislación existente en todo lo que no sea incompatible con el RGPD por otros motivos o introduciendo nuevas regulaciones.

El mismo criterio, aunque de un modo más confuso, lo aplica el Reglamento al tratamiento de datos sensibles con fines de archivística pública, investigación científica, históricos y estadísticos.

La continuidad que el Reglamento mantiene respecto a la Directiva 95/46 respecto a los principios generales del tratamiento, bases jurídicas y datos sensibles se extiende también a los derechos de los interesados, aunque también hay novedades que apuntan a un reforzamiento del control de los interesados sobre sus datos personales.

Estas novedades comienzan con la información que debe proporcionarse a los afectados para el tratamiento de sus datos.

El Reglamento trata la información en el contexto de un principio más general, que es el de transparencia. Este principio alcanza tanto al contenido y formato de la información como al modo en que deben articularse los mecanismos para que los interesados ejerzan sus derechos como a la forma en que debe responderse a esos ejercicios de derechos.

En el Reglamento se amplía el contenido de la información que los responsables deben ofrecer a los interesados al tratar sus datos, tanto cuando los obtienen directamente de ellos como cuando proceden de otros responsables. Al mismo tiempo, se exige que esa información se proporcione de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.

En materia de derechos de los interesados, se consagran los conocidos como derechos ARCO, es decir, los derechos de acceso, rectificación, cancelación (que el RGPD denomina supresión) y oposición, añadiéndose como nuevos derechos el de limitación en el tratamiento y el de portabilidad.

El derecho de limitación de tratamiento supone que las operaciones de tratamiento de datos deben suspenderse en determinadas circunstancias para favorecer los intereses de los afectados. Estas circunstancias son de dos tipos. Por un lado, los casos en que el interesado ha ejercido su derecho de rectificación u oposición. Cuando esto ocurra, el responsable deberá suspender el tratamiento hasta que decida sobre la solicitud. Las razones son evidentes. Si los datos que están siendo tratados son incorrectos o si los motivos del interesado para oponerse son fundados, seguir tratando los datos puede generar algún tipo de daño para los interesados. La suspensión actúa como medida preventiva en favor de los afectados.

El otro supuesto de limitación tiene que ver con la operación de tratamiento consistente en el borrado de los datos. El Reglamento prevé que el interesado pueda solicitar que los datos que hubieran debido ser borrados se conserven por el responsable cuando sean necesarios para que el interesado pueda gestionar reclamaciones o cuando el interesado así lo solicite en los casos de tratamiento ilícito.

El derecho a la portabilidad se puede considerar, hasta cierto punto, como una modalidad avanzada del derecho de acceso. Básicamente consiste en que el interesado puede solicitar al responsable que le transmita los datos que está tratando a fin de enviarlos a otro responsable para su tratamiento, o incluso que esa transmisión sea directa entre responsable y responsable cuando sea técnicamente posible.

El derecho solo puede ejercerse respecto a datos que el interesado haya proporcionado al responsable y que le conciernan y cuando el tratamiento se lleve a cabo por medios automatizados. Además, solo afecta a tratamientos que estén fundados en el consentimiento del interesado o en la necesidad de utilizar los datos para ejecutar un contrato.

Es interesante subrayar que este derecho a la portabilidad se establece y regula desde la perspectiva de la protección de datos y, en ese sentido, complementa o completa otras formas de portabilidad que puedan existir en sectores concretos como podrían ser el bancario, el de telecomunicaciones o el sanitario. En las aproximaciones sectoriales, la portabilidad se asocia con los derechos de consumidores y usuarios, mientras que en el terreno de la protección de datos es este derecho fundamental el que se promueve otorgando al interesado una posibilidad adicional de control de su información personal.

El segundo de los grandes ejes que se mencionaban al principio es el del nuevo enfoque en las obligaciones de quienes tratan datos personales. Un nuevo enfoque que se articula sobre los conceptos de "responsabilidad proactiva" o preventiva ("accountability", según el término inglés) y riesgo.

El primero de ellos, que como se ha indicado el Reglamento trata como principio general, supone que el responsable está obligado a aplicar medidas técnicas y organizativas eficaces para garantizar que cumple con el RGPD y estar en condiciones de poder demostrarlo.

Desde esta perspectiva puede decirse que el Reglamento va más allá del planteamiento de cumplimiento imperante en la actualidad, basado en que hay una obligación de cumplir la norma y si se producen incumplimientos puede haber sanciones o reparaciones determinadas por los tribunales, a un enfoque centrado en la prevención y el manejo consciente y responsable de quienes tratan datos.

Se espera que quien trata datos no solo no incumpla la ley, sino que implante medidas que aseguren razonablemente que la ley no se va a infringir. La razón fundamental para esta nueva aproximación es que, debido a las características de los actuales modelos de tratamiento de información, cuando se produce una vulneración del marco legal se pueden causar a los afectados daños irreparables que difícilmente se compensan con la sanción o incluso con indemnizaciones.

El catálogo de medidas de cumplimiento incluye:

- Mantener un registro de actividades de tratamiento
- Aplicar medidas de Protección de Datos desde el Diseño y de Protección de Datos por Defecto.
- Aplicar medidas de seguridad adecuadas.
- Llevar a cabo Evaluaciones de Impacto.
- Consultar con las autoridades de protección de datos la puesta en marcha de determinados tratamientos.
- Designar a un Delegado Protección de Datos (DPD).

- Notificación de Quiebras de Seguridad.
- Posibilidad de adhesión a códigos de conducta y esquemas de certificación…

Algunas de estas medidas están ya presentes en la legislación actual, como sucede con las relativas a la seguridad de los tratamientos. Otras, como sería el caso del registro de actividades de tratamiento, son una versión actualizada de medidas también existentes, en concreto de la obligación de notificar ficheros y tratamientos a la autoridad de supervisión, que desaparece como tal en el RGPD. Otras se aplican solo sectorialmente, como ocurre con la obligación de notificar quiebras de seguridad, que en la actualidad solo está vigente en el ámbito de las comunicaciones electrónicas.

Otro grupo, sin embargo, resulta más innovador, al menos en lo que se refiere a la legislación española. La realización de evaluaciones de impacto sobre la protección de datos, el nombramiento de un delegado de protección de datos en determinadas organizaciones y la introducción de los esquemas de certificación, junto con los códigos de conducta, como instrumentos para poder acreditar el cumplimiento de la normativa son ejemplos de estas nuevas medidas de cumplimiento.

Junto con la dimensión proactiva y preventiva, el segundo criterio usado por el RGPD es el del riesgo. Es obvio que no todos los tratamientos pueden afectar de igual modo a los derechos o intereses de los afectados. Un tratamiento que incluye gran cantidad de datos sobre millones de personas o categorías especiales de datos tendrá potencialmente más impacto sobre los afectados que uno que afecte solo a unos pocos cientos o que se limite a datos demográficos básicos.

Por ello, el Reglamento prevé que las medidas de cumplimiento se apliquen teniendo en cuenta ese riesgo diferenciado que los tratamientos pueden suponer para los ciudadanos.

El riesgo en el RGPD funciona en un doble sentido. Por un lado, algunas medidas deberán implantarse solo si el tratamiento previsto supone un alto riesgo para los derechos y libertades. Es lo que sucede con las evaluaciones de impacto, que solo deberán realizarse en ese supuesto.

En otros casos, el riesgo sirve como factor de modulación de las medidas a aplicar. Así ocurre con las medidas de seguridad o las medidas de protección de datos desde el diseño y por defecto, que deberán decidirse y ponerse en práctica teniendo en cuenta las circunstancias que rodean el tratamiento y, señaladamente, el nivel y tipo de riesgo que suponga para los derechos de los interesados.

El hecho de que la aplicación de las medidas de cumplimiento esté ligada al riesgo de los tratamientos implica que las organizaciones que tratan datos han de llevar a cabo necesariamente un análisis de esos riesgos como requisito previo al inicio de cualquier tratamiento o cuando varíen significativamente las circunstancias que rodean un tratamiento.

Un aspecto en el que se proyectan igualmente estos criterios es el de las relaciones entre los responsables de tratamiento, que el RGPD sigue definiendo como los que deciden sobre los fines y medios de un tratamiento, sobre su propia existencia, y los encargados, que son quienes llevan a cabo operaciones de tratamiento por cuenta del responsable.

El RGPD regula con detalle esas relaciones, estableciendo como premisa básica que el responsable solo podrá encargar operaciones de tratamiento a personas u organizaciones que ofrezcan las garantías suficientes para aplicar medidas apropiadas para que el tratamiento sea conforme con el Reglamento y garantice la protección de los derechos del interesado. Dicho en otros términos, el RGPD extiende las consecuencias del principio de responsabilidad proactiva a los encargados de tratamiento, si bien es el responsable el que está obligado a verificar que estos satisfacen los requisitos exigidos.

Por otra parte, el Reglamento incluye una lista extensa, aunque no exhaustiva, de los contenidos que necesariamente han de incluirse en los instrumentos que formalicen las relaciones entre responsables y encargados. El objetivo es, nuevamente, asegurar que cuando el responsable externaliza operaciones de tratamiento lo hace ejerciendo plenamente su responsabilidad sobre el tratamiento.

No obstante, y como novedad, el Reglamento asigna también obligaciones y responsabilidades propias a los encargados, por ejemplo, en lo que se refiere a medidas de seguridad, a la nece-

sidad de informar al responsable de quiebras de seguridad o a la obligación de designar un delegado de protección de datos.

Aunque no se relaciona de un modo tan directo con la aproximación de "accountability", en la regulación que el Reglamento hace de las transferencias internacionales de datos hay también algunos elementos que pueden atribuirse a la influencia de este enfoque.

El modelo de transferencias que el RGPD establece es paralelo al que ahora conocemos. El principio general es que los datos solo pueden enviarse a países, o sectores dentro de países, y organizaciones internacionales que ofrezcan un nivel de protección adecuado. La noción de "nivel de protección adecuado" fue precisada por el Tribunal de Justicia de la Unión Europea en su Sentencia sobre el caso Schrems, en la que señalaba que ese nivel ha de ser "sustancialmente equivalente" al que reciben los datos dentro de la Unión.

En los casos en que no se haya reconocido formalmente que el país de destino otorga protección adecuada a los datos, podrá recibirlos siempre que el exportador ofrezca garantías suficientes para la operación u operaciones de transferencia concretas.

La novedad en el Reglamento es que se amplía el número y la naturaleza de los instrumentos por los que se pueden ofrecer esas garantías y también el hecho de que en la gran mayoría de los casos, y dependiendo del tipo de instrumento empleado, no será preciso obtener la autorización de las autoridades de supervisión.

La última posibilidad, en ausencia de declaración de adecuación y de garantías específicas para una transferencia o grupo de transferencias es que pueda aplicarse alguna de las causas de excepción que el Reglamento establece. La lista de excepciones es también muy similar a la contenida en la Directiva del 95, si bien se ha añadido una que evoca muy claramente el principio de "accountability".

Se trata de que puedan realizarse transferencias que no sean repetitivas y que afecten solo a un número limitado de interesados cuando sean necesarias para satisfacer "intereses legítimos imperiosos" perseguidos por el responsable del tratamiento sobre los que no prevalezcan los intereses o derechos y libertades del interesado, siempre que el responsable haya evaluado todas las circunstancias de la transferencia y aplicado las garantías adecuadas.

El tercer y último aspecto central del RGPD es el relativo al sistema de supervisión.

También aquí el Reglamento es tributario del modelo consagrado por la Directiva y opta por mantener la protección del derecho por la vía administrativa a a través de autoridades administrativas independientes y especializadas. Las comúnmente conocidas como autoridades de protección de datos, que el Reglamento denomina "autoridades de control".

El Reglamento refuerza la independencia, posición y poderes de estas autoridades, ampliando a todas ellas, por ejemplo, la potestad sancionadora, que hasta ahora solo habían incluido en sus legislaciones nacionales algunos Estados Miembros, entre ellos España.

Al mismo tiempo, el Reglamento establece un paralelismo entre su ámbito de aplicación, que es toda la Unión Europea, con los procedimientos de supervisión y control, introduciendo criterios de cooperación y coherencia dirigidos a conseguir tanto que los tratamientos que tengan un alcance supranacional sean controlados a ese nivel como que las decisiones que puedan tomar las autoridades de control sean consistentes en toda la Unión.

Pieza clave de esta dimensión europea de la supervisión es el Comité Europeo de Protección de Datos. El Comité, que sucede al actual Grupo Europeo de Autoridades de Protección de Datos, el conocido como Grupo del Artículo 29, se crea como organismo de la Unión Europea, con personalidad jurídica propia e integrado por un representante de las autoridades de supervisión de cada Estado Miembros.

Al Comité se le atribuyen amplias funciones consultivas y de guía y directriz en la aplicación del RGPD, así como la posibilidad de adoptar dictámenes que vinculan a sus Miembross en algunas materias y de dictar decisiones jurídicamente vinculantes para resolver las discrepancias entre autoridades en determinados casos.

A través de estos dictámenes y decisiones, el Comité interviene en los denominados mecanismos de cooperación y de consistencia.

El mecanismo de cooperación está basado en la

idea de que cuando un responsable o encargado está establecido en varios Estados Miembros o trata datos de personas en varios Estados Miembros, la supervisión de sus actividades debe llevarse a cabo de forma cooperativa por todas las autoridades de control de los Estados afectados, bajo la coordinación de una autoridad de control, que será la del Estado donde el responsable o encargado tenga su establecimiento principal.

Cuando en un caso concreto, que puede ser el resultado de una reclamación o de una investigación emprendida por las autoridades, existe acuerdo entre todas ellas sobre una propuesta de decisión que presenta la autoridad líder, la decisión puede ser adoptada. Cuando, por el contrario, alguna o alguna de las autoridades afectadas discrepa de esa decisión, el caso es elevado al Comité Europeo, que zanja esas discrepancias mediante las mencionadas decisiones vinculantes.

El sistema es complejo y no es este el lugar para desarrollarlo in extenso, pero lo fundamental respecto a él es que en todos los casos en que una organización esté establecida en varios Estados de la Unión o trate desde un único Estado datos de personas en varios Estados Miembros, las decisiones sobre la conducta de esa organización no podrán ser ya adoptadas unilateralmente por una autoridad de supervisión respecto al establecimiento que la organización tenga en el correspondiente Estado. Las decisiones deberán ser consensuadas entre todas las autoridades afectadas y la coordinación del proceso corresponderá a la autoridad del establecimiento principal y no necesariamente a la autoridad que recibió una reclamación o que consideró necesario iniciar una investigación.

Se ha indicado que en la nueva regulación se concede a todas las autoridades de supervisión potestad sancionadora. Esa previsión va acompañada en el RGPD de un régimen sancionador completo, que incluye tanto medidas correctivas a aplicar frente a una infracción como un catálogo de los casos en que podrá producirse una infracción.

Entre las medidas correctivas se incluyen las sanciones económicas, que podrán establecerse en cuantías cuyos límites el Reglamento fija no sólo por referencia a cantidades absolutas, sino también en relación con el volumen de negocio anual global de la organización sancionada. Enconcreto, y dependiendo de qué disposición del RGPD se haya infringido, las multas podrán llegar hasta 10 millones de euros, o en el caso de empresas un 2 por ciento del volumen de negocio anual global, y hasta 20 millones de euros o un 4 por ciento del volumen de negocio.

El Reglamento se hace eco de la realidad existente en varios Estados Miembros de la Unión, en los que las entidades públicas no son objeto de sanciones económicas, y ha incluido una disposición dando a los Estados la posibilidad de decidir en su legislación si se impondrán, y en qué medida, multas a autoridades y organismos públicos.

Con este Reglamento General de Protección de Datos, que se complementa con la Directiva sobre protección de datos en los ámbitos policial y judicial penal y, en el futuro, con la norma que reemplace a la vigente Directiva 2002/58, sobre privacidad en las comunicaciones electrónicas, la Unión Europea ha pretendido diseñar un marco de protección adaptado a las exigencias de los desarrollos tecnológicos, económicos y legales que han tenido lugar en los últimos años.

Los cambios que se proponen tendrán, sin duda, un impacto en las organizaciones que manejan datos personales. Algunos de estos efectos se extenderán a todas ellas. Otros, como puede ocurrir en el ámbito sanitario, tendrán características propias y diferenciadas, derivadas fundamentalmente del tipo de datos que se manejan y de la existencia de normativas sectoriales propias.

El Reglamento entró en vigor inmediatamente después de su publicación, en mayo de 2016, pero no será aplicable hasta el 25 de mayo de este año 2018. Este periodo transitorio puede parecer muy amplio, pero lo cierto es que la implantación de algunas de las garantías, procedimientos o medidas contempladas en el RGPD puede llevar tiempo, especialmente en grandes organizaciones.

Es por ello necesario preparar la fecha de aplicación del nuevo Reglamento con la antelación y los recursos suficientes como para asegurar que en ese momento las organizaciones están en condiciones de cumplir con sus disposiciones.

El Delegado de Protección de Datos

Manuel Villaseca
Agencia Española de Protección de Datos

DENTRO DE LAS MEDIDAS QUE EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD) ESTABLECE EN EL MARCO DEL PRINCIPIO DE RESPONSABILIDAD PROACTIVA Y DEMOSTRABLE SE INCLUYE LA DESIGNACIÓN DEL DELEGADO DE PROTECCIÓN DE DATOS. ESTA FIGURA CONSTITUYE UNO DE LOS ELEMENTOS CLAVES DEL RGPD Y UN GARANTE DEL CUMPLIMIENTO DE LA NORMATIVA DE PROTECCIÓN DE DATOS EN LAS ORGANIZACIONES.

Esta previsión ya se encontraba recogida en la Directiva 95/46 ligada a la exención de la obligación de notificación de los tratamientos a la autoridad de control, aunque solamente fue transpuesta al derecho nacional en algunos Estados miembros. En el caso de España, el legislador optó por no contemplar la designación de esta figura ni en la ley de 1992 (LORTAD) ni en la LOPD de 1999.

El RGPD regula de forma detallada las circunstancias a tener en cuenta para la designación del Delegado de Protección de Datos, estableciendo una serie de supuestos de designación obligatoria por parte de los responsables y encargados cuando:

- El tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial.
- Las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o
- Las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.

Además, el RGPD abre la posibilidad de que los países de la Unión, a través de su normativa específica puedan establecer otros supuestos en que haya que nombrar a un DPD.

En este sentido, el proyecto de Ley Orgánica de Protección de Datos de Carácter Personal que se está tramitando, recoge, entre los supuestos en que se debe nombrar obligatoriamente un delegado, "los centros sanitarios legalmente obligados al mantenimiento de las historias clínicas de los pacientes con arreglo a lo dispuesto en 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".

Sin perjuicio de estos supuestos de obligatoriedad, la normativa recoge la posibilidad de que exista una designación voluntaria de un delegado protección de datos.

Sobre la intervención del Delegado de Protección de Datos en caso de reclamación ante las autoridades de protección de datos, es de destacar que el proyecto de Ley Orgánica de Protección de Datos de Carácter Personal que se encuentra en vía de tramitación, recoge la previsión de que las reclamaciones que no se hayan formulado previamente al Delegado de Protección de Datos podrán ser remitidas por la Agencia al delegado antes de resolver sobre la admisión a trámite.

De esta forma el Delegado de Protección de Datos está llamado a desempeñar un papel esencial en la resolución de las reclamaciones y los conflictos con los pacientes o el propio personal estatutario, sin tener que llegar a una sanción en el caso de un hospital privado o a una declaración de infracción en el supuesto de un establecimiento sanitario público.



FUNCIONES

Las funciones del Delegado de Protección de Datos serán de información, asesoramiento y supervisión y se encuentran especificadas en el artículo 39 del RGPD, pudiéndose concretar estas labores de información, asesoramiento y supervisión en las siguientes áreas:

RESPECTO AL CUMPLIMIENTO:

- Cumplimiento de principios relativos al tratamiento, como los de limitación de finalidad, minimización o exactitud de los datos.
- Identificación de las bases jurídicas de los tratamientos.
- Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.
- Existencia de normativa sectorial que pueda determinar condiciones de tratamientos específicos distintas de las establecidas por la normativa general de protección de datos.
- Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación responsable-encargado.
- Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la organización y de las razones que justifiquen la transferencia.
- Diseño e implantación de políticas de protección de datos.
- Auditoría de protección de datos.
- Establecimiento y gestión de los registros de actividades de tratamiento.

RESPECTO A LA RELACIÓN CON LOS INTERESADOS:

- Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.
- Establecimiento de mecanismos de recepción y gestión de las solicitudes de ejercicio de derechos por parte de los interesados.
- Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.

RESPECTO A LA SEGURIDAD:

- Análisis de riesgo de los tratamientos realizados.
- Medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.
- Procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación

a las autoridades de supervisión y a los afectados.

RESPECTO A LA PREVENCIÓN:

- Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos.
- Medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos.

RESPECTO A LA FORMACIÓN:

- Implantación de programas de formación y sensibilización del personal en materia de protección de datos.

RESPECTO A LA COOPERACIÓN CON LA AUTORIDAD DE CONTROL:

- Actuar como punto de contacto entre las autoridades de protección de datos y los interesados.

En el proyecto de LOPD se prevé que cuando el responsable o el encargado del tratamiento hubieran designado un Delegado de Protección de Datos el afectado podrá, con carácter previo a la presentación de una reclamación contra aquéllos ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, dirigirse al Delegado de Protección de Datos de la entidad contra la que se reclame.

Además, esta previsión afecta a cuando el interesado presente una reclamación ante la Agencia Española de Protección de Datos o, en su caso, ante las autoridades autonómicas de protección de datos, sin haberse dirigido previamente al Delegado de Protección de Datos. En este caso, las autoridades de protección de datos podrán remitir la reclamación al Delegado de Protección de Datos a fin de que este responda en el plazo de un mes.

LA CERTIFICACIÓN Y LOS ESQUEMAS DE CERTIFICACIÓN DE DELEGADOS DE PROTECCIÓN DE DATOS

Otra de las medidas de responsabilidad activa incluidas en el RGPD tendentes a facilitar la demostración del cumplimiento de lo dispuesto en el Reglamento se refiere al establecimiento de mecanismos de certificación y sellos y marcas de protección de datos que permitan a los interesados evaluar con mayor rapidez el nivel de protección de datos de los productos y servicios correspondientes. Por ello, insta a los Estados miembros, autoridades de control, Comité Europeo de Protección de Datos y Comisión Europea a promover la creación de mecanismos de certificación en materia de protección de datos y de sellos y marcas de protección de datos a fin de demostrar el cumplimiento del Reglamento en las operaciones de tratamiento y hace una mención especial a tener en cuenta sobre las necesidades específicas de las microempresas y las pequeñas y medianas empresas.

En el caso del RGPD el mecanismo de certificación afecta tanto a responsables como a encargados del tratamiento, es decir, ambos pueden utilizar este mecanismo para estar en disposición de demostrar el cumplimiento del mismo.

En este marco, y con el objetivo de ofrecer seguridad y fiabilidad tanto a los profesionales de la privacidad como a las empresas y entidades que van a incorporar esta figura a sus organizaciones o que necesitan contratar los servicios de un profesional cualificado, la AEPD ha optado por promover un Esquema de Certificación de DPD en colaboración con la Entidad Nacional de Certificación (ENAC), Este Esquema es un sistema de certificación que permite certificar que los DPD reúnen la cualificación profesional y los conocimientos requeridos para ejercer la profesión. Las certificaciones serán otorgadas por entidades certificadoras debidamente acreditadas por ENAC.

Aunque esta certificación no es obligatoria para poder ejercer como DPD y se puede ejercer la profesión sin estar certificado bajo éste o cualquier otro esquema, la Agencia ha considerado necesario ofrecer un punto de referencia al mercado sobre los contenidos y elementos de un mecanismo de certificación que pueda servir como garantía para acreditar la cualificación y capacidad profesional de los candidatos a DPD.

En el Esquema también se incluye toda aquella información, requisitos y procedimiento exigidos a las entidades de certificación para poder otorgar, suspender o retirar certificados. En la página web de la AEPD se pueden consultar los documentos que conforman el citado esquema de certificación.

RGPD: Evaluaciones de impacto

Rosario Heras
Agencia Española de Protección de Datos

EL 25 DE MAYO DE 2018 SE CUMPLEN DOS AÑOS DESDE QUE SE PUBLICÓ EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD O REGLAMENTO) Y ESE DÍA SERÁ EL QUE MARQUE EL INICIO DE SU PLENA APLICABILIDAD. EN ESA FECHA TANTO LOS RESPONSABLES COMO LOS ENCARGADOS DEL TRATAMIENTO DE DATOS PERSONALES DEBERÁN CUMPLIR CON LOS REQUERIMIENTOS Y OBLIGACIONES QUE INCLUYE ESTA NUEVA NORMATIVA.

El Reglamento supone un cambio importante, ya que tradicionalmente todas aquellas entidades que tratasen datos de carácter personal estaban habituadas a la LOPD, normativa de protección de datos en la que estaban claramente definidas todas las actuaciones que el responsable de ficheros o tratamientos debía realizar para cumplir con la misma, especialmente en lo relativo a las medidas de seguridad que debía implantar según la tipología de datos tratados. Sin embargo, el RGPD plantea un modelo más dinámico enfocado en los riesgos asociados al tratamiento de datos personales y es el responsable o encargado del tratamiento quien debe estar en disposición de demostrar que cumple con el mismo una vez analizados los riesgos a los que está expuesto y sobre todo a los riesgos desde el punto de vista de su afectación a los derechos y libertades de ciudadanos.

Esta responsabilidad de cumplimiento viene establecida como un principio relativo al tratamiento de los datos personales en el artículo 5.2 del Reglamento. Así cita textualmente: *"el responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo (responsabilidad proactiva)"*. El apartado 1 citado, a su vez, hace referencia a cómo deben ser tratados los datos (de forma lícita, leal y transparente) , a cómo a deben ser recogidos (limitación de la finalidad), al principio de minimización (los datos deben ser adecuados, pertinentes y limitados en relación con los fines para los que son tratados), a la situación de los datos respecto de sus titulares (exactitud), a cuánto tiempo han de conservarse (limitación del plazo de conservación) y finalmente hace referencia a garantizar su seguridad (integridad y confidencialidad). Por tanto, este principio de responsabilidad requiere que los responsables y encargados de tratamientos de datos personales analicen qué datos tratan, con qué finalidad lo hacen y que tipos de operaciones de tratamiento llevan a cabo con el objetivo de determinar cuáles son las medidas más adecuadas que debe implantar en su organización para cumplir con lo dispuesto en el RGPD.

El RGPD establece un conjunto de medidas para ayudar a las entidades que tratan datos de carácter personal al cumplimiento de este principio de responsabilidad pero no existe un listado concreto o un solo artículo del RGPD sino que se extienden a lo largo de todo el texto y dentro de las medidas se encuentran las evaluaciones de impacto. El Grupo de Autoridades Europeas de "Protección de Datos" del artículo 29 (GTP29) en las "Directrices adoptadas el 4 de abril de 2017 sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento "entraña probablemente un alto riesgo" a efectos del Reglamento" deja claro ya en su introducción que "una EIPD es un proceso utilizado para reforzar y demostrar el cumplimiento".

La evaluación de impacto en términos de protección de datos personales (EIPD) es una herramienta que permite evaluar de forma anticipada cuáles son los riesgos a los que están expuestos los datos personales según los tratamientos que el responsable o encargado del tratamiento lleve a cabo con los mismos. Se podría

> ***Una evaluación de impacto ha de realizarse cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas derecho"***

afirmar que la evaluación de impacto es un análisis de riesgos para un determinado tratamiento que permite identificar los riesgos sobre los datos de los interesados y establecer una serie de medidas para reducirlos hasta conseguir un nivel de riesgos aceptable por el responsable o encargado.

Por tanto, la EIPD se puede considerar como recurso de carácter preventivo que debe utilizar el responsable o encargado del tratamiento para poder identificar, evaluar y gestionar los riesgos a que están expuestas sus operaciones de tratamiento con el objetivo de garantizar los derechos y libertades de los interesados. Al tratarse de una herramienta de carácter preventivo, el responsable o encargado debe tenerla en consideración desde el inicio del tratamiento de datos personales, es decir en la fase de diseño de un producto, servicio o sistema de información debe desarrollar las acciones preventivas necesarias para poder identificar, evaluar y tratar los riesgos asociados al tratamiento de datos personales que va realizar con la puesta en funcionamiento de ese producto, servicio o sistema de información para así asegurar el cumplimiento de los principios de protección de datos recogidos en el Reglamento y garantizando los derechos y libertades de las personas afectadas por ese tratamiento.

Es importante destacar que todas aquellas organizaciones que tengan ya implantadas herramientas de análisis de riesgos pueden utilizarlas siempre que añadan los riesgos relativos a los derechos y libertades de las personas físicas y a los requerimientos del RGPD de tal forma que permita evaluar y tratar los riesgos de una forma adecuada.

¿CUÁNDO REALIZAR UNA EVALUACIÓN DE IMPACTO?

En el artículo 35.1 se explica cuándo ha de realizarse una evaluación de impacto: "cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas". Además, añade que la evaluación deberá realizarse antes de iniciarse el tratamiento.

Posteriormente, se establecen los casos en los cuales se ha considerado que un tratamiento entraña un alto riesgo para los derechos y libertades de las personas físicas. "Se requerirá en particular en caso de":

- Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas que les afecten significativamente de modo similar
- Tratamientos a gran escala de las categorías especiales de datos o datos sobre condenas e infracciones penales.

  Es importante señalar que el RGPD cuando se refiere a categorías especiales de datos personales incluye aquellos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, así como el tratamiento de datos genéticos o biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.
- Observación sistemática a gran escala de una zona de acceso público.

A la vista de lo anterior, teniendo en cuenta los distintos tratamientos que realizan los hospitales, consultas médicas o laboratorios bien sean públicos o privados y con independencia de su tamaño, se puede afirmar que son entidades obligadas a realizar evaluaciones de impacto de los tratamientos que realizan o pretendan iniciar.

La obligación o el deber de realizar una evaluación de impacto no se cierra exclusivamente a los casos anteriormente citados. Así, el RGPD establece que las autoridades de control establecerán y publicarán una lista de los tipos de

operaciones de tratamiento que requieran una evaluación de impacto, aunque también podrá establecer y publicar la lista de los tipos de tratamientos que no la requieren. Respecto de esto último, el WP29 cita ciertos supuestos a tener en cuenta por ejemplo cuando la naturaleza, el alcance, el contexto y las finalidades del tratamiento son muy similares a las de un tratamiento para el que ya se ha hecho una evaluación. En este caso, aunque no se haga la EIPD, se debe argumentar que el tratamiento encaja en esa circunstancia.

Con el fin de ofrecer un conjunto más concreto de operaciones de tratamiento que requieran una EIPD debido a su inherente alto riesgo, el GT29 establece nueve criterios que se deben considerar por quienes tratan datos de carácter personal:

1. Evaluación o scoring, incluida la elaboración de perfiles o predicciones, especialmente entre otros, de aspectos relacionados la salud.
2. Toma de decisiones automatizadas con efecto legal o similar como por ejemplo en los casos en los que el tratamiento puede conducir a la discriminación de personas.
3. Observación sistemática, hace referencia a tratamientos que se utilizan para observar o controlar a las personas físicas, incluidos aquellos datos que se recopilen a través de redes sociales y en circunstancias en las que los interesados pueden no ser conscientes de quién está recopilando datos y cómo se usarán.
4. Datos sensibles o muy personales, aquí se incluirían las categorías especiales de datos personales. En este apartado incluye el ejemplo de un hospital general que guarda historiales médicos de paciente.
5. Tratamiento de datos a gran escala. El GT29 recomienda que se tengan en cuenta los siguientes factores a la hora de determinar si el tratamiento que se pretende iniciar se realiza a gran escala:
   a. El número de interesados afectados, bien como cifra concreta o como proporción de la población correspondiente
   b. El volumen de datos o la variedad de elementos de datos diferentes que se procesan
   c. La duración, o permanencia de la actividad de tratamientos de datos
   d. El alcance geográfico de la actividad de tratamiento

   En este punto se puede constatar que, aunque el GT29 recomienda factores a tener en cuenta para determinar el concepto de gran escala, realmente corresponde al responsable o encargado del tratamiento tomar la decisión cuántica de cada uno de los factores de cara a realizar o no la EIPD.
6. Asociación o combinación de conjuntos de datos.
7. Datos relativos a personas vulnerables, aquí se incluirían los menores y segmentos más vulnerables de la población como personas con enfermedades mentales, pacientes de un hospital ancianos…
8. Uso innovador o aplicación de nuevas soluciones tecnológicas como combinar el uso de huella dactilar y reconocimiento facial para mejorar el control físico de acceso, etc.
9. Finalmente, cuando el propio tratamiento impida a los interesados ejercer un derecho o utilizar un servicio o ejecutar un contrato.

Dado que una EIPD es un mecanismo que permite cumplir con la protección de datos desde el diseño y por defecto, así como con los principios de responsabilidad activa, se considera una buena práctica ante cualquier duda realizar una EIPD y centrándonos en el ámbito sanitario, queda claro que tanto por el volumen de datos tratados, la variedad de los mismos y el estado actual de la tecnología es muy aconsejable realizar evaluaciones de impacto antes de iniciar cualquier tipo de tratamiento. Además, el Reglamento insta al responsable a examinar si un tratamiento es conforme con la evaluación de impacto al menos cuando exista un cambio del riesgo que representan las operaciones de tratamiento.

Esto nos lleva a afirmar que una EIPD es un proceso que perdura a lo largo del tiempo y que debe revisarse siempre que se modifique o actualice cualquier aspecto relevante de las operaciones de tratamiento.

¿QUÉ INCLUIR EN UNA EVALUACIÓN DE IMPACTO?

El contenido de una evaluación de impacto está regulado en el artículo 35 del RGPD, en su apartado 7, debe incluir como mínimo:



- Descripción sistemática de las operaciones de tratamientos previstas y de los fines del tratamiento, incluyendo el interés legítimo perseguido por el responsable del tratamiento cuando así proceda.
- Evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad.
- Evaluación de los riesgos para los derechos y libertades de los interesados y
- Medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales y a demostrar la conformidad con el RGPD teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

Lo anterior implica que el responsable debe establecer una metodología que recoja los procedimientos que le permitan identificar los tratamientos, gestionar los riesgos, implantar medidas de control para garantizar la protección de los derechos y libertades de las personas físicas y revisar esas medidas. En la guía de evaluación de impacto publicada por la Agencia Española de Protección de Datos se establece un modelo de EIPD con distintas etapas a desarrollar durante su ejecución, estas etapas serían:

- Análisis preliminar del riesgo potencial al que puede estar sometido el tratamiento para determinar si es necesario realizar una EIPD.
- Analizar la necesidad y proporcionalidad del tratamiento.
- Describir el ciclo de vida del tratamiento.
- Identificar amenazas y riesgos al que están expuestas las operaciones de tratamiento.
- Evaluar los riesgos en términos de probabilidad e impacto.
- Tratamiento de los riesgos al objeto de minimizar probabilidad de ocurrencia e impacto.
- Plan de acción y conclusiones.
- Supervisión e implantación de la puesta en marcha de las operaciones de tratamiento.

Llegados a este punto es importante añadir que si la conclusión de la EIPD no es favorable, el responsable o encargado del tratamiento debe analizar la posibilidad de incluir medidas de control adicionales que permitan reducir el nivel de riesgo y su impacto tratando de disminuirlo hasta un nivel aceptable. Si no fuese posible esta reducción, el tratamiento no debe iniciarse y es necesario activar un procedimiento de consulta previa a la Autoridad de Control (Agencia Española de Protección de Datos).

Teniendo en cuenta lo anterior, es importante disponer de un proceso sistemático para garantizar la homogeneidad y comparabilidad en la ejecución de una EIPD e implantar procedimientos para poder realizar un seguimiento de las actuaciones realizadas durante cada una de las fases citadas.

Finalmente añadir que el responsable del tratamiento debe recabar el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

Seguridad, Análisis de Riesgos y Auditorías en el RGPD

Joaquín Pérez
Agencia Española de Protección de Datos

PARA JUSTIFICAR LA EVOLUCIÓN DEL ACTUAL MARCO NORMATIVO DE PROTECCIÓN DE DATOS DADO POR LA DIRECTIVA 95/46 AL REGLAMENTO 679/2016 O REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD), QUE SERÁ APLICABLE EL 25 DE MAYO DE 2018, BASTA CON MENCIONAR QUE LA APARICIÓN DE GOOGLE SE PRODUCE EN 1998, ES DECIR CON POSTERIORIDAD A LA DIRECTIVA QUE ES DEL AÑO 1995.

Si ello no fuera suficiente podemos añadir que el resto de grandes empresas asociadas a Internet: *Amazon, Facebook, Twitter, Pay Pal, Whatsapp,* etc., así como toda una serie de tecnologías emergentes y hoy omnipresentes en nuestro entorno como el *Cloud, Big Data, Internet de las Cosas, Smart Cities, Block Chain,* etc. también son posteriores a la Directiva, poniéndose claramente de manifiesto su obsolescencia derivada de la ausencia de mecanismos adecuados para abordar y dar respuestas a los nuevo escenarios y sus desafíos.

Este cambio de marco normativo también va a traer consigo cambios en lo que es el objeto del presente artículo, esto es, la seguridad de datos de carácter personales. Para analizar dichos cambios tenemos que tener en cuenta dos vertientes, la europea y la nacional.

A nivel europeo, el marco de seguridad de la Directiva se encuentra perfectamente definido en su considerando 46, que establece la obligación para el responsable de tratamiento de garantizar el objetivo de la seguridad, es decir, la confidencialidad, integridad y disponibilidad de los datos personales mediante la aplicación de medidas técnicas y organizativas adecuadas para cuya adopción se deberá tener en cuenta el contexto, viniendo éste determinado por el estado del arte de la tecnología, los riesgos a que están expuestos los datos, su naturaleza y el coste de las medidas. Este marco de seguridad resulta básico y se encuentra ampliamente reflejado en la literatura especializada en materia de seguridad de la información.

A nivel nacional, esta estrategia supuso en su momento el desarrollo y adopción de una normativa específica[1] que, en aras de ayudar a los responsables, simplificaba en tres los tipos de riesgos, clasificando todos los ficheros que tuvieran datos de carácter personal en uno de entre los niveles *básico*, *medio* y *alto*, estableciéndose para cada uno de ellos objetivos concretos en diferentes áreas de seguridad, junto con la obligación para el responsable de documentar por escrito las medidas técnicas y organizativas que decidiera implantar para alcanzar dichos objetivos. También se establecía, para los ficheros de nivel medio y alto, la obligación de designar un responsable de seguridad y de realizar una auditoría de seguridad con periodicidad bienal. En definitiva, la normativa española simplificaba el análisis de riesgos marcando unas líneas de actuación concretas que servían de guía al responsable del tratamiento que además se veía asesorado por su responsable de seguridad en los ficheros de nivel de riesgos medios y alto.

Si bien el nuevo marco europeo del RGPD hereda lo recogido en la Directiva en materia de seguridad, a nivel nacional deja sin efecto la normativa española descrita en el párrafo anterior. Y es razonable que la ausencia de estos criterios y líneas de actuación dé lugar a una cierta confusión entre muchos responsables de tratamientos ante el dilema ¿y ahora qué? en materia de seguridad para cumplir con el RGPD.

El primer mensaje que hay que transmitir es el de eliminar toda alarma y desasosiego. No hay fun-

1. Real Decreto 1720/, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal. Título VIII: De las medidas de seguridad en el tratamiento de datos de carácter personal.

damento para ello. Tanto el marco anterior como el actual fijaban objetivos de seguridad de alto nivel y no descendían a un nivel de detalle que suponga que lo que tengamos implantado para el marco anterior no nos sirva para el nuevo. De hecho, los objetivos de alto nivel son los mismos, garantizar la confidencialidad, integridad y disponibilidad de los datos personales mediante medidas técnicas y organizativas en función del riesgo, el coste, el estado del arte y la naturaleza de los datos por lo que, no habiendo cambio de rumbo, lo razonable es que simplemente tengamos que afrontar, en su caso, pequeños "ajustes finos" en las medidas técnicas y organizativas ya implementadas, sobre todo en aquellas pequeñas y medianas empresas cuyo objeto de negocio no está enfocado al tratamiento de datos personales y que constituyen la mayoría del tejido empresarial del país.

Los tratamientos de grandes volúmenes de datos y que, como ocurre en el caso del sector sanitario incorporan también datos de salud sujetos a protección adicional, quedaron clasificados por la citada normativa española de seguridad en el nivel alto de riesgo, debiendo las organizaciones responsables de dichos tratamientos aplicar una serie medidas de seguridad reforzadas. Bajo el RGPD estas mismas organizaciones, conscientes de ese nivel alto de riesgo, deberían proceder a realizar un análisis de riesgos propio con un mayor nivel de detalle, de forma que las medidas técnicas y organizativas ya implantadas se reajusten en consonancia con el nuevo análisis de riesgos, no descartándose que surja la necesidad de incorporar nuevas medidas adicionales a las ya implantadas.

La Directiva en su momento no proporcionaba una metodología para realizar el análisis de riesgos de seguridad. Por esta razón, la Agencia Española de Protección de Datos promovió la regulación nacional en materia de seguridad que resolvía dicho análisis con la clasificación en tres niveles y sus respectivos criterios. El RGPD tampoco aporta metodología alguna para realizar dicho análisis, pero a diferencia de la Directiva, tampoco permite desarrollarlo legalmente, de aquí que la normativa española actual se vea desplazada con los mismos efectos que si estuviera derogada.

La solución ante esta carencia de directrices legales pasa por utilizar metodologías de análisis de riesgo en materia de seguridad que, a modo de estándares "de facto", se encuentran disponibles en el mercado. Tal es el caso de *Magerit*, de uso obligado en la Administración Pública española y que cuenta con la herramienta informática Pilar para su implementación. En el ámbito privado puede utilizarse esta u otra metodología. Lo importarte no es tanto qué metodología se utilice sino que se utilice alguna, ya que permite de una manera estructurada y coherente evaluar si la información, o los servicios que se prestan gracias a ella, son valiosos, así como saber cuánto valor está en juego, proporcionando directrices para su protección. En definitiva, se trata de una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista.

Una vez realizado el análisis de riesgos se debe proceder a la definición e implantación de las medidas técnicas y organizativas que eliminen, o reduzcan a un nivel aceptable, dichos riesgos. Para ello, es conveniente también aplicar un proceso metódico que también aquí nos aleje de la improvisación y la arbitrariedad, siendo muy recomendable acudir para ello a estándares al efecto, como por ejemplo, las normas sobre seguridad de la familia ISO 27000, por citar alguna, y sin que ello se interprete en detrimento de otras que también existen y que son igual de buenas, ya que todas ellas conducen a los mismos objetivos de seguridad.

En este sentido, si bien el RGPD no hace referencia a ninguna metodología de análisis de riesgos ni de seguridad, sí que contempla que la adhesión por parte del responsable del tratamiento a códigos de conducta o a mecanismos de certificación que cuenten con la aprobación establecida en el propio RGPD podrá servir de elemento para demostrar el cumplimiento de los requisitos de seguridad requeridos en el RGPD.

Aunque a día hoy, cuando todavía no es aplicable el RGPD, ni por lo tanto ningún estándar de seguridad ha podido ser validado por el propio RGPD, no cabe duda de que la utilización de un estándar de seguridad, tras el correspondiente análisis de riesgos, va a situar a la organización en muy buena posición de cara a hacer frente a las obligaciones del RGPD en materia de seguridad.

Tras el análisis de riesgos y la definición e implementación de las medidas técnicas y organizativas, el RGPD establece, en función del riesgo y otros factores, la obligación de implantar un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento, lo que

en la literatura especializada de seguridad comúnmente se conoce como los procesos de monitorización y auditoría de la seguridad.

La monitorización consiste en una supervisión continua y en tiempo real de los aspectos clave de las medidas técnicas y organizativas implantadas y permite saber si los controles definidos están o no funcionando como se espera. La auditoría por su parte, consiste en evaluaciones puntuales, acerca de la eficacia y eficiencia de los controles implantados y de su adecuación al negocio. Ambas, monitorización y auditoría, se complementan y resultan parte esencial de la arquitectura y gobierno de la seguridad de una organización.

En la normativa española de seguridad se establecía la obligación de realizar auditorías de seguridad bienales para los ficheros clasificados como de nivel medio y alto. Sería un error pensar que al quedar desplazada dicha normativa tal obligación desaparece. Como se ha señalado, el RGPD incorpora estos procesos de auditoría y monitorización que no estaban en la Directiva y que de hecho vendrán también incorporados en cualquier estándar de seguridad que el responsable utilice para implantar la seguridad, si bien la frecuencia de las mismas no tendrá por qué ser realizada con periodicidad bienal y deberá ser fijada de forma razonable por el responsable dentro de su política de cumplimiento normativo.

Las auditorias pueden ser internas, externas e incluso ambas, como ocurre en las grandes organizaciones que se lo pueden permitir, ya que ambas se complementan y contribuyen al proceso de mejora de la organización. En el caso de las auditorías internas, las buenas prácticas generalmente aceptadas señalan que lo importante es que el órgano que lleve la auditoría a efecto sea independiente del órgano auditado y reporte a la más alta instancia de la organización. En cuanto al personal que realice la auditoría, tanto si es interna como externa, se debe de exigir que cuente con las habilidades y conocimientos suficientes para llevarla a cabo y no se vea sujeto a ningún conflicto de intereses en relación con dicha auditoría, como el que surgiría por ejemplo, si algún auditor hubiera participado con anterioridad en la definición o implantación de alguna de las medida técnicas y organizativas objeto de la auditoría. Existen diferentes certificaciones muy reconocidas en el mercado que acreditan la función de auditor de sistemas de información.

Si se ha señalado anteriormente como error el considerar que la auditoría ya no es necesaria bajo el RGPD, lo mismo tendríamos que decir sobre el Responsable de Seguridad. Esta figura que la normativa nacional establecía como obligatoria cuando el responsable dispusiera de ficheros clasificados en los niveles medios o alto, adquiere bajo el RGPD una mayor relevancia aunque no aparezca citada de forma explícita en él. No es que la figura del Delegado de Protección de Datos le sustituya, ya que sus funciones no son las mismas, pero no cabe duda que sean dos figuras que deben de entenderse y coordinarse.

La figura del responsable de seguridad tiene su justificación y será necesaria en toda organización donde el nivel de riesgo implique hacer un análisis de riesgos específico mediante un proceso metódico y una posterior definición e implantación de las medidas técnicas y organizativas al efecto. Es en este escenario donde la existencia de un responsable de seguridad puede jugar un papel determinante a la hora de que la organización logre los objetivos de seguridad. Es importante que quien desempeñe este papel en la organización cuente con las habilidades y conocimientos necesarios y a tal efecto existen certificaciones muy reconocidas en el mercado.

Finalmente, entre las medidas adicionales que incorpora el RGPD y que no figuraban en la Directiva se encuentran también las relativas a las quiebras de seguridad de los datos personales que sufra un tratamiento y la obligación para su responsable de notificarlas a la Agencia Española de Protección de Datos y a los propios afectados cuyos datos se hayan visto comprometidos, a los efectos de que se puedan tomar las medidas adecuadas para minimizar los daños. El RGPD recoge para cada notificación las condiciones que deben concurrir para que cada una de ellas tenga lugar, así como el momento, contenido y forma en que cada una de estas notificaciones debe producirse.

Como conclusión, en materia de seguridad podemos decir que el RGPD aporta una arquitectura de seguridad más madura, profesional y flexible para la organización, dotándola de mejores y eficientes mecanismos para afrontar los nuevos retos, haciendo que el responsable del tratamiento sea quien asuma y gestione su responsabilidad de forma transparente ante los ciudadanos y ante la autoridad de protección de datos, garante del cumplimiento de la norma.

Guías y Herramientas de Apoyo para Adaptarse al RGPD

Julián Prieto
Agencia Española de Protección de Datos

EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD) NO SUPONE UN CAMBIO DE LOS PRINCIPIOS Y VALORES DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS, PERO SÍ IMPLICA UNA IMPORTANTE MODIFICACIÓN EN LA CULTURA DEL CUMPLIMIENTO DE LAS OBLIGACIONES POR PARTE DE LOS SUJETOS OBLIGADOS, TANTO RESPONSABLES COMO ENCARGADOS DEL TRATAMIENTO.

Este cambio se sustenta básicamente en dos elementos o principios: el principio de responsabilidad proactiva y el denominado enfoque del riesgo, que se proyectan sobre las obligaciones que establece el RGPD.

Por el principio de responsabilidad proactiva, el responsable del tratamiento deberá adoptar las medidas técnicas y organizativas apropiadas no sólo para cumplir con las disposiciones del Reglamento, sino para poder demostrar que se está cumpliendo. Medidas y diligencias que los responsables y encargados del tratamiento han de llevar a cabo y que se recogen en el RGPD.

En aplicación de este principio, que exige una actitud consciente, diligente y proactiva en todos los tratamientos de datos que se realicen, se habrá de constituir un registro de las actividades de tratamiento que se lleven a cabo, adoptar medidas que garanticen la privacidad desde el diseño y por defecto, realizar un análisis de los riesgos y, en su caso, una evaluación de impacto con el fin de valorar la particular gravedad y probabilidad de un alto riesgo, determinando las medidas, garantías y mecanismos para mitigarlo.

Por su parte, el enfoque del riesgo implica que a la hora de adoptar las medidas se deberá tener en cuenta, además de la naturaleza, el ámbito, el contexto y los fines del tratamiento de los datos personales, el riesgo que éste suponga para los derechos y libertades de los titulares de los datos, como pueden ser daños y perjuicios físicos, materiales e inmateriales, discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, perdida de confidencialidad o cualquier otro perjuicio económico y social significativo. Dependiendo del nivel de riesgo, que deberá ponderarse mediante una evaluación objetiva que lo determine, se habrán de adoptar las medidas oportunas para garantizar un nivel de seguridad adecuado.

La Agencia Española de Protección de Datos (AEPD) es consciente de las implicaciones que supone la aplicación del RGPD para los sujetos obligados, entre ellos los responsables del sector sanitario que por su actividad han de tratar categorías especiales de datos, como son los de salud, por lo que, con la finalidad de informar, orientar y ayudar en la tarea de adecuación al nuevo marco legal, la AEPD ofrece una serie de recursos disponibles en su página web.

La AEPD ha creado un espacio específico en su web dedicado al RGPD donde se puede acceder a la documentación, herramientas, guías y otros recursos y materiales que se vienen elaborando para informar sobre el impacto y las consecuencias del Reglamento europeo y facilitar la adaptación a sus disposiciones.

De este contenido, por su enfoque eminentemente práctico sobre cómo afrontar el tránsito de la LOPD al RGPD, hay que destacar las siguientes guías y herramientas:

- "Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento", elaborada en colaboración con la Agencia Vasca de Protección de Datos y la Autoridad Catalana de Protección de Datos, en la que se presentan de manera sistemática los principales aspec-

> ***La AEPD ha creado un espacio específico en su web dedicado al RGPD donde se puede acceder a la documentación, herramientas, guías y otros recursos y materiales para informar sobre las consecuencias del Reglamento europeo y facilitar la adaptación a sus disposiciones"***

tos que las entidades deberán tener en cuenta a la hora de aplicar el RGPD.

La legitimación para el tratamiento de los datos; la obligación de transparencia e información a los interesados; los derechos, a los que el RGPD incorpora dos nuevos: el de limitación del tratamiento y el de portabilidad; las relaciones responsable-encargado del tratamiento; las medidas de responsabilidad activa como el registro de actividades de tratamiento, análisis de riesgos, la protección de datos desde el diseño y por defecto, las medidas de seguridad, las evaluaciones de impacto, la notificación de las brechas de seguridad, la figura del delegado de protección de datos, las transferencias internacionales de datos y el tratamiento de datos de menores son objeto de esta Guía. Medidas sobre las que se señalan las cuestiones a tener en cuenta y se efectúa una serie de recomendaciones.

La Guía se completa con una lista de verificación que pretende servir de ayuda a los sujetos obligados para que puedan realizar de forma sistemática una evaluación de su situación y contrastarla con las obligaciones que introduce el RGPD. La lista se dispone también en versión simplificada para aquellos responsables que realicen un limitado tratamiento de datos que, en principio, presente un escaso nivel de riesgo para los derechos y las libertades de los interesados.

- *"Guía para el cumplimiento del deber de informar"*, elaborada también en colaboración con la Agencia Vasca de Protección de Datos y la Autoridad Catalana de Protección de Datos.

  La transparencia en el tratamiento de los datos y la información que al respecto se debe proporcionar a los interesados se configura como uno de sus derechos y, a la vez, una de las obligaciones de los responsables del tratamiento, que resulta fundamental para permitir a los interesados disponer del control sobre sus datos y garantizarles el ejercicio de sus derechos. En consecuencia, el RGPD amplía la información que se ha de facilitar y, a su vez, establece que se deberá proporcionar de forma concisa, transparente inteligible, y de fácil acceso y en un lenguaje claro y sencillo.

  Para que la información sea realmente efectiva se ha elaborado esta Guía en la que las tres Autoridades de Protección de Datos armonizan su contenido y sus características y recomiendan, en particular cuando estemos ante medios electrónicos, facilitarla por capas, niveles o fases, para lo que se ofrecen varios modelos para orientar a los responsables de tratamiento.
- *"Directrices para la elaboración de contratos entre responsables y encargados del tratamiento"*, también realizada en colaboración con la Agencia Vasca de Protección de Datos y la Autoridad Catalana de Protección de Datos.

  Otra de las novedades que introduce el RGPD, y que afecta a un número importante de entidades, es en la relación entre responsable y encargados del tratamiento que, dada la evolución de los servicios tecnológicos en particular los servicios de cloud computing, cada vez son más frecuentes en todos los sectores y, por tanto, también en el sanitario.

  El RGPD incorpora expresamente un deber de diligencia de los responsables a la hora de la elegir y contratar al prestador de servicios que va a tratar los datos personales por su encargo y, a su vez, amplía el contenido del contrato en cuanto a las obligaciones que han de cumplir los encargados de tratamiento, lo que supone un cambio significativo con respecto a la regulación que establece la LOPD actualmente aplicable.

  Para aclarar la figura del encargado del tratamiento, las obligaciones del responsable en su contratación, el contenido del contrato se ha elaborado esta Guía, que contiene un modelo de contrato que puede servir de guía y ser utilizado como modelo para formalizar las relaciones responsable-encargado.
- *"Orientaciones y garantías en los procedimientos de anonimización de datos persona-*

les", cuya finalidad engarza con el enfoque del riesgo que informa la regulación del RGPD.

Una de las medidas que se pueden adoptar por los responsables para minimizar los riesgos en el tratamiento de datos personales es la anonimización o disociación de los datos personales. De la relevancia que esta medida puede tener para determinadas actividades del sector de la salud, como los ensayos clínicos, ya se da cuenta a fondo en otro artículo de este número.

La anonimización de datos debe considerarse como una forma de eliminar las posibilidades de identificación de las personas. El avance de la tecnología y la información disponible hacen difícil garantizar el anonimato absoluto, especialmente a lo largo del tiempo, pero, en cualquier caso, la anonimización ofrece mayores garantías de privacidad a las personas.

El objetivo es garantizar la irreversibilidad de la anonimización y para ello se han de valorar tanto las fuentes de información disponibles en los diferentes medios y, en particular, a través de Internet, como la tecnología aplicable en los procesos de anonimización y en los de reidentificación.

El RGPD insiste en este tipo de medidas, cuando no puede llegarse a la irreversibilidad completa de la información, con figuras como la seudonimización de los datos personales, proceso cuya finalidad es que no se puedan atribuir a una persona sin utilizar información adicional, siempre que ésta figure por separado y esté sujeta a medidas técnicas y organizativas que garanticen que los datos no se atribuyen a una persona identificada o identificable (artículo 4.5 del RGPD). Los datos seudonimizados están sujetos a la regulación del Reglamento europeo, pero al disminuir los riesgos del tratamiento permiten facilitan el resto de medidas de seguridad a adoptar.

Estas orientaciones contienen los principios y las fases del proceso de anonimización, así como las garantías, la formación a proporcionar a quienes la lleven a cabo y la información a facilitar a los afectados, las auditorías y la documentación de las políticas de privacidad.

Asímismo, la Agencia ha desarrollado las siguientes herramientas:

- Un servicio de obtención automatizada de copia de la inscripción de ficheros. El RGPD ha suprimido la obligación de notificar los ficheros de datos de carácter personal a las Agencia Española de Protección de Datos, así como, en su caso, a las Autoridades Autonómicas, si bien estipula la obligación de los responsables y encargados de llevar un registro propio de las actividades de tratamiento que realicen.

  Para facilitar la constitución de estos registros a los responsables, que bien puede partir de los ficheros actualmente inscritos en el Registro General de Protección de Datos, la Agencia ha desarrollado una nueva funcionalidad de este servicio, que ya se ofrecía de manera no automatizada, por la que los responsables de ficheros ya inscritos en el Registro, a través de la sede electrónica de la Agencia, pueden descargarse de forma automática y editable (Excel o XML) el contenido completo de la inscripción de sus ficheros.
- FACILITA RGPD, es una herramienta de ayuda a los responsables del tratamiento para su adaptación a la normativa del RGPD, aunque en principio no resultaría aplicable en el sector sanitario pues está diseñada para aquellos tratamientos de datos que a priori presentan un bajo nivel de riesgo, como serían los de empleados, clientes, proveedores y los que se tratan a través de un sistema de videovigilancia, para ayudar a los responsables en su adecuación al RGPD.

Guías y herramientas que, junto con otros materiales también de interés, están disponibles en la página web de la Agencia Española de Protección de Datos (www.agpd.es), a la que se irán incorporando los nuevos recursos y que tienen la finalidad de facilitar y ayudar a responsables y encargados de tratamientos de datos personales a cumplir con la nueva normativa de protección de datos. Guías como la de Análisis de Riesgos y de Evaluación de Impacto, de próxima presentación, con las que se quiere facilitar una metodología que pueden utilizar aquellas entidades que en su actividad realicen tratamientos de datos que impliquen cierto nivel de riesgo, o alto riesgo para los derechos y libertades de los interesados, y que puede ser de gran utilidad para los responsables del sector sanitario, en cuya actividad es consustancial el tratamiento de datos de salud.

Resultados del Plan de Inspección Sectorial de Oficio de Hospitales Públicos

Desarrollado por la Agencia Española de Proteccion de Datos (Año 2016- 2017)

Rafael Calvo
Agencia Española de Protección de Datos

UNO DE LOS NUEVE ARTÍCULOS DEL JURAMENTO HIPOCRÁTICO SEÑALA *"LO QUE ACASO EN EL EJERCICIO DE LA PROFESIÓN, Y AÚN FUERA DE ÉSTA, VIERE U OYERA ACERCA DE LA VIDA DE LAS PERSONAS, Y QUE NO DEBA ALGUNA VEZ SER REVELADO, CALLARÉ, CONSIDERÁNDOLO SECRETO."*

Este canon pone de manifiesto la importancia del escrupuloso respeto a la intimidad por parte de la profesión médica ya desde la antigüedad, resaltando la importancia de que las instituciones sanitarias garanticen la confidencialidad de la información relacionada con los servicios que prestan, así como, en un sentido más amplio, la protección de los datos personales de los pacientes.

Debe tenerse en cuenta que los datos de salud se encuentran incluidos, en el Reglamento General de Protección de Datos (RGPD) que será aplicable el 25 de mayo de 2018, entre los denominados como categorías especiales de datos, cuyo tratamiento se caracteriza por exigir garantías reforzadas.

Por otro lado, los tratamientos de datos de salud se enfrentan hoy a una revolución digital en la que la cantidad de datos que se acumulan sobre las personas crece enormemente y con una conectividad sin precedentes. Todo ello plantea nuevos retos para la protección de datos de carácter personal, más aún cuando el acceso a la Historia Clínica y su compartición entre diferentes instituciones sanitarias se considera imprescindible para prestar una mejor asistencia médica.

Y es que los tratamientos de datos realizados por los hospitales tienen unas características distintivas, porque, además de tratase de datos de categorías especiales y constituirse en grandes volúmenes, la necesidad de accesibilidad a la información del paciente para prestarle la debida asistencia médica hace que el riesgo de exposición de los datos sea muy alto.

El análisis de la adecuación a la legislación vigente de estos tratamientos a gran escala de datos sensibles ha llevado a contemplar, dentro del Plan estratégico 2015-2019 de la Agencia Española de Protección de Datos, un programa dedicado a la Sanidad, donde se engloba el Plan de Inspección de oficio de Hospitales Públicos.

Los planes de oficio de la Agencia, que se realizan con carácter preventivo, analizan el cumplimiento de la normativa en sectores o áreas específicas para obtener una visión integral y conjunta que permita detectar deficiencias y realizar las recomendaciones correspondientes de manera transversal.

El plan se ha centrado en los procedimientos técnicos y políticas de actuación seguidos en los hospitales públicos, con la valoración de su nivel de adecuación a las previsiones de la normativa de protección de datos teniendo como objetivo final el de elevar el nivel de cumplimiento del sector en esta materia, así como generar confianza en las actuaciones de las instituciones sanitarias tanto en el ámbito asistencial como en el de la investigación.

ANTECEDENTES

En el año 1995, la Agencia Española de Protección de Datos realizó un Plan Sectorial de Oficio con el objetivo de analizar el nivel de adecuación del sector de la asistencia hospitalaria pública a la normativa de protección de datos entonces vigente. Las actuaciones finalizaron el año 1996

con la elaboración de un informe de conclusiones que ponía de manifiesto las deficiencias detectadas, que de forma resumida fueron:

- No se informaba a los afectados de los puntos indicados en el artículo 5 de la Ley Orgánica de Protección de Datos (LOPD).
- No existían procedimientos para ofrecer información a los afectados ante el ejercicio de su derecho de acceso.
- No existía el necesario conocimiento e implicación por parte de los órganos directivos de los centros, en lo que a protección de datos se refiere, así como tampoco una mentalización adecuada respecto de los problemas de seguridad.
- No existían definiciones de nivel de confidencialidad de los datos que se utilizan desde los distintos puntos de tratamiento de los centros.
- No estaban definidos ni documentados los procedimientos en materia de cesión de datos médicos ni los requisitos legales necesarios para su cesión a otros centros.
- No existía control de salida de datos de los centros.
- No existía un Plan de Seguridad ni conciencia respecto de los riesgos asociados a una seguridad deficiente.

Durante el año 2010 se realizó un seguimiento del plan anterior, mediante un cuestionario remitido a todos los hospitales del Catálogo Nacional, públicos y privados, obteniéndose un informe de situación en el que se reflejaba que, en los centros públicos, las mayores diferencias de cumplimiento se presentaron en las cláusulas informativas de los formularios de recogida de datos y en la realización de la auditoría bienal de seguridad. Otros aspectos con carencias detectados en el sector público fueron los carteles informativos sobre protección datos, las revisiones del documento de seguridad, el registro de los accesos a los datos, la seguridad en el almacenamiento de las historias clínicas en papel para evitar accesos no autorizados, así como la adopción de medidas para evitar la sustracción, pérdida o acceso indebido a la documentación durante su transporte.

PLAN DE INSPECCIÓN 2016-2017

La Agencia ha realizado nuevas actuaciones de inspección dirigidas a los centros hospitalarios de titularidad pública, teniendo en cuenta los gestionados tanto de forma directa como indirecta, y centrando la auditoria en los aspectos con más carencias detectadas en las actuaciones anteriores, en concreto, en las medidas de seguridad implementadas.

Aunque en términos generales las Administraciones Sanitarias públicas han asumido una apuesta firme por la historia clínica electrónica, que debe valorarse positivamente, en la actualidad coexisten en España hospitales con diferentes grados de automatización de la historia clínica, existiendo desde centros que utilizan la historia clínica totalmente en formato papel, hasta centros relativamente recientes que han tenido desde su nacimiento toda la historia clínica electrónica, si bien siempre, al menos en el momento actual, también coexisten en papel determinados documentos como pueden ser los consentimientos informados para las intervenciones quirúrgicas, para los procedimientos diagnósticos y terapéuticos invasores u otros procedimientos que así lo exijan.

Por ello, se auditaron hospitales con diferente grado de implantación de la historia clínica electrónica, incluidos hospitales que utilizan exclusivamente la historia clínica en papel. Por otro lado, han sido inspeccionados diversos servicios hospitalarios entre los que se encuentran: Admisión, Urgencias, Consultas Externas, Anatomía Patológica, Unidad de Cuidados Intensivos, Laboratorio de Análisis Clínicos, Farmacia Hospitalaria, Departamento de Informática, Atención al Paciente, Servicios Sociales y Biobanco.

En la actualidad, todos los hospitales disponen de un complejo Sistema de Información que se encuentra principalmente ubicado en su Centro de Proceso de Datos, dotado con una serie de servidores centrales en los cuales se encuentran instaladas la mayoría de aplicaciones con datos personales utilizadas por el personal sanitario, incluido el HIS.

Según el grado de implementación de la Historia Clínica Electrónica, este sistema central es más o menos completo e integra en mayor o menor medida los elementos auxiliares del Hospital, siendo estos básicamente los comúnmente denominados LIS (Sistema de Información Laboratorio), RIS (Sistema de Información de Imágenes médicas) y PHIS (Sistema de Información de la Farmacia Hospitalaria).

Adicionalmente todos estos sistemas conviven con un importante número de aplicaciones departamentales específicas que permiten a los departamentos tratar los datos obtenidos de los pacientes y elaborar informes de las actuaciones que practican, si bien la mayoría de los Centros tienen implementado un modelo centralizado en el que las aplicaciones se instalan y administran en los servidores ubicados en el centro de proceso de datos, y los usuarios acceden remotamente a las aplicaciones desde sus puestos de trabajo.

Esta centralización de la información es la tendencia actual y tiene repercusiones positivas para la protección de datos, ya que en la situación anterior de descentralización, que aún persiste en algunos casos, el control de la implementación de las medidas de seguridad es mucho más complejo.

Por otro lado, se ha detectado un esfuerzo importante en la normalización de los procedimientos de seguridad, con una tendencia favorable a la asunción progresiva de la normativa y de los principios y la cultura de protección de datos, notándose una mayor concienciación e implicación de la dirección, y en general, una evolución positiva en el sector.

Con el diagnóstico derivado del plan de inspección efectuado, se ofrece un punto de referencia para que el sector sanitario pueda abordar la adaptación de sus sistemas y procedimientos a los nuevos requerimientos que impone el RGPD.

Hay que indicar que los errores detectados durante la inspección de oficio no constituyen comportamientos generales, sino aspectos puntuales que se pueden y deben mejorar, entre los que hay que destacar los siguientes:

- En relación a la información ofrecida a los pacientes se considera conveniente elaborar y situar en lugar visible, al menos en las áreas de admisión y urgencias, carteles informativos sobre la identificación del responsable del fichero, el modo de ejercitar los derechos ARCO y de la dirección o departamento al que deben dirigirse para ello.

  Además, en todos los documentos mediante los que se recaben datos de los pacientes se debe de incluir toda la información prevista en el artículo 5 de la LOPD.
- Es necesario recabar el consentimiento del paciente para saber si desea que su presencia y ubicación en el hospital sea comunicada a las personas o familiares que pregunten por ello. Si el paciente no se opone, el hospital puede informar sobre si se encuentra en urgencias o ingresado y el número de habitación, sin indicar datos de salud o la atención médica prestada.
- Todos los Hospitales deberían establecer normas internas que obliguen a la confidencialidad de los datos, tanto al personal del Hospital como a todo aquel que pueda tener acceso datos de los pacientes como médicos residentes, estudiantes o personal externo. Todos estos colectivos, deberían suscribir un compromiso de confidencialidad antes de empezar a desempeñar sus funciones, mediante el cual se acepte las normas internas descritas.
- El plan de inspección, realizado necesariamente con la normativa en vigor, ha arrojado algunas deficiencias con relación a las medidas de seguridad. Si bien el enfoque de la seguridad de los Sistemas de Información va a sufrir un cambio con la plena aplicabilidad del nuevo Reglamento Europeo en mayo de 2018, se considera que las medidas de seguridad que se relacionan a continuación, de obligado cumplimiento en la actualidad, son una buena base para un adecuado cumplimiento de la nueva normativa, y en cualquier caso, orientativas de cara a las resultantes del Análisis de Riesgo y las Evaluaciones de Impacto que se van a tener que realizar.

Las deficiencias de seguridad detectadas más importantes están relacionadas con los siguientes aspectos:

- Registro de incidencias. No implantación de un procedimiento de gestión de incidencias como tal, limitándose en la mayoría de los casos a su tramitación por medio de los centros de atención al usuario, y, en algunos casos no se registran ni documentan los procesos de recuperación.
- Control de Acceso, Perfiles y Gestión de usuarios. La mayoría de las aplicaciones auditadas permiten que un facultativo acceda sin restricciones a datos de pacientes que no tiene asignados. Se recomienda el establecimiento de alertas de confidencialidad que se muestren al usuario del sistema cuando acceda a los datos de un paciente que no tiene asignado.

  En algunas aplicaciones corporativas se ha comprobado que algunos colectivos o perfiles de usuarios tienen acceso a datos que no

necesitan para sus funciones, tales como por ejemplo los administrativos que tienen acceso a alertas e informes médicos que no son necesarios para sus funciones.

- Autenticación/contraseñas. Todos los tratamientos de datos de salud auditados autentican la identidad del usuario mediante contraseñas, no obstante se han encontrado las siguientes deficiencias puntuales en algunos centros:
  - Carencia de una política de cambio de contraseñas que garantice que el periodo de vigencia sea inferior a un año,
  - No solicitar autenticación del usuario tras el cierre la sesión o cuando lleva un tiempo sin actividad.
  - Contraseñas de los usuarios almacenadas sin codificar.
  - Mecanismos de distribución de contraseñas que no garantizan su confidencialidad.
  - Se permite la reiteración ilimitada de intentos de acceso.
- Auditoría de seguridad. Se ha detectado que, en muchos casos, el plazo máximo de dos años para la realización de auditorías de las medidas de seguridad sobre todos los ficheros es superado, realizándose en todo caso auditorías parciales en una selección de ficheros, y en algunas ocasiones no se subsanan las deficiencias encontradas.
- Registro de Accesos. No todas las aplicaciones disponen de registro de accesos y las que lo tienen tampoco disponen, en todos los casos, de un periodo definido de conservación, ni conservan las actuaciones concretas que se han realizado sobre un determinado paciente. Habitualmente no se realizan auditorías con la información que consta en los registros de acceso.
- Comunicaciones cifradas. Todas las comunicaciones de datos de salud que se realicen a través de redes públicas de telecomunicaciones se deben efectuar utilizando un medio robusto de cifrado o utilizando otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros. No está por tanto permitida, por ejemplo, la remisión de datos de salud vía fax sin cifrado.
- Islas de información departamentales. En algunos Hospitales se ha detectado un número significativo de aplicaciones instaladas sin conocimiento del responsable de Seguridad del Centro, que no controla las medidas de seguridad implementadas.
- Documentos en papel. Deben implantarse medidas para el traslado de documentación médica en papel fuera del hospital que eviten que la historia clínica sea accedida o modificada durante el traslado, tales como sobres cerrados con procedimiento de notificación de recepción por parte de los centros de destino, o bien que fuese trasladada por personal específico que se encargue de su custodia ininterrumpida. Así mismo, se deben establecer mecanismos de comprobación de la integridad de la historia clínica en papel.

Por último, el Plan de inspección desarrollado se acompaña de un decálogo básico dirigido al personal sanitario y administrativo de los centros para que, de una forma práctica, se eleve el nivel de cumplimiento de la normativa de protección de datos. El decálogo reza así:

1. Trata los datos de los pacientes como querrías que tratasen los tuyos.
2. ¿Estás seguro de que tienes que acceder a esa historia clínica? Piénsalo. Sólo debes hacerlo si es necesario para los fines de tu trabajo.
3. Recuerda: tus accesos a la documentación clínica quedan registrados en el sistema. Se sabe en qué momento y a qué información has accedido. Los accesos son auditados posteriormente.
4. Evita informar a terceros sobre la salud de tus pacientes salvo que estos lo hayan consentido o tengas una justificación lícita.
5. Al salir del despacho, asegúrate de cerrar la sesión abierta en tu ordenador. No facilites a nadie tu clave y contraseña; si necesitas un acceso urgente contacta con el servicio de informática.
6. No envíes información con datos de salud por correo electrónico o por cualquier red pública o inalámbrica de comunicación electrónica; si tienes que hacerlo, no olvides cifrar los datos.
7. No tires documentos con datos personales a la papelera; destrúyelos tú mismo o sigue el procedimiento implantado en tu centro.
8. Cuando termines de pasar consulta, cierra con llave los armarios o archivadores que contengan documentación clínica.
9. No dejes las historias clínicas a la vista sin supervisión.
10. No crees por tu cuenta ficheros con datos personales de pacientes; consulta siempre antes con el departamento de informatica.

Tutelas y Denuncias Relevantes del Sector Sanitario

La praxis sanitaria: singularidades del contexto en referencia a la protección de los datos personales

María Azpeita
Agencia Española de Protección de Datos

LOS DATOS RELATIVOS A LA SALUD CONSTITUYEN PARTE DE LA ESFERA MÁS ÍNTIMA DE LAS PERSONAS, PARTICULARMENTE, AQUÉLLOS CUYO CONOCIMIENTO POR TERCEROS PUEDE AFECTAR AL DESARROLLO DE LA PERSONALIDAD, COMO LA ORIENTACIÓN SEXUAL, EL PADECIMIENTO DE ENFERMEDADES PSIQUIÁTRICAS O DE TRANSMISIÓN SEXUAL, ENTRE OTROS.

Su tratamiento inadecuado puede vulnerar otros derechos fundamentales, como el derecho a la no discriminación, y de ahí que gocen de una elevada protección: se clasifican como datos "especialmente protegidos" (Art. 7.3 de la Ley 15/1999, de 13 de diciembre, de protección de datos de carácter personal –en adelante, LOPD-) y deban tratarse en consonancia, con las más exigentes medidas de seguridad[1].

En el ámbito sanitario encontramos una tipología documental bastante estandarizada, cuya piedra angular es la historia clínica[2]. Otros tipos documentales relacionados serían las recetas[3], o los partes de incapacidad, bajas y altas, por citar algunos.

Al igual que en todos los demás sectores, el progreso de la ciencia ha propiciado una tecnificación de la medicina. Se emplean las nuevas tecnologías para la realización de pruebas diagnósticas, en la aplicación de tratamientos, para gestionar la información de los pacientes y programar su seguimiento. Disponiendo de los datos en sistemas centralizados se puede procurar, con carácter general, un acceso inmediato a los mismos, lo cual redunda en una atención sanitaria más eficiente. En definitiva; se almacenan y procesan, normalmente empleando sistemas informáticos, volúmenes ingentes de datos sensibles. La otra cara de esta moneda son los riesgos inherentes a la concentración de la información.

Según la ley, el titular de la información clínica y su destinatario es el propio paciente.

"El artículo 7.1 de la Ley 41/2002, de 14 de no-

1. El RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley 15/1999 LOPD dispone, en su art. 81.3, que las medidas de seguridad de nivel alto se aplicarán en los ficheros o tratamientos de datos de carácter personal que se refieran, entre otros, a datos de salud.
2. El art. 3 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, define la historia clínica como "el conjunto de documentos que contiene los datos, valoraciones e informaciones de cualquier índole sobre la situación y evolución clínica de un paciente a lo largo del proceso asistencial".
3. Las medidas de protección de la confidencialidad de los datos de la receta se establecen en los artículos 11 y 19 del Real Decreto 1718/2010, de 17 de diciembre, de receta médica.

viembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica -en adelante, LBAP- establece que toda persona tiene derecho a que se respete el carácter confidencial de los datos referentes a su salud, y a que nadie pueda acceder a ellos sin previa autorización amparada por la Ley. En el art. 3 de la citada Ley se define el concepto de información clínica, referido a "todo dato, cualquiera que sea su forma, clase o tipo, que permite adquirir o ampliar conocimientos sobre el estado físico y la salud de una persona, o la forma de preservarla, cuidarla, mejorarla o recuperarla".

No obstante lo anterior, en nuestra sociedad es habitual que el paciente acuda al médico en compañía de familiares, por lo que a menudo los acompañantes participan en la relación médico-paciente y tienen conocimiento de la información. Hay que tener en cuenta además la diversidad de la casuística: no siempre se trata de pacientes adultos con plena capacidad cognoscitiva. Hay pacientes que padecen trastornos mentales y a consecuencia de ello carecen de autonomía, pacientes adultos que en el curso de su evolución clínica pierden la capacidad de decidir, o pacientes menores de edad pero maduros desde un punto de vista intelectivo, por poner sólo algunos ejemplos.

En lo relativo al otorgamiento del consentimiento por representación, habrá que estar a lo dispuesto en el artículo 9.3 c) de la LBAP. En cuanto al ejercicio directo de derechos por parte de menores, el menor de edad mayor de catorce años podrá, en general, ejercitar por sí solo el derecho de acceso a la historia clínica, sin menoscabo de la facultad que también asiste para ello a los titulares de la patria potestad.

Por lo que respecta a los datos clínico-asistenciales, el artículo 6 LOPD dispone que el tratamiento de los datos de carácter personal requiere el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa. A continuación, y de manera especifica para datos de salud, el artículo 7.3 LOPD establece que sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente[4]. No obstante lo anterior, el artículo 6.2 LOPD establece

"No será preciso el consentimiento [...] cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley..."

en relación con el 7.6 LOPD, que dispone:

"No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta, asimismo, a una obligación equivalente de secreto.

También podrán ser objeto de tratamiento los datos a que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento."

Por su parte, el artículo 8 LOPD habilita a las entidades y centros sanitarios, tanto públicos como privados, y a los profesionales, a proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratadas en los mismos, de acuerdo con la legislación estatal o autonómica sobre sanidad.

Estas excepciones se refieren únicamente al tratamiento de datos que se realice para proporcio-

4. Cabe recordar, en relación a la excepción dirigida a la salvaguarda de la salud pública, que la llegada al entorno occidental de brotes epidémicos foráneos han dado lugar a situaciones excepcionales desde el punto de vista de la salud pública. A este respecto, el artículo 41.2 de la Ley 33/2011, de 4 de octubre, General de Salud Pública, dispone que no será necesario el consentimiento del interesado para el tratamiento de sus datos personales, relacionados con la salud, ni para su cesión a otras Administraciones Públicas sanitarias, cuando ello sea estrictamente necesario para la tutela de la salud de la población.

nar servicios sanitarios –diagnosis, terapia, etc-, pero no son válidas para otras finalidades, como pudiera ser la gestión del personal del centro médico.

LA ACTUACIÓN DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

La labor de la Agencia Española de Protección de Datos se orienta, por un lado, a mejorar el conocimiento de la sociedad para inculcar buenas prácticas y prevenir conductas de riesgo, y por otro, a tutelar los derechos de los ciudadanos, e inspeccionar y sancionar las infracciones que constate.

La LOPD recoge una serie de derechos personalísimos de los ciudadanos, como son el derecho de acceso, el de rectificación y de cancelación de sus datos personales, y el de oposición al tratamiento de los mismos, que han de ejercerse por el ciudadano ante el responsable del fichero que trata sus datos.

Si el responsable del fichero no atiende esa solicitud, el ciudadano puede reclamar la asistencia de la AEPD para que el ejercicio de sus derechos sea efectivo, conforme a lo dispuesto en el art. 18 LOPD (reclamación de tutela de derechos). El procedimiento, regulado en los artículos 117 a 119 del RD 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley 15/1999 LOPD –en adelante, Reglamento LOPD-, se inicia a solicitud del afectado, expresando los hechos que fundamentan su reclamación y los preceptos de la LOPD que se consideran vulnerados. Recibida la reclamación, la AEPD la traslada al responsable del fichero, para que pueda formular alegaciones. Recibidas las alegaciones o transcurrido el plazo estipulado, la Agencia, previos los demás la informes, pruebas y otros actos de instrucción pertinentes -incluida la audiencia del afectado y nuevamente del responsable del fichero-, resolverá sobre la reclamación formulada, en un plazo máximo de 6 meses.

De otra parte, la Agencia tiene la potestad de sancionar las infracciones de la legislación. Quienes dispongan de pruebas o indicios de que se ha producido alguna de las infracciones definidas en el art. 44 LOPD, pueden denunciarlo ante la AEPD. A la vista de los hechos denunciados, conforme a lo establecido en los arts. 122 a 126 del Reglamento LOPD, la Agencia podrá realizar actuaciones previas de investigación, con objeto de precisar los hechos que pudieran justificar la incoación de un procedimiento sancionador, identificar la persona u órgano que pudiera resultar responsable y fijar las circunstancias relevantes del caso. Para ello, podrá solicitar cuanta documentación estime oportuna, realizar visitas de inspección por parte de los inspectores designados, en los locales o sede del inspeccionado, o donde se encuentren ubicados los ficheros.

En caso de apreciarse la comisión de una infracción, se iniciaría de oficio un procedimiento sancionador o de infracción de las Administraciones Públicas, conforme a lo establecido en los arts. 127 a 129 del Reglamento LOPD.

Cabe recordar que, según lo dispuesto en el art. 116.1 del Reglamento LOPD, las resoluciones de la Agencia se publican para general conocimiento en su página web, una vez que han sido notificadas a los interesados.

TUTELA DE DERECHOS

En los dos últimos años (del 1 de enero de 2016 a 1 de enero de 2018), la Agencia ha tramitado 305 procedimientos de tutela de derechos relacionados con el ámbito de la sanidad.

La inmensa mayoría de ellos a raíz de incidencias en el ejercicio del derecho de acceso a la documentación clínica y pericial en poder de los centros médicos y las entidades aseguradoras. En ocasiones el paciente considera que la información que se le ha facilitado no está completa. Otras veces el interesado aduce que la entidad médica no ofrece el acceso a los datos mediante un sistema sencillo y gratuito, tal como señala la ley (p.ej. exige al paciente que aporte un CD o pendrive para grabar en este soporte una copia). En algún caso el reclamante ha solicitado la cancelación de sus datos personales obrantes en la historia clínica de un determinado centro médico, pero su pretensión se rechazó puesto que el centro argumentó que los datos deben conservarse durante el tiempo establecido en la legislación aplicable. A este respecto, cabe recordar que la Ley 41/2002 (LBAP) dispone en su artí-

culo 17 que los centros sanitarios conservarán la documentación clínica durante el tiempo que sea preciso en cada caso para garantizar la asistencia al paciente, y como mínimo, cinco años desde la fecha del alta[5].

En consecuencia, dado que los datos contenidos en la historia clínica son relevantes para preservar la salud del paciente, deberán custodiarse en condiciones que garanticen la confidencialidad de la información y la intimidad de los pacientes, durante el tiempo adecuado a cada caso -a criterio médico-, no procediendo cancelar dichos datos cuando pudiera perjudicarse la salud futura del paciente al que se refieren los mismos, sin olvidar otros intereses legítimos de terceros.

También es interesante el caso de un ciudadano que había solicitado a una Dirección Provincial de Educación la realización de un diagnóstico clínico completo de sus hijos menores de edad, en el que se determinase si tenían alguna necesidad específica de apoyo educativo. El interesado requirió copia de dicho diagnóstico y de las pruebas empleados para su elaboración. También pidió conocer el número de alumnos que presentasen alguna dificultad específica de aprendizaje en el mismo centro escolar de sus hijos, a cuántos se les había realizado una segunda evaluación, causas que la justificaron, y otros datos para tener conocer mejor la situación de los menores afectados.

Se resolvió estimar la reclamación en lo concerniente al acceso a los datos de salud de los hijos menores del reclamante, de tal modo que la AEPD instó a la Dirección Provincial de Educación a que le facilitase el acceso a tales datos. Por el contrario, se rechazó la parte de la solicitud referente al acceso a otros menores sobre los cuales el interesado no ostentaba ninguna representación.

Para concluir esta reseña referente a las tutelas, es interesante indicar que en varios casos los ciudadanos han solicitado conocer la identidad de todos los empleados que han accedido a los datos obrantes en las historias clínicas del centro médico, en base a la presunción de que aquéllos pudieran haberlos cedido a terceros. Sin embargo, esa solicitud no se ajusta al contenido del derecho de acceso a datos personales que reconoce al titular de tales datos el artículo 15 de la LOPD.

PROCEDIMIENTOS SANCIONADORES

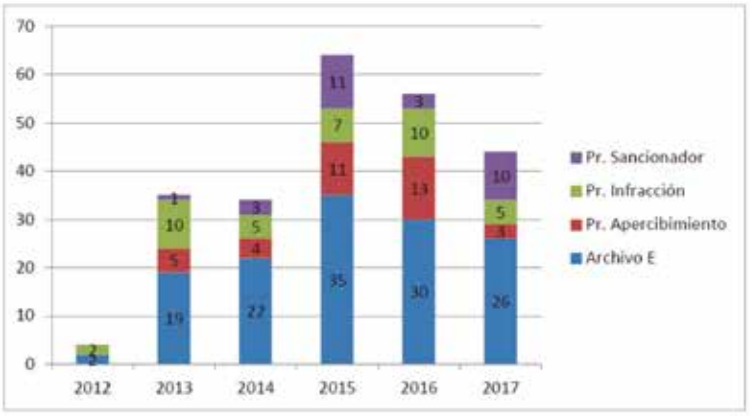
Lo cierto es que las infracciones de este sector no son cuantitativamente numerosas, en comparación con las de otros tipos. Entre octubre de 2012 y octubre de 2017 se emitieron 237 resoluciones referentes a expedientes de sanidad, que representan un 2,19% del total.

En el período 2016-2017 se han registrado 214 denuncias. De ellas, 58 eran casos referidos a hospitales públicos, 17 a hospitales privados, 41 a mutualidades, 45 a centros médicos o clínicas y 14 a aseguradoras de salud.

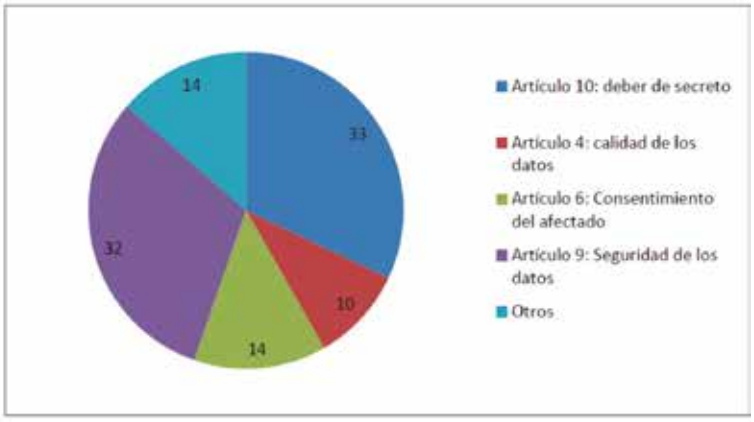
En lo concerniente a las sanciones que conllevan la imposición de multa, se observa que la tendencia es decreciente. Desde el año 2012 y hasta 2015 el volumen de sanciones fue creciendo –

5. Ley 41/2002 LBAP, Art. 17 "1. Los centros sanitarios tienen la obligación de conservar la documentación clínica en condiciones que garanticen su correcto mantenimiento y seguridad, aunque no necesariamente en el soporte original, para la debida asistencia al paciente durante el tiempo adecuado a cada caso y, como mínimo, cinco años contados desde la fecha del alta de cada proceso asistencial. No obstante, los datos de la historia clínica relacionados con el nacimiento del paciente, incluidos los resultados de las pruebas biométricas, médicas o analíticas que en su caso resulten necesarias para determinar el vínculo de filiación con la madre, no se destruirán, trasladándose una vez conocido el fallecimiento del paciente, a los archivos definitivos de la Administración correspondiente, donde se conservarán con las debidas medidas de seguridad a los efectos de la legislación de protección de datos.
2. La documentación clínica también se conservará a efectos judiciales de conformidad con la legislación vigente. Se conservará, asimismo, cuando existan razones epidemiológicas, de investigación o de organización y funcionamiento del Sistema Nacional de Salud. Su tratamiento se hará de forma que se evite en lo posible la identificación de las personas afectadas. Sin perjuicio del derecho al que se refiere el artículo siguiente, los datos de la historia clínica relacionados con las pruebas biométricas, médicas o analíticas que resulten necesarias para determinar el vínculo de filiación con la madre del recién nacido, sólo podrán ser comunicados a petición judicial, dentro del correspondiente proceso penal o en caso de reclamación o impugnación judicial de la filiación materna."

Entre octubre de 2012 y octubre de 2017 se firmaron un total de 237 resoluciones de expedientes de sanidad que representan un 2,19% del total, que fueron 10.804



Si nos fijamos en los que terminaron con un apercibimiento, procedimiento sancionador, o procedimiento de infracción de las AAPP, estos los artículos de la LOPD incumplidos:



en el año 2015, se impusieron sanciones por un importe total de 132.001 €-, para descender, en 2017, hasta los 38.700 €.

A continuación se reseñan los tipos de denuncias más frecuentes que se vienen presentando en los últimos años, y se comentan algunos casos significativos.

- Los accesos injustificados a la historia clínica de una persona (Vulneración de las medidas de seguridad).
  - Se denuncian accesos indebidos a la historia clínica de un paciente. En la inspección realizada se constató que la empresa encargada del tratamiento de la aplicación informática de un servicio autonómico de salud, se disponía de un usuario genérico conocido por todos los empleados, con acceso pleno a todos los recursos de la aplicación. A la vista de los hechos, se inició un procedimiento de infracción de las Administraciones Públicas, por la vulneración de las medidas de seguridad, puesto que el responsable debe velar por que el encargado del tratamiento reúna las garantías para el cumplimiento de lo dispuesto en el Reglamento LOPD.
  - Se denuncian los accesos a la historia clínica de un trabajador de un hospital. Se averigua que han accedido dos compañeros empleando la clave del jefe de servicio. A la vista de los hechos, se inició un procedimiento de infracción de las Administraciones Públicas, por el tratamiento sin consentimiento de los datos de la denunciante, y la falta de medidas de seguridad adecuadas.
  - Se denuncian accesos indebidos a la historia clínica de un médico trabajador de un servicio público de salud, por parte de sus compañeros médicos. Se investiga el incidente y

se comprueba que el sistema informático de gestión tiene incorporadas las medidas de seguridad adecuadas para registrar los accesos. El expediente de infracción de Administraciones Públicas se archiva, mientras que la Administración Pública competente incoa expediente disciplinario a los empleados que accedieron indebidamente a esos datos.

Cabe subrayar que los usuarios de un sistema (médicos, enfermeros, auxiliares, etc de un servicio de salud) tienen que acceder siempre con la debida justificación que requiera el cumplimiento de la tarea clínico-asistencial concreta que tengan atribuidos. La Ley 41/2002 (LBAP), en su artículo 16 dedicado a los usos de la historia clínica, dispone:

"1. [...] Los profesionales asistenciales del centro que realizan el diagnóstico o el tratamiento del paciente tienen acceso a la historia clínica de éste como instrumento fundamental para su adecuada asistencia.

2. Cada centro establecerá los métodos que posibiliten en todo momento el acceso a la historia clínica de cada paciente por los profesionales que le asisten.

[...]

4. El personal de administración y gestión de los centros sanitarios sólo puede acceder a los datos de la historia clínica relacionados con sus propias funciones.

5. El personal sanitario debidamente acreditado que ejerza funciones de inspección, evaluación, acreditación y planificación, tiene acceso a las historias clínicas en el cumplimiento de sus funciones de comprobación de la calidad de la asistencia, el respeto de los derechos del paciente o cualquier otra obligación del centro en relación con los pacientes y usuarios o la propia Administración sanitaria.

6. El personal que accede a los datos de la historia clínica en el ejercicio de sus funciones queda sujeto al deber de secreto.

7. Las Comunidades Autónomas regularán el procedimiento para que quede constancia del acceso a la historia clínica y de su uso."

A su vez, la LOPD regula en su artículo 4 el principio de calidad de datos que resulta aplicable a estos supuestos, según el cual los datos no pueden usarse para una finalidad incompatible con aquélla para la que fueron recogidos:

"1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos".

Sintetizando las previsiones legales puede afirmarse que:

a) Las operaciones y procedimientos técnicos automatizados o no, que permitan el acceso –la comunicación o consulta- de datos personales, es un tratamiento[6] sometido a las exigencias de la LOPD.

b) Los ficheros[7] que contengan un conjunto organizado de datos de carácter personal así como el acceso a los mismos, cualquiera que sea la forma o modalidad en que se produzca están, también, sujetos a la LOPD.

c) La LOPD impone al responsable del fichero la adopción de medidas de seguridad, cuyo detalle se remite a normas reglamentarias, que eviten accesos no autorizados.

En el sector sanitario, los sistemas deberán estar dotados de medidas de seguridad de nivel alto, ya que los ficheros o tratamientos de datos de carácter personal se refieren a datos de salud -art. 81.3.a) del Reglamento LOPD-. El artículo 88 del Reglamento LOPD, por su parte, configura los elementos que compondrán el documento de seguridad, mientras que los elementos que debe componer el "registro de accesos" se establecen en su art.

6. La LOPD, en su art. 3.c), define tratamiento de datos a las *"operaciones y procedimientos técnicos de carácter automatizado o no, que permitan la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias."*

7. Fichero es *"todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso" (LOPD, art. 3. b).*

103[8]. Es particularmente importante destacar que el responsable de seguridad debe revisar al menos una vez al mes la información de control registrada y elaborar un informe de las revisiones realizadas y los problemas detectados (art. 103.5 Reglamento LOPD).

d) El mantenimiento de ficheros carentes de medidas de seguridad que permitan accesos o tratamientos no autorizados, cualquiera que sea la forma o modalidad de éstos, constituye una infracción tipificada como grave (art. 44.3.h) de la LOPD).

Por tanto, la actuación de la Agencia se encamina a comprobar si el responsable del fichero tiene implementadas medidas de seguridad adecuadas para que cada usuario acceda únicamente a los datos que necesite para ejecutar su trabajo, y que todos los accesos queden registrados. Y ello en base al art. 9 de la LOPD, que establece el principio de "seguridad de los datos", imponiendo la obligación de adoptar las medidas de índole técnica y organizativa que garanticen aquélla, añadiendo que tales medidas tienen como finalidad evitar, entre otros aspectos, el "acceso no autorizado".

Si un usuario del sistema accediera a otras historias clínicas sin requerirlo la prestación asistencial que le competa, debe quedar constancia de ello en los informes mensuales y auditorías bienales preceptivos del sistema, lo que permitirá al responsable del fichero adoptar las medidas disciplinarias o sancionadoras correspondientes[9].

- La publicación de la imagen de un paciente o de imágenes radiográficas con datos personales en internet –en youtube, en redes sociales, y en otros medios- (Esta actuación supone un tratamiento no consentido de datos y vulneración del deber de secreto).

En relación con lo anterior, cabe señalar que la proliferación masiva de los smartphones ha propiciado también un aumento de las denuncias por la grabación no consentida de las consultas médicas, empleando esas grabaciones como medio de presión a los profesionales sanitarios.

- El extravío de historias clínicas en los centros

8. Con relación al "Registro de accesos" el Reglamento LOPD, en su artículo 103, establece:
"1. De cada intento de acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.
2. En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.
3. Los mecanismos que permiten el registro de accesos estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.
4. El período mínimo de conservación de los datos registrados será de dos años.
5. El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.
6. No será necesario el registro de accesos definido en este artículo en caso de que concurran las siguientes circunstancias:
a) Que el responsable del fichero o del tratamiento sea una persona física.
b) Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.
La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad."

9. En este sentido, el articulo 46 LOPD dispone que:
"1. Cuando las infracciones a que se refiere el artículo 44 fuesen cometidas en ficheros de titularidad pública o en relación con tratamientos cuyos responsables lo serían de ficheros de dicha naturaleza, el órgano sancionador dictará una resolución estableciendo las medidas que procede adoptar para que cesen o se corrijan los efectos de la infracción. Esta resolución se notificará al responsable del fichero, al órgano del que dependa jerárquicamente y a los afectados si los hubiera.
2. El órgano sancionador podrá proponer también la iniciación de actuaciones disciplinarias, si procedieran. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones Públicas.
3. Se deberán comunicar al órgano sancionador las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores."



médicos (Vulneración de las medidas de seguridad).

- Se investigó el extravío de miles de pruebas radiológicas en un centro hospitalario. Se averiguó que la pérdida se produjo a consecuencia de un fallo en el sistema informático de copia y respaldo del fichero de imágenes.

- La inclusión, en una historia clínica, de datos pertenecientes a otro paciente (Incumplimiento de las medidas de seguridad y vulneración del deber de secreto).
- El abandono de documentación en vías públicas, con datos personales de salud (Vulneración de las medidas de seguridad).

  Este tipo de hechos es frecuentemente denunciado por las Fuerzas y Cuerpos de Seguridad del Estado. La mayor parte de los centros sanitarios cuenta con un protocolo para la destrucción de la documentación que no es necesario conservar. En los casos denunciados, no se llevaron a cabo las medidas pertinentes de eliminación segura de la documentación.
- Diversas conductas que suponen una vulneración del deber de secreto
  - Denuncia a un servicio de salud por facilitar datos personales de los pacientes que precisaban prótesis ortopédicas a una entidad de ortopedia, sin su consentimiento. Esta práctica constituye una vulneración del deber de secreto.
  - Denuncias a consecuencia de informar por teléfono a un familiar, del estado de una paciente, que estaba ingresada. El incidente supone una vulneración del deber de secreto.
  - Se entregó a un familiar distinto de la persona ingresada, la factura de una clínica psiquiátrica. Esa factura se empleó posteriormente en un procedimiento civil.
- El empleo de los datos recabados para fines distintos a los estipulados.
  - Se denuncia que el número de teléfono proporcionado por un paciente en una clínica fue empleado por el auxiliar que tomó sus datos para enviarle un mensaje de tipo personal (Desvío de finalidad).

REFERENCIAS

- Decálogo de protección de datos para el personal sanitario y administrativo (AEPD) [http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2017/DecalogoPersonalSanitario.pdf]
- Informe nº 0222/2014, de la Agencia Española de Protección de *Datos, sobre Menores e historia clínica. Consentimiento y derechos de acceso y oposición. [http://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/common/pdf_destacados/2014-0222_Menores-e-historia-cl-ii-nica._Consentimiento-y-derechos-de-acceso-y-oposici-oo-n.pdf]*
- Artículo de Javier García Amez, "La protección de datos del usuario de la sanidad: derecho a la intimidad y asistencia sanitaria", DS: *Derecho y salud*, ISSN 1133-7400, Vol. 20, Nº. 1, 2010, págs. 43-69.
- Ponencia de Juan Luis Beltrán Aguirre, "La protección de los datos personales relacionados con la salud [https://www.navarra.es/NR/rdonlyres/517A4434-9C3B-442E-8651-61A7AE0490AD/226320/pdps.pdf]

Elementos clave del RGPD: Inventario de tratamientos y Evaluación de impacto

Jaime Martínez Sánchez
Responsable de soluciones de privacidad y protección de datos
Grupo SIA

A FINALES DEL PRÓXIMO MES DE MAYO, EL REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, DE 27 DE ABRIL DE 2016, RELATIVO A LA PROTECCIÓN DE LAS PERSONAS FÍSICAS EN LO QUE RESPECTA AL TRATAMIENTO DE DATOS PERSONALES Y A LA LIBRE CIRCULACIÓN DE ESTOS DATOS Y POR EL QUE SE DEROGA LA DIRECTIVA 95/46/CE (EN ADELANTE, REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS O RGPD) RESULTARÁ PLENAMENTE APLICABLE, POR LO QUE, EL CUMPLIMIENTO DE SUS REQUISITOS Y EXIGENCIAS PODRÁ SER FISCALIZABLE POR PARTE DE LAS AUTORIDADES DE CONTROL COMPETENTES EN LA MATERIA.

A la fecha, las organizaciones responsables y encargadas del tratamiento deberían de: (i) tener definido, al menos, el plan de adecuación (conjunto de proyectos a abordar), así como el plan de acción asociado (la secuenciación temporal de dichos proyectos, ordenados a partir de la priorización resultante de la valoración de diferentes magnitudes –riesgo, coste, beneficio…), partiendo de las deficiencias y oportunidades de mejora identificadas en el análisis inicial de cumplimiento previamente realizado; y (ii) estar en proceso de definición e implantación de las diferentes acciones concretas en las que se descomponen cada uno de los proyectos identificados.

Ello cobra especial importancia en el ámbito de las organizaciones que prestan servicios de naturaleza sanitaria, en base a la especial criticidad y sensibilidad de muchos de los tratamientos de datos personales llevados a cabo en el desempeño de sus competencias y actividades. Ello, debido a que los datos personales relativos a la salud se incluyen entre las *categorías especiales* de datos (como ya viene ocurriendo en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, donde tienen la consideración de *especialmente protegidos*), quedando su tratamiento limitado a casos concretos, y habiendo de garantizarse unas condiciones reforzadas de protección.

Así, a continuación, se realiza un breve recorrido por dos de las principales novedades introducidas por el Reglamento general de protección de datos, así como en enfoque con el que se recomienda abordar su cumplimiento:

REGISTRO DE ACTIVIDADES DE TRATAMIENTO (INVENTARIO DE TRATAMIENTOS):

Este elemento, regulado en el artículo 30 del RGPD, requiere que las organizaciones que manejen datos personales realicen inicialmente un levantamiento minucioso de todas las actividades de tratamiento efectuadas, lo que implica la necesidad de revisar la práctica totalidad de procesos existentes en dichas organizaciones.

No resulta suficiente ni aconsejable la mera identificación de finalidades genéricas o abstractas adscritas al catálogo de ficheros inscritos por las organizaciones en el registro de la autoridad de control en materia de protección de datos personales. Ello, debido a que el registro de actividades de tratamiento se configura como elemento previo y de consulta recurrente desde otros de los ámbitos regulados por el Reglamento general de protección de datos como,



por ejemplo, y especialmente, la evaluación de impacto a la protección de datos.

De lo anterior se desprende la necesidad e importancia de enfocar adecuadamente la construcción del registro de actividades de tratamiento, no sólo con una visión de cumplimiento formal del requisito establecido en el citado artículo 30, sino con una visión estratégica, concibiéndose como uno de los pilares fundamentales sobre el que se apoye el sistema de gestión de la protección de datos en las organizaciones. De ahí la importancia de obtener información asociada al mayor número de atributos de cada una de las operaciones de tratamiento que se identifiquen, y no sólo limitarse a la estructura tasada que propone el RGPD.

EVALUACIÓN DE IMPACTO A LA PROTECCIÓN DE DATOS:

La realidad actual, presidida por la innovación, la especialización y la diferenciación, se caracteriza por la contínua puesta en circulación o producción de nuevos elementos (productos, servicios, iniciativas, proyectos, sistemas, etc.) apoyados, como no podía ser de otra manera, en el tratamiento de información que, en la mayoría de los casos, incluye datos personales pertenecientes a diferentes colectivos de interesados.

El tratamiento de datos personales en el contexto de estos nuevos elementos se encuentra expuesto a una serie de riesgos cuya materialización generaría un impacto negativo, no sólo a las organizaciones que la manejan (desde el punto de vista de incumplimientos legales, crisis reputacionales, etc.), sino también a los titulares de la misma, especialmente entre el colectivo de pacientes. Se ha de tomar en consideración, además, que, en los últimos tiempos, el sector sanitario ha sido uno de los más afectados desde el punto de vista de ciberataques, por encontrarse altamente expuesto en base a la sensibilidad y el valor de los datos manejados.

Por tanto, resulta primordial, por una parte, analizar y gestionar, en una etapa temprana, los riesgos que para la privacidad tiene, o podría tener, la puesta en circulación o producción de los elementos indicados anteriormente y, por la otra, crear y madurar una cultura de hacerlo de forma repetible en base al procedimiento definido. Es lo que, en conjunto, se conoce como "*privacy by design/by default*".

Así, el proceso iterativo para la realización de la evaluación de impacto, introducida por el artículo 35 del RGPD, debería de incluir, al menos, las siguientes fases:

1. Descripción de los tratamientos de datos de pacientes previstos (previamente identificados en el registro de actividades de tratamiento).
2. Evaluación de la necesidad y proporcionalidad.
3. Descripción de medidas de seguridad existentes.
4. Evaluación de los riesgos para los derechos y libertades de los pacientes.
5. Implementación de medidas para reducir el nivel de riesgo.
6. Documentación del proceso.
7. Monitorización del estado de implementación de las medidas, y repetición del proceso.

El Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal

Agustín Puente
Agencia Española de Protección de Datos

EL PROFUNDO CAMBIO EN EL MODELO DE REGULACIÓN DEL DERECHO FUNDAMENTAL A LA PROTECCIÓN DE DATOS QUE SUPONE LA APROBACIÓN DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS AFECTA NECESARIAMENTE AL RÉGIMEN DE ESTE DERECHO EN NUESTRO PAÍS.

En efecto, el Reglamento es una norma de aplicación directa en los Estados miembros que desplaza a las leyes nacionales de protección de datos en cuanto no resulten conformes con él o regulen la misma materia en un modo que no sea estrictamente el establecido en la norma de derecho de la Unión.

Por otra parte, el Reglamento otorga a los Estados miembros a lo largo de muchos de sus preceptos la posibilidad de establecer ciertas especialidades o aclaraciones en el régimen jurídico que el mismo establece. Así, por poner sólo algunos ejemplos significativos, los Estados miembros podrán establece la edad a la que el menor podrá prestar su consentimiento para el tratamiento de sus datos personales, siempre que tal edad sea superior a trece años (artículo 8.1), la posibilidad de prever que el consentimiento del interesado no baste por sí solo para levantar la protección de los denominados datos especialmente protegidos (artículo 9.2 a), la posibilidad de establecer determinadas limitaciones a la aplicación de ciertos preceptos relacionados con los principios y los derechos del afectado, siempre con una serie de garantías adicionales (artículo 23), la delimitación de los tratamientos que no requerirán de la realización de una evaluación de impacto en la protección de datos (artículo 35.4) o la fijación de supuestos en los que los responsables de los tratamientos deberán designar un delegado de protección de datos (artículo 37.4).

Además, dentro del cambio de modelo que el Reglamento representa, es especialmente necesario que los sujetos obligados por la norma y los titulares del derecho fundamental dispongan de instrumentos que les aporten la necesaria seguridad jurídica para garantizar, por una parte, la garantía adecuada del derecho y, por otra, que no puedan producirse situaciones en las que, incluso en la convicción subjetiva del cumplimiento de la norma, la conducta pueda suponer una vulneración de la misma que despliegue la aplicación del especialmente gravoso régimen sancionador establecido por el Reglamento.

Todo ello conduce a la necesidad de adoptar una disposición de derecho interno que adapte el mismo a las exigencias del derecho de la Unión, regule aquellas materias en que el Reglamento otorga un margen de maniobra a los Estados miembros y, en definitiva, aporte seguridad jurídica a los operadores que han de aplicarla.

En este contexto el Gobierno aprobó el 10 de noviembre de 2017 el Proyecto de Ley Orgánica de Protección de Datos de carácter personal, cuyo objeto principal, conforme indica el artículo 1.1, es "adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones".

El Proyecto, dada la finalidad que acaba de indicarse, no implica una regulación integral del derecho fundamental a la protección de datos, toda vez que la mayor parte de las normas que

garantizan este derecho aparecen recogidas expresamente en el Reglamento General de Protección de Datos, centrándose en regular aquellas materias que requieren de un desarrollo o una adecuada clarificación dentro del marco general del ordenamiento español. De este modo, son continuas las remisiones al Reglamento, que por su propia naturaleza no puede ser objeto de un mera reproducción por el derecho interno, aunque ciertamente su considerando 8 otorga un cierto margen de reproducción cuando ello permita clarificar aquellas materias sobre las que cabe una regulación específica por el derecho interno.

La extensión de este trabajo impide llevar a cabo un estudio exhaustivo del contenido del Proyecto de Ley. De este modo, debemos limitar nuestro análisis a las principales novedades que dicho texto aporta, sin entrar tampoco en el estudio de aquellas cuestiones en que es el Reglamento y no el Proyecto de Ley el que introduce por sí solo una modificación sustancial del régimen de las garantías de la protección de datos. Para ello, seguiremos la estructura del propio texto del Proyecto, centrándonos en particular en las normas de carácter sustantivo recogidas en sus cinco primeros Títulos.

El Título I del Proyecto establece las disposiciones generales. Tras recoger el objeto ya mencionado, y recordar que el derecho fundamental se ejercerá conforme al Reglamento y el propio texto legal, el artículo 2 tiene por objeto resolver el problema derivado del distinto ámbito de aplicación del derecho interno y del de la Unión Europea, sometiendo al Reglamento y al propio Proyecto aquellos tratamientos respecto de los que son exigibles las garantías del derecho fundamental a la protección de datos pero no están sometidas de forma directa al Reglamento, al no ser materias sometidas al derecho de la Unión. A título de ejemplo, se hace referencia a los tratamientos electorales, los penitenciarios o los registros dotados de fe pública, así como a los ficheros judiciales, si bien tal lista no tiene un carácter exhaustivo.

También dentro de estas disposiciones es especialmente relevante el artículo 3, que permite a los herederos de un fallecido, su albacea testamentario y en determinados supuestos al Ministerio Fiscal el ejercicio de los derechos de acceso, rectificación y supresión de los datos del causante. Este precepto se complementa con la disposición adicional séptima, que prevé el acceso por estas personas a los contenidos gestionados por los servicios de la sociedad de la información del fallecido, como germen del denominado "testamento digital".

> ***Es especialmente relevante el artículo 3, que permite a los herederos de un fallecido, su albacea testamentario y en determinados supuestos al Ministerio Fiscal el ejercicio de los derechos de acceso, rectificación y supresión de los datos del causante"***

Dentro de las disposiciones del Título II del Proyecto, referidas a los principios de protección de datos son especialmente relevantes las disposiciones relacionadas con el consentimiento de los afectados y el tratamiento de las ahora denominadas categorías especiales de datos.

En relación con el primero, como es sabido, el régimen establecido en el Reglamento impone que el consentimiento del interesado haya de ser explícito, lo que supone una profunda modificación del régimen preexistente en nuestro país, en que se admitía, para datos no especialmente protegidos, el denominado "consentimiento tácito". El Proyecto, con un afán ciertamente didáctico reproduce en su artículo 6.1 el concepto de consentimiento previsto en el Reglamento y añade en su disposición transitoria quinta, siguiendo lo previsto en el considerando 171 del Reglamento, que "Cuando el tratamiento se base en un consentimiento otorgado con anterioridad a la aplicación del Reglamento (UE) 2016/679, no será necesario recabar nuevamente dicho consentimiento si la forma en que se otorgó se ajusta a las condiciones del Reglamento (UE) 2016/679". De este modo, no será válido el tratamiento basado en un consentimiento tácito anterior a la entrada en vigor del Reglamento a menos que se recabe un nuevo consentimiento o el responsable pueda amparar el tratamiento en alguna de las restantes causas de legitimación establecidas en las letras b) a f) del artículo 6.1 del Reglamento, en particular, en la existencia de un interés

legítimo prevalente. En este sentido, y aunque referido a un concreto sector de actividad, puede ser interesante revisar el informe 195/2017 de la Agencia Española de Protección de Datos, accesible en su página web.

También en relación con el consentimiento, el Proyecto hace uso en artículo de la facultad otorgada a los Estados miembros por el artículo 8.1 del Reglamento, rebajando la edad para el consentimiento del menor de edad a los trece años, si bien excluye de dicha rebaja "los supuestos en que la ley exija la asistencia de los titulares de la patria potestad o tutela para la celebración del acto o negocio jurídico en cuyo contexto se recaba el consentimiento para el tratamiento", con el objeto, según se indica en la exposición de motivos, de asimilar el sistema español al de otros Estados de nuestro entorno.

En relación con las categorías especiales de datos, los tradicionalmente llamados "datos especialmente protegidos", entre los que el reglamento ahora incluye también los datos biométricos y, en todo caso, los genéticos, el Proyecto incluye en primer lugar, dentro del margen ofrecido por el Reglamento una regla que impide la creación de las denominadas "listas negras" basadas en informaciones referidas a la ideología, afiliación sindical, religión, orientación sexual, creencias u origen étnico. Estos datos podrán tratarse al amparo de alguna de las excepciones a la prohibición general previstas en los apartados b) y siguientes del artículo 9 del Reglamento, pero no basado en el mero consentimiento del afectado.

Particularmente relevante en el ámbito de la salud, el artículo 9.2 se refiere a la habilitación legal para el tratamiento de los datos "especialmente protegidos". Ello no supone una derogación de las habilitaciones legales actualmente existentes, sino el mantenimiento de la regla que hasta ahora establece el artículo 7.3 de la Ley Orgánica 15/1999. Además, el párrafo segundo de este precepto reconoce la licitud del tratamiento de estos datos que sea llevado a cabo en el ámbito de la salud "cuando así lo exija la gestión de los sistemas y servicios de asistencia sanitaria y social, pública y privada, o la ejecución de un contrato de seguro del que el afectado sea parte", lo que legitima el tratamiento de los datos de salud de los afectados sin necesidad de recabar el consentimiento del paciente tanto en el ámbito de la sanidad pública como en el del seguro privado de asistencia sanitaria.

El Título III regula los derechos de los interesados, diferenciando el denominado derecho de información (o principio de transparencia) de los restantes derechos consagrados por el Reglamento. En relación con el primero, es especialmente relevante el artículo 11, que clarifica que en el ámbito de determinados tratamientos, esencialmente en los supuestos en que los datos son recogidos a través de servicios de la sociedad de la información, el responsable podrá cumplir su obligación de informar a través de sistemas de "información por capas", de forma que se facilite al interesado una información esencial, que el propio Proyecto enumera, facilitando un enlace que permita al interesado "acceder de forma sencilla e inmediata a la restante información". En este punto puede resultar interesante la consulta de la guía para el cumplimiento del deber de informar, disponible en la página web de la Agencia Española de Protección de Datos.

En lo que se refiere a los restantes derechos, el Proyecto se remite, con carácter general, al Reglamento. No obstante es interesante lo establecido en el artículo 12.2, en que se prevé, siguiendo la doctrina del Tribunal Supremo la posibilidad de otorgamiento del derecho de acceso pueda otorgarse facilitando al afectado un sistema de acceso remoto, directo y seguro a los datos personales que garantice, de modo permanente, el acceso a su totalidad. En este caso, se entenderá que el responsable al que se solicite el acceso lo otorga cuando comunique al interesado el modo en que puede acceder de forma permanente a sus datos.

El Título IV establece normas aplicables a tratamientos concretos, tratando de aportar a los operadores la seguridad jurídica a la que nos referimos al comienzo de este texto. Así, se establecen supuestos en los que, sin establecer una habilitación legal expresa para el tratamiento de los datos, se contiene una presunción *iuris tantum* acerca de la posible prevalencia en el tratamiento del interés legítimo del responsable. Así sucede en relación con el tratamiento de datos de empresarios individuales o personas de contacto, que antes aparecía excluido de la legisla-

ción de protección de datos, pero que ahora está sometido a ella por imperativo del Reglamento, o con tratamientos respecto de los que o bien existía con anterioridad algún tipo de previsión en la Ley Orgánica 15/1999 y sus disposiciones de desarrollo o bien estaban necesitados de una regulación específica que clarificase determinadas cuestiones relacionadas con los mismos. Entre los primeros cabe hacer referencia al régimen de los sistemas de información crediticia, los tratamientos con fines de videovigilancia y los sistemas de exclusión publicitaria. Entre los segundos, se regulan los sistemas de información de denuncias internas en el sector privado. Además, se regulan igualmente los tratamientos de datos con fines estadísticos o de archivo en interés público, así como el régimen de tratamiento de los datos referidos a infracciones y sanciones administrativas.

Finalmente, el Título V, bajo la rúbrica "responsable y encargado del tratamiento" regula las obligaciones de responsabilidad activa previstas en el Capítulo IV del Reglamento, partiendo en el artículo 28 del principio general de que las medidas de responsabilidad activa previstas en la normativa de protección de datos exigirá, en todo caso, la previa realización de un análisis de los riesgos que para los derechos de los afectados pueden derivarse de la realización del tratamiento. Ese análisis, que ha de llevarse siempre a cabo, puede conducir a la necesidad de realizar posteriormente una evaluación de impacto en la protección de datos o a consultar acerca de la procedencia del tratamiento a la autoridad de protección de datos, conforme a lo exigido por el artículo 36 del Reglamento.

Dentro de las obligaciones de responsabilidad activa, el Proyecto se refiere también al registro de actividades de tratamiento, que, a fin de clarificar su estructura "podrá organizarse en torno a conjuntos estructurados de datos, deberá especificar, según sus finalidades, las actividades de tratamiento llevadas a cabo y las demás circunstancias establecidas en el citado reglamento", aproximando esta figura al concepto de fichero que existía en la legislación anterior.

Finalmente, el Proyecto se refiere particularmente al régimen del Delegado de protección de datos y a los sistemas de autorregulación.

En cuanto al delegado de protección de datos se establece un régimen detallado, con el objeto de clarificar el perfil y la actividad de esta figura, que no existía en el derecho español con anterioridad. En particular, se enumeran determinados sectores en que se considera necesaria, y por tanto obligatoria, la existencia de esta figura, se clarifica que el delegado de protección de datos no será responsable por las infracciones cometidas por el responsable o encargado, al excluírsele del régimen de responsabilidad del Proyecto, y se prevé la existencia de esquemas de certificación no obligatorios para la acreditación de las competencias para el desempeño de estas funciones.

> ***El Proyecto incluye una regla que impide la creación de las denominadas "listas negras" basadas en informaciones referidas a la ideología, afiliación sindical, religión, orientación sexual, creencias u origen étnico"***

Además, el Proyecto prevé que el afectado podrá someter sus reclamaciones al delegado de protección de datos con carácter previo a la presentación de las mismas ante la autoridad de protección de datos y la posibilidad de que éstas puedan remitir la reclamación al delegado con anterioridad a su tramitación en caso de no haberse acudido a él previamente.

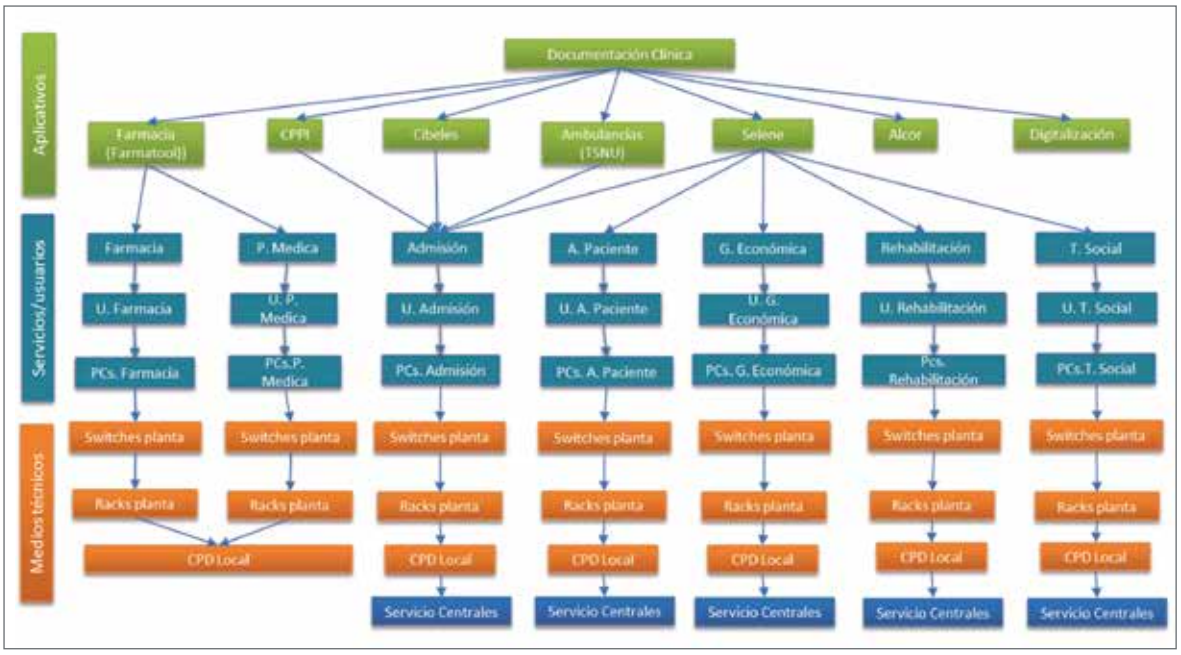
En relación con la autorregulación, el Proyecto se refiere a los códigos de conducta que tengan un carácter exclusivamente nacional, contemplando la posibilidad de que puedan incluso promoverse por "los organismos o entidades que asuman las funciones de supervisión y resolución extrajudicial de conflictos a los que se refiere el artículo 41 del Reglamento (UE) 2016/679". En este caso, los adheridos deberán someter al organismo de supervisión y resolución de conflictos las reclamaciones que les hubieran sido formuladas en caso de considerarlas improcedentes, pudiendo igualmente la autoridad de control, con carácter previo a la tramitación de una reclamación que no se hubiera elevado a aquellos, remitírsela para lograr una solución que garantice la celeridad y la indemnidad en la satisfacción del derecho del interesado.

Nuevos retos normativos para el ámbito sanitario
RGPD y PIC, casi nada

José Manuel Laperal González
Responsable de Seguridad de Sistemas de Información Sanitaria
Dirección General de Sistemas de Información del Servicio Madrileño de Salud.

YA ESTÁ AQUÍ EL RGPD, Y AUNQUE YA LLEVAMOS UN TIEMPO CON ÉL A VUELTAS, LA TAREA DE SU APLICACIÓN NO ES COSA FÁCIL EN UNA ORGANIZACIÓN SANITARIA, NADA FÁCIL. DAREMOS EN ESTE ARTÍCULO UNA BREVE PERSPECTIVA A VISTA DE PÁJARO DE LOS RETOS Y ESFUERZOS QUE EN SUS PUNTOS PRINCIPALES NOS ESTÁ SUPONIENDO, A LA PAR QUE COMPARTIMOS ALGUNAS REFLEXIONES.

Como primer elemento a destacar es este nuevo principio de responsabilidad activa o *Accountability*, que en palabras de la AEPD se define como *la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento*.
Se basa, en resumen, la obligación de prevención que corresponde a todas las empresas que tratan datos. Seremos por tanto los responsables de definir las medidas, de garantizar que sean efectivas y de poder demostrarlo cuando así se nos requiera. Si alguno ha pensado que ya nos podíamos liberar de las medidas del Reglamento 1720/2007 que desarrollaba la LOPD, casi mejor que sea que no y nos quedemos con ellas, para poder demostrar nuestra diligencia y porque además el ENS no se ha olvidado de nosotros y nos las seguirá pidiendo.
Entrando en otros aspectos, nos encontramos primeramente con la modificación del paradigma de "gestión por ficheros de datos personales", para evolucionarlo hacia un registro de actividades de tratamiento. Esto supone algo más que un cambio de nombre, pero parece que en principio puede ser abordado dentro de un proceso de racionalización en el que, revisando los ficheros existentes, podemos construir una nueva organización en la que unos ficheros se agrupan o eliminan para terminar construyendo una nueva clasificación por tratamientos. No es algo simple con más de 700 ficheros, pero puede abordarse con tiempo y una caña.
El aspecto de la necesidad de identificación de finalidades y base jurídica de los tratamientos, no debería presentar problemas en el caso de la Sanidad Pública, no obstante, se debe de ser cuidadoso en los casos de docencia y de investigación (especialmente en Big Data), como comentaremos más adelante.
Al entrar en la problemática del consentimiento, se complican las cosas por cuanto se insiste en que éste ha de ser informado, libre y otorgado mediante manifestación claramente expresa y afirmativa. Aplicar este requerimiento legal nos lleva más allá de la modificación del clausulado informativo que se realiza en Admisión, puesto que se prohíbe, además, el consentimiento tácito (basado en inacción), incluso para tratamientos iniciados con anterioridad. Para el tratamiento asistencial no supone problema alguno, ya que éste está amparado por una ley pero hay otras circunstancias especiales en las que sí tiene impacto. Por ejemplo, para el caso de la docencia, el acceso de estudiantes de pregrado debe de ser controlado (ya estábamos en ello por indicaciones del Ministerio de Sanidad) ya



que no pueden acceder a un repositorio donde estén todos los pacientes, sino sólo a los que hayan manifestado su conformidad o bien estén anonimizados. Esto implica la necesidad construir nuevos sistemas de información específicos para los estudiantes en los que se preserve los derechos de los pacientes, ya no por recomendación ministerial, sino por imperativo legal a nivel europeo. Es una lástima que las modificaciones regulatorias no vengan nunca acompañadas de dotaciones presupuestarias, ya que no tenemos sueños baratos, si me permiten el plagio y la ironía.

Además el consentimiento, al ser tan específico nos complica bastante más la gestión puesto que por ejemplo en los ámbitos de investigación (que ya lo era) aparece una problemática especial con el uso de las nuevas tecnologías porque cuando se realiza una explotación avanzada de los datos (entiéndase que hablamos de Big Data) pueden aparecer como resultado nuevas finalidades (de alto interés para investigador y paciente) distintas a las que el usuario dio el consentimiento en el momento de la recogida de los datos y no se puede inferir que equivalencia entre consentimientos. Se produce entonces una situación en la que sería necesario reevaluar la validez del mismo y quizá la necesidad de volver a solicitarlo. Como si fuera

> ***El aspecto de la necesidad de identificación de finalidades y base jurídica de los tratamientos, no debería presentar problemas en el caso de la Sanidad Pública, no obstante, se debe de ser cuidadoso en los casos de docencia y de investigación (especialmente en Big Data)"***

tan fácil hacer esto, ¿verdad? Creo que estos aspectos van a requerir todavía algo más de recorrido e incluso de apoyo de las autoridades de control. Si me permiten una crítica, considero una carencia importante que una legislación nueva ya adolezca desde el primer día una cobertura o apoyo que permitiera instrumentalizar las nuevas posibilidades que nos ofrece el análisis de datos, en las que el cruce con fuentes de información heterogéneas y no estructuradas nos permite obtener asociaciones no visibles hasta el momento, lo cual es la esencia misma de la investigación. Eso, si es que no hemos inutilizado los datos con procesos de anonimización agresivos como se sugiere en el Grupo de Trabajo 29 (GT-29) de la Comisión Europea. Sobre esto como cabe suponer, habrá que trabajar todavía bastante. Espero.



Otro reto, que reconozco me provocó una sonrisa muy al principio, es el de ofrecer mucha más información al ciudadano, pero eso sí de forma más resumida. Lo que parecía un acertijo sin embargo queda bastante bien resuelto con el planteamiento de hacerlo por capas, un poco en la línea de lo que ya venía haciendo el sector privado en el que las políticas de uso de nuestros datos se localizaban detrás de capas y capas de información. Lo bueno es que ya nos habíamos acostumbrado a ello. No obstante, de este reto se derivan una serie de actividades de modificación en formularios, páginas web o cartelería, que sin suponer especialidad complejidad técnica, sí supone un esfuerzo en tiempo y recursos.

Por su parte, los derechos ARCO ya venían siendo bien gestionados y afortunadamente la adaptación no nos hace partir de cero. No obstante, han de incorporarse los medios electrónicos a los mecanismos visibles, accesibles y sencillos, junto con los dos nuevos derechos (limitación del tratamiento y portabilidad) que afortunadamente se quedan en uno ya que el último no nos aplica en la Sanidad Pública.

En lo relativo a los encargados de tratamiento, se nos pide una mayor diligencia en la verificación del cumplimiento por su parte, que en principio no es demasiado compleja de articular mediante los oportunos clausulados en pliegos y contratos, sin que se nos deba olvidar que en las situaciones en las que estamos realizando una prueba de concepto, o estudio piloto, se debe de entender que sí existe tratamiento de datos aunque no exista una relación contractual aún formalizada (no hay un pliego licitado, estamos haciendo pruebas caray!), y por tanto se deben de firmar obligatoriamente los oportunos documentos en los que el proveedor es consciente y asume las responsabilidades pertinentes en materia de protección de datos. Es decir, es un encargado de tratamiento a todos los efectos, aunque no lo demos ese nombre.

Y en este punto aparece la necesidad de realización de análisis de riesgos en los tratamientos de datos. Mejor tomen asiento, si tienen la responsabilidad de llevarlo a cabo en un Servicio de Salud, donde las aplicaciones se cuentan por centenas y los activos se cuentan por miles. Un ejemplo ilustrativo se muestra en el cuadro siguiente, representativo de una abstracción a alto nivel realizada para un centro hospitalario de tipo pequeño y sencillo.

En esta clasificación nos encontramos que para cada tratamiento (documentación clínica en el ejemplo) se establece una relación de dependencias, utilizando la metodología que nos sugiere el CCN con la herramienta PILAR (ver imagen superior).

En el primer nivel encontramos una serie de aplicaciones y sistemas de información que dan servicio al tratamiento de los datos correspondientes. Para cada uno de ellos, se establecen los usuarios o Servicios del centro que los utilizan, con sus unidades organizativas y puestos de trabajo. A su vez, estos servicios están soportados por una serie de medios técnicos (rack, switches, servidores) que podrán estar en su CPD o en centros de datos externos.

Definir y cargar en PILAR todo el entramado que define a un centro sanitario es una tarea de muchísimo tiempo, para la que la mayoría de los centros precisarán ayuda desde los Servicios Centrales, sobre todo si se quiere mantener una homogeneidad y armonía en la gestión de la seguridad, estrategia de probada eficacia. En este punto cabe dudar si abordar esta cuestión con un nivel de detalle menos ambicioso, utilizando alguna otra herramienta fabricada al efecto que nos sirva para un acercamiento algo más sencillo. A riesgo de equivocarnos, en este momento en el Servicio Madrileño de Salud pensamos que no, que es mejor coger el toro por los cuernos esperando que los beneficios compensen los esfuerzos invertidos y quere-

mos apostar por PILAR. Si ustedes tienen una o varias herramientas de control de inventario para sus tareas de monitorización de red o soporte, vayan pensando en tener una más. Tengan cuidado cuando pidan los datos a los centros para cargarla no sea que se hagan daño.
Lo bueno de utilizar PILAR es que después será una ayuda para la tarea de la realización de las actividades de análisis de impacto que (ya lo han adivinado) es otro de los regalos del RGPD. Las funciones que ofrece PILAR para el control y visualización de interdependencias ante el fallo de un activo, son desde luego de gran utilidad, junto con la variedad de explotación gráfica que aporta la herramienta. Otros aspectos serían mejorables, pero eso será otra cuestión.
El siguiente reto a comentar es la nueva figura del "Delegado de Protección de Datos", el cual se integra perfectamente en la RPT de su organización (Relación de Puestos de Trabajo, es broma por supuesto), nos ayudará en la tarea. Ironías aparte, esta nueva figura tiene el reto de demostrar su efectividad, que por mi parte sí le supongo en principio.
Me hace pensar en positivo, por un lado, la simplificación que supone para muchas gestiones, como órgano centralizador que llevará la interlocución con ciudadanos y otras autoridades. Por otra parte, está la necesidad de interlocución al más alto nivel, de enorme utilidad para asegurar que las cuestiones de protección de datos se traten con la importancia necesaria. Nuestra visión es tratarlo como una figura operativa, articulado bajo una forma colegiada en un reducido Comité (subdirector y jefe de Área) el cual, apoyado por una unidad de expertos (externalizable) podrá dar respuesta a las necesidades de todo el Servicio de Salud de forma homogénea. Consideramos centralizada como mejor estrategia, porque entendemos que un desmembramiento en múltiples DPO en la organización sanitaria produciría sin duda una heterogeneidad nada deseable y una necesidad de coordinación posterior, mucho más complicada de llevar a la práctica con eficiencia. De esta manera, se sigue la línea de la provisión de servicios de seguridad y protección de datos, de forma horizontal a todo el Servicio de Salud, evitando los mayores costes que supondría que cada centro tuviera que dotarse de medios independientes, con altos costes al requerirse alta especialización.

> ***Se sigue la línea de la provisión de servicios de seguridad y protección de datos, de forma horizontal a todo el Servicio de Salud, evitando los mayores costes que supondría que cada centro tuviera que dotarse de medios independientes, con altos costes al requerirse alta especialización"***

Y, en este punto, llegamos a la notificación de incidentes de seguridad. Esto también es nuevo, no estábamos acostumbrados a comentar hacia afuera según qué cosas. Desde luego da recelo, pero en este nuevo ciber-mundo que nos hemos dado, potenciar esta actividad es algo fundamental. Porque cada caso de incidente de seguridad conocido en otra organización es una palanca en nuestra perpetua lucha por mayores recursos, esto lo sabemos, pero es que además, las amenazas y vulnerabilidades se multiplican de una forma impensable hace pocos años, haciendo por tanto indispensable la colaboración, incluso más allá de la publicación de incidentes. Porque saber qué aplicaciones le han fallado al vecino cuando ha aplicado tal o cual parche, sus tiempos, o las buenas estrategias que ha utilizado, es algo sencillamente crítico. Eso sí, en esta tarea de reporte, esperemos que no tengamos que realizarla en distintas puertas y con distinta información. Bueno parece ser que gracias a la trasposición de la Directiva NIS, tendremos coordinación. Por favor, que sea cierto.
Porque el hecho de compartir los errores aprendidos de unos y otros, que se conozcan las buenas prácticas, el liderazgo desde organismos estatales y la coordinación eficaz entre responsables TIC de las Administraciones, es ahora señores, una cuestión de Seguridad Nacional. Con mayúsculas.
Si esto se consigue, encajará muy bien con la aplicación de la Ley de Infraestructuras Críticas en el Sector Salud, que es lo siguiente que nos espera. ¡Ahí vamos!

RGPD, un Reglamento que afecta a todas las Organizaciones, Públicas y Privadas, en Europa ¿Estamos Preparados?

Javier Antón
Western Europe, Middle East e India (WEMEI) Fujitsu

ACTUALMENTE, LA CAPACIDAD DE LAS ORGANIZACIONES PARA FUNCIONAR Y CRECER SE SUSTENTA CON SU MODO DE GESTIONAR Y UTILIZAR LA INFORMACIÓN. SIN EMBARGO, PROTEGER PLENAMENTE ESTOS ACTIVOS DE DATOS Y LA PROPIEDAD INTELECTUAL RESULTA CADA VEZ MÁS DESAFIANTE.

Según los analistas de IDC, los ejecutivos sitúan la mejora de la seguridad de TI como una de las principales prioridades en 2018 en estas, que deben mantenerse al ritmo de un entorno de seguridad que no deja de cambiar, lo que plantea una variedad de exigencias estratégicas y operativas, entre las que se incluyen las seis siguientes:

- Un número creciente de requisitos normativos y de cumplimiento como es el RGPD.
- Amenazas internas y externas que no dejan de evolucionar.
- El riesgo de filtraciones de datos y la pérdida de propiedad intelectual.
- Permitir el uso de dispositivos móviles de trabajo y personales por parte de los empleados.
- Aprovechar los servicios en la nube para impulsar la productividad.
- Garantizar la continuidad del negocio y del servicio.

La gestión y la reducción de estos riesgos resulta cada vez más costosa y compleja para las Organizaciones, en un momento en el que los presupuestos de seguridad se someten a un escrutinio más estricto. Además, las Organizaciones se la juegan más que nunca, ya que se esfuerzan por hacer algo más que simplemente proteger su información crítica, salvaguardar su reputación y sus ingresos, especialmente en estos momentos, donde los datos y su protección se convierten en una máxima para gobiernos.

¿CUÁLES SON LAS PRINCIPALES NOVEDADES DEL NUEVO RGPD, Y CÓMO AFECTAN AL SECTOR SANITARIO?

En primer lugar, ya no se trata de una Ley española, sino de un Reglamento Europeo que homogeniza la protección de los datos de las personas en los estados miembros. En segundo, tiene como objetivo mejorar la protección de la privacidad del ciudadano, "adaptándose" a las nuevas ciencias como la Biomedicina, incluyendo definiciones como la genética o tecnologías como el Big Data, BYOD, Redes Sociales, Servicios Cloud y la capacidad para tratar de forma masiva y en tiempo real datos personales, que pueden definir perfiles de usuario tan avanzados y poderosos que el propio usuario ni siquiera imagina. Este Reglamento representa un giro radical en la distancia que solíamos observar entre la velocidad de avance de las leyes y la tecnología.

Desaparecen los tres tipos de datos personales y el Reglamento de Medidas de Seguridad que

orientaban la Ley a un requerimiento principalmente del departamento de IT, para alinearse con una estrategia más amplia de Gobierno y Cumplimiento, al igual que lo hizo el Código Penal mediante el establecimiento de la responsabilidad Penal Directiva. Las Organizaciones deberán abordarla desde un plano Organizativo, Técnico y Legal.

Particularmente aquellas que traten datos sensibles, como lo es el sector Sanitario, estarán obligadas a realizar una evaluación de impacto que permita identificar los riesgos concretos del tratamiento para adecuar las medidas de seguridad, valorando el volumen de negocio, los riesgos específicos derivados de la naturaleza del tratamiento, en lugar de aplicar el mismo rasero a todos los negocios como establece la LOPD.

Aparece la figura del Delegado de Protección de Datos, no con el fin de descargar únicamente la responsabilidad sobre éste, sino con el objeto de impulsar la protección de los datos y darle la debida importancia dentro de todas las áreas de las Organizaciones. Los organismos Públicos estarán obligados a designar uno. Se trata de copiar el modelo de éxito del Delegado de Prevención de Riesgos Laborales que durante más de dos décadas ha contribuido a reducir los accidentes laborales.

Se introducen nuevos derechos para el ciudadano que la tecnología ha propiciado, como el Derecho al Olvido, a la Portabilidad o la prohibición de elaboración de Perfiles vía tratamiento automatizado. Si pensamos en buscadores de internet, copias de seguridad, memoria Caché, ¿somos hoy día capaces de borrar todos los datos cuando un usuario desee ejercer este derecho? No será trivial para los organismos, pero existe cierto margen en el Reglamento, en función de las posibilidades de cada organización.

En cuanto al derecho de Portabilidad, éstos estarán obligados a ceder los datos al tercero que el usuario solicite. ¿Disponemos de la estructura de datos y automatismos adecuados para facilitar sólo aquellos datos que el usuario nos facilitó, sin revelar el resto de información derivada del negocio?

Frente al ocultismo actual de los incidentes de seguridad relacionados con datos personales por miedo de las organizaciones a la pérdida de reputación, será obligado comunicarlos a la Autoridad de Control estatal y por supuesto al interesado.

> ***Se introducen nuevos derechos para el ciudadano que la tecnología ha propiciado, como el Derecho al Olvido, a la Portabilidad o la prohibición de elaboración de Perfiles vía tratamiento automatizado"***

Se establece el principio de Seguridad por Defecto, estableciendo los requisitos de protección de la información desde la fase más temprana de diseño de un nuevo servicio que contemple el uso de datos personales. Debido a la sensibilidad de la información manejada por el sector Sanitario, podría representar un hándicap económico y tecnológico para nuevos sistemas, y un quebradero de cabeza para su integración con terceros existentes.

Al igual que existen certificaciones de Gestión de la Seguridad, aparecen los Códigos de Conducta y Certificaciones de Terceros como elementos de gobierno y declaración de buenas intenciones, actuando como atenuantes en caso de incidentes y sanciones.

El capítulo de las sanciones cobra especial relevancia por el incremento de la cuantía para las empresas privadas, pudiendo alcanzar hasta 20 M€ o bien un 4% del volumen total de negocio de la matriz, optando por la de mayor cuantía, frente a aquellos 0,6 M€ que en el caso de grandes multinacionales carecía de importancia.

Dada la magnitud de los cambios, Fujitsu ha estado asesorando a organizaciones a comprender el nuevo reglamento y guiarles hacia el cumplimiento durante el plazo de adaptación de dos años que finaliza el 25 de mayo de 2018, derogando la LOPD y entrando en vigor el Reglamento General de Protección de Datos. Con una extensa experiencia en seguridad de la información, En Fujitsu apostamos por la prestación de servicios integrales de seguridad a nuestros clientes, blindándolos antes las nuevas amenazas y ayudándolos en el cumplimiento de los requisitos del RDGP.

Una "hoja de ruta" para la Adecuación de las Organizaciones Sanitarias Públicas al #RGPD

Pedro Alberto González González
Agencia Vasca de Protección de Datos

EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (EN ADELANTE, RGPD) DE LA UNIÓN EUROPEA RESULTARÁ DE PLENA APLICACIÓN A PARTIR DEL 25 DE MAYO DE 2018, FECHA EN LA QUE TODOS LOS RESPONSABLES Y ENCARGADOS DE TRATAMIENTO HABRÁN DE HABERSE ADECUADO A SUS PREVISIONES.

Las Organizaciones Sanitarias (OOSS) actúan como responsables y encargados de tratamientos de datos personales en el desarrollo de muchas de sus actividades. En consecuencia, se verán afectadas por las consecuencias del nuevo RGPD, tanto en los principios y obligaciones generales como en aquellas previsiones específicas que el RGPD contempla y son aplicables al ámbito sanitario público.

El Reglamento General de Protección de Datos (en adelante, RGPD) de la Unión Europea resultará de plena aplicación a partir del 25 de mayo de 2018, fecha en la que todos los responsables y encargados de tratamiento habrán de haberse adecuado a sus previsiones. Las Organizaciones Sanitarias (OOSS) actúan como responsables y encargados de tratamientos de datos personales en el desarrollo de muchas de sus actividades. En consecuencia, se verán afectadas por las consecuencias del nuevo RGPD, tanto en los principios y obligaciones generales como en aquellas previsiones especificas que el RGPD contempla y son aplicables al ámbito sanitario público.

La mayor parte de estas OOSS ya están cumpliendo adecuadamente el marco legal establecido por la LOPD de 1999, por lo que no parten de cero, y muchas de las medidas hasta ahora adoptadas seguirán siendo válidas a partir del 25 de mayo. Sin embargo, resulta necesario que procedan a una revisión sistemática de la situación particular de sus tratamientos, a fin de adecuarlos al nuevo marco. En este artículo se sugiere una "hoja de ruta" para la adecuación, destacando aquellos aspectos más importantes y sugiriendo un orden para su abordaje.

A modo de resumen, el proceso de adecuación de las OOSS al RGPD que se sugiere puede sintetizarse en los siguientes ocho pasos:

1. Designar un Delegado de Protección de Datos (DPD)
2. Establecer el Registro Interno de Tratamientos
3. Revisar la legitimación de los tratamientos
4. Revisar la información que se ofrece a los interesados
5. Revisar los procedimientos de ejercicio de derechos
6. Revisar los contratos con Encargados de Tratamiento
7. Efectuar Análisis de Riesgos y revisar las medidas de seguridad
8. Determinar la necesidad de efectuar Evaluaciones de Impacto

A continuación se explican cada uno de los pasos y sus implicaciones:

1. DESIGNAR EL DPD

El *Delegado de Protección de Datos* (DPD) es una figura prevista en el RGPD, que no existía en nuestra LOPD, pero que ya había sido implantada por otros países miembros de la UE.
No todos los responsables de tratamientos están obligados a designar un DPD, pero sí que lo están las OOSS, por el hecho de tratar datos, como son los datos de salud, catalogados como "categorías especiales" en el RGPD. Asimismo, también las "autoridades u organismos públicos" habrán de designar un *Delegado de Protección de Datos*. Abundando en ello, el Proyecto de LOPD-2018, recientemente remitido al Parlamento, establece la obligación de designar un DPD para los centros sanitarios obligados al mantenimiento de historias clínicas con arreglo a la Ley 41/2002.
Las funciones principales del DPD, según se establece en el RGPD, son las siguientes:

a) informar y asesorar al responsable o al encargado del tratamiento;
b) supervisar el cumplimiento del RGPD por el responsable o encargado, incluyendo:
   - la asignación de responsabilidades,
   - la concienciación y formación del personal
   - las auditorías correspondientes;
c) asesorar acerca de las Evaluaciones de Impacto (EIPD) y supervisar su aplicación;
d) cooperar y actuar como punto de contacto con la autoridad de control;

También establece el RGPD cuáles habrán de ser los criterios para su designación, como son el tener cualidades profesionales y conocimientos en derecho y práctica de la protección de datos, su posición en la organización.

- *La designación del DPD debe comunicarse a las autoridades de protección de datos.*
  - Asimismo, se debe facilitar que los interesados puedan contactar con el DPD.

- *Se sugiere que la primera medida a adoptar de cara a la adecuación de las AAPP al RGPD sea la de regular la figura del Delegado de Protección de Datos.* Para ello se debe:
  - identificar la unidad en que se habrá de integrar el DPD dentro de cada órgano u 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.
  - su configuración para asegurar su criterio independiente y en ausencia de conflicto de intereses.

2. ESTABLECER EL REGISTRO INTERNO DE TRATAMIENTOS

La actual exigencia de creación de los ficheros y tratamientos mediante una *disposición* general, *publicada* en un Diario Oficial, y su *notificación* a la Autoridad de Protección de Datos para su inscripción en el Registro de Ficheros, *desaparece con el RGPD.*
En cambio, el RGPD establece la necesidad de la *llevanza de un registro interno de actividades de tratamiento*, como instrumento primordial para demostrar el cumplimiento y facilitar la supervisión de los tratamientos.
  - Debe llevarse tanto por Responsables como por Encargados de tratamiento.
  - El RGPD establece el contenido mínimo de ese registro,

- *Deberá mantenerse actualizado y a disposición de las autoridades de protección de datos.*
  - como medida de transparencia, las AAPP deberían de hacer público su inventario de actividades de tratamiento, accesible por medios electrónicos.

3. REVISAR LA LEGITIMACIÓN DE LOS TRATAMIENTOS

Las OOSS deberán identificar con precisión las *finalidades y la base jurídica de los tratamientos* que llevan a cabo. Esta obligación deriva de:
  - la necesidad de cumplir con el principio de legalidad establecido en el RGPD,
  - la información a proporcionar a los interesados (transparencia)
  - su constancia en el registro de actividades de tratamiento.

La identificación de finalidades y base jurídica tiene exigencias adicionales en los casos en que

se traten datos de los considerados como objeto de *especial protección,* que incluyen, entre otros, los *datos sobre salud, los genéticos* o *biométricos y los relativos a la vida u orientación sexual.*

- El tratamiento de estos datos está, con carácter general, prohibido, y sólo podrá llevarse a cabo si es aplicable alguna de las excepciones previstas en el art. 9.2 del RGPD.

- En el caso de que el tratamiento esté basado en el consentimiento, habrá de tenerse en cuenta que se han reforzado los requisitos para obtenerlo (*"informado, libre, específico y otorgado mediante una clara acción afirmativa"*), lo cual *invalida los consentimientos "tácitos",* es decir, basados en una inacción u omisión de acción por parte del interesado.

Cuando las OOSS efectúen *transferencias de datos a terceros países,* el RGPD amplía los mecanismos ya existentes (decisiones de adecuación, garantías adecuadas y normas corporativas vinculantes) con algunas previsiones específicas sin necesidad de autorización previa, como son la existencia de instrumentos *jurídicamente vinculantes y exigibles entre autoridades y organismos públicos.* Sin embargo, los meros *acuerdos administrativos* requerirán *autorización* de las Autoridades de Control.

4. REVISAR LA INFORMACIÓN QUE SE OFRECE A LOS INTERESADOS

La información que se ofrece a los interesados cuando se recogen sus datos (por ejemplo, en formularios web o papel, o de un tercero) *debe revisarse,* pues se ha reforzado la transparencia hacia el interesado, siendo la información a facilitar más amplia que la requerida hasta ahora.

- Para mayor información, se recomienda la consulta de la *"Guía para el cumplimiento del deber de informar"* elaborada por las tres Autoridades de Protección de Datos (AEPD, APDCAT y AVPD), disponible para su descarga en la URL: *http://www.avpd.euskadi.eus/contenidos/informacion/20161118/es_def/adjuntos/modeloclausulainformativa-es.pdf*

5. REVISAR LOS PROCEDIMIENTOS DE EJERCICIO DE DERECHOS

El RGPD mantiene y amplía los tradicionales derechos de "acceso, rectificación, cancelación y oposición", debiendo los responsables y encargados de tratamientos tener en cuenta lo siguiente:

- establecer mecanismos *visibles, accesibles y sencillos*, incluidos los medios electrónicos, para el ejercicio de derechos.
- establecer procedimientos que permitan responder a los interesados en los *plazos previstos* por el RGPD.

- *Se sugiere incorporar la supervisión del DPD cuando se vaya a resolver negativamente.*

6. REVISAR LOS CONTRATOS CON ENCARGADOS DE TRATAMIENTO

El RGPD también ha reforzado los requisitos respecto de la contratación de servicios con los encargados de tratamiento, como son:

- El RGPD establece que la relación entre responsables y encargados deberá formalizarse siempre mediante un contrato o un acto jurídico que vincule al encargado y, además:
- Establece una obligación de diligencia debida en la elección de los encargados de tratamiento por parte de los responsables, contratando únicamente encargados que estén en condiciones de cumplir con el RGPD.

En el caso de las OOSS será frecuente que el encargo de tratamiento se establezca mediante actos jurídicos, por ejemplo en la norma de creación de órganos encargados de la prestación de servicios informáticos.

- *Será necesario revisar y adecuar los contratos de encargo actualmente suscritos para contemplar el contenido mínimo que exige el RGPD.*
- Para mayor información, se recomienda la consulta de la guía *"Directrices para la elaboración de contratos entre responsables y encargados del tratamiento"* elaborada por las tres Autoridades de Protección de Datos (AEPD, APDCAT y AVPD), disponible para su descarga en la URL: *http://www.avpd.euskadi.eus/contenidos/informacion/*

20161118/es_def/adjuntos/directricescontratos-es.pdf

7. EFECTUAR ANÁLISIS DE RIESGOS Y REVISAR LAS MEDIDAS DE SEGURIDAD

Hasta ahora, las medidas de seguridad exigibles venían claramente enumeradas en el Reglamento de Desarrollo de la LOPD (RD-1720-2007), estableciéndose tres niveles de exigencia (Básico, Medio y Alto).

Sin embargo, el RGPD no establece cuáles han de ser las medidas de seguridad, sino que indica que: *"Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo".*

Lo anterior significa que es necesario efectuar un *análisis de riesgo* para *los* derechos y libertades de los ciudadanos de los tratamientos de datos que se lleven a cabo, revisando las *medidas de seguridad* que actualmente se estén aplicando y, en su caso, completándolas a la luz de sus resultados.

- *En el ámbito de las OOSS, las medidas de seguridad exigibles serían las derivadas de la aplicación del Esquema Nacional de Seguridad, aprobado por Real Decreto 3/2010, de 8 de enero.*
- *La metodología para Análisis de Riesgos es "MAGERIT", publicada por el CCN-CERT*
- Adicionalmente, el RGPD introduce la necesidad de gestionar las ***violaciones de seguridad*** de los datos, ***notificando a la Autoridad de Control*** cuando tal violación constituya un riesgo para los derechos y libertades de los afectados.

8. DETERMINAR LA NECESIDAD DE EFECTUAR EVALUACIONES DE IMPACTO

Finalmente, el RGPD también prevé la necesidad de efectuar una *Evaluación de Impacto sobre la Protección de Datos (EIPD)* con anterioridad a su puesta en marcha de nuevos tratamientos, siempre que puedan suponer un *alto riesgo* para los derechos y libertades de los interesados.

- *El RGPD determina algunos de los casos en que se presumirá que existe ese alto riesgo y prevé que las autoridades nacionales de protección de datos publiquen listas de otros tratamientos de alto riesgo.*

Las evaluaciones de Impacto sobre la privacidad consisten en:

a) una *descripción sistemática* de:
   - las operaciones de tratamiento previstas
   - los fines del tratamiento,
   - cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;

b) una evaluación de *la necesidad y la proporcionalidad* de las operaciones de tratamiento con respecto a su finalidad;

c) una *evaluación de los riesgos* para los derechos y libertades de los interesados

d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales.

La metodología necesaria para llevar a cabo tales evaluaciones de impacto requiere una cierta especialización. La AEPD está trabajando actualmente en una guía que ayude a la realización de dichas Evaluaciones de Impacto. Mientras tanto, existe una *"Guía para una Evaluación de Impacto en la Protección de Datos Personales"*, editada en 2014, disponible en la URL:

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf

El RGPD también prevé que se puedan efectuar *EIPDs para proyectos de medidas legislativas,* o su desarrollo, que se refieran a tratamientos de datos. En tales casos, los tratamientos particulares derivados de tales medidas legislativas, que se legitimen en base a la consecución de fines de *interés público*, o vinculados al *ejercicio de poderes* públicos, no necesitarán llevar a cabo una nueva evaluación de impacto.

Ciberseguridad en salud: Un desafío inevitable





Carlos Royo
Director de Desarrollo de Negocio de Salud de GMV Secure e-Solutions
Maole Cerezo
Asesora de Comunicación y Marketing de GMV Secure e-Solutions

LA RELACIÓN ENTRE MÉDICO Y PACIENTE ESTÁ CAMBIANDO Y EVOLUCIONANDO GRACIAS A UN MAYOR ACCESO A LA INFORMACIÓN Y A LA CAPACIDAD DE ELECCIÓN QUE ÉSTE ÚLTIMO DISFRUTA, TANTO POR EL INCREMENTO DE PERSONAS QUE DISPONE DE UNA PÓLIZA DE SALUD PRIVADA, COMO PORQUE ALGUNOS SERVICIOS DE SALUD AUTONÓMICOS HAN BRINDADO A SUS CIUDADANOS ESTE DERECHO.

No hace mucho, factores como la calidad de la asistencia o de las instalaciones podían determinar las decisiones de los "clientes" de salud, el proceso de transformación digital que está llevando a cabo la sanidad y la puesta en valor de una medicina humanista, añade a éstos otros tales como la capacidad de innovación, la relación multicanal, la asistencia colaborativa e integral... etc. En este contexto, la confianza que sustenta la relación médico-paciente podrá hacerse extensiva a la garantía de protección y seguridad de los datos de salud.

La información que custodian hospitales, clínicas, farmacias, laboratorios o mutuas es confidencial y considerada por Ley como crítica. Si bien los recursos propios de la Revolución 4.0 como la movilidad, el cloud, los Big Data, la analítica avanzada, etc. brindan nuevos beneficios a la asistencia personalizada y de precisión, así como a la investigación en materia de prevención, diagnóstico y nuevos tratamientos.

La necesidad de impulsar medidas para proteger la información crítica de Estados y organizaciones se constata en iniciativas como la puesta en marcha del Centro Global para el Ciberespacio, que según se informó en el Foro de Davos estará operativo a partir de marzo, o la Organización Europea de Ciberseguridad (ECSO), asociación público-privada que resulta del paquete de medidas "Cyber Security Package" lanzado por la Comisión para equipar mejor a Europa contra ciberataques, cuyo grupo de salud está pilotado por Julio Vivero, Jefe de Sección de Ciberseguridad de GMV.

UN PASO POR DELANTE DE LOS CIBERLADRONES

La compraventa de datos sanitarios en el mercado negro, según apuntan distintas informaciones especializadas, se disputa el primer lugar del volumen de negocio junto con la información de origen bancario y los datos personales o de identidad en redes sociales. Sin ir muy lejos, el pasado mes de enero, fueron robados los datos sanitarios de más de la mitad de la población noruega por "un profesional avanzado". El Equipo de Respuesta ante Emergencias Informáticas de la sanidad noruega (HelseCERT) identificó tráfico sospechoso procedente de la red de Health South-East, y tras una investigación, se llegó a identificar una importante brecha de datos. Y el pasado mes de junio, el laboratorio estadounidense Merck fue víctima del ciberataque mundial del virus "Petrwrap", una versión modificada del ransomware "Petya" utilizado por piratas informáticos el año pasado.

Aunque la seguridad y la privacidad de los datos electrónicos no constituyen un problema exclusivo del sector de la salud, los proveedores de ciberseguridad confirman que en este sector es necesario hacer un mayor esfuerzo en el cifrado, protección y custodia de los datos, tanto por parte de centros sanitarios como de empresas.

Un informe titulado "El Estado de la Ciberseguridad" realizado por el "think tank" Instituto Ponemon de Michigan asegura que, en promedio, todas las organizaciones que participan en la investigación han sufrido casi un ataque al mes en el último año. Casi la mitad (48%) de los encuestados reconoce que su organización experimentó un incidente que supuso la pérdida o exposición de información de sus pacientes durante ese año, y el 26% de los encuestados no supo qué responder. (1)

Este mismo informe cifra en un 125% el aumento de los ciberataques contra la sanidad estadounidense en los últimos cinco años, afectando a uno de cada tres de sus ciudadanos, con un coste estimado anual de 6.000 millones de dólares para el sistema de salud americano. En EEUU, la compañía UCLA Health, reconoció ser víctima de un ciberataque. Los hackers habrían podido acceder a los datos personales y médicos de 4,5 millones de pacientes porque no estaban debidamente cifrados. De igual forma, los datos de 80 millones de personas se vieron comprometidos por un ataque a la aseguradora de salud Anthem, al conseguir los ciberdelincuentes las credenciales de cinco profesionales con accesos de alto nivel al sistema.

La Ley Orgánica de Protección de Datos (LOPD) establece que los datos de carácter personal relacionados con nuestra salud deben estar especialmente protegidos con medidas de seguridad de nivel alto. El Reglamento de Protección de Datos 1720/2007 que desarrolla la ley, fija que los sistemas de tratamiento y almacenamiento de datos han de someterse a una auditoría interna o externa al menos cada dos años, obliga al cifrado de los datos, detalla que se han de registrar los intentos de acceso y determina protocolos de autenticación de los usuarios. A su vez, el 25 de mayo es la fecha marcada por el Reglamento General de Protección de Datos (RGPD) para que las organizaciones que gestionen datos de los ciudadanos europeos "tengan a punto" sus sistemas de seguridad de la información.

No obstante, la implementación de las medidas de seguridad que se recomiendan en la LOPD, si bien resulta necesaria, no es suficiente como para considerar que los sistemas de TI de hospitales, laboratorios, aseguradoras no puedan ser vulnerables. Aunque se inviertan recursos para asegurarlos, siempre habrá ciberdelincuentes con recursos y tecnología capaces de desafiar su seguridad. Ante esta realidad, es necesario invertir en innovación para tomar la delantera e ir un paso por delante de los rateros.

NUESTRAS CAPACIDADES

GMV, líder en ciberseguridad, pionera en el despliegue y optimización de soluciones forenses de red avanzadas y en servicios de ciberinteligencia para la toma de decisiones, está desarrollando nuevos mecanismos de detección capaces de diferenciar el comportamiento humano frente al del malware en entornos complejos aplicando algoritmos de aprendizaje automático en entornos como el de Salud.

Los servicios prestados por GMV abarcan todo el ciclo de vida de la Ciberseguridad. Analizamos y diagnosticamos entornos específicos desde el punto de vista de cumplimiento o de riesgos, elaboramos planes que desarrollan normas como la Protección de Infraestructuras Críticas, el GDPR o los Esquemas Nacionales. Incorporamos soluciones tecnológicas específicas, gestionamos la operación de las infraestructuras tecnológicas de Ciberseguridad y dotamos de la visibilidad necesaria para la toma de decisiones y el buen gobierno.

Asimismo, fruto de su apuesta por la innovación, ha desarrollado un servicio de vigilancia digital, atalaya, capaz de monitorizar diversas fuentes en tiempo real (24x7), con el objetivo de identificar información que permita detectar publicaciones accidentales o premeditadas susceptibles de poner en riesgo la organización o perjudicar su imagen.

La ciberseguridad afecta a cualquier ámbito y es clave para generar confianza y retener a los clientes, más aún cuando éste deposita en su proveedor sus datos más confidenciales, los de salud.

*https://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map

1. Para llegar a estas conclusiones encuestaron a 535 profesionales de TI y de seguridad de TI en organizaciones de salud de distinta índole: proveedores privados y públicos de servicios de salud y agencias gubernamentales. De ellos, el 64% trabajan en las organizaciones encuestadas y el 36% en empresas externas.

VII REUNIÓN

Plataforma Tecnológica para la Información en Salud

LA SEIS CELEBRÓ LA VII REUNIÓN DE LA PLATAFORMA TECNOLÓGICA LOS PASADOS 22 Y 23 DE NOVIEMBRE EN SAN SEBASTIÁN, CON EL FIN DE SINTONIZAR A TODOS LOS ACTORES QUE TIENEN QUE VER CON LAS TECNOLOGÍAS APLICADAS PARA BENEFICIO DE LA SALUD.

ACTO INAUGURAL



Los principales objetivos de la Reunión fueron: el desarrollo de una cultura de innovación en salud, identificar profesionales que puedan liderar ideas y proyectos, preparar el sistema para nuevos modelos organizativos que surgirán de la irrupción de la medicina personalizada y el cambio de estrategia en el manejo de las enfermedades crónicas, redefinir el papel del ciudadano en el sector sanitario y, por último, activar fuentes de financiación para la innovación en salud.

La inauguración oficial estuvo presidida por María Aguirre Rueda, directora de Investigación e Innovación Sanitaria del Departamento de Salud del Gobierno Vasco. Estuvieron presentes en la mesa Pedro Cortegoso Fernández, secretario general del Instituto de Salud del Carlos III y Luciano Sáez, presidente de la SEIS.

Luciano Sáez, agradeció a todos su presencia en el acto apertura y se mostró satisfecho de poder celebrar de nuevo una actividad de la SEIS en el País Vasco, en Donostia, gracias al apoyo del Departamento de Salud del Gobierno Vasco y Osakidetza.

Sáez agradeció también la presencia de Pedro Cortegoso, secretario general del ISCIII, organismo de ámbito estatal, promotor de la investigación y la innovación en el sector sanitario y con el que la SEIS dispone de un convenio marco de colabOración realizado en 2013 con el objetivo de desarrollar acciones en formación en TIC para la salud, elaboración de estudios e informes técnicos y acciones difusoras y programas para el impulso de la innovación.

La SEIS, en su plan de acción 2012-2015 incorporó la creación de la "plataforma tecnológica para la innovación en salud" con la misión de facilitar un escenario donde la industria, las or-

ganizaciones sanitarias, los grupos de investigación, los parques tecnológicos y los profesionales, impulsen el desarrollo y la implantación de proyectos innovadores.
La SEIS es consciente de las dificultades actuales para financiar proyectos, pero también considera que deben emprenderse acciones que refuercen la inversión TIC mediante algunas medidas que puedan incrementar el gasto TIC en un 1% adicional del gasto sanitario. "Estamos convencidos de que el retorno real que se va a producir con esos nuevos 550 M de € será muy superior en otras partidas presupuestarias.
Sáez apuntó que la SEIS "se pone a disposición de todos los agentes, para la puesta en marcha de iniciativas que impulsen la innovación en el sector salud. Agradecemos a la industria innovadora que ha apoyado la organización de esta reunión y a todos ustedes por participar y acudir a nuestra convocatoria". Además, hizo extensivo su agradecimiento a todos los que han hecho posible la VI Reunión.

A continuación tomó la palabra **Pedro Ortegoso**, que tras agradecer a la SEIS el hecho de intervenir en el acto inaugural, relató brevemente las iniciativas del Instituto de Salud Carlos III en el ámbito de las TIC. Para ello, citó los tres roles con los que se desarrolla la actividad del Instituto: financiación, centro de investigación y centro formativo. Respecto a la financiación, comentó que desde el año 2014 se pusieron en marcha dos iniciativas dirigidas especialmente al ámbito de la innovación.

Por último intervino **María Aguirre**, que afirmó que "en el País Vasco compartimos los grandes retos y las grandes necesidades que se plantean tanto en reuniones como esta como en las redes sociales. Llevamos ya unos años embarcados en estos temas de salud con la creación de las organizaciones sanitarias integradas con las que pretendemos proporcionar algunas mejoras en la continuidad asistencial. En estos momentos, estamos embarcados en una segunda fase de la integración de la innovación realmente en el code, en el núcleo de una actividad sanitaria, que tiene que ir encontrando su espacio y sus apoyos.

PRIMERA SESIÓN



Moderada por **Pedro Cortegoso**, estuvo dedicada a la presentación de iniciativas, estrategias y oportunidades para el desarrollo de proyectos innovadores en el sistema nacional de salud.

En primer lugar intervino **Cecilia Hernández Rodríguez**, del CDTI. Comenzó diciendo que el CDTI está de cumpleaños ya que celebra su cuarenta aniversario, durante los cuales, su objetivo ha sido aumentar la productividad y competitividad de las empresas españolas a través de I+D+i. CDTI gestiona cualquier sector o tecnología.
Se refirió tal caso de SEDECAL, que en julio obtuvo el Premio Nacional de Innovación 2017; a Neos Surgery, Aelix Therapeutics, etc. Y finalizó

su intervención recordando que CDTI tiene programas internacionales de I+D en 86 países.

Laura Díaz Gómez, subdirectora adjunta de Sanidad, de la Dirección de Servicios Públicos Digitales de red.es, trató a continuación sobre la transformación digital como oportunidad para avanzar hacia un modelo de coordinación asistencial de la cronicidad y la dependencia.
Comenzó mostrando la evolución y planes de referencia de red.es, desde el año 2005 hasta el 2020, en lo que se llama la Agenda Digital Europea. Mencionó el llamado Plan Avanza que tiene como punto de partida una moción del Senado aprobada por unanimidad el 19 de octubre de 2004, así como representantes del sector TIC y por deferentes colectivos sociales y empresariales. También citó la Agenda Digital para España.
Posteriormente dedicó un tiempo a hablar del Programa de Sanidad en Línea, poniendo el foco en el programa de Salud y Bienestar Social, cuyo objetivo los resume en la Historia Clínica Electrónica Regional (HCE), la Historia Clínica Digital del SNS (HCOSNS), la Receta Electrónica (RE), la Receta Electrónica del SNS (RESNS) y la Vita por Internet.

La tercera ponencia corrió a cargo de Lorea Mendoaza Arteche, responsable del programa INNOSASUN, de la Fundación Vasca de Innovación e Investigación Sanitarias-BIOEF, que versó sobre "Interacción y Colaboración del Sector Empresarial con el sistema sanitario público vasco en materia de I+D+i: Programa INNOSASUN".
Citó los fines funcionales de la Fundación Vasca de Innovación e investigación Sanitaria (BIOEF) que es el instrumento creado por el Departamento de Salud para promover la innovación y la investigación en el sistema sanitario público vasco. Mendoaza refirió al programa INNOSASUN, que facilita la interacción entre el sistema sanitario y el sector empresarial y agentes relacionados, dando respuesta a sus necesidades en materia de innovación
Terminó comentando los casos de éxito en los proyectos de I+D+i.

La última intervención fue de Gorka Sánchez, responsable de Innovación en la Subdirección General de Proyectos e Innovación del Servicio Murciano de Salud (SMS). En cuanto a innovación en el SMS consideró 4 puntos. El primero es liderar la innovación desde la demanda y, dentro de estas, priorizando las acciones. El segundo, buscar la mejor financiación que nos permita hacer pilotos, evaluar los resultados y extender los que hayan tenido éxito. El tercero, conseguir una red de innovación identificando profesionales y experiencias innovadoras. Y por último, consolidar al SMS como Living Lab, potenciando a la región murciana como vanguardia.
Presentó dos proyectos europeos: PROEMPOWER y inDemand.

SEGUNDA SESIÓN

Estuvo dedicada a presentar retos y oportunidades para la innovación en salud; Innovación y sostenibilidad; Ideas en acción y Proyectos inno-vadores que hayan contribuido a la sostenibilidad del sistema o hayan supuesto una mejora significativa: IMPRESIÓN 3D. El moderador fue Rafael Sánchez Herrero, director general de Innovación y Resultados en Salud, de la Gerencia Regional de Salud del Gobierno de Castilla y León.

Dio la palabra, en primer lugar a Jon Zabaleta Jiménez, médico especialista en Cirugía Torácica de Osakidetza. Zabaleta expuso que "el proyecto de impresión 3D para mejorar el estudio preoperatorio de pacientes con patología torácica comenzó en noviembre de 2016. Entonces nos planteamos hacer este tipo de estudio para pacientes con tumores endobronquiales, solicitamos un botton-up y decidimos contactar con Tecnun-Universidad de Navarra para organizar un curso de impresión 3D para médicos (realizado en febrero de 2017). Después del curso y con la concesión del botton-up, se creó un grupo de trabajo multidisciplinar entre cirujanos (todo el equipo de Cirugía Torácica de la OSI Donostialdea), radiólogos (Mikel Mendoza y Ainhoa Galardi) e ingenieros biomédicos (Luis Matey y Andrea Larrañaga).



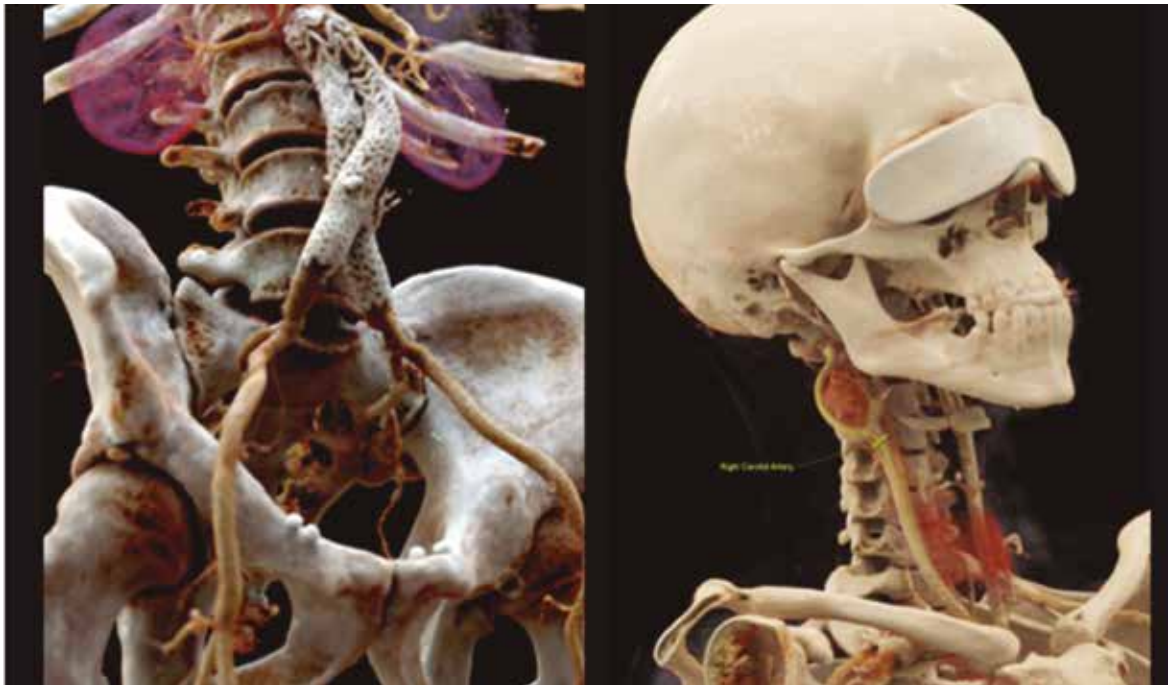
Para la creación de los acuerdos con Tecnun y Tknika y mantener una relación fluida con todos los organismos ha sido fundamental la labor de Sandra Ahedo y Arantza Abad de Biodonostia. Además, para aumentar el número de casos y aprender más sobre la creación de biomodelos en cirugía Torácica, se ha creado un Grupo de trabajo 3D en la Sociedad Española de Cirugía Torácica, liderado por los cirujanos de este Hospital, donde participan 24 Hospitales del estado, 1 de Alemania y 1 de Uruguay. Cuando un cirujano de cualquiera de estos hospitales tiene un caso en el que podría beneficiarse de un modelo, se pone en contacto con nosotros, nos manda el TAC y nosotros le hacemos la reconstrucción, imprimimos el modelo y se lo mandamos por mensajero de forma completamente gratuita.

En segundo lugar intervino Sergio García Casado, especialista de Producto de Informática Clínica de Philips. Habló sobre "Imagen Tangible, Estado del Arte y Aplicación Clínica".
Su ponencia se resume en tres apartados: la tecnología para la bioimpresión de tejido humano. La innovación en el campo de la medicina sigue avanzando día a día, gracias a investigaciones y estudios que combinan los últimos descubrimientos con las más novedosas tecnologías para aportar soluciones y abrir nuevos campos de experimentación. Uno de los campos con más potencial y que más posibilidades tiene para revolucionar el sector es la impresión 3D. Dentro del campo de la investigación en impresión 3D surge el concepto de bioimpresión y que trata, como el propio nombre indica, de la impresión de tejido humano. "Mirando hacia un futuro cercano, la bioimpresión 3D abre infinitas posibilidades como la impresión de órganos para trasplantes o tratamiento de lesiones complejas. Estuvo dedicada a presentar retos y oportunidades para la innovación en salud; Innovación y sostenibilidad; Ideas en acción y Proyectos innovadores que hayan contribuido a la sostenibilidad del sistema o hayan supuesto una mejora significativa: IMPRESIÓN 3D. El moderador fue Rafael Sánchez Herrero, director general de Innovación y Resultados en Salud, de la Gerencia Regional de Salud del Gobierno de Castilla y León.

Unai García de la Torre, responsable de Productos de Servicios Digitales de Siemens Healthineers, habló sobre el "Presente y futuro de la radiología, del cinematic rendering a la impresión 3D". Comentó que desde hace varias décadas Siemens Healthineers trabaja en sus aplicaciones con inteligencia artificial en la búsqueda de la mejora y la ayuda en el diagnóstico por la imagen. "Tradicionalmente en el flujo de trabajo de radiología el personal radiológico realiza tareas de postproceso para la obtención de imágenes 3D que ayuden en el diagnóstico y seguimiento de las patologías. En la búsqueda de nuevas aplicaciones que ayuden a este proceso se lanza la aplicación syngo. via que permite preprocesar la imagen de forma automática para que la imagen esté directamente disponible y preparada para hacer postproceso, además de usar algoritmos que permiten la detección automática de posibles patologías,

medidas, comparación con estudios previos, en una plataforma multimodalidad que pueda ser accesible desde cualquier pc o dispositivo móvil. En su mejora y evolución surge la plataforma syngo.via Frontier que proporciona un kit de herramientas de uso amigable y sencillo para la generación de prototipos en diferentes áreas de interés. Se trata de una plataforma de investigación que forma parte de una red global de colegas investigadores en diferentes campos de investigación, de forma que se puede contribuir a la discusión científica internacional a través del intercambio global con otros investigadores. Está respaldada por un grupo de expertos y con seguimiento diario por el grupo de desarrollo de Siemens.

El último en intervenir fue Julián Pérez Aragón, account manager Healthcare Digital ICA GE Healthcare que trató sobre "Del hospital fimless a la impression 3D". La impresión 3D es ya una realidad y empieza a contar con experiencias relevantes que sin duda van a ser la puerta de entrada a la adopción más extendida de esta tecnología, y se postula como un ámbito de actuación disruptivo que aporta mejoras tangibles e inmediatas para el paciente.
Además del dispositivo de impresión, el fungible y las consideraciones técnicas propias que permitirán la obtención de un modelo 3D de calidad, es importante considerar que uno de los puntos clave para la adopción de la impresión en la realidad de la actividad clínica va a ser facilidad de uso y su capacidad de adaptación a las necesidades concretas de las cuales el beneficiario final va a ser el paciente. En este sentido, las empresas tecnológicas con soluciones en el ámbito del diagnóstico por la imagen tienen mucho que aportar. El enfoque que podemos considerar ya un estándar en sus propuestas se centra en integrar en las soluciones IT de diagnóstico las herramientas que permitirán exportar los modelos creados en estas soluciones clínicas a los formatos adecuados para su impresión.
De esta forma se facilita la adopción de la tecnología 3D, al eliminar la necesidad de aplicaciones complementarias, normalmente alejadas del ámbito clínico y centradas en el aspecto estrictamente informático del proceso. Estas soluciones además de proximidad clínica a la necesidad real que trata de cubrir la impresión de un modelo 3D, aportan las garantías y certificaciones de calidad necesarias para su comercialización global. También permiten crear flujos de trabajo alrededor de una tecnología ya existente e instaurada en el ámbito del diagnóstico por la imagen, venciendo de inicio barreras como la forma ción necesaria para el uso de nuevas soluciones, o la inversión necesaria para su adopción.



PRESENTACIONES LIBRES

Moderada por **José Luis Monteagudo**, presidente del Comité Científico, la sesión de presentaciones libres contó con las siguientes comunicaciones presentadas fueron:

- Identificación de pacientes fuera de CC AA": E. Alonso Suero, D. Alonso, J.E. Viego de la Roz.
- "Distribución de informes e imagen en el SESPA": E. Alonso Suero, J.I. Rodríguez, D. Alonso, J.E. Viego de la Roz.
- "Portal electrónico para profesionales: acceso a la información farmacoterapéutica completa del Paciente": F. Pérez Hernández, L.M. López Arce, M. Martínez Cabarga, C. de las Cuevas Terán, A. Tejerina Puente, R. Martínez Santiago.
- "Presentación de ApInvest, una aplicación para la gestión de Plataformas de Investigación": J. A. Fernández Sandá, C. M. Tilve Alvárez, L. Carrajo García, G. Vázquez González.
- "Desarrollo de nuevos inhibidores farmacológico basados en estudios bioinformáticos Docking": J.M. Bañales
- "Hacia la estructuración del texto libre clínico: identificación de términos médicos en español": N. Pérez Miguel, M. Cuadros Oller, A. del Pozo Echezarreta.

TERCERA SESIÓN. DEBATE



La sesión fue moderada por **José Manuel Ladrón** de Guevara, director gerente de la Organización Sanitaria Integrada Donostialdea.

José Manuel Ladrón de Guevara indicó que para la organización que dirige, que abarca más de 30 centros de Atención Primaria y el Hospital Universitario Donostia, la innovación es un elemento diferenciador, una herramienta clave para el desarrollo de los profesionales y de la organización. El modelo de gestión de Osakidetza es el Modelo de Gestión Avanzado(de la Fundación Euskalit, http://www.euskalit.org/); se trata de un modelo derivado del EFQM, más simplificado y en el que introduce explícitamente la innovación como un elemento clave y diferenciador.

Julio Arrizabalaga Aguirreazaldegui, director del Instituto de Investigación Sanitaria Biodonostia (http://www.biodonostia.org), presentó la organización del Instituto y su relación con el Hospital. Se trata de un centro que tiene unas peculiaridades únicas que la hacen especial.

Se trata de un centro con personalidad jurídica propia, pegado físicamente al Hospital Universitario Donostia, bajo el paraguas del Sistema Sanitario Vasco que, además, está asociado con varios centros tecnológicos (Cidetec o Vicomtech).
Comenta que participa en la red ITEMAS y facilita la realización de proyectos Bottom-Up. En este punto, explicó el origen de los proyectos Bottom Up y que en 2013 se lanza la primera convocatoria de proyectos Bottom-Up.

Mikel Ogueta Lana, de la Sudirección de Calidad y Sistemas de Información de Osakidetza, presentó las TIC como elemento innovador. En Osakidetza las TICs quieren dar solución a aspectos como la Continuidad Asistencial, la Integración Sanitaria entre entidades sanitarias, los nuevos roles profesionales, el Empoderamiento de Pacientes y los Resultados en Salud. Todo ello on-line...
Uno de los aspectos más innovadores de los últimos años en Osakidetza ha sido la Historia Clínica Electrónica, centrada en el paciente. A ella se le han ido añadiendo más herramientas como la receta electrónica, la codificación estandarizada o la Carpeta Salud (en sus versiones web y APP).
No obstante, hizo hincapié en las barreras que impiden que se manifieste toda esa fuerza descomunal que ofrecen las TIC.

Jesús M. Bañales, investigador de Biodonostia, comentó el escenario existente en el Instituto que le permite interactuar con otros agentes de innovación, otros centros tecnológicos que se dedican a la Investigación, clínicos del Hospital, etc, en el que encuentra un equipo multidisciplinar con distintos perfiles profesionales con los que realizar proyectos.

En su experiencia en el Instituto, considera que la creación de Institutos de Investigación permiten a los investigadores trabajar en un entorno en los que las tareas son compartimentadas. La tarea del investigador sea investigar; el resto de tareas colaterales pueden ser abordados por las OTRIs y Unidades de Investigación en los se descarga la realización de otras tareas (burocráticas, financieras, legales...).

Ramón Lerchundi, subdirector de Sistemas de Información de OSI-Donostialdea, explicó aspectos que se dan en el día a día de los Sistemas de Información y la Innovación. Centró sus ideas en estos tres aspectos: La necesidad de creación de un ecosistema en el que puedan trabajar empresas innovadoras en Tecnologías de Información junto con los Servicios de Salud, codo con codo, las dificultades en congeniar la Innovación y la Producción en los sistemas de Información y la necesidad de que los profesionales TIC actuales participen en acciones de Formación Continua en Innovación y en proyectos de Innovación de ámbito sanitario.
El abordar estos tres aspectos permitiría una mayor velocidad en la percepción de los resultados de los proyectos de Innovación por parte de la Sociedad.

En último lugar intervino Pedro Alberto González Gonzáles, responsable del Registro de Ficheros y Auditoría de Ficheros. Agencia Vasca de Protección de Datos. Su intervención se resume en los siguientes puntos:

- La ponencia pretende aportar, desde un punto de vista externo a los profesionales más implicados en la Innovación en Salud, una reflexión sobre las implicaciones del marco regulatorio de la protección de datos sobre algunas de las facetas que pueden intervenir en dicha innovación, como son los sistemas de gestión sanitaria y, especialmente, las actividades de investigación relacionadas con la salud. Todo ello contando, como punto de partida, con la existencia de una percepción, en nuestra opinión equivocada, de que la protección de datos puede suponer más una barrera que una solución para la innovación en muchas organizaciones.

- Tal errónea percepción de que la protección de datos puede suponer una barrera a la innovación procede, probablemente, del hecho de que sea necesario el consentimiento como principio legitimador para el tratamiento de datos personales. Sin embargo, la legislación general sobre Protección de Datos (LOPD) incluye diversos principios, obligaciones y derechos aplicables a todo tipo de tratamientos, estableciendo, ciertamente,

el consentimiento como principio legitimador, pero contemplando también la existencia de otras posibles habilitaciones, siempre que estén previstas en la Ley, y permitiendo el tratamiento posterior de los datos con fines históricos, estadísticos o científicos. Sin embargo, a nuestro entender, las garantías que ponen límites al tratamiento de los datos personales con fines de investigación en el ámbito de la salud provienen, en buena medida, de la legislación sectorial específica.

- En el caso de los sistemas de gestión sanitaria, el consentimiento no juega un papel central, puesto que la LOPD legitima el tratamiento de los datos de salud cuando resulte necesario para la prevención, diagnóstico o tratamiento médicos, la prestación de asistencia o la gestión de servicios sanitarios, siempre que tales tratamientos de datos se realicen por profesionales sanitarios sujetos al secreto profesional. La protección de datos se halla muy integrada en la arquitectura de sistemas como puede ser Osabide, dentro del ámbito vasco de la salud, siempre de acuerdo con el conocimiento parcial que desde la Agencia Vasca de Protección de Datos podemos tener de ella. Dicha arquitectura contempla, por ejemplo, una correcta gestión de identidades, incluyendo la definición de roles de los profesionales que intervienen asistencialmente, las relaciones de éstos con los pacientes y los permisos y autorizaciones de accesos que en cada caso correspondan. Incluye, además, una trazabilidad de los accesos que se producen. Lógicamente, en casos de duda, debe primar la posibilidad de facilitar la asistencia, con lo que estos sistemas han de contemplar ciertos "grados de libertad", que habrán de ser oportunamente auditados cuando los accesos se producen según la excepción y no la norma.
- Respecto del ámbito de la investigación relacionada con la salud, las circunstancias son claramente diferentes pues, además de la legislación de carácter general, como es la actualmente vigente LOPD, interviene también la legislación sectorial, que en este caso serían la Ley de Autonomía del Paciente y la Ley de Investigación Biomédica. Como ya se ha comentado, la LOPD considera "compatible" el tratamiento posterior de los datos personales con fines científicos, si bien la delimitación de lo que habría de entenderse por "fines científicos" quedaba un tanto difusa. Con posterioridad, el Reglamento de Desarrollo LOPD precisó que se habría de estar a lo indicado en la legislación específica y, en lo tocante a la finalidad científica, a la Ley 13/1986, de Fomento y Coordinación General de la Investigación Científica y Técnica. Por lo tanto, el carácter investigador del tratamiento de datos personales no lo establece, sin más, el promotor de la investigación, sino su inclusión en el marco del Plan Nacional de Investigación Científica y Desarrollo Tecnológico. Fuera de estos casos, habrá que estar a la legislación específica que, como ya se ha indicado, son las leyes de Autonomía del Paciente y de Investigación Biomédica.
- En el caso de los tratamientos necesarios para la prestación asistencial, la Ley de Autonomía del Paciente permite el acceso a la historia clínica con fines de investigación o de docencia, pero estableciendo límites: se deberán preservar los datos de identificación personal del paciente, separados de los de carácter clínico-asistencial, de manera que, como regla general, quede asegurado el anonimato, salvo que el propio paciente haya dado su consentimiento para no separarlos.

Por otro lado, la Ley de Investigación Biomédica establece el consentimiento estricto como base para la participación en investigaciones. Prohíbe, expresamente, la utilización de datos personales para una investigación diferente a aquella para la cual se otorgó el consentimiento inicial. Incluso exige un consentimiento específico para los casos en que resultase necesario publicar los resultados con identificación de los participantes. Únicamente exime de la necesidad de consentimiento en los casos de imposibilidad o necesidad de esfuerzos desproporcionados para obtenerlo, en cuyo caso se requiere el dictamen favorable del Comité de Ética en Investigación correspondiente.

En definitiva, las garantías que pueden suponer límites al tratamiento de los datos personales con fines de investigación en el ámbito de la

CUARTA SESIÓN



salud provienen, en buena medida, de su legislación sectorial específica.
"Innovar innovando. Ideas en acción. Presentación de proyectos" fue el título de la cuarta sesión moderada por **Alejandro Pazos Sierra,** doctor en Medicina y Cirugía; catedrático de Ciencias de la Computación e Inteligencia Artificial Grupo RNASA-IMEDIR de la Universidad de A Coruña.

El primer ponente fue **Josh Davidson**, CEO de Insulin Algorithms, T-Systems, que dio importantes cifras sobre el coste de la diabetes en España. Dado que la diabetes va creciendo, es necesario dedicar más atención a su tratamiento y sus cuidados, ya que, a pesar de estar adheridos a sus medicamentos, el 56.1% de los pacientes tenían un control glucémico deficiente. Esto sugiere que los médicos, farmacéuticos y otros proveedores pueden necesitar monitorear los regímenes de tratamiento con más cuidado, fomentar comportamientos saludables e intensificar el tratamiento farmacológico según sea necesario.

El siguiente ponente fue **Aitor Moreno Fernández de Leceta**, experto en Sistemas Inteligentes de Control y Gestión y habló sobre "Reflexiones sobre proyectos, Big Data, lecciones aprendidas". Lleva desde el 2009 colaborando en distintos proyectos de innovación en salud. Proyecta una diapositiva en la que se podría apreciar si la letra fuera de mayor tamaño, la base de datos con el histórico de todos los proyectos en los que han intervenido. Terminó mencionando el proyecto EHR4CR, un ecosistema europeo.

David Pérez del Rey, doctor en Ingeniería Informática y titular de Universidad del Área de Ciencias de la Computación e Inteligencia Artificial (Grupo GIB) de la Universidad Politécnica de Madrid, habló de "Métodos de integración utilizados en una plataforma europea para el uso secundario de HCE en Investigación". Dijo que llevaban más de 15 años con investigando y empezaban a explotar los resultados en una plataforma que está lista. En el 2002 tuvieron el primer proyecto en esta área; en 2011 intervinieron en varios proyectos europeos, sobre todo para contar con los datos de las HCE. Mencionó el proyecto Eureca y terminó mencionando el proyecto EHR4CR, un ecosistema europeo.

"Versión Pro de E-Back: Big Data en wereables" fue el tema que abordó **Juan Manuel Rabiñal Dopico,** doctor en Ingeniería Informática y Titular de Universidad del Área de Ciencias de la Computación e Inteligencia Artificial. Grupo RNASA-IMEDIR. Universidad de A Coruña. Presentó la versión pro de un dispositivo presentado en Valladolid hace ya unos años, dedicado al

control postural para evitar dolores de espalda y el dolor lumbar que ocasiona más bajas.
Para finalizar la cuarta sesión intervino **Jesús Ruiz,** del Comité Técnico de ALASTRIA, que habló del consorcio que nace para desarrollar el ecosistema BlockChain en España, una nueva iniciativa que necesita gozar de buena salud. Comenzó su intervención diciendo que la iniciativa de la que iba a hablar es única en el mundo. "El problema que se intenta solucionar está causado por lo que ya se sabe y es que todo está conectado. Tenemos edificios inteligentes, fábricas inteligentes, automóviles inteligentes y hogares que también son inteligentes. Y hay muchos problemas. Todo está interconectado". Comentó que, aunque todos hemos oído hablar de la transformación digital de las empresas, el problema que estamos encontrando no es la transformación digital de mi empresa si no como se digitaliza todo el ecosistema: "Hay una serie de actores. Por ejemplo, cada empresa, puede actuar una de las muchas técnicas que existen de digitalización, lo cual permite una digitalización más segura y más eficiente, donde además pueden venir empresas que utilicen smart contracts o contratos inteligentes y hacer aplicaciones en BlosckChain que no se podrían haber hecho nunca de ninguna otra manera". Definió ALASTRIA desde una visión genera.,

CLAUSURA



El acto de clausura estuvo presidido por **Julio Arrizabalaga** e intervinieron **José Luis Monteagudo** y **Guillermo Vázquez**. Vázquez, además de mostrar su agradecimiento a todos los participantes, fue el encargado de realizar un somero repaso de todo lo abordado durante la VI Reunión, sesión por sesión, realizando un interesante análisis de lo dicho por todos los ponentes.

José Luis Monteagudo comentó que el objetivo principal es desarrollar una cultura de innovación, lo que es un ecosistema de innovación abierto. "Cada vez interesa más presentar proyectos innovadores, como se han presentado en esta VI Reunión. La sanidad como tal es muy compleja. Uno de los componentes que se han planteado en la estrategia era conseguir el liderazgo de los profesionales ante los detractores de la innovación. Se refirió a las subvenciones tradicionales del CDTI o de res.es y agradeció a los autores todas las comunicaciones presentadas. Tras afirmar que todas tuvieron gran calidad, reveló la dificultad de premiar la titulada "Desarrollo de nuevos inhibidores farmacológicos basados en estudios bioinformáticos Docking", firmada por **J.M. Bañales.**

Para finalizar la clausura, el presidente de la mesa, **Julio Arrizabalaga**, agradeció a la SEIS la celebración de esta VI Reunión en Donostia. Felicitó a todos por el nivel alcanzado en las mesas y, tras animarles a seguir trabajando para alcanzar los objetivos propuestos, dio por clausurada la VI Reunión de la Plataforma Tecnológica para la Innovación en Salud.

XXI CONGRESO NACIONAL DE INFORMÁTICA DE LA SALUD

Salud Digital: Un Proyecto Colaborativo

CELEBRAMOS EL XXI CONGRESO NACIONAL DE INFORMÁTICA DE LA SALUD BAJO EL LEMA "SALUD DIGITAL: UN PROYECTO COLABORATIVO" Y, LA COINCIDENCIA CON EL SIGLO NOS HACE PENSAR EN DAR UN NUEVO IMPULSO A ESTE CONGRESO.

OBJETIVOS

En este sentido, queremos que éste sea el año de la apertura hacia la colaboración. Esta colaboración iría desde nuestros profesionales de la medicina, la enfermería, la farmacia y los gestores hasta los ciudadanos como objetivo central de todas nuestras actuaciones. Trabajamos en un entorno donde los ciudadanos nos exigen cada vez más en todos los aspectos: información, inmediatez, prevención, atención personalizada, asistencia virtual, seguimiento, etc. y como todos nosotros sabemos, esto exige una mayor colaboración entre los diferentes niveles asistenciales y de servicio.

Quizás este es el momento para que hagamos que INFORSALUD sea un referente aún más integrador de esta colaboración que vivimos en el día a día, y un foro donde poder abordar junto con profesionales de fuera del ámbito de la informática el reto de la Salud Digital, planteándonos cómo ayudar a mejorar la asistencia y cómo hacerlo garantizando la sostenibilidad del sistema, para lo que contaremos con gestores que nos aporten sus puntos de vista y necesidades.

Este será el Congreso que podría marcar el inicio de un nuevo ciclo, en el que todos aportemos y aprendamos, desde las empresas de tecnología, las de suministros sanitarios y farmacológicos y de nuevo, los colectivos que conformamos las organizaciones asistenciales para buscar la aportación en conjunto que entendemos que es el valor real y el objetivo que todos buscamos. Aportar en conjunto. Asimismo, abordaremos la necesidad de desarrollar y promocionar profesionales del negocio como líderes digitales. La tecnología ya está a nuestro servicio para poner en marcha lo que nos demanda la sociedad. Las empresas de tecnología son ya líderes en los respectivos ámbitos de servicios que nos ofertan, ellos son nuestros socios tecnológicos, quienes siempre nos ayudan a alcanzar resultados. Pero, además debemos aprender a escuchar a nuestros líderes internos para trabajar nuevos proyectos y conseguir que estos sean una realidad. Los proyectos que promueven los líderes digitales son siempre un éxito porque nos ayudan en las diferentes fases: diseño, construcción, desarrollo, implantación… y esto es muy complicado de hacer sin ellos.

Todo esto nos lleva a valorar el papel clave de los profesionales sanitarios en la atención asistencial, por lo que necesitamos que sus conocimientos y destrezas digitales estén acorde con las necesidades de nuestros ciudadanos, teniendo en cuenta , además, que estas capacidades, como ya hemos dicho, deben estar orientadas a convertirles en los líderes de esta transformación.

Estos líderes gestionarán herramientas tan solicitadas por nuestros profesionales como el IoT, herramientas que conseguirán que seamos más sostenibles, sobre todo en el mantenimiento de nuestras infraestructuras y las

automatizaciones a implantar. Mientras tanto, seguimos nuestro trabajo del día a día, intentando minimizar riesgos y con el objetivo de ser siempre un servicio 24x7, trabajando en el cumplimiento de los presupuestos de nuestra área, mientras abordamos tantos y tantos objetivos, que además cada vez más se ven amenazados por los Ciberataques y sus consecuencias. Esta
lucha será continua y debemos saber minimizar sus consecuencias en todos los sentidos. Nuestros ciudadanos son cada vez más digitales y esto implica que debemos garantizar su accesibilidad y su motivación para conseguir de ellos una actuación en mejora de su propia salud y al final de todo el sistema sanitario, ayudando a lograr una Medicina Personalizada. Pero lo dicho, todo esto solo es posible con un Proyecto Colaborativo.

Este INFORSALUD 2018 ofrece una oportunidad única para que los profesionales de la salud, tecnólogos, investigadores, gestores, industria, administraciones públicas y organizaciones sanitarias y sociales (públicas y privadas) puedan exponer y compartir sus demandas y necesidades, así como debatir sobre la forma de cómo avanzar en el empoderamiento de los ciudadanos en el cuidado de la salud. Los comités organizador y científico aceptamos la responsabilidad que esto supone y trabajamos para ofrecer desde la SEIS un congreso donde compartir, formar, desarrollar y acompañar a todos los profesionales en el buen uso de las TIC.

A este fin, el programa del Congreso incluye mesas redondas y sesiones de debate con relevantes ponentes implicados en la digitalización de la salud. Además se considera imprescindible recoger las experiencias de los investigadores y profesionales que se desean facilitar con sesiones reservadas a su participación en forma de comunicaciones orales o en forma de pósteres y la presentación de proyectos innovadores, estas últimas en sesiones abiertas al público.

INFORSALUD 2018 es una cita imprescindible para todos los interesados en el sector de las TIC en Salud y en su contribución a la transformación sanitaria para la mejora de la calidad y a la eficiencia de los sistemas sanitarios.

AVANCE DE PROGRAMA

	HORARIO	SALA 1	SALA 2	SALA 3
Martes 13 de marzo	16.00 - 16.30	Recogida de Documentación		
	16.30 - 17.00	Inauguración Oficial		
	17.00 - 17.30	Visita Oficial Área Exposiciones		
	17.30 - 19.00	Sesión de Apertura de Autoridades Sanitarias		
	19.00 - 20.00	Sesión Debate "Salud Digital: un proyecto colaborativo"		
Miércoles 14 de marzo	09.30 - 11.00	Mesa Debate 1 "Los profesionales sanitarios ante la Salud Digital"	Sesión de Comunicaciones 1	Sesión Tecnológicas 1
	11.00 - 11.30	Café y visita área de exposiciones		
	11.30 - 13.00	Mesa Debate 2 "La Salud Digital necesita líderes"	Sesión de Comunicaciones 2	Sesión Tecnológicas 2
	13.00 - 14.30	Mesa Debate 3 "¿La imagen médica impulsora de la transformación digital?"	Sesión de Comunicaciones 3	Sesión Tecnológicas 3
	14.30 - 16.00	Descanso		
	16.00 - 17.30	Mesa Debate 4 "IOT: Nuevas herramientas para la asistencia"	Sesión de Comunicaciones 4	Sesión Tecnológicas 4
	17.30 - 18.00	Visita Área de Exposiciones		
	18.00 - 19.30	Mesa Debate 5 "Minimizando el impacto asistencial de la Ciberseguridad"	Sesión de Comunicaciones 5	Sesión Tecnológicas 5
Jueves 15 de marzo	09.30 - 11.00	Mesa Debate 6 "Big Data vs. Small Data: ¿medicina personalizada?"	Sesión de Comunicaciones 6	Sesión de Comunicaciones 7
	11.00 - 11.30	Café y visita Área de Exposiciones		
	11.30 - 13.00	Mesa Debate 7 "¿Cómo atender las necesidades del paciente digital?"	Mesa Redonda "Interoperabilidad e Innovaciones en receta electrónica"	Sesión Tecnológicas 6
	13.00 - 14.30	Cierre de Autoridades Sanitarias		
	14.30 - 16.00	Descanso		
	16.00 - 18.00	Sesión de Proyectos 1	Sesión de Proyectos 2	
	18.00	Clausura y Entrega de Premios		

El Ministerio de Sanidad, Servicios Sociales e Igualdad continúa impulsando la transformación digital en el ámbito de la salud

El Ministerio de Sanidad, Servicios Sociales e Igualdad ha firmado un convenio con la Sociedad Española de Informática de la Salud (SEIS), mediante el que esta Sociedad pone su conocimiento y experiencia en este campo al servicio del Sistema Nacional de Salud.

FIRMA CONVENIO MSSSI Y SEIS



El Secretario General de Sanidad y Consumo, José Javier Castrodeza Sanz, y el Presidente de la Sociedad Española de Informática de la Salud, D. Luciano Sáez Ayerra, han firmado un convenio marco de colaboración con el que se muestra una vez más la importancia de trabajar por la innovación y la eficiencia del sector sanitario.

La constante evolución y la generalización del uso de las Tecnologías de la Información y de las herramientas digitales ofrecen nuevas oportunidades en la mejora de la salud de las personas y de la sociedad en general. Por eso, contar con el apoyo de expertos como la SEIS en esta materia, supone un gran aval para seguir avanzando tanto desde el punto de vista asistencial como desde la optimización de los recursos existentes y disponibles en el sistema sanitario.



LÍNEAS DE TRABAJO DEL CONVENIO

Este convenio, que se ha firmado por dos años y podrá ser prorrogado por periodos de un año mediante acuerdo expreso de las partes, supone un marco de colaboración tanto científico como técnico, mediante el que SEIS pone a disposición del Ministerio, entre otros, su asesoramiento, sus programas de actividades, sus grupos de trabajo y la elaboración de informes y propuestas...

Las líneas de trabajo establecidas pasan por potenciar la capacidad de recursos humanos del Sistema Nacional de Salud, promover la participación activa del paciente en sus cuidados, realizar estudios preliminares y propuestas que conduzcan a la explotación de los datos disponibles, incorporar nuevos modelos de salud digital a los procesos asistenciales y promover el desarrollo y la innovación mediante proyectos TIC.

FORO DE
TELEMEDICINA

Coordina: **Óscar Moreno**

El informe «El estado de la salud en la UE» recomienda la transformación digital de la salud y la asistencia

"La transformación digital de la salud y la asistencia tiene un gran potencial para fortalecer la eficacia de los sistemas de salud", ésta es la principal conclusión del informe semestral sobre el Estado de la Salud en la UE. Como apoyo a esta conclusión cita que las plantillas socio-sanitarias en estos ámbitos debe estar preparada para la innovación técnica y los pacientes deben ser el centro de mejores datos sanitarios en la práctica y en las políticas.

La Comisión (DG SANTE) ha publicado 28 Perfiles Nacionales de Salud de los Estados Miembros de la UE junto con un informe complementario para 2017. Esta iniciativa de dos años denominada «El Estado de la Salud en la UE» proporciona a los responsables políticos, grupos de interés y profesionales de la salud datos fácticos comparativos y conocimientos sobre la sanidad y sistemas de salud en los países de la UE.

Los informes, elaborados en cooperación con la Organización para la Cooperación y el Desarrollo Económicos (OCDE) y el Observatorio Europeo de Sistemas y Políticas de Salud, sugieren que solo repensando nuestros sistemas de salud podremos garantizar que sigan siendo aptos para el propósito y proporcionen asistencia centrada en el paciente.

RESULTADOS CLAVE

Cinco conclusiones transversales se han presentado en el Informe Complementario:

- Los pacientes deben estar en el centro de la próxima generación de datos de salud mejores para la práctica y las políticas. La transformación digital de la sanidad y la asistencia tiene un gran potencial para fortalecer la eficacia de los sistemas de salud. Los datos de salud centrados en el paciente contribuyen a los resultados en los pacientes, a la vez que reducen el gasto ineficiente en la asistencia médica.
- La promoción de la salud y la prevención de enfermedades allanan el camino para un sistema de sanitario más eficaz y eficiente. Además de las inversiones desequilibradas en la prevención, las desigualdades sociales deben abordarse, como se ilustra por las diferencias en el cribado del cáncer o por la actividad física entre las personas con mayores y menores ingresos y educación.
- Una atención primaria sólida guía eficazmente a los pacientes a través del sistema de salud y ayuda a evitar gastos innecesarios. El 27% visita los departamentos de urgencia debido a una atención primaria inadecuada. Solo 14 países de la UE requieren una derivación de atención primaria a atención especializada; Otros 9 países tienen incentivos económicos para las derivaciones.
- La asistencia integrada garantiza que un paciente reciba atención conjunta. Evita la situación que vemos actualmente en casi todos los países de la UE, donde la asistencia está fragmentada y los pacientes tienen que buscar su ruta a través de un laberinto de instalaciones asistenciales socio sanitarias.
- La planificación y previsión proactiva de las plantillas socio-sanitarias hace que los sistemas de salud sean resistentes a las evoluciones futuras. La UE tiene 18 millones de profesionales de la salud y se crearán 1,8 millones más para 2025. Las autoridades sanitarias deben preparar a su personal para los próximos cambios: envejecimiento de la población y multimorbilidad, necesidad de políticas de reclutamiento sólidas, nuevas habilidades e innovación técnica.

Más información:

- Comisión Europea - https://ec.europa.eu/digital-single-market/en/
- Informe "El estado de salud en la UE" - https://ec.europa.eu/health/state/summary_en
- Informe Complementario - https://ec.europa.eu/health/sites/health/files/state/docs/2017_companion_en.pdf

FORO DE
INTEROPERABILIDAD

Coordina: **Adolfo Muñoz Carrero**

UNE –EN ISO13940 – PROCESO

Continuamos con la exposición de los conceptos definidos por la Norma. En esta entrega se van a tratar los conceptos relacionados con los procesos. Como siempre, en la lista que sigue, las descripciones aparecen con el término del concepto en negrita con la definición normalizada más destacada. Otros conceptos que también estén definidos en la Norma aparecen en dicha descripción en itálica, tanto si están incluidos en la misma sección como en otra diferente.

CONCEPTOS RELATIVOS AL PROCESO

- **Proceso sanitario:** conjunto de *actividades sanitarias* interrelacionadas o que interactúan y que convierten entradas en salidas. Un proceso sanitario no tiene por qué estar limitado a una unidad organizativa
- **Proceso clínico:** proceso sanitario que abarca todas las *actividades de proveedor sanitario* y otras *actividades sanitarias* prescritas que abordan *temas de salud* identificados o especificados. La entrada y salida primarias de un proceso clínico son *estados de salud*. El proceso clínico es clave para la continuidad asistencial e incluye *actividades de autocuidado* prescritas o recomendadas por *profesionales sanitarios*. Desde el punto de vista de los *procesos clínicos* existe una distinción relevante entre la entrada primaria (el *estado de salud* inicial del *sujeto de la asistencia*) y las entradas secundarias (los recursos aportados para la realización del proceso).
- **Gestión de la calidad sanitaria:** actividades coordinadas para dirigir y controlar a una *organización sanitaria* en lo referente a la calidad. Estas actividades se centran en los *procesos clínicos* e incluyen el establecimiento de una política de calidad, la fijación de objetivos, la realización de auditorías y la evaluación.
- **Administración sanitaria:** actividades administrativas relacionadas con *procesos sanitarios*. Ejemplos de estos procesos son la elaboración de presupuestos y la asignación de recursos, la documentación no clínica, etc.
- **Evento adverso:** evento no intencionado que tiene una influencia negativa sobre el *proceso sanitario*. Pueden ocurrir durante actividades sanitarias apropiadas y comúnmente están causados por iatrogénesis y pueden causar daño. Ejemplos de evento adverso son las infecciones adquiridas durante la estancia en el hospital, las alergias causadas por un medicamento (cuando la alergia no era conocida previamente) y accidentes conectados con una *actividad sanitaria*
- G**estión de evento adverso:** conjunto de *actividades sanitarias* realizadas en respuesta a un evento adverso. Este conjunto de actividades incluye tanto las llevadas a cabo para revertir o minimizar las consecuencias del evento como para prevenir el tipo de *evento adverso* en el futuro.
- **Servicio sanitario:** servicio que es el resultado de un *proceso sanitario*. Una prueba diagnóstica y su informe de resultados serían un ejemplo de *servicio sanitario*.
- **Directorio de servicio sanitario:** directorio de tipos de *servicios sanitarios* ofertados por uno o más *proveedores sanitarios*.

FORO DE
GOBERNANZA

Coordina: **Martín Begoña**

GOBIERNO TI, RECURSOS HUMANOS Y TRANSFORMACIÓN DIGITAL (2)

Las competencias digitales

En el artículo anterior se introdujo el modelo DIGCOMP, un marco para desarrollar las competencias digitales en Europa.

El marco DIGCOMP, desarrollado por el JRC-IPTS de la Comisión Europea (Joint Research Centre, Institute for Prospective Technological Studies), contribuye al debate sobre la comprensión y el desarrollo de la competencia digital para todos los ciudadanos. Proporciona descripciones detalladas de las capacidades necesarias para ser competente en entornos digitales y las describe en términos de conocimientos, habilidades y actitudes. La competencia digital es una de las ocho competencias clave para el aprendizaje permanente y es esencial para la participación en una sociedad cada vez más digitalizada, por lo que es necesario entender y definir qué es y en qué consiste la competencia digital.

El marco DIGCOMP consiste en 21 competencias divididas en cinco áreas. Para cada competencia, hay tres niveles de dominio y ejemplos de conocimientos, habilidades y actitudes. Las cinco áreas de competencia digital, que se identifican, son las siguientes:

1. Información: identificar, localizar, recuperar, almacenar, organizar y analizar la información digital, juzgando su relevancia y finalidad.
2. Comunicación: comunicarse en entornos digitales, compartir recursos a través de herramientas en línea, vincularse y colaborar con otros a través de herramientas digitales, interactuar y participar en comunidades y redes.
3. Creación de contenidos: crear y editar nuevos contenidos (procesamiento de textos, imágenes y video); integrar y re-elaborar conocimientos y contenidos previos; producir expresiones creativas, salidas de medios y programación; conocer y aplicar los derechos de propiedad.
4. Seguridad: protección personal, protección de datos, identidad digital, medidas de seguridad, uso seguro y sostenible.
5. Solución de problemas: Es útil para identificar necesidades y recursos digitales, para tomar decisiones informadas sobre la mayoría de las herramientas, de acuerdo con el propósito o necesidad, para resolver problemas a través de los medios digitales, para resolver problemas técnicos y para actualizar la propia competencia y la de otros.

Las cinco áreas son de igual importancia, sin embargo, la información, la comunicación y la creación de contenidos se componen de actividades y usos específicos, mientras que la seguridad y la solución de problemas son más transversales, es decir, se aplican a cualquier tipo de actividad que se realice a través de dispositivos digitales.

Aunque cada área tiene su propia especificidad, hay varios puntos superpuestos y referencias cruzadas a otras áreas. Por ejemplo, la creación de contenidos implica en algún momento las competencias relacionadas con la comunicación, ya que se va a compartir el conocimiento y el contenido que se ha producido.

Las competencias dentro de cada área varían de 3 a 6. La primera competencia en cada área es la que incluye los aspectos más técnicos: en estas competencias específicas, los conocimientos, las habilidades y las actitudes tienen procesos operativos como componente dominante.

El marco DIGCOMP se está utilizando como apoyo al diseño de políticas públicas. Desde el Gobierno TI de la organización, se debe colaborar con el Departamento de Recursos Humanos en la definición de perfiles de competencias digitales profesionales, utilizando DIGCOMP como marco de referencia. Estos perfiles pueden servir para evaluar la situación de los profesionales, en relación con las competencias digitales, y definir los itinerarios formativos que se precisen para posibilitar la madurez digital de la organización.

SECTOR
ENFERMERÍA

Coordina: **Azucena Santillán**

Tecnología punta humana

Big data, transformación digital, salud digital... todos estos conceptos parecen estar cambiando radicalmente el escenario de los cuidados en salud. La tecnología está presente en prácticamente todos los procesos sanitarios y desde hace algún tiempo se debate sobre la posible deshumanización de los cuidados a costa de la tecnificación y digitalización.



Es un hecho que el ecosistema sanitario esta cambiando y también es un hecho que ha habido grades resistencias al cambio, pero pasados los primeros años de "crisis" podemos decir que los profesionales y los pacientes atravesamos ahora un periodo de adaptación que tal vez sea demasiado corto. Grandes innovaciones, muchos cambios... el poder hipnótico de las pantallas es palpable, y cuando nos paramos a respirar nos preguntamos ¿desplazará la tecnología a los humanos? ¿desplazara a los profesionales sanitarios? Pensando en avances como el Da Vinci y tantos otros podemos pensar que tal vez si y haciendo este análisis de la situación podemos pensar que la tecnología va a deshumanizar los cuidados. ¿Y qué opinan los pacientes de todo esto? Pues parece que desean lo mejor de ambos mundos. Es decir, que se les trate con el mayor humanismo posible, con toda la información y el respeto, a la vez que se les ofrezca las ventajas de la mejor tecnología disponible.

En este momento no debemos olvidar el término acuñado por Carmen Segovia "tecnología punta humana" y es aquella que todos llevamos dentro, la que tenemos a mano y quizás muchas veces la que tenemos menos explotada o desarrollada. Proyectos como HUCI (Humanización Cuidados Intensivos) giran en torno a esta idea y es que la alta sofisticación informática y tecnológica no puede sustituir el calor humano, la empatía y los sentimientos. Esta visión holística de la sanidad y de sus nuevos escenarios es absolutamente imprescindible para no perdernos en una visión en túnel hacia la excelencia tecnológica mal aplicada. Cuando lo que se necesita es presencia y contacto no podemos empeñarnos en basar la atención en entornos virtuales, no funcionaría.

En los últimos meses los foros profesionales y mesas de debate de eventos y congresos giran recurrentemente en torno a este tema: la humanización de los entornos sanitarios y eso incluye el ámbito de la eSalud. Es más, una pregunta que se debate con obsesión es si la tecnología deshumaniza los cuidados, si los vuelve fríos y distantes, si roban demasiado tiempo y al final del día se dedica menos a mirar, hablar y tocar a los pacientes. Los proveedores de las tecnologías sanitarias deben reflexionen sobre este aspecto e incluirlo en su discurso.

Pero la percepción de la tecnología sanitaria no tiene por qué ser percibida como algo negativo. Esta la visión de las tecnologías de acercamiento, que son aquellas que ponen en contacto a las personas, conectan fuentes de información y permiten relaciones horizontales. Tal y como suele defender Cepeda "las 'tecnologías de acercamiento' suponen en definitiva una oportunidad para situar al paciente en el centro, mediante la creación de contextos humanizados que ayuden a redefinir la forma en que las personas nos implicamos en el mantenimiento de la salud y nos acercamos a otros pacientes y profesionales".

Referencias

1. Tecnología punta humana. En Humanizando Cuidados Intensivos (blog), Disponible en http://humanizandoloscuidadosintensivos.com/es/tecnologia-punta-humana/ Consultado el 10 de Enero de 2018

INFORMÁTICA **MÉDICA**

Coordina: **José Sacristán**

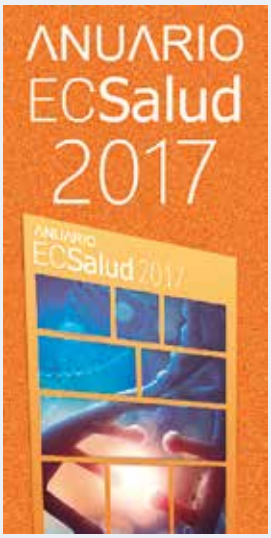


Publicación del libro: **Las 7 competencias clave hacia una #saluddigital**

Está dirigido a todos aquellos profesionales de la salud que quieren ser mejores en su trabajo, que tienen curiosidad o que buscan formas alternativas de hacer las cosas. Profesionales a los que a pesar de todas las trabas que les impone el sistema y sus quehaceres diarios no les importa dedicar parte de su tiempo libre a buscar nuevo conocimiento que les ayude a mantenerse actualizados en su trabajo. Aquellos que ven en la formación y la investigación una vía para explorar y abrir nuevos campos. Está escrito en definitiva para todas esas personas inquietas que independientemente del puesto que ocupan en su organización, piensan que siempre hay una forma mejor de hacer las cosas.

https://saludconectada.com/nuevo-libro-las-7-competencias-clave-hacia-una-saluddigital/

La **Aemps** impulsa un proyecto informático para facilitar los tratamientos antibióticos



Este trabajo se desarrollará en el marco del Plan Nacional frente a la Resistencia a los Antibióticos (PRAN) con el objetivo de evaluar la implantación de la aplicación informática WASPSS en siete centros hospitalarios de seis comunidades autónomas.

https://www.consalud.es/saludigital/91/aemps-impulsa-proyecto-informatico-facilitar-tratamientos-antibioticos_44896_102.html



SECTOR
FARMACIA

Coordina: **Alberto Gómez Lafón**

Modelización del Conocimiento Lingüístico de los Datos Clínicos incluidos en las Fichas Técnicas de Medicamentos

Actualmente la AEMPS tras el proceso de autorización de un medicamento resume toda la información del producto en un documento denominado Ficha Técnica orientado a la compresión humana en formatos PDF y HTML, aprovechando el estado del arte en la tecnología de representación del conocimiento y procesamiento del lenguaje natural, la AEMPS, con el proyecto presentado en este artículo pretende ampliar ese horizonte y de forma paralela y simultánea a su publicación en PDF/HTML implantar un proceso sostenible que permita extraer y alojar el conocimiento existente en la Ficha Técnica en un contenedor orientado a máquinas que sea de utilidad a los sistemas del SNS.

Jose Manuel Simarro Escribano
Responsable de S.I. de la AEMPS

EL PROYECTO

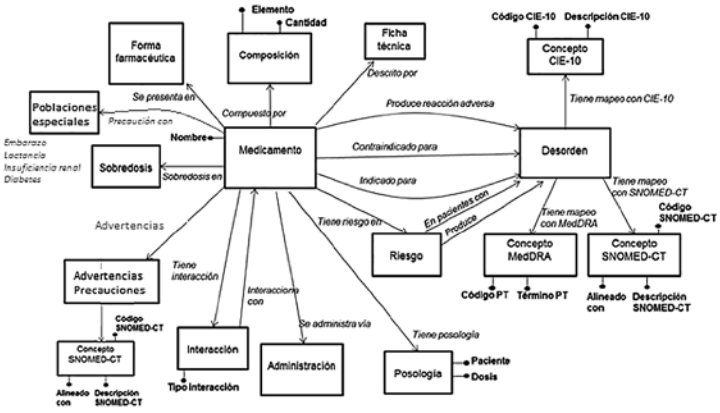
La AEMPS se encuentra actualmente trabajando en la creación y población de un modelo que permita la representación del conocimiento clínico incluido en el texto libre de la sección 4 (Datos Clínicos) de las fichas técnicas de medicamentos. Este proyecto surge como consecuencia de disponer ya de las fichas técnicas de los medicamentos fraccionadas por secciones y ante la oportunidad que representa aplicar el estado del arte de las tecnologías asociadas al lenguaje de procesamiento natural y de representación del conocimiento a las fichas técnicas. La información a modelizar es tan amplia que son los expertos clínicos del Departamento de Medicamentos de Uso Humano los que priorizan y delimitan el dominio a procesar. Para la población de este modelo ha desarrollado un sistema capaz de reconocer y extraer del texto libre términos clínicos ayudado de recursos externos tales como terminologías SNOMED-CT y medDRA patrones léxico-sintácticos y conjuntos de términos sinónimos. Sobre el conocimiento modelizado, el sistema permitirá responder a preguntas simples (ej, lista de reacciones adversas graves de un medicamento, indicaciones de un medicamento, que medicamento tomar para una indicación si se pertenece a una población especial ...) y en un último estadío de desarrollo a preguntas complejas (ej medicamento indicado en el tratamiento de los pacientes adultos con mieloma múltiple resistente al tratamiento o recidivante que hayan recibido al menos dos tratamientos previos, incluyendo lenalidomida y bortezomib, y que hayan experimentado una progresión de la enfermedad en el último tratamiento). El esquema de la página siguiente representa el modelo de partida que aloja la información extraida.

El procesamiento de la información en texto libre de la ficha técnica y la población del modelo se abordan de forma incremental, considerando que algunos de los conceptos a poblar en el modelo mostrado son más fáciles de obtener que otros (ej reacciones adversas vs interacciones). Por otra parte la información clínica está dividida en dominios habitualmente asociados secciones concretas que se pueden encontrar en cualquier ficha técnica, como son: Indicaciones terapéuticas, posología y forma de administración, contraindicaciones, advertencias y precauciones, Interacción con otros medicamentos, fertilidad, embarazo y lactancia, efectos sobre conducción y manejo de máquinas pesadas, reacciones adversas y sobredosis. Al analizar cada sección de forma individual, se determina el subconjunto SNOMED-CT/medDRA contra el que realizar el mapeo de conceptos para esa sección y se

ajustan los recursos externos de forma iterativa para extraer el conocimiento lingüístico de la sub-sección a procesar. Los recursos externos están en español y son creados con la ayuda de expertos, sirven para dotar al sistema del conocimiento base para realizar la extracción de conceptos y se refinan iterativamente a la vez que se optimiza la extracción de términos. En la definición del modelo, los conceptos, los atributos de los conceptos y las interrelaciones entre los conceptos también se definen de forma progresiva, mejorando el modelo inicial mostrado en la figura. Conforme se abordan las secciones se amplia y afina el modelo. La complejidad de algunas subsecciones obliga a que los expertos limiten inicialmente los conceptos de interés sus atributos e interrelaciones a incorporar en el modelo. La población del modelo se realiza de forma automatizada e iterativa conforme se vayan extrayendo los términos y alojando el conocimiento lingüístico adquirido por el sistema existiendo al final una validación humana realizada por expertos clínicos. La principal ventaja que presentan las fichas técnicas a la hora de realizar tareas de procesamiento del lenguaje natural es la ausencia de errores ortográficos graves, ya que las descripciones de los medicamentos son revisadas y actualizadas por la AEMPS. A pesar de esta ventaja, cabe señalar que el contenido de las secciones no está estandarizado, por ejemplo la sección 4.8 de reacciones adversas puede incluir distintos tipos de tablas con diferentes combinaciones de celdas y la complejidad del lenguaje natural hace que sea difícil manejar la búsqueda de entidades en los documentos. Por ello, para esta sección de reacciones segmenta el texto antes de procesarlo, con segmentos generados principalmente a partir de las celdas de tabla y de los párrafos. Para garantizar la sostenibilidad del proyecto, todos sus módulos y tareas de configuración son documentados con claridad para que puedan ser asumidas por la AEMPS y aplicadas a nuevas fichas técnicas y modificaciones en las ya existentes.

METODOLOGÍA

Actualmente ya se han procesado las secciones 4.1 Indicaciones terapéuticas y la sección 4.8 Reacciones Adversas y se continuará hasta procesar toda las secciones indicadas en el apartado anterior. La identificación de términos clínicos y farmacológicos se realiza mediante un proceso de reconocimiento de entidades nombradas definidas por los expertos. Este proceso utiliza como entrada un corpus creado por los segmentos de información correspondiente a la sub-sección procesada. Estos segmentos de información se obtienen limpiando el texto HTML(OPENXML) correspondiente a la sección a procesar teniendo como ámbito el conjunto de medicamentos no genéricos autorizados en España (3500 aproximadamente). Este proceso se apoya en recursos externos, sinónimos, patrones léxico-sintácticos etc. Los términos identificados se pasan por un proceso de mapeo en el que se busca un término equivalente dentro de la terminología a aplicar a esa sección SNOMD-CT o medDRA. Debido a que el proyecto se enmarca en el ámbito médico, la técnica de mapeo de enfermedades es lo más restrictiva posible, focalizándose en el grupo nominal de la enfermedad para evitar falsos positivos como resultados. Se prefiere tener una granularidad menor a devolver un término erróneo con el mismo número de palabras en común (ej., "cirrosis hepática grave" devolvería el término MedDRA "cirrosis hepática" frente a "cirrosis biliar grave"). A la hora de buscar un candidato óptimo dentro del diccionario, se generan tantas combinaciones léxicas como posibles variaciones de la entidad permitidas. El conjunto de estas combinaciones se usará en el algoritmo de mapeo durante la búsqueda del mejor resultado de entre todos los términos. Como resultado final, el sistema inyecta los términos, atributos y relaciones en el modelo.



NOTICIAS DEL SECTOR

Coordina: **Diego Sáez**

- **Cysnet lidera la integración e interoperabilidad de la clínica Universidad de Navarra en Madrid**. Cysnet Ha diseñado e implementado la arquitectura para acceder en tiempo real a todos los datos de los pacientes, sincronizando las sedes de Madrid y Pamplona. Su labor ha consistido en integrar tanto los servicios médicos como el aparataje clínico con el sistema de información del hospital, único para ambas sedes, colaborando con el equipo de TI de la institución en la optimización de sus procesos internos. Se ha utilizado InterSystems Ensemble, la plataforma Entreprise Service Bus (ESB).

- **El centro que la Cruz Roja tiene en Palma de Mallorca**, con casi 70 años de trayectoria como hospital de carácter privado benéfico, ha decidido dar el salto a la digitalización integral de su gestión de la mano de Green Cube, el software de historia clínica electrónica desarrollado por TICH Consulting, del grupo ASISA, y que ya es herramienta de gestión de otros 76 centros sanitarios nacionales e internacionales. Por su parte, el hospital mallorquín además, realiza cirugía ambulatoria y cuenta con hospital de día geriátrico dentro de sus más de 4.200m2 de instalaciones, que también albergan 60 camas de hospitalización, 13 locales de consultas externas o gimnasio de rehabilitación, entre otros servicios que, tras la implantación de Green Cube, arrojarán información completa y en tiempo real que permitirá a sus gestores potenciar la eficiencia, agilidad y calidad de los servicios que ofrecen.

- **El Servicio de Salud de Castilla-La Mancha ha invertido 430.000 euros en la renovación de la Red de Registro** y Verificación Oncológica Radioterápica (ARIA) que gestiona los parámetros del tratamiento que reciben los pacientes del servicio de Oncología Radioterápica en el Hospital General Universitario de Ciudad Real. Esta Red es una base de datos específicamente diseñada para pacientes oncológicos en tratamiento radioterápico que, además de la historia clínica, registra todos los datos, imágenes, sesiones administradas, informes clínicos y todas aquellas actuaciones realizadas sobre el paciente.

- **El Servicio de Salud de Castilla-La Mancha ha extendido los servicios que se pueden presentar por vía telemática** a las solicitudes de reintegro de gastos por prestaciones sanitarias, con el objetivo de facilitar al paciente el ejercicio de sus derechos y la gestión de los trámites, . Una de las nuevas solicitudes incluidas es el reintegro de gastos por prestación ortoprotésica con cargo al SESCAM, en su modalidad de prótesis externas, sillas de ruedas, ortesis y ortoprótesis especiales. Igualmente, se podrá solicitar por medios electrónicos el reintegro por gastos de desplazamiento para recibir asistencia a centros de atención especializada situados tanto fuera del área sanitaria y provincia de residencia como dentro su área o provincia de residencia.

- **El SESCAM pone en marcha una campaña de la APP** gratuita para pedir cita online

- **El Grupo Scanner Vizcaya construye su plataforma de interoperabilidad sobre la solución HealthShare Health Connect de InterSystems** de la mano de Ibermática. El proyecto es fruto de la colaboración iniciada entre la Unidad de Salud de Ibermática e InterSystems y permitirá al Grupo Scanner Vizcaya integrar sus sistemas con uno de sus principales clientes (Osakidetza – Servicio Vasco de Salud) para compartir y acceder a la información de los servicios prestados por Scanner Vizcaya en el ámbito del diagnóstico por imagen. Una vez estabilizada la plataforma Scanner Vizcaya estará en disposición de extender el modelo de integración al resto de sus clientes entre los que destaca el Grupo IMQ. El proyecto en cuestión, implantación de la solución de interoperabilidad líder en el entorno salud (InterSystems), junto con los servicios de integración especializados en estándares sanitarios requeridos para su puesta en marcha (Ibermática), permite a Ibermática Salud dar forma a la línea de la Interoperabilidad lanzada en el plan 2017 – 18 de la Unidad.

- **DKV ha seleccionado InterSystems HealthShare® para abordar su ambicioso proyecto de transformación digital** de todas sus áreas. La

organización está realizando un énfasis especial en el área de Servicios de Sanidad. Por ello, y para asegurar el éxito del proceso, la compañía ha apostado por la tecnología de InterSystems para disponer de los componentes software clave. Entre ellos se encuentra el ESB Corporativo o Bus de Servicios. DKV ha elegido InterSystems Health Connect como ESB por sus capacidades en el manejo de estándares de comunicación en Sanidad, como HL7, el nuevo enfoque FHIR y el soporte de numerosos perfiles IHE. Otros elementos clave del proyecto son el soporte de BPL (Business ProcessLanguage) y la orquestación de procesos de negocio, que permitirá gestionar las tareas más complejas de forma dinámica, sencilla y visual.

IN MEMORIAM



Jesús Díaz González

El 25 de diciembre fallecía de forma repentina Jesús Díaz González, Chus, Coordinador de Servicios Informáticos del SESPA.

Chus comenzó su andadura como informático del ámbito sanitario en 1989 en el Hospital Carmen y Severo Ochoa. Desde 1993, a raíz de la creación de la Coordinación Provincial de Informática, empezó a trabajar en la Dirección Provincial del Insalud. Desde esta unidad Chus ha colaborado en todos los procesos de la informatización de la sanidad en Asturias (Plan días, PRT 1996). A partir de 2002, una vez realizadas las transferencias, es nombrado Coordinador en la Unidad de Coordinación de Mantenimiento de Sistemas en los Servicios Centrales del SESPA.

Durante toda su trayectoria de más de 25 años de trabajo en sistemas de información sanitarios, ha participado en proyectos tan importantes para la sanidad de esta comunidad como el desarrollo de los sistemas de información de los hospitales y centros de salud, en su parte administrativa inicialmente, allá por los años 90, y también después en la implantación de la historia clínica electrónica.

No cabe duda de que no sólo su familia y amigos le echarán de menos, sus compañeros echamos en falta su presencia, su carácter siempre dispuesto a colaborar e implicarse en todos los proyectos, y también sus anécdotas de pesca. Además era un defensor incansable de los intereses del SESPA y, de sus compañeros, trabajador, cumplidor y carismático, una persona especial que nunca pasaba indiferente y que no olvidaremos.

Su valía profesional, modestia, rigor y compromiso con el ciudadano y con la Organización servirán de inspiración a sus compañeros, intentarán seguir sus pasos y recordar que las TIC en el ámbito sanitario tienen como objetivo prestar un servicio de mayor calidad posible tanto a profesionales como ciudadano.

Desde estas páginas, queremos rendirle un homenaje y expresar nuestras más sentidas condolencias a sus allegados.

AGENDA 2018

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

- **XV REUNIÓN DEL FORO DE SEGURIDAD Y PROTECCIÓN DE DATOS DE SALUD**
  Lugar: Valencia
  Fechas: 14 y 15 de Febrero de 2018

- **XXI CONGRESO NACIONAL DE INFORMÁTICA DE LA SALUD "INFORSALUD-2018"**
  Lugar: Madrid
  Fechas: 13, 14 y 15 de Marzode 2018

- **ÍNDICE SEIS - 2017**
  Lugar: Madrid
  Fechas: Marzo de 2018

- **PRIMER FORO DE ENFERMERÍA DIGITAL**
  Lugar: Tomelloso (Ciudad Real)
  Fechas: 12 y 13 de Abril de 2018.

- **VIII REUNIÓN DEL FORO DE INTEROPERABILIDAD**
  Lugar: A Coruña
  Fechas: 9 y 10 de Mayo de 2018

- **XXV JORNADASDE INNOVACIÓN Y SALUD EN ANDALUCÍA**
  Sede: Málaga - Torremolinos
  Fechas: 13, 14 y 15 de Junio 2018

- **VII REUNIÓN DE LA PLATAFORMA TECNOLÓGICA PARA LA INNOVACIÓN EN SALUD**
  Lugar: Murcia
  Fechas: 26 y 27 de Septiembre de 2018

- **XVI REUNIÓN DEL FORO DE SALUD CONECTADA**
  Lugar: Santander
  Fechas: 24 y 25 octubre de 2018

- **VIII REUNIÓN DEL FORO PARA LA GOBERNANZA DE LAS TIC EN SALUD**
  Sede: Palma de Mallorca
  Fechas: 21 y 22 de Noviembre de 2018

TRABAJANDO POR LA INNOVACIÓN TIC EN SALUD
40 AÑOS

XV FORO de Seguridad y Protección de Datos de Salud

"RGPD: ¿Qué nos exige a las Organizaciones Sanitarias?"

Siguenos en twitter: @SEISeSalud

Organiza

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

Con la colaboración de

GENERALITAT VALENCIANA | TOTS A UNA veu
CONSELLERIA DE SANITAT UNIVERSAL I SALUT PÚBLICA

VALENCIA
14 y 15 de febrero de 2018

Aula Magna del rectorado de la Universidad de Valencia
Av. de Blasco Ibáñez, 13, 46010 Valencia

COLABORADORES TECNOLÓGICOS

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

XXI Congreso Nacional de Informática de la Salud

2018 Infors@lud

"Salud Digital: un proyecto colaborativo"

TRABAJANDO POR LA INNOVACIÓN TIC EN SALUD
40 AÑOS

Organiza

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

Hotel NH Collection Madrid Eurobuilding
c/ Alberto Alcocer 8
28036 Madrid

MADRID, 13, 14 y 15 de marzo

Colaboradores Tecnológicos

Atos · connectis · FUJITSU · gmv · Ibermática · indra

INFORMÁTICA El Corte Inglés · intel · InterSystems · SIEMENS Healthineers · PHILIPS · T-Systems