NÚMERO
128

I+S

ABRIL
2018

REVISTA DE LA SOCIEDAD ESPAÑOLA DE INFORMÁTICA Y SALUD

ESPECIAL

BLOCKCHAIN EN SALUD
¿Quimera o realidad?



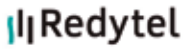
"40 AÑOS TRABAJANDO POR LA INNOVACIÓN TIC EN SALUD"

ENTIDADES ASOCIADAS

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD





































































SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

Director
Salvador Arribas Valiente

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

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

Colaborador Técnico
Diego Sáez

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

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

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

5 **EDITORIAL**

6 **ESPECIAL** BLOCKCHAIN EN SALUD. ¿QUIMERA O REALIDAD?

6 Un viaje a Itaca
8 Blockchain: La disrupción del rol del paciente en el ámbito de la salud
11 Blockchain y el Sector Salud
15 Blockchain en Sanidad
22 Blockchain en el ámbito de la Sanidad
24 Blockchain: Cambiando los modelos de relación y confianza
27 Blockchain, más allá de la tecnología
30 El impacto de la tecnología Blockchain en Sanidad
32 Sistema de Intercambio de Información Clínica basado en Blockchain
35 Una aproximación blockchain al ámbito de la salud
38 Blockchain, una oportunidad tecnológica para el Sector Salud

41 **ACTIVIDADES DE LA SEIS**

41 XXIII Premios Nacionales de Informática y Salud.
49 XV Foro de Seguridad y Protección de Datos en Salud

67 **AGENDA**

68 **FOROS Y SECTORES**

68 Foro de Salud Conectada
69 Foro de Interoperabilidad en Salud
70 Foro de Seguridad y Protección de Datos en Salud
71 Sector de Informática Médica
72 Sector de Enfermería Digital
73 Sector de Farmacia

74 **NOTICIAS DEL SECTOR**

Los artículos revisiones y cartas publicadas en I+S, representan la opinión de los autores y no reflejan la de la Sociedad Española de Informática de la Salud. Queda prohibida la reproducción total o parcial sin citar su procedencia.

ENTIDADES
COLABORADORAS

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

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

Se puede avanzar mucho más

No queremos dejar de destacar los 40 años que lleva la Sociedad Española de Informática y Salud (SEIS) trabajando por la innovación del sector salud. Durante este tiempo, han ocurrido muchas cosas en todos los ámbitos, pero todos los que nos iniciamos entonces en la incorporación de las TIC al sector sanitario sabemos que nunca se ha aprovechado el potencial tecnológico que hemos tenido disponible... Nuestra materia prima es la información y el conocimiento y las TIC son la herramienta para ello.

No podemos decir que no se haya avanzado. Se ha hecho y de forma considerable, ya que incluso somos referente en el ámbito internacional en muchos de los proyectos TIC puestos en marcha en España, pero creemos que con una organización sanitaria como la española y con unos profesionales del máximo nivel se podía y se puede avanzar mucho más.

Vamos a publicar en breve el nuevo ÍNDICE SEIS correspondiente a su edición 2017 y los datos obtenidos no son especialmente optimistas. El sector sanitario sigue sin aprovechar todo el potencial que la tecnología puede ofrecerle hoy en día. Hemos trasladado al sector la oportunidad de aprovechar la crisis económica para innovar los procesos, reduciendo costes y mejorando la atención sanitaria, con avances en la labor de los profesionales y en la corresponsabilidad del ciudadano en su salud... Pero es necesario obtener recursos adicionales, hay que invertir inicialmente para obtener el retorno adecuado. Seguimos pensando que existe margen presupuestario y fondos para poder acometer una transformación ambiciosa del sector salud, planificada y dirigida desde una política general orientada al ciudadano y contando evidentemente con los profesionales.

La tecnología disponible, la nueva cultura digital y los avances científicos están provocando un cambio en la forma de prestar los servicios de salud, la aparición de nuevos servicios y la desaparición de otros. Tenemos que prever que el sistema de salud, en unos años, tiene que asumir un cambio profundo.

Y este cambio, si bien debe ser liderado por los responsables de las organizaciones, es imprescindible que cuente con la colaboración, apoyo y el conocimiento de los profesionales sanitarios.

Confiemos que no nos siga pasando como en el pasado inmediato, que la transformación digital, que se va a producir ineludiblemente, se realice a partir de iniciativas de profesionales innovadores sin el correspondiente apoyo institucional o corporativo, lo que conllevaría, posteriormente, a poner en marcha planes de reingeniería que permitiesen integrar las diferentes soluciones desarrolladas, con el inevitable coste económico y de oportunidad.

Un viaje a Itaca

Así, sabio como te has vuelto, con tanta experiencia,
entenderás ya qué significan las Itacas.
Cavafis

Francisco José Martínez del Cerro
Coordinador del número especial de la revista. Profesor asociado de la UC3M.
Miembro de la Junta Directiva de la SEIS

ACTUALMENTE CASI TODO EL MUNDO HABLA DE BLOCKCHAIN. UN TÉRMINO NACIDO EN EL MUNDO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y DE LAS COMUNICACIONES, Y QUE GRACIAS AL AUGE DE LAS CRIPTODIVISAS SE HA CONVERTIDO EN UN TÉRMINO DE USO GENERAL EN LOS MEDIOS DE COMUNICACIÓN. PERO ¿PARA QUÉ SIRVE ESTA TECNOLOGÍA?

La respuesta no es simple. Según Axel Pierron, Managing Director at Opimas, LLC, "Blockchain es una solución buscando un problema". Existen múltiples definiciones y explicaciones de lo que es. La más extendida es que funciona como un libro de contabilidad donde se apuntan todas las transacciones y que estas no pueden ser modificadas. En su descripción más técnica, es una base de datos descentralizada y distribuida cuya principal característica es la inmutabilidad y encriptación de los datos almacenados. Los informáticos dicen que es el modelo de intercambio de información en el futuro. Y ahora todos los analistas tecnológicos plantean utilizarla en la mayoría de los sectores industriales y de servicios, gracias fundamentalmente a su capacidad de desintermediación en los servicios. Y la mayoría de los ciudadanos siguen sin entender que es esto.

Si observamos el ecosistema de Blockchain veremos que hay muchas iniciativas basadas en esta tecnología. La que más visibilidad tiene es la aplicación en el entorno financiero con las criptodivisas y las ICO (Initial Coin Offering), que permiten resolver el problema del doble pago, que es el motivo por el que Satoshi Nakamoto desarrolló en 2008 la base de esta tecnología. Pero no es la única. Existen aplicaciones de blockchain en trading de mercancías, en seguros, deportes, en el control de votaciones, para el almacenamiento seguro en la cloud (www.storj.io), en educación (www.tutellus.io), salud, etc. Todas ellas tienen un elemento en común: la gestión eficiente y segura de un valor o activo, denominado token, en un entorno donde no hay confianza entre los actores que intervienen en el proceso. Ese token puede ser una moneda, un voto, un documento del registro, 1 KW de energía, un informe clínico, un seguro médico, etc.

Si analizamos esta tecnología desde un punto de vista de sistemas de información, hablamos de una red de usuarios conectados todos con todos. Unos nodos de esta red validan las operaciones realizadas en su aplicación mediante un protocolo de consenso establecido a priori, y guardan mediante códigos, las operaciones, cantidades, fechas y participantes, en una base de datos replicada en todos los nodos autorizados de la red. Y los usuarios autorizados pueden realizar operaciones y consultar la base de datos. Pero. ¿quién gobierna esta red? El éxito de Bitcoin y Ethereum se basa en que son redes públicas, permissionless, en las que nadie centraliza y cualquier usuario puede conectarse y validar las transacciones, pero esto implica bajos throughput. Existen también redes privadas, permissioned, donde el acceso y la validación las controla una organización. Y también existen consorcios, hybrid networks, donde el

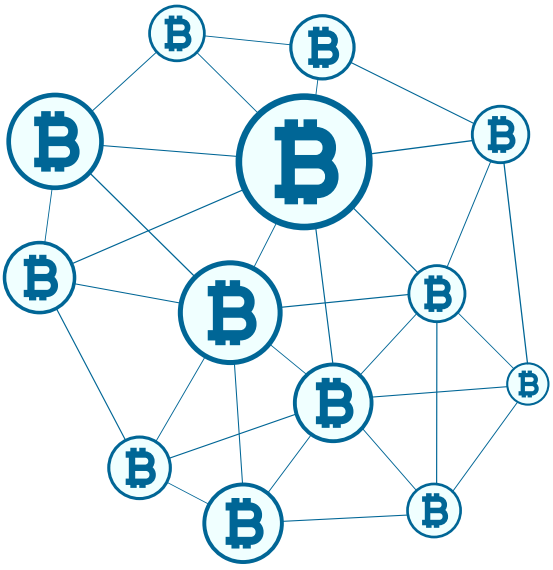
acceso es público pero un consorcio controla la gestión. Hay ejemplos de todos estos tipos de red: públicas como Bitcoin o Ethereum; privadas como Hyperledger, R3 o Ripple; hibridas como Alastria, BigchainDB o Evernym.

Desde el punto de vista de almacenamiento de datos, la red blockchain no es una solución eficiente para almacenar grandes cantidades de datos debido a que la base de datos tiene que estar replicada en todos los nodos de la red. Por este motivo, la red almacena transacciones o bien índices que apuntan a información fuera de la red blockchain. La autenticidad de los datos fuera de la red se garantiza por el uso de técnicas criptográficas y resúmenes digitales (funciones hash). Igualmente puede haber problemas de rendimiento debido a que por su carácter distribuido, las transacciones no son válidas hasta que todos los nodos tienen actualizada la base de datos, lo que puede dar lugar a retardos inaceptables.

También es importante la regulación. Hay dos puntos del RGPD que son críticos para esta tecnología: el derecho al olvido y el derecho a la portabilidad. En una red blockchain, donde no se puede cambiar ningún dato de las transacciones, el derecho de un ciudadano a borrar su historial es difícilmente compatible con esta tecnología. La solución podría estar en garantizar que el ciudadano controla totalmente el acceso a sus datos, lo que indirectamente garantiza que si el ciudadano no da permiso, nadie puede ver sus datos. El derecho a la portabilidad implica que un ciudadano debe poder cambiar de red blockchain sin problemas y sin la perdida de datos. Esto tiene implicaciones en los protocolos de consenso de las redes.

Otro aspecto a tener en cuenta cuando analizamos blockchain es el uso de los contratos inteligentes (Smart Contracts). Piezas de software que, incluidas en la red de blockchain, permiten que las cláusulas de un contrato se ejecuten sin necesidad de un intermediario físico. Ethereum es la plataforma más destacada actualmente de la red en este ámbito. En este caso, los activos llevan información adicional de forma que se pueden hacer transacciones con estos activos utilizando los Smart Contracts.

Y finalmente, habría que analizar el tema de estándares y el coste que puede suponer un servicio



basado en blockchain, ya que aunque no haya intermediación y por tanto no hay que pagar comisiones, los costes totales pueden ser incluso más altos ya que en las redes actuales hay que pagar por cada transacción.

Y como se utiliza esta tecnología en el sector salud. Existen múltiples iniciativas: gestión de la identidad para controlar el acceso a las Historias Clínicas (caso de Estonia), la trazabilidad de productos farmacéuticos, la contratación de seguros médicos (https://linda.healthcare), desarrollo de ensayos clínicos, etc. No obstante, todavía es una tecnología muy inmadura, con muy pocos profesionales expertos, y con muchos interrogantes abiertos. Y este es el motivo por el que la Sociedad Española de Informática de la Salud ha decidido publicar este número especial de la revista I+S dedicado al uso de Blockchain en salud. El objetivo no es explicar las bases de la tecnología o explicar proyectos concretos, sino que se ha pedido a los colaboradores que den su punto de vista del presente y futuro de esta tecnología en el sector salud, analizando todos los aspectos introducidos en los párrafos anteriores, y que pueda servir para ampliar el conocimiento de todos aquellos que directa o indirectamente tienen alguna responsabilidad en los sistemas sanitarios del país, y les ayude en el viaje a su Itaca. La SEIS cumple así con sus objetivos de potenciar la innovación y un uso eficiente de las tecnologías de la información y de las comunicaciones en el sector salud.

Blockchain: La disrupción del rol del paciente en el ámbito de la salud

Alfonso Tamés Llana
Managing Director Accenture Technology
Responsable de Innovación, Blockchain e Inteligencia Artificial para España, Portugal e Israel

ESTAMOS EXPERIMENTANDO LA REVOLUCIÓN QUE HA PROVOCADO LA LLEGADA DE UNA NUEVA TECNOLOGÍA, BLOCKCHAIN, Y QUE LOS ANALISTAS COMPARAN CON EL EFECTO QUE, EN LA DÉCADA DE LOS 70, GENERÓ LA PUBLICACIÓN DEL MODELO DE TCP/IP, POR PARTE DE V. CERF Y R. E. KHAN, Y QUE FUE EL EMBRIÓN DE "INTERNET".

Quizás la comparación sea un poco exagerada, pero sí que opino que hay similitudes en la manera en que Blockchain ha abierto un nuevo frente de discusión. Este frente que se va extendiendo cada día, y que plantea nuevas opciones a la hora de resolver problemas ya resueltos, de la misma manera que, salvando las distancias, el email de Internet nos brindó una alternativa al correo tradicional.

Y este contexto lo que está marcando el ritmo al que Blockchain se propaga. Por un lado, el salto tecnológico no es tan notable como el que introducía Internet y por tanto sus beneficios y su potencial puede que no resulten tan evidentes. Por otro lado, y creo que esto es lo más relevante, por norma general, no va a permitirnos hacer cosas nuevas que no podamos hacer con las tecnologías ya disponibles, simplemente va a permitirnos hacerlas de una forma diferente (pero esto también es innovación) simplificando procesos, eliminando intermediarios y brindándonos más transparencia y control sobre la información.

Vuelvo un paso atrás e insisto de nuevo, si me lo permitís, en el carácter de Blockchain como tecnología, es decir, como facilitador, sobre la que desarrollar productos y soluciones. Voy a evitar, en este artículo, entrar en los detalles "crípticos" de cómo funciona la "cadena e bloques" (smartcontracts, hash, distributed ledgers, private/public keys, etc), para centrarme en lo que creo más importante, que es qué podemos hacer con esta plataforma y por qué sería interesante cambiar el paso y movernos a Blockchain en lugar de seguir recurriendo a los sistemas actuales con los que ya nos sentimos confortables. Pido, a cambio, un poco de la fe que todos depositamos en otras tecnologías que usamos a diario (teléfono móvil, televisión o la propia electricidad), creedme, Blockchain funciona y es seguro. Lo ha demostrado en el entorno financiero y a las criptomonedas, como Bitcoin y estos son, seguramente, los únicos casos de uso que nos suenan, pero en cada industria podemos encontrar escenarios interesantes en los que tiene sentido pensar en esta plataforma. Alrededor de los servicios de la salud, también.

LAS BASES DE BLOCKCHAIN. El principal beneficio que nos proporciona Blockchain es la "desintermediación", es decir, la eliminación de los intermediarios, en un determinado proceso, y a los que, en líneas generales, introdujimos en su momento como custodios o garantes de la integridad y fiabilidad de éste. Estos intermediarios son los certificadores actuales de que una operación se realiza con garantías, y en los que confiamos, para que velen por el proceso, cuando realizamos alguna transacción de activos con un tercero.

El inconveniente es que estos intermediarios, en la mayoría de los casos, nos fuerzan a ceder o depositar este activo con el que operamos (token, en terminología Blockchain) cuyo intercambio regulan. Introducen además condiciones, comisiones, acciones, requisitos y en general, costes y tiempo, que debemos soportar si queremos operar con "nuestros" tokens. El concepto de la propiedad también se diluye, no es tan relevante

cuántos o qué activos tenemos como cuántos o cuáles son los tokens que estos intermediarios reconocen (o están dispuestos a avalar) que están a nuestra disposición para operar.
Blockchain nos brinda la opción de desplazar a estos intermediarios y sustentar las garantías no en una entidad, sino en una comunidad, en un consorcio. Se apalanca en el concepto, por decirlo de alguna manera, del "círculo de confianza" un circulo, tan extenso (o público) como queramos, en el que todos los actores y participantes en el proceso velan por la integridad de éste. Se confirma que una transacción es viable porque todo el consorcio la ratifica y la registra en caso de ejecutarse. Y este círculo de confianza se mantiene y no se degrada porque Blockchain implementa otro mecanismo como base, la información se puede leer y se puede añadir, pero no es posible modificarla o borrarla. Todo el consorcio es testigo y registra cada una de nuestras intervenciones, simplificando notablemente la resolución de disputas y evitando que se produzcan conflictos del tipo "yo no dije 68, yo dije 6 u 8")
La aplicación en el caso de transacciones u operaciones con tokens de moneda, es un ejemplo fácil de entender y el motivo por el que Blockchain se ha introducido tan rápido como alternativa a las transacciones financieras desplazando a los bancos, pero si abrimos un poco la mente y empezamos a jugar a los tríos proceso - activo (o token) - (intermediario o garante o custodio) podemos empezar a vislumbrar hasta dónde se pueden extender los casos de usos de esta tecnología. Solo por poner algunos ejemplos comprar – casa – (registro de la propiedad o inmobiliaria), firmar – acuerdo - notaría, contratar – titulado - agencia de selección personal, compartir - expediente médico – servicio de salud.

LA DISRUPCIÓN PARA EL PACIENTE Y LOS SERVICIOS DE SALUD. Si, por poner un caso hipotético a modo de ejemplo, nos encontráramos con un diabético tipo 1 que viviera en Barcelona, pero, por trabajo, se viera obligado a viajar regularmente a Madrid y Andalucía y tuviera familia en Asturias, a la que visita en vacaciones, y le preguntáramos cómo es su vida "normal", más allá del impacto que tiene en su día a día el tratamiento, seguro que llegamos a la conclusión de que parece innecesariamente complicada y que tiene recorrido de mejora.
A pesar de que el expediente médico/clínico en teoría es propiedad del paciente, son los Servicios de Salud de la comunidad, en este caso, los custodios y depositarios de esa información, pero, o no cubren el registro de toda la información que para este diabético puede ser relevante, o registrar estos informes adicionales se convierte en un proceso tedioso y que consume tanto tiempo para el individuo, que normalmente éste desiste. Si este paciente recurre a cualquier otro médico privado o, por ejemplo, a un nutricionista o a cualquier otro especialista fuera del circulo de los servicios de salud, los informes que éstos elaboran, terminan finalmente en una carpeta que va llevando de un sitio a otro y que hace que el tiempo medio de sus revisiones se multipliquen, al menos por dos, a medida que le va poniendo al día a su médico (que también invierte tiempo en ordenar y procesar esta información) pasándole papel tras papel y explicándole, lo mejor que puede, cuando y porqué se ha generado dicha información. Si por algún motivo se produce un cambio de médico, o le atiende un doctor que no sea el suyo habitual, esa cita se convierte, ya, en todo un ejercicio de memoria histórica.
Pero el escenario se puede complicar aún más si este diabético requiere cualquier tipo de consulta durante sus viajes o vacaciones, ya sea por motivo de cualquier otro tipo de enfermedad, o incluso porque requiera recetas para su tratamiento con insulina. En este caso se encontrará con que los servicios de salud de otras comunidades no tendrán acceso a su historial al estar bajo la custodia de otros servicios y puede darse el caso de que tenga que repetir pruebas o análisis para obtener el tratamiento requerido en los centros de esta nueva comunidad.
Creo que este es un escenario interesante, porque los Servicios de Salud son a la vez actores en el proceso (requieren acceso a la información y generan información adicional para el paciente), pero sólo son custodios de parte de lo que podríamos considerar el historial completo del individuo e intermediarios, sólo, en algunos de puntos del proceso. Hay otros actores, otros servicios médicos, otras especialidades, farmacias e incluso actividades de la vida cotidiana del paciente (alimentación, ciclos del sueño, actividad física, con-

sumo de otros fármacos sin receta, etc.) que al final, en su conjunto, influyen en su tratamiento y son requeridos cara a consolidar lo que realmente sería su historial completo y personalizado.

Y en este escenario, personalmente creo que Blockchain tendría mucho que aportar como plataforma de soporte al registro del historial médico/clínico del paciente, en el que éste se convirtiera en el propietario y custodio de la información y desde donde pudiera 1) autorizar el registro de información certificada y validada, ya no solo por parte de los servicios de salud de su comunidad, sino también de otros centros privados o de otras comunidades o de otro tipo de profesionales que aporten datos complementarios – nutricionistas, entrenadores personales, etc – que puedan ser relevantes para el paciente; 2) gestionar el acceso y la cesión de esa información a cualquier centro o servicio de la red o consorcio de esta Blockchain; 3) disponer de un repositorio completo de información asociada a su salud y 4) facilitar la extensión del registro o consumidores de estos datos abriendo la puerta a nuevos actores y miembros del consorcio.

Me gustaría hacer un breve zoom en este último cuarto punto. Hasta este momento he destacado como Blockchain puede aportar valor en escenarios de "transacciones" de información médica entre facultativos o profesionales de servicios asociados a la salud y el propio paciente, pero esta tecnología puede soportar además protocolos de transacción entre personas y máquinas o dispositivos, es decir, tiene capacidad para integrar de la misma, información del paciente capturada por "wearables", como las populares pulseras que monitorizan el sueño y actividad física, o aparatos de análisis que podamos encontraren las farmacias; siempre que estos se conecten a nuestra Blockchain. De esta manera, una vez que el paciente disponga de un repositorio completo, veraz y certificado que agrupe tanto su información médica como su actividad personalizada, podremos dar un paso más en el desarrollo de servicios automáticos personalizados o medicina preventiva si él nos autoriza el acceso a estos datos.

Por poner un ejemplo de este último caso, si el dispositivo de medición de niveles de azúcar de este paciente envía sistemáticamente los datos que registra a la Blockchain, en donde están registrados, igualmente, el plan de actividades planificadas que ha desarrollado para él su entrenador personal. Si el paciente ha recurrido a un endocrino o nutricionista privado que ha registrado la dieta que ha recomendado y toda esta información se completa con el histórico de actividad física recogido por un wearable, entonces, este paciente, podría decidir ceder estos datos a un servicio que, en base a toda esta información, podría calcular diversas combinaciones y alternativas para la próxima comida, y cuál sería la dosis de insulina que le correspondería en cada caso.

LOS RETOS. Puede parecer que todo esto es un poco futurista, pero la verdad es que son escenarios reales y realistas, al alcance de nuestra mano con esta tecnología. Las preguntas obvias, entonces, serían, ¿y por qué no los hemos desarrollado aún? ¿y por qué si además, como parece, no solo aportaría calidad de vida y valor al paciente, sino que también, al eliminar el rol de custodio de los datos a los servicios de salud pueden simplificarse el cumplimiento de la nueva normativa GDPR de seguridad de los datos y facilitar la portabilidad de la información entre comunidades o racionalizar el paso por consulta de enfermos crónicos para la obtención de recetas o la repetición de pruebas, por poner algún ejemplo, que un paciente se haya realizado en otros centros o a través de dispositivos certificados en farmacias? ¿por qué con todos estos beneficios aparentes para todos los actores, la penetración de Blockchain en el área de la salud es tan insignificante comparada con la que ha tenido en el área de servicios financieros?

¿Mi opinión personal?, puede que el motivo sea que, a lo hora de la verdad, la salud no sea lo primero. También creo que influye y mucho, las propias bases de la Blockchain, que se sustentan en el concepto de consorcio y círculo de confianza.

Es necesario, para que Blockchain despegue en el área de la salud, que los participantes más relevantes (al menos pacientes, médicos, servicios de salud y farmacias) se adhieran y decidan dar un paso adelante en esa dirección. Es a fin de cuentas un reto, pero no tanto un reto tecnológico, como un reto social, de espíritu de comunidad y de compromiso y de atrevernos a participar y empujar este cambio, porque vemos y creemos en los beneficios que aporta, en lugar de quedarnos esperando a ver si otro se mueve primero.

Blockchain y el Sector Salud

Alejandro Dovale, Jaime Morales
Grant Thornton Corporación S.L.P.

BLOCKCHAIN ES UN PROTOCOLO DISTRIBUIDO QUE PERMITE EL INTERCAMBIO DE INFORMACIÓN O VALOR (TOKENS), ENTRE DOS O MÁS PARTES. LA INFORMACIÓN, EN FORMA DE TRANSACCIONES, CONTENIDA EN LA RED ES VALIDADA A TRAVÉS DEL CONSENSO. LA RED BLOCKCHAIN ACTÚA COMO FUENTE ÚNICA DE CONFIANZA ENTRE LAS PARTES.

Es decir, es un protocolo para generar confianza en un sistema distribuido. Un sistema o aplicación blockchain es un software que implementa dicho protocolo, mientras que una red blockchain es aquella formada por participantes que ejecutan el mencionado software en sus ordenadores.

La mayor parte de redes para el intercambio de valor actuales son centralizadas, es decir, dependen de un punto central que garantice la validez de los intercambios. Además, no garantizan ni la unicidad ni la autenticidad de la información de una forma unívoca. Con blockchain, podrían funcionar de forma distribuida: las transacciones de valor se podrían hacer directamente entre los interesados, por lo que el rol de los intermediarios se transforma. De este modo, se consigue una mayor disponibilidad y se abre la puerta a nuevos modelos de negocio de economía colaborativa. Blockchain toma el papel del tercero de confianza validando las transacciones.

El protocolo establece que cada participante de la red almacene los datos válidos en una estructura de datos, llamada también blockchain o cadena de bloques (de ahí el nombre de esta tecnología). Las reglas del protocolo y el diseño de la propia cadena de bloques, hacen que esa estructura de datos sea un registro inmutable de transacciones entre pares. Un bloque no es más que un conjunto de transacciones hechas en la red, mientras que la cadena es una lista de bloques enlazados criptográficamente entre sí. Dicho enlace otorga inmutabilidad a la cadena porque hace prácticamente imposible modificar cualquier "eslabón" de la misma.

La tecnología blockchain tiene 3 propiedades fundamentales, las cuales a su vez aportan valor a cualquier caso de uso donde se aplique:

1. Integridad de los datos: como la cadena de bloques es inmutable, se garantiza la integridad de los datos. Por este motivo (y porque la cadena guarda transacciones) blockchain se puede considerar como un libro mayor distribuido e incorruptible.
2. Consistencia: todos los nodos tienen la misma versión de los datos, una vez añadida a la blockchain.
3. Tolerancia a fallos: la información está replicada en varios nodos, por tanto estará disponible incluso en caso de fallo de un miembro de la red.

Es importante destacar que existen redes blockchain públicas y privadas. A las públicas puede acceder cualquier persona, como es el caso de Bitcoin, mientras que las privadas están destinadas a grupos cerrados, con participantes autorizados.

SMART CONTRACTS

El potencial de blockchain va más allá de ser un libro distribuido, porque puede suplir muchos otros tipos de problemas de confianza entre pares. Simplemente se debe definir qué información almacenar en la cadena de bloques, es decir, que datos son los que se quieren validar y compartir; posteriormente, se deben establecer las reglas que deben cumplir esos datos.

Para poder definir reglas específicas sobre los activos representados en la red de blockchain se utilizan los Smart Contracts. Un Smart Contract es un programa que se ejecuta en una block-

chain y que es creado por un usuario de esta. Normalmente, tienen como objetivo la gestión de activos digitales, permitiendo plasmar acuerdos entre diferentes usuarios de la red.

Así, este tipo de contratos permite la automatización de transacciones que cumplan con reglas o lógica de negocio específicas. De hecho, se han llegado a implementar empresas enteras en plataformas blockchain, como The DAO (Organización Autónoma Descentralizada, por sus siglas en inglés), plasmando toda la lógica de negocio en Smart Contracts en la red de Ethereum.

Cualquier transacción hecha por este tipo de programas queda registrada en la cadena de bloques, con lo cual todos los participantes pueden comprobar la validez de la información transmitida.

Las tres características principales de un Smart Contract son las siguientes:

- Neutralidad: Un Smart Contract contiene reglas y condiciones que los miembros acuerdan previamente. Dicho contrato no puede ser manipulado posteriormente, ya que el código queda grabado en un bloque de la propia cadena de bloques.
- Atomicidad: La ejecución de un Smart Contract siempre queda en un estado consistente. Si se produce un error en su ejecución, cualquier cambio hecho es revertido automáticamente.
- Transparencia: Al estar embebidos en blockchain, todos los miembros de la red tendrán almacenada una "copia" del código del contrato, pudiendo verificar por sí mismos el cumplimiento y la validez de las reglas programadas en éste.

BLOCKCHAIN EN EL CONTEXTO ACTUAL

La tecnología blockchain ha despertado gran interés a nivel global tanto en el ámbito académico como el empresarial. Así lo demuestra la gran cantidad de pruebas de concepto y aplicaciones productivas aplicadas a numerosos sectores en varios países.

El sector financiero es el más activo con diferencia. Existen importantes consorcios a nivel mundial entre los cuales destaca R3, formado por más de 80 entidades financieras multinacionales y con una inversión que supera los 107 millones de dólares. En España, el consorcio financiero más importante está encabezado por Cecabank y Grant Thornton el cual reúne al 33% del sistema financiero español y donde se trabaja continuamente para desarrollar nuevos casos de uso en este sector. También en España, existe uno de los mayores consorcios multisectoriales a nivel mundial denominado Alastria.

Por otra parte, en el sector público, entre los principales avances, se encuentra el prototipo Catena del gobierno de Canadá, donde se almacena en un registro público cualquier financiación hecha por el estado a entidades privadas. Adicionalmente, Gran Bretaña ha apostado por incorporar blockchain como un servicio más dentro de su marco G-Cloud 8 para que organismos públicos compren servicios en la nube.

En este sentido, el sector público también está realizando investigaciones para otros trabajos futuros que pueden ser de gran utilidad, como puede ser: el sistema de votación digital, gestión de identidades, títulos de propiedad, sellado de tiempo de documentos oficiales, etc.

La Unión Europea también se ha implicado en la investigación y desarrollo de esta tecnología. Entre las iniciativas propuestas, merece la pena destacar el proyecto Decode (parte del programa H2020), donde participan universidades españolas y cuenta con un fondo de €5 millones para la implementación de identidades digitales mediante blockchain. Como parte de los programas FP7 y H2020, se estima que para 2020 se habrán invertido €340 millones para investigación de blockchain. Así mismo, el pasado día 1 de febrero la Comisión Europea inauguró el "*Foro y Observatorio de Blockchain de la UE*", orientado a informar y promover avances en esta materia.

En el sector energético el hito más representativo es la primera compra-venta de energía a través de esta tecnología, llevada a cabo por Gas Natural y Endesa, con un volumen de 5,95 GWh de gas natural.

El impacto de blockchain no se limita a los ámbitos citados. Entre otros potenciales usos de esta tecnología destacan los mercados predictivos, la trazabilidad de diamantes, la fragmentación de la propiedad de obras de arte, la gestión de historiales académicos o dotar de confianza y trazabilidad a proyectos de construcción.



BLOCKCHAIN EN EL SECTOR SALUD

El sector salud puede ser testigo de una mejora sustancial gracias al potencial de la tecnología blockchain. Diversas encuestas revelan que el interés en la cadena de bloques ha aumentado considerablemente, así como se estima que para finales de 2018 existirán numerosos aplicativos productivos. Son muchos los casos de uso:

MEDICINA E IOT

El Internet de la cosas (IoT) puede mejorar considerablemente los sistemas de salud actuales. Dispositivos como pulseras electrónicas, marcapasos, sensores de azúcar, etc, pueden aportar información clínica de pacientes en tiempo real, ayudando a tener datos más precisos y actualizados de cada paciente. En ese contexto, es crucial garantizar la seguridad y el correcto transporte de la información generada. Un sistema blockchain puede funcionar como plataforma de intercambio de información mediante la cual dichos dispositivos médicos transmitan los datos recopilados sobre la salud de los pacientes. Gracias a las propiedades de esta tecnología, se podría dotar a los pacientes de una identidad digital, donde los datos se podrían compartir de forma segura, garantizando la integridad de los mismos.

LUCHA CONTRA LA FALSIFICACIÓN DE MEDICAMENTOS

Un medicamento falso es aquel cuyos ingredientes carecen de principios activos o bien no contiene las proporciones adecuadas de estos, pudiendo causar graves daños a los pacientes. El medio principal para prevenir la distribución de medicinas falsas consiste en trazar los medicamentos a lo largo de toda la cadena de suministro de forma que se pueda verificar la autenticidad y legitimidad de su origen. A este método se le conoce como "serialización de medicamentos".

Gracias a la tecnología blockchain se puede crear un registro compartido por todos los interesados de la cadena de suministros en el cual trazar el ciclo de vida de ingredientes y medicamentos. Dicho registro puede ser de ámbito global, permitiendo tanto a usuarios como proveedores verificar electrónicamente y de una forma fácil que el ciclo de vida de un medicamento es legítimo, comprobando así la autenticidad de una medicina.

CASO PRÁCTICO GRANT THORNTON: INTEROPERABILIDAD DE HISTORIALES CLÍNICOS

Los Historiales Clínicos Electrónicos (HCE) son el tipo de activo principal de cualquier sistema informático relacionado con el sector sanitario. Sin embargo, en el contexto tecnológico actual, no existe una infraestructura estandarizada que permita a diversos tipos de proveedores sanitarios intercambiar información acerca de pacientes; por ejemplo, un hospital público no puede compartir registros con uno privado. Como consecuencia, el historial con el que trabaja un médico está incompleto, porque no contiene los datos aportados por otros proveedores. Esto puede dar lugar a una atención médica ineficiente e, incluso, poner en riesgo la salud del paciente. Además, los pacientes no pueden fácilmente controlar el acceso a sus historiales, ni decidir compartirlos entre proveedores sanitarios públicos y privados.
Para abordar esta problemática, Grant Thornton ha investigado una prueba de concepto que consiste en una aplicación distribuida basada en blockchain. El objetivo es mejorar la gestión de la información clínica de pacientes, otorgándoles el derecho a decidir quién accede a sus datos y garantizando la integridad, privacidad y consistencia de la información. Adicionalmente, se facilita la compartición de datos entre diferentes instituciones sanitarias, gracias a que la aplicación funciona como plataforma común de intercambio entre diversas instituciones.
En este aplicativo, la cadena de bloques almacena información sobre el estado de una historia clínica, que, además, permite comprobar la integridad de dichos datos clínicos. Adicionalmente, la cadena guarda meta-datos que indican los permisos de acceso a los historiales dados por pacientes a proveedores. Dichos permisos se otorgan (y revocan) mediante *Smart Contracts* embebidos en la blockchain.
Cuando una persona va a una consulta, el médico solicita, a través de la aplicación, la última versión del historial médico del paciente. Para ello, la aplicación verifica que el hospital en cuestión ha sido autorizado por el paciente para acceder al historial clínico. Posteriormente, descarga el historial desde las bases de datos de otros proveedores. Al descargarse, se verifica la integridad de los datos a partir de los meta-datos almacenados en la cadena de bloques.
Una vez atendido el paciente, el colegiado actualiza la historia clínica y en blockchain se produce una transacción indicando el nuevo estado de ese historial. Adicionalmente, se notifica al resto de proveedores (autorizados por el paciente) de que ha ocurrido una actualización, con lo cual podrán descargar en sus sistemas la última versión de los datos clínicos.
Los beneficios aportados son considerables:

- Al existir una única versión de cada historial clínico, el cual es actualizado por diferentes especialistas de distintos centros sanitarios, se puede ofrecer una atención más precisa a los clientes, mejorando su calidad de vida y, potencialmente, representando una ventaja competitiva.
- La cadena de bloques puede funcionar como mecanismo para garantizar el cumplimiento de los proveedores con las normativas vigentes de protección de datos, ya que registra los permisos dados por los pacientes, así como el uso que se hace de los historiales clínicos.
- Los pacientes derivados desde sanidad pública a privada podrían transferir sus historiales con los proveedores privados de forma electrónica, automática y sencilla. Esto agiliza la compartición de los datos, lo cual permite atender a los pacientes en menor tiempo, mejorando así la calidad de la atención sanitaria.
- Al permitir disponer de un repositorio de datos médicos consistente, preciso y actualizado, esta aplicación podría ser la base sobre la cual asentar diversos servicios para mejorar aún más la atención sanitaria, como son inteligencia artificial que permita predecir las futura dolencias de un paciente a partir de su historial clínico, pagar mediante criptodivisas a las personas que aporten información anónima para la investigación de enfermedades, entre muchos otros.

Como se ha visto, blockchain promete ser el motor impulsor de una nueva revolución tecnológica en el paradigma del intercambio de valor. Gracias a la inmutabilidad, tolerancia a fallos y transparencia que la caracterizan, esta tecnología puede eliminar la necesidad de un tercero de confianza que vele por la seguridad de las transacciones, democratizar el control sobre la información e interconectar de forma transparente y segura redes de intercambio o repositorios de datos aislados, dando lugar así a una nueva etapa la gestión de la información y abriendo la puerta a infinidad de posibilidades.

Blockchain en Sanidad

Pablo Carretero Sánchez[1], Pedro de la Peña Tejeda[2], Aitor Moreno Fdz. de Leceta[3]
1. Head of Blockchain Strategy @Ibermática, Pedro de la Peña Tejeda.
2. Responsable técnico de los proyectos de I+D+i de @Ibermatica
3. Responsable área de Inteligencia Artificial en Ibermatica

BLOCKCHAIN ES UNA BASE DE DATOS DESCENTRALIZADA QUE ALMACENA REGISTROS DE ACTIVOS Y TRANSACCIONES EN UNA RED *PEER TO PEER*. ES COMO UN LIBRO PÚBLICO QUE COTEJA QUIÉN ES EL PROPIETARIO DE UN ACTIVO Y QUIÉN LO GESTIONA. LAS TRANSACCIONES Y SU DETALLE SON ALMACENADOS EN BLOQUES QUE MÁS TARDE SON ENCRIPTADOS MEDIANTE ALGORITMOS CRIPTOGRÁFICOS.

INTRODUCCIÓN

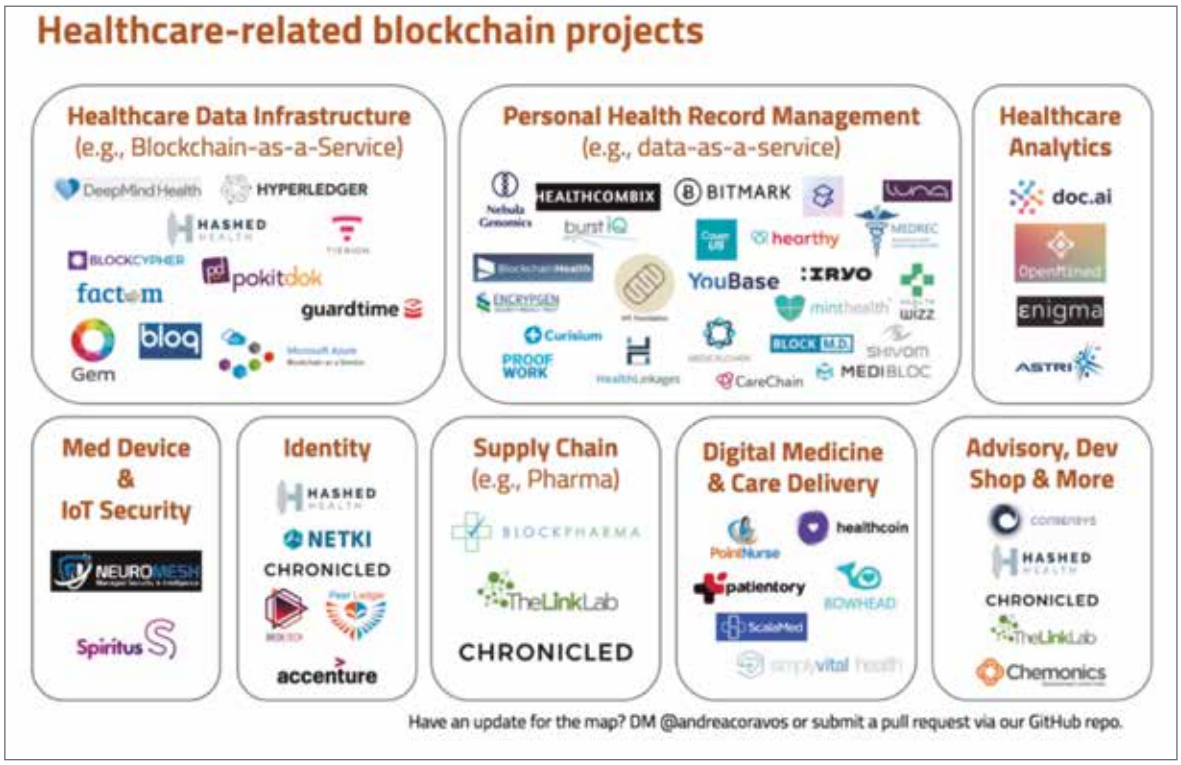
Así se construye un libro de registro con todas las transacciones de la red que permanece en el tiempo inalterable e infalsificable, y del que todos los nodos de la red tendrán una copia. En definitiva, Blockchain está permitiendo explorar nuevas formas de actuar sin intermediarios, nuevos modelos para intercambiar valor y mecanismos para tomar decisiones, y el sector sanitario ahora también se puede beneficiar de ello. El auge de las criptomonedas y de las IOC (Initial Coin Ofering) ha aflorado nuevos modelos de negocio y nuevas formas de operar en internet gracias a las principales características de la tecnología Blockchain:

- Seguridad: Utilización de protocolo criptográfico de llave pública y privada, haciéndola virtualmente inquebrantable.
- Transparencia: Cualquier miembro de la red puede consultar registros, sin posibilidad de modificarlos.
- Confianza: Una vez verificada una información (y registrada) permanece inmutable, reduciendo las posibilidades de fraude.
- Descentralización: El registro y verificación de transacciones se produce sin la intervención de terceros, fundamentándose en el consenso de los nodos.
- Economía: Se reducen costes operativos, al eliminar tareas de registro, control y distribución de datos.
- Escalabilidad: Ofrece una alta capacidad de reacción y respuesta sin comprometer la calidad del sistema ni interrumpir los intercambios de información.

Si bien es cierto que blockchain nació para el registro de transacciones bitcoin, todos los sectores e industrias están explorando blockchain en algunos de sus procesos de negocio: industria, transporte, salud y telcos son solo algunos ejemplos más maduros. Buscan en blockchain calidad, identidad y propiedad de la información.

ESTADO ACTUAL

Dentro de la salud se está comenzando a experimentar con las posibilidades y los distintos modelos de uso que finalmente adoptará esta tecnología: esto hace que en los últimos años se haya producido una eclosión de proyectos, que permiten superar alguna de las limitaciones en la creación de las actuales plataformas de HCE (Historia Clínica Electrónica), como por ejemplo la necesidad de crear una red de confianza de nodos conocidos, lo que obliga a codificaciones únicas y conocidas de pacientes entre todos los nodos, con el consecuente gasto en infraestructura al requerir desarrollos específicos para el intercambio entre cada par de nodos. Frente a esta situación, la capacidad de Blockchain de crear redes distribuidas, con toda la información en los distintos nodos y el uso de identificadores basados en claves públicas/privadas para la identificación de pacientes, permite una re-



https://blog.andreacoravos.com/where-are-the-healthcare-blockchains-8fcf6a3e28f8

ducción en el coste por transacción, a la vez que disminuye el coste asociado al intercambio de información. Blockchain también permite que frente a otra de las debilidades de la actual situación en la que información es provista únicamente desde las HCE del proveedor de servicios sanitarios y con unas reglas de acceso a la misma fijadas por el propio proveedor y opacas para el paciente que no puede saber quién y bajo qué circunstancias accede a sus datos. Frente a esto, Blockchain permite que la información sea accesible por el propio usuario, así como que la soberanía y la gestión de dicha información pertenezca al propio paciente, algo que hasta ahora parecía impensable permitiéndole establecer reglas de acceso claras y auditables basadas en contratos inteligentes, sobre quien accede a su información y bajo qué circunstancias lo hace. Tal y como se muestran en el siguiente grafico las iniciativas que se están dando en el entorno Blockchain salud, las podemos agrupar en 8 áreas (ver gráfco superior), que aprovechan las distintas posibilidades que ofrecen la tecnología: Entre las iniciativas que se han comenzado poner en marcha en los últimos años gracias a Blockchain están aquellas que, mediante el uso de "Smart Contracts" o "Contratos inteligentes" permiten automatizar bonificaciones en áreas como los hábitos saludables, como por ejemplo, horas de ejercicio semanales, o niveles de glucosa / colesterol entre limites, etc, Un ejemplo de esto es Healthcoin orientado a la prevención de la diabetes , obesidad y riesgo cardiaco, mediante la incentivación del paciente a seguir hábitos saludables ofreciéndole este incentivo en forma de una moneda virtual , en este caso Healthcoin. Otro área de que está suscitando especial interés, es la relacionada con la creación de plataformas de almacenamiento de datos médicos en Blockchain, donde existen múltiples iniciativas como CareChain, Block M.D. o Medibloc entre otras muchas, que permiten almacenar en una cadena única los datos provistos tanto por distintos proveedores de salud, como por el propio paciente, aprovechando las características de la tecnología, como por ejemplo, que la información no pueda ser eliminada ni modificada, gracias a la distribución de la información en distintos nodos, con control de acceso en manos del dueño de la información. Estas plataformas permiten empoderar al paciente en el control de sus datos de salud. Toda estos movimientos y las

posibilidades que ofrece la tecnología en el sector médico, han impulsado a que el Parlamento Europeo lanzase a mediados de febrero 2018 un borrador de Propuesta de Resolución sobre tecnologías de contabilidad distribuida instando a los Estados Miembro a la utilización y creación de cadenas distribuidas en los principales sectores estratégicos y haciendo especialmente hincapié en el sector la salud, donde propone "empoderar a los ciudadanos proporcionándoles la propiedad de sus propios datos".

También destaca este borrador, el potencial de estas tecnologías para mejorar la eficiencia de gestión los datos y los informes de ensayos clínicos. En este sentido el Parlamento Europeo considera que la tecnología BlockChain permite a los ciudadanos proteger y poseer sus datos de salud, incluido su uso por parte de las compañías de seguros.

En este sentido, pide a la Comisión que explore los casos de uso basados en BlockChain relacionados con la gestión de los sistemas de asistencia sanitaria. En esta situación hay países como Estonia, líder europeo en temas relacionados con ciudadanía digital y la ciberseguridad, ya llevan desde el año 2012 con una solución en esta área, siendo el primer país en registrar información de diversos ámbitos, entre ellos la salud, en esta tecnología.

EL FUTURO EN BLOCKCHAIN: IA & SEMÁNTICA & BLOCKCHAIN

Las ventajas de la aplicación de técnicas de Inteligencia Artificial como sistemas avanzados en la gestión del conocimiento, validación de evidencias, descubrimiento de indicios, así como la creación de sistemas de apoyo a la decisión en la eficiencia diagnóstica y terapéutica, está sobradamente demostrada con los cientos de "papers" que se publican diariamente al respecto. Y sin embargo, sigue existiendo un problema insalvable en la excelencia analítica, principalmente en el contexto de la salud: poder disponer de datos de calidad, desagregados y compartidos por todos los centros de salud a nivel mundial: hospitales, laboratorios, bancos de tejidos y centros de investigación. Los beneficios y la potencia de este escenario son inimaginables. Pero su logro no es un problema tecnológico. Ya existe la tecnología que permite compartir toda esta información de una manera abierta, plástica e inteligente (véase, como ejemplo, el paradigma de "LinkedData", ideada ya hace muchos años por los creadores de Internet.

El reto es superar un problema de confianza, confianza en la pertenencia de los datos, y en la responsabilidad de su consumo. Pero imaginen un sistema en el que la información se registra de forma distribuida, codificada, en un entorno global, en el que, a pesar de que existan distintas codificaciones (UMLS, Cie-9, CIE-10, Snomed, Hl7,...), ciertos agentes son capaces de negociar los contenidos llegando a acuerdos de codificación universales y estandarizados, y en el que la información que se mantiene es segura: sólo aquellos que tienen acceso a la misma pueden recuperar parte de dicho conocimiento, y no existen intermediarios entre los agentes. Aunaríamos el valor de la "Internet del Conocimiento" (web semántica), con la "Internet del Valor" (Blockchain), en el sueño de la mayoría de los investigadores, disponer del mayor nivel de conocimiento sobre el mayor número de pacientes y el mayor número de contextos médicos.

Blockchain, con sus propiedades en cuanto a la privacidad y a los contratos inteligentes, permitiría disponer de toda esa información resolviendo el problema de la interoperabilidad en una única plataforma. Pero extraer el conocimiento de esta ingente fuente de datos, de una forma segura y anónima, sólo se puede hacer de una manera, generando algoritmos de extracción inteligente (los actuales algoritmos de minería de datos), pero desde el interior de las cadenas de Blockchain.

De esta forma, los datos no saldría nunca fuera de la cadena, sólo suministraríamos a nuestros consumidores agregados, patrones y perfiles de pacientes, y las reglas de cuáles son las mejores terapias para cada perfil, de una forma agregada, y en forma de conclusiones, evidencias o indicios. Así, la empresa que consiga aplicar mejores algoritmos de pronóstico o de perfilado internamente sobre los datos de las cadenas, será la que más venda sus conclusiones a terceros, en un nuevo paradigma de "app store" del conocimiento más valor. Y este prometedor futuro sólo puede provenir de la unión de los tres grandes hitos de la nueva tecnología: la Inteligencia Artificial, l Semántica y el Blockchain.

La revolución en la gestión de los datos de salud

La transformación de los sistemas de salud genera muchos datos

Alberto Borrego
Everis Health

DURANTE LOS ÚLTIMOS AÑOS, ASISTIMOS A UNA TRANSFORMACIÓN INEXORABLE DE LOS SISTEMAS DE SALUD, DESDE PLANTEAMIENTOS REACTIVOS ORIENTADOS AL TRATAMIENTO DE LA ENFERMEDAD HACIA SISTEMAS QUE ACTÚAN DE FORMA PROACTIVA SIGUIENDO LOS DENOMINADOS PRINCIPIOS DE LA MEDICINA 4P: PREVENTIVA, PREDICTIVA, PERSONALIZADA Y PARTICIPATIVA.

En efecto, la prevención ha pasado a desempeñar un papel muy relevante asociado en buena medida a la importancia que el estilo de vida tiene en el desarrollo y pronóstico de muchas enfermedades. Por su parte, la medicina predictiva trata de identificar y cuantificar la susceptibilidad o la resistencia a determinadas enfermedades en el individuo sano, con frecuencia haciendo uso de información genética. Información que también utiliza la medicina personalizada de precisión, que busca proporcionar el tratamiento adecuado al paciente adecuado mediante el conocimiento de las características de sus genes, proteínas y entorno ambiental. Por último, la medicina participativa busca la involucración y participación del paciente y su entorno en la toma de decisiones relativas a su salud en un concepto que se ha denominado más globalmente como empoderamiento del paciente y que tiene profundas implicaciones en la superación del modelo paternalista en que se ha basado tradicionalmente la asistencia sanitaria.

Para situar adecuadamente la transformación de los sistemas de salud es necesario considerar también los grandes retos demográficos relativos fundamentalmente al envejecimiento y, como consecuencia, los cambios en el perfil epidemiológico y en la prevalencia de enfermedades crónicas, donde toma un papel cada vez más destacado, no sólo la esperanza de vida, sino la calidad de la misma. Todo esto conlleva un reto que aún no ha sido adecuadamente resuelto como es la necesaria convergencia de prestaciones y servicios sociosanitarios en lo que se ha denominado integración de cuidados.

Asimismo, es necesario tener en cuenta los grandes avances que las tecnologías, tanto conocidas como emergentes ponen a disposición del cuidado de la salud (imagen médica, medicina nuclear, nanotecnología, impresión 3D, inteligencia artificial, sensores, tecnologías móviles) y que suponen un reto en crecimiento exponencial, tanto desde el punto de vista de su gestión como tecnologías sanitarias, como por las implicaciones derivadas en el ámbito de las profesiones sanitarias.

Todos estos aspectos deben considerarse atendiendo a un elemento no menos relevante como es la sostenibilidad de los sistemas de salud; un sistema sanitario basado en la atención reactiva y paternalista a la enfermedad, y que hace uso indiscriminado de una tecnología cada vez más cara no será viable durante mucho tiempo, ni en términos económicos ni de calidad de vida. Por



Creativeart / Freepik

tanto, es necesario promover su transformación utilizando también las herramientas que la economía de la salud puede poner a nuestra disposición.

Por último, todos los ejes de la transformación de los sistemas de salud citados anteriormente tienen un elemento en común: producen y requieren para su correcto funcionamiento grandes cantidades de datos. Datos procedentes de múltiples fuentes y de diferente naturaleza, desde historias clínicas, o ficheros de secuenciación genética a imágenes médicas, bases de datos biológicas, datos procedentes de dispositivos de monitorización, datos sociodemográficos, o incluso de redes sociales. Datos que deben poder ser utilizados, analizados, intercambiados y visualizados de forma ágil para poder generar el conocimiento que permita dar respuesta a los retos que se plantean.

> ***La principal iniciativa en el ámbito de interoperabilidad sanitaria es el proyecto de Historia Clínica Digital del SNS valor"***

EL RETO DE LA INTEROPERABILIDAD SIGUE ABIERTO

La interoperabilidad entre los sistemas que utilizan información de salud es reconocida como uno de los aspectos clave para mejorar la efectividad y la eficiencia de los servicios que se ofrecen a los ciudadanos.

De este modo, en el marco de la Agenda Digital para Europa, la UE ha desarrollado la Estrategia Europea de Interoperabilidad y el Marco Europeo de Interoperabilidad con el objetivo de promover el desarrollo de la interoperabilidad y las normas asociadas a la misma. Específicamente en el ámbito sanitario, el *Plan de acción sobre la salud electrónica 2012-2020: atención sanitaria innovadora para el siglo XXI*, pretende alcanzar una mayor interoperabilidad en el ámbito de la salud electrónica, así como desarrollar la investigación y la innovación y favorecer la cooperación internacional en este ámbito.

Estos planes se han materializado en un conjunto de proyectos, de los que epSOS es quizá el más conocido, con el objetivo de mejorar la interoperabilidad de los sistemas de información en el sector sanitario, especialmente en lo relativo al acceso transfronterizo de la Historia Clínica



Creativeart / Freepik

Resumida (Patient Summary) y la receta electrónica (ePrescription). Sin embargo, proyectos piloto de este tipo aún no se han desplegado a escala europea.

A nivel nacional, la principal iniciativa en el ámbito de interoperabilidad sanitaria es el proyecto de Historia Clínica Digital del SNS (HCDSNS), iniciado en el año 2006 con el objetivo de favorecer el acceso de ciudadanos a su información clínica y que los profesionales tengan acceso a la información relevante de un paciente independientemente de la comunidad autónoma en la que se haya generado.

Asimismo, el proyecto de interoperabilidad de la Receta Electrónica en el Sistema Nacional de Salud (RESNS) establece un sistema de intercambio de información relativo a la receta electrónica que garantice la prestación farmacéutica a todos los ciudadanos en cualquier parte del territorio nacional.

A pesar de las evidentes ventajas, el desarrollo de estos proyectos ha permitido poner de manifiesto múltiples barreras de tipo legal, cultural, organizativo y operativo que han dificultado su puesta en marcha a lo largo de los años y que es necesario superar para hacer efectiva la interoperabilidad de la información en salud. En este sentido cabe añadir que un reciente estudio de la Fundación IDIS revela que la situación de la interoperabilidad sanitaria en España es considerada mala o muy mala por el 69% de los expertos consultados.

Si a estas barreras añadimos la complejidad de un entorno real mucho más dinámico en el que una parte significativa de la información no procede de los servicios públicos de salud sino de prestadores privados, o de compañías de seguros, o de farmacias, o de dispositivos de monitorización, o de secuenciación genética o de redes sociales, enseguida comprendemos que el reto de la interoperabilidad en salud bajo los modelos actuales se transforma en una auténtica quimera.

Cabe señalar en este punto que ya el citado estudio de la Fundación IDIS apunta hacia la necesidad de establecer un nuevo paradigma de interoperabilidad en el que el ciudadano sea el principal actor a nivel organizativo.

BLOCKCHAIN COMO HERRAMIENTA PARA EMPODERAR AL CIUDADANO EN LA GESTIÓN DE SUS DATOS DE SALUD

Es generalmente conocido que blockchain o cadena de bloques es una base de datos distribuida que registra transacciones de forma segura, confiable e irreversible. La tecnología blockchain nació ligada a *bitcoin* y las criptomonedas, por lo que las primeras aplicaciones surgieron en el ámbito del registro de transacciones contables y financieras.

Sin embargo, las implicaciones derivadas del establecimiento de un marco de confianza para las transacciones en la era digital sin necesidad de intermediarios han provocado que todos los sectores socioeconómicos estén buscando casos de aplicación y analizando la posibilidad

de implementar blockchain en sus modelos de negocio. Es oportuno señalar en este punto que blockchain nace con la vocación de hacer innecesarios los gigantescos intermediarios digitales que han surgido con la primera generación de comercio electrónico durante los últimos 20 años, en gran medida debido a la necesidad de generar confianza en las transacciones.

Tal y como recoge Deloitte en su estudio *Blockchain: opportunities for healthcare,* el sector de la salud no es ajeno a esta tendencia y ha identificado un gran potencial en diferentes ámbitos, pero especialmente en el establecimiento de un marco común para facilitar la interoperabilidad de datos de salud. Datos que, como indica Curaesalud en su *Guía de blockchain* para el sector de la salud, pueden hacer referencia entre otras fuentes a la historia clínica de los pacientes, la información generada en ensayos clínicos, los datos genómicos, la información procedente de dispositivos conectados (*Internet of Healthcare Things*), los procesos de reclamación y pago de servicios sanitarios o la cadena de suministro de medicamentos, entre otros.

Es conveniente señalar que blockchain es un registro de transacciones y, por tanto, no está pensado para sustituir las bases de datos ni los sistemas corporativos de registro de información clínica. En todo caso, como capa de transacciones puede almacenar información de dos formas, directamente en la cadena de bloques (on-chain) o registrando de forma segura e irrefutable enlaces a la información almacenada en repositorios externos tradicionales (off-chain).

El almacén de información médica directamente en la cadena asegura todas las propiedades y capacidades de blockchain en cuanto a seguridad de la información y es inmediatamente accesible para todos los usuarios con permiso, pero al mismo tiempo ralentiza la velocidad de procesamiento de los bloques y presenta problemas de escalado.

Por el contrario, los enlaces encriptados ocupan un tamaño mínimo y pueden activarse cuando un usuario con la clave privada adecuada accede a los mismos, facilitando entonces el acceso al repositorio externo que contiene la información; sin embargo, este planteamiento reduce algunas ventajas potenciales blockchain como el acceso inmediato a la información y requiere el desarrollo de microservicios y capas adicionales de interoperabilidad con los sistemas origen.

La mayor parte de casos de uso propuestos hasta la fecha (p.ej. MedRec) están basados en soluciones *off-chain* que incorporan un conjunto específico de datos basados en estándares almacenados en la cadena de bloques. Las transacciones en los bloques corresponden a cada una de las interacciones de la persona con un prestador de servicios o, en general, con un sistema reconocido y capaz de registrar datos de salud e incorporar al blockchain un enlace encriptado de acceso a los mismos con la correspondiente huella digital y sellado de tiempo. De este modo, blockchain actúa realmente como un control de acceso a toda la información de salud de una persona y ofrece una alternativa al problema de la interoperabilidad de datos de salud.

En relación con la seguridad de la información, una cadena de bloques interoperable puede ayudar a reforzar la integridad de los datos de salud, reduciendo vulnerabilidades y preservando al mismo tiempo la identidad digital de los pacientes, gracias a sus características como el acceso mediante criptografía asimétrica, los datos distribuidos o los algoritmos de consenso basados en prueba de trabajo. En concreto, es posible que los pacientes puedan compartir su información personal a diferentes niveles en función de las necesidades de cada organización, reduciendo de este modo la necesidad de almacenar información personal en múltiples sistemas.

Pero independientemente del detalle de la solución técnica, el aspecto más relevante y poderoso de este planteamiento es el revolucionario papel que asigna al ciudadano que, de esta forma, tendría acceso total y control sobre sus datos de salud así como capacidad para decidir cómo y con quién compartirlos. Asimismo, podría disponer de capacidades de auditoría para saber quién y cuándo ha accedido a su información.

DESAFÍOS PARA LA IMPLANTACIÓN DE BLOCKCHAIN EN EL SECTOR SALUD

A pesar de las oportunidades que ofrece para el sector salud y de las enormes expectativas generadas durante los últimos años la revolución aún se ve lejos. La tecnología blockchain carece aún de la madurez suficiente y deberá superar

Blockchain en el ámbito de la Sanidad

Roberto Fernández Hergueta
Global Head de Blockchain. Everis

BLOCKCHAIN ES UNA FILOSOFÍA/TECNOLOGÍA EMERGENTE QUE PUEDE ACELERAR, EN EL CONTEXTO ACTUAL, LA NECESIDAD DE TRANSFORMACIÓN DEL SECTOR SANITARIO. EL SECTOR SANITARIO HA LANZADO MÚLTIPLES INICIATIVAS ORIENTADAS A LA DIGITALIZACIÓN (TECNIFICACIÓN DE LOS PROCESOS DE NEGOCIO) PERO ES HORA DE TRANSFORMAR (REPENSAR, REINVENTAR LOS CITADOS PROCESOS).

Esto implicará una redefinición de gran parte de la operativa y variar el concepto actual de generación del valor, incrementando sustancialmente la eficiencia de los procesos y la creación de nuevas formas de prestación de los servicios, implicando a todos los actores involucrados.

Para facilitar la identificación de casos de uso y aplicaciones prácticas de los nuevos modelos descentralizados en la Sanidad, es necesario tener presente las siguientes cuestiones:

1. **Blockchain presenta una serie de características inherentes:** transparencia, inmutabilidad, trazabilidad, integridad, seguridad, simplicidad y acceso rápido a la información.
2. **Toda iniciativa que se puede llevar a cabo en Blockchain puede implementarse con las tecnologías actuales.**
   ¿Cuándo tiene sentido Blockchain?
   En aquellos procesos end to end, con falta de transparencia, un número elevado de participantes y un alto componente de tareas manuales y documentación asociada, la redefinición de los procesos vía tecnología Blockchain supone, frente a las soluciones actuales, un ahorro de costes por tratarse de iniciativas que requieren menor esfuerzo y tiempo asociado.
3. **Blockchain habilita un nuevo escenario de internet.** Permite el intercambio de valor de forma digital y descentralizada, sin necesidad de una entidad central de confianza que imponga su criterio a los participantes, con un añadido: el valor es programable, gracias al uso de los contratos inteligentes.

Todo activo de una compañía puede disponer de un gemelo digital, es decir, una representación digital (token). Tokenizar es representar en blockchain la propiedad de un bien mediante un código criptográfico.

Blockchain, una oportunidad de reinventar la Sanidad

Habilitar una plataforma blockchain permitirá la interoperación de todos los actores de la cadena de valor con ahorro de costes y agilizando la gestión de la información, proporcionando mejoras sustanciales en los servicios e incrementando, por tanto, la experiencia de los pacientes.

Adicionalmente, la tokenización de los diferentes documentos (informes médicos, historial clínico, etc.) y el registro de los mismos en la cadena de bloques permitirá la optimización de los procesos de negocio.

Identidad digital:

Como pacientes no tenemos ningún control sobre nuestros datos. Nuestros datos radican en múltiples repositorios de diferentes compañías y/o organizaciones, a modo de silos.

Blockchain, a través del concepto de identi-

dad digital soberana (self-sovereign identity), busca solucionar esta cuestión empoderando al paciente y devolviendo el control de sus datos al mismo, mediante la tokenización de los atributos de la identidad digital. El sistema se basa en "claims" y certificados emitidos por diferentes atestadores. Estos modelos facilitaran incluso la cesión anónima de datos médicos para estudios y análisis.

Trazabilidad de medicamentos

La capacidad de Blockchain permite disponer de un seguimiento fiable de activos sensibles en el ámbito de la Sanidad, evitando fraudes y permitiendo detectar inicidencias.

Tratamiento de la información

Blockchain facilitará la gestión de la información y las transacciones entre los diferentes stakeholders (pacientes, médicos, hospitales) mediante la tokenización de archivos, registros médicos y acuerdos, lo cual conllevará una eficiencia de los procesos de negocio.

Adicionalmente, esta tecnología permite la tokenización de los atributos de los registros médicos favoreciendo la creación del historial clínico y una visión única de información para los pacientes.

Registros de salud integrales e interoperables. La mayor seguridad y capacidad para establecer la confianza entre las entidades son dos razones por las que esta tecnología puede ayudar a resolver el problema de interoperabilidad mejor que las tecnologías actuales.

Respaldar los imperativos administrativos y estratégicos con contratos inteligentes. Blockchain podría recopilar automáticamente registros de acuerdos, transacciones y otros conjuntos de información valiosa, luego unir la información y actuar sobre los datos mediante contratos inteligentes.

Es tiempo de aprender la nueva realidad del mundo descentralizado, de empezar a equivocarse, de asumir riesgos para hallar el rol de la Sanidad en la nueva sociedad del valor.

> ***"Blockchain actúa realmente como un control de acceso a toda la información de salud de una persona y ofrece una alternativa al problema de la interoperabilidad de datos de salud"***

múltiples pruebas antes de poder ser aplicada de manera generalizada como alternativa para el intercambio de información de salud.

Por una parte, aparecen cuestiones organizativas y culturales asociadas al establecimiento de nuevos roles y responsabilidades que es necesario calibrar y dimensionar. Por otra parte, características intrínsecas de blockchain como el hecho de tratarse de un sistema distribuido genera dudas sobre los aspectos legales de la solución relativos a responsabilidad o subsidiariedad en caso de fallo o fraude.

Pero las principales dudas surgen desde el punto de vista tecnológico y hacen referencia a aspectos como la escalabilidad de los procesos de verificación, la velocidad de las transacciones o el propio límite de datos que puede gestionar una cadena.

Por otra parte, el consumo energético ineficiente en que se basan los métodos de prueba por trabajo acabará también siendo un problema que afectará a la escalabilidad de la solución.

No obstante, parece que casos como el de Estonia, el país "nativo digital", que apoya su infraestructura de identificación ciudadana en tecnología blockchain para permitir el acceso a la información clínica almacenada en bases de datos tradicionales puede ofrecer un punto de partida prometedor.

También podemos citar el caso del gobierno de Dubai que en el ámbito de la iniciativa Smart Dubai aspira a convertirse en el primer gobierno digital soportado por tecnología blockchain en el año 2020 y que en el ámbito de la salud pondrá en marcha una prueba de integridad de datos, seguridad y confianza el intercambio de registros digitales entre los diversos proveedores de salud.

En todo caso será cuestión de tiempo, según el modelo del Hype Cycle de Gartner, en aproximadamente 5 años seremos capaces de tener una idea clara de hasta dónde nos puede llevar realmente la revolución blockchain en la gestión de los datos de salud.

Blockchain: Cambiando los modelos de relación y confianza

Diego Rodríguez Roldán
Director del Centro de Innovación de Risk Advisory de Deloitte.

LA APARICIÓN DE LA TECNOLOGÍA BLOCKCHAIN ES PROBABLEMENTE EL CAMBIO TECNOLÓGICO MÁS DISRUPTIVO QUE HA OCURRIDO EN LOS ÚLTIMOS AÑOS. PERO, ¿POR QUÉ ESTÁ TENIENDO UN IMPACTO MEDIÁTICO TAN IMPORTANTE? LA RAZÓN ES QUE LO REALMENTE DISRUPTIVO NO ES LA TECNOLOGÍA BLOCKCHAIN EN SI MISMA SINO LAS IMPLICACIONES QUE ESTA TECNOLOGÍA TIENE EN LA FORMA EN LA QUE LAS PERSONAS SE RELACIONAN Y CONFÍAN ENTRE SÍ.

Blockchain soluciona uno de los grandes problemas a la hora de interactuar entre nosotros, de forma muy resumida, que no nos fiamos entre nosotros.

Es por esa necesidad o falta de confianza que cada vez que realizamos transacciones importantes, utilizamos intermediarios que nos aporten la tranquilidad que necesitamos.

- Cuando compramos o vendemos una vivienda, lo anotamos en el registro de la propiedad para tener la confianza de que nadie podrá dudar que es nuestra en el futuro.
- Cuando transferimos cantidades importantes de dinero lo hacemos a través de entidades financieras donde queden registradas sin lugar a duda esas transferencias.
- Cuando estamos en desacuerdo sobre el cumplimiento de las condiciones de un contrato, recurrimos a la justicia
- Cuando inventamos algo lo registramos en la oficina de patentes para que nadie pueda reclamar su propiedad en nuestro lugar, al igual que hacemos cuando desarrollamos una nueva vacuna, o medicamento, etc.

Y eso es exactamente lo que ha venido a cambiar la tecnología blockchain: la confianza sin la necesidad de un intermediario, a través de un sistema que permite registrar cualquier información directamente en una archivo compartido entre varios usuarios con la tranquilidad de saber que esta anotación es legítima y la confianza de que ninguno de estos usuarios podrá cambiar esa anotación en el futuro.

Si bien hasta aquí blockchain no parece mucho más que un nuevo registro más o menos novedoso, lo que lo hace completamente distinto a los demás es que en blockchain no existen servidores ni registros centrales que aporten la confianza que necesitamos, sólo existen los propios miembros o "nodos" de la red conectados entre sí, y son precisamente estos nodos de la red los que se aportan confianza recíprocamente.

De forma muy simplificada, la legitimidad de cada anotación en el archivo es validada por consenso entre los nodos de la red sin que intervenga ningún registro central y, una vez validadas, las anotaciones se consolidan en blockchain mediante mecanismos de cifrado en cadena que hacen que ninguno de los nodos pueda ya cambiar esta anotación en el futuro.

Pero el modelo descentralizado de confianza que propone blockchain va más allá del simple registro de datos y hoy está muy centrado en el registro de procesos mediante la publicación de programas informáticos denominados "smart-contracts" que serán inalterables una vez publi-

cados en la red y que al ejecutarse contarán con el consenso de la red respecto a los resultados de esa ejecución.

¿PERO ES ESTE MODELO SUFICIENTEMENTE SEGURO?

El caso estrella de la tecnología blockchain es Bitcoin

Bitcoin es sencillamente un registro descentralizado y automático de la propiedad de un token (poco más que un número) absolutamente digital, el "Bitcoin".

Lo único que existe en bitcoin es un archivo compartido entre los nodos de la red en el que están anotadas todas las transacciones realizadas con estos tokens y en el que por consenso automático de los nodos de la red se valida la legitimidad de cada nueva transacción con la confianza de que, una vez registrada, esta transacción no podrá ya nunca ser alterada por ninguno de los nodos. Sin servidores, sin registros centrales, sólo nodos iguales entre si conectados en una red blockchain dándose confianza entre ellos. ¿Es fiable el sistema? Esperemos que sí, el valor de los tokens anotados en este archivo hoy es equivalente al producto interior bruto de un país como Panamá.

En resumen, blockchain es un registro descentralizado, pero, ¿por qué esto es tan disruptivo?

Porque más allá de la tecnología, o mejor dicho gracias a ella, blockchain cambiará transcendentemente la forma en la que confiaremos unos en otros. Con blockchain ya no es necesario disponer de autoridades o registros centrales que den confianza a los usuarios ya que los propios usuarios se dan confianza entre ellos por consenso. Y tampoco son por tanto necesarios los a veces complicados y lentos procesos que requiere interactuar con estos registros. La red valida de forma online y casi inmediata las nuevas anotaciones a la vez que cualquier nodo puede validar de forma autónoma la validez de las anotaciones históricas.

Centrándonos ya más en el mundo de la Salud, la tecnología Blockchain resulta de especial utilidad en situaciones en las que es necesario registrar o compartir información con terceros, tal vez desconocidos, con los que no tiene por qué existir una confianza previa. Y además permite colaborar y compartir información de forma inmediata, transparente, segura y auditable. Cuando pensamos en cómo podría mejorar blockchain la salud, nos vienen a la cabeza innumerables aplicaciones.

Blockchain puede ser un gran aliado para la gestión de los historiales de los pacientes por la protección que aporta contra la manipulación de los datos históricos o la pérdida de estos garantizando su fiabilidad. Al ser un sistema sencillo, fiable e inalterable, blockchain es el repositorio perfecto para almacenar toda la información de un paciente con independencia de la fuente, pero garantizando la procedencia de los datos.

Con blockchain, los datos no se almacenan en los sistemas de un determinado hospital o médico, sino en la propia red con mecanismos de cifrado adicionales que permitan al usuario decidir con quién quiere compartir su historial, pero con la garantía de que los datos permanecen inalterables y son trazables desde su inclusión en el historial.

Al ser un sistema de registro sencillo y online, esta información puede contener diagnósticos y tratamientos registrados por los médicos, síntomas registrados por el paciente o por sensores y dispositivos médicos específicos o información de vacunación y alergias. De esta manera, durante una atención de urgencia en la que sea necesario consultar, por ejemplo, si está vacunado del tétanos, el paciente podrá permitir que el centro médico haga la consulta. De manera análoga se podrá consultar si es alérgico a un medicamento antes de practicarle un tratamiento ante una emergencia y así evitar consecuencias mayores.

Por último el sistema añade transparencia al proceso mediante el registro del acceso a la información, para garantizar el cumplimiento legal.

Otro ámbito de aplicación interesante es la investigación, donde blockchain permite que los investigadores puedan compartir (y registrar) resultados de los estudios practicados, sin necesidad de esperar a que sean publicados en congresos o revistas, y sin peligro que otro pueda atribuirse la autoría. En este caso blockchain



Onlyyouqj / Freepik

permite demostrar sin lugar a duda quién es el autor original de la información y cuándo fue publicada.

Cambiando radicalmente de ámbito, desde la perspectiva más económica, será posible codificar programas en blockchain que calculen las prestaciones a que tienen derecho los pacientes mediante la aplicación de baremos, sin necesidad de intervención humana y con la garantía de un cálculo transparente, predefinido y aceptado por todas las partes.

Pero más allá de los anteriores casos de uso, y reconociendo que en estos momentos nos podemos encontrar aún en la fase hype de adopción de esta tecnología, la tecnología blockchain ofrece una capacidad de disrupción tal que exigirá a las Organizaciones plantearse las siguientes cuestiones:

- ¿Qué nuevos procesos podemos acelerar cubriendo las necesidades de registro mediante un registro online automático y por consenso de la propia red basado en blockchain?
- ¿Qué procesos actuales podemos hacer más eficientes cambiando los sistemas de registro actual por otros con menos necesidades de desarrollo, mantenimiento y vigilancia basados en blockchain?
- Y la más interesante, ¿Qué procesos que eran inviables en un modelo de registro tradicional se pueden desarrollar usando blockchain como registro de confianza rápido, fácil, descentralizado, anónimo y transparente?

Para responder a este tipo de cuestiones, desde el Centro de Innovación de Risk Advisory de Deloitte se ha creado y probado una metodología propia (Blockstorm), para ayudar a las Organizaciones a entender las posibilidades que ofrece la tecnología de blockchain e identificar y evaluar posibles casos de uso con los que resolver alguna de las preguntas anteriores.

Mediante un enfoque gamificado en el que participan diferentes equipos de trabajo multidisciplinares, esta metodología permite abstraer a los equipos participantes de los aspectos técnicos que subyacen a la tecnología blockchain, facilitando la identificación de estos posibles casos de uso.

De este modo, prácticamente en cada sesión de Blockstorm que se realiza, se identifican nuevos casos de uso totalmente disruptivos en todo tipo de organizaciones y en todo tipo de procesos.

En resumen, más allá de las criptomonedas, la tecnología blockchain está ya disponible y ofrece un universo de posibilidades esperando a ser descubierto, también en el sector sanitario.

Blockchain, más allá de la tecnología

Alex Puig
Founder de Alastria y CTO de Caelum Labs

LAS IMPLICACIONES DE LA DESCENTRALIZACIÓN. ES NECESARIO UN ESTUDIO DETALLADO DEL FENÓMENO BLOCKCHAIN PARA TENER UNA VISIÓN HOLÍSTICA DEL PROCESO QUE NOS HA LLEVADO HASTA AQUÍ Y ASÍ PODER ENTENDER EL CAMBIO REAL QUE SE ESTÁ PRODUCIENDO. ESTO NO VA DE BLOCKCHAIN, O NO SÓLO DE BLOCKCHAIN VA DE OPEN SOURCE, CRIPTOGRAFÍA, ARQUITECTURAS DESCENTRALIZADAS Y RESPONSABILIDAD PERSONAL.

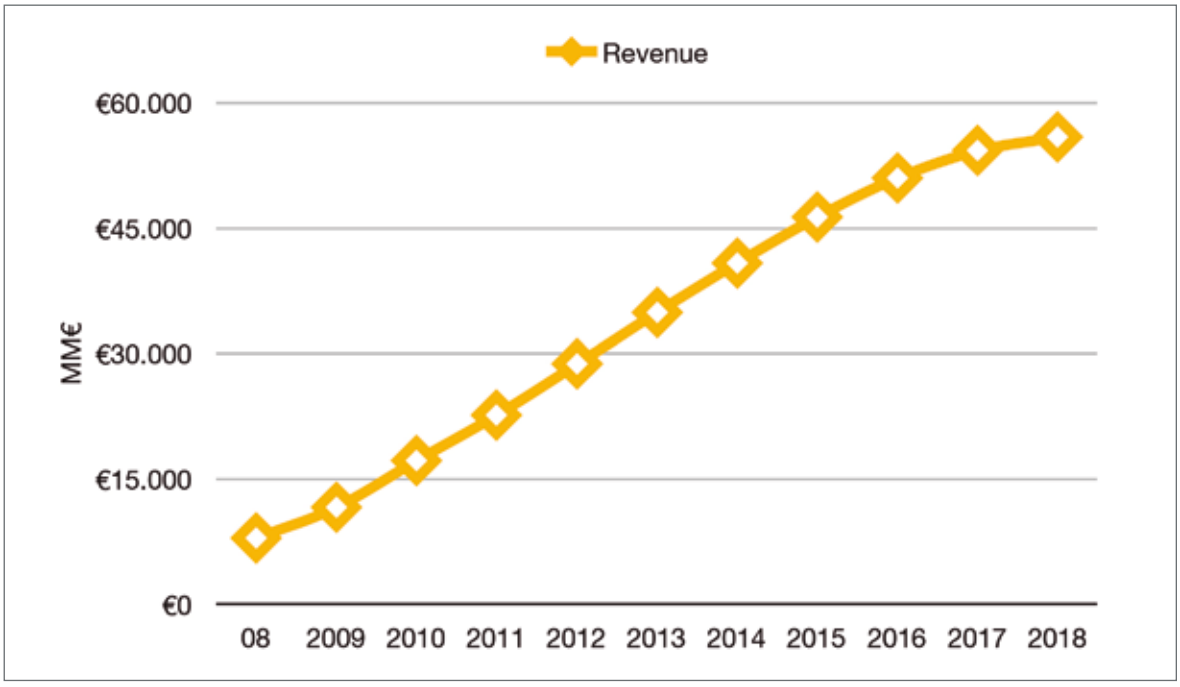
OPEN SOURCE

Compartir la información ha sido una parte esencial de la evolución de la cultura humana. Matemáticas, Ciencia, Filosofía se ha compartido permitiendo la mejora de herramientas, técnicas de agricultura, medicina… El contrario viene a ser la "propiedad intelectual", representada por la idea de que el conocimiento debe ser monetizado y protegido (cerrado).

Una empresa farmacéutica investiga sobre un determinado componente, y es capaz con los resultados obtenidos de producir un medicamento que, a un precio determinado, puede ayudar a mucha gente. Invierte en investigación y protege los resultados de la misma.

Imaginemos por un momento que toda investigación sobre nuevos medicamentos fuera abierta, permitiendo la colaboración de los científicos de todo el mundo y el análisis de los resultados (éxitos y fracasos). Probablemente los avances en medicina serían exponenciales y el coste de la investigación (al ser colaborativo) sería mucho menor.

Aunque pueda sonar muy ingenuo, este es el principio que está revolucionando el sector de las TICs en los últimos años, principalmente



desde 2008. En tecnología se separa el modelo de negocio de la empresa (el entregable, la aplicación, el servicio) de las herramientas básicas que la empresa necesita para ello. Dichas herramientas se están desarrollando colaborativamente por programadores de todo el mundo, que se aprovechan de este conocimiento compartido pero que a su vez devuelven a la comunidad las mejoras hechas al mismo.
El software utilizado en Blockchain es mayoritariamente de Código Abierto, lo que ha permitido la rápida evolución del mismo manteniendo altos niveles de seguridad. Es más, las aplicaciones desarrolladas sobre Blockchain son también de código abierto. Un Smart Contract por defecto se instala en todos los nodos de una red Blockchain, por lo que todo programa descentralizado instalado en una red pública para a ser visible por todos.
En el caso de Blockchain el Código Abierto ha propiciado un ecosistema de innovación abierto en el cual constantemente se generan y comparten nuevas ideas. Estamos viendo tan sólo la punta del Iceberg mientras miles de programadores empiezan a abrazar Open Source como filosofía de trabajo.

CRIPTOGRAFÍA

Otro de los secretos tras el éxito de Blockchain ha sido la entrada en escena de la criptografía. Vista hasta ahora como algo extremadamente complicado (que lo es) y exclusivo para uso de especialistas y genios matemáticos (que no).
El hecho que no entendamos algo, o mejor dicho, que no entendamos como funciona, no debería limitar a nadie para hacer el esfuerzo de entender para que sirve y cuales son sus aplicaciones prácticas. La mayoría de las aplicaciones de Internet de hoy en día están siendo pensadas y diseñadas desde negocio pensando en el servicio que quieren ofrecer, no en la base tecnológica y como funciona.
Gracias al auge de Blockchain y de su uso de la criptografía son cada día más las personas que entienden las aplicaciones que esta tiene. Un ejemplo claro de ello es Zero Knowledge Proof, la base criptográfica que permite transacciones privadas dentro de una red pública. La capacidad de realizar operaciones sobre información encriptada tiene el potencial para abrir las colaboraciones entre empresas, aparentemente competidoras, a un nivel nunca visto hasta ahora.

DESCENTRALIZACIÓN

Es quizás el elemento olvidado en Blockchain, y por experiencia, el cambio de paradigma que más cuesta asimilar. Hemos estado trabajando en sistemas centralizados mucho tiempo, sistemas en los cuales teníamos el control absoluto (y la responsabilidad absoluta si algo fallaba).
Cada día interactuamos con empresas que nos ofrecen un servicio de custodia (dinero, información, productos digitales…). Por ejemplo, operamos con normalidad con el banco, el cual es responsable de cuidar de nuestro dinero, pero si yo quiero interactuar con los assets que el banco guarda para mi (Euros), no tengo manera de hacerlo. No puedo desarrollar un programa y pedirle al banco que lo instale en sus servidores. Y es lógico, las implicaciones de seguridad serían enormes y el banco nunca lo permitiría.
En un sistema descentralizado, donde estos assets están representados en una red pública yo sí puedo programar mi interacción con ellos mediante Smart Contracts. Como usuario gano flexibildad en la interacción con mis propiedades sin perder en seguridad.

Johnston's Law
"Everything that can be decentralized will be decentralized"

Cuando se habla de redes descentralizadas se tiende a pensar en una gran red publica como Bitcoin o Ethereum. Es importante entender la diferencia entre pública y privada, o siendo más correctos, redes permisionadas o no permisionadas. No es correcto comparar una red abierta a una sitio web y una red cerrada a una intranet.
Una red no permisionada corresponde a un sistema donde no hay que pedir permiso ni darse de alta para operar. Bitcoin y Ethereum, por ejemplo, son redes en las que tan sólo tienes que bajarte el código desde el repositorio público, ejecutarlo y automáticamente entras a formar parte de la red. También se las conoce como redes abiertas.
Las redes permisionadas por otro lado, pueden seguir siendo abiertas, pero para formar parte del sistema tienes que pedir permiso al mismo. De hecho tienes que pedir permiso a toda la red de forma democrática. Una red cerrada (y permisionada por defecto) sería un consorcio de

	No Permisionada	Permisionada
Pública	Bitcoin & Ethereum	Alastria
	- Seguridad muy alta - Precio por tx alto - Pocas tx por segundo - Muchos participantes - No regulada - Gran comunidad de desarrolladores - P2P & B2C - Alta transparencia	- Seguridad alta - Precio por tx muy bajo - Muchas tx por segundo - Muchos participantes - Regulada - Gran comunidad de desarrolladores - P2P & B2B & B2C - Alta Transparencia
	X	Hyperledger
Cerrada		- Seguridad alta - Precio por tx muy bajo - Muchas tx por segundo - Pocos participantes - B2B & BTC - Opaco

Esquema de las ventajas e inconvenientes de los distintos tipos de redes

empresas que instalan una red Blockchain compartida sólo por ellos.
En España, hemos desarrollado Alastria, una red nacional pública permisionada. Está abierta a todo el mundo pero sólo los socios pueden tener nodos de aplicaciones. Es en realidad una asociación sin ánimo de lucro con la misión de construir un Blockchain público de alcance nacional. Además, el hecho de tener carácter nacional nos permite adecuar la tecnología a la regulación vigente de España.

RESPONSABILIDAD PERSONAL

La consecuencia directa de la descentralización, lógicamente, es el reparto de poder y el movimiento de la toma de decisiones desde el centro (empresas) hasta los nodos periféricos (usuarios). Pero, ¿estamos preparados para ello?
Con Bitcoin descubrimos que era posible crear un sistema financiero alternativo colaborativo, pero el precio a pagar era alto, ya que el papel de custodio, que tradicionalmente cubren los bancos, pasa a manos del usuario final. Nosotros nos erigimos en custodio de nuestras propiedades digitales (nuestros Bitcoins).
Si olvidamos el pin para operar con nuestra tarjeta de crédito tan sólo tenemos que acercarnos a una oficina y pedir que lo cambien por otro. Es práctico y seguro, y el usuario no es responsable de la custodia de nuestra riqueza.
En Bitcoin, en lugar de pin, tenemos una clave privada, que nos da acceso a nuestra criptomonedas, pero a diferencia del sistema tradicional, si yo pierdo esta clave, voy a perder mis bitcoin para siempre y no podré recuperarlos. No hay red de seguridad.
Y no estamos hablando sólo de dinero. Nos estamos moviendo paulatinamente a una identidad soberana (self sovereign identity) en la que cada ciudadano debe hacerse responsable de sus propios datos. Nuestra identidad digital, en manos ahora de empresas como Facebook o Google, podrían por primera vez estar bajo nuestro control. Es una gran responsabilidad para la cual quizás no estemos preparados todavía.
Pero si superamos el miedo inicial, con la ayuda de la tecnología (open source, criptografía y descentralización) y gracias a brillantes emprendedores que están trabajando en identidda digital soberana en todo el mundo, tenemos la capacidad para devolver al ciudadano lo que ya se conoce como oro digital, y no es dinero, es información.

El impacto de la tecnología Blockchain en Sanidad

Juan Carlos Sánchez Rosado
Director de Salud en IBM España

¿ES ÚTIL TENER EL HISTORIAL SANITARIO COMPLETO DE UN PACIENTE? ¿QUÉ VENTAJAS APORTARÍA TENER DE FORMA CONJUNTA Y QUE SE PUDIERA CONSULTAR RÁPIDAMENTE LA INFORMACIÓN DISPONIBLE ASOCIADA AL CUIDADO DE LA SALUD DE UNA PERSONA (VISITAS, DIAGNÓSTICOS, PRUEBAS, TRATAMIENTOS, INTERVENCIONES, ETC)?

Si consiguiéramos tener todos estos datos juntos y accesibles de manera segura por el personal adecuado, podría aumentar la calidad y la coordinación de la atención sanitaria, las posibilidades de utilizar datos anonimizados para impulsar la investigación biomédica, los costes y riesgos asociados a no tener estos datos podrían disminuir y los pacientes tendrían más control y acceso a su propia información a través de un consentimiento verificable.

Y estas son razones de peso por las cuales la tecnología Blockchain podría ser de gran ayuda en la industria de la salud. Veamos cómo: los datos de un paciente se podrían compartir en una cadena de bloques (blockchain) en tiempo real a través de un grupo de individuos e instituciones que estuvieran dados de alta en dicho proceso con sus pertinentes autorizaciones. Cada evento o transacción tendría un sello de tiempo y se convertiría en parte de una cadena o registro permanente, que sería inmutable una vez realizado. En esta cadena, la privacidad se puede llevar a cabo mediante un acuerdo sobre qué partes pueden ver qué transacciones y dónde, enmascarando la identidad de la parte allí donde sea necesario. De esta forma, las cadenas de bloques desplazarían a los sistemas dónde la información se mantiene bajo la custodia de un único propietario, ya sean historiales médicos, registro de recetas, pruebas diagnósticas, etc.

Un área de especial interés son los datos de dispositivos médicos. Si los registros médicos ya se consideran el epicentro de la transformación, los datos de los médicos dispositivos podrían ser la próxima frontera, que hasta ahora se mantiene difícil de alcanzar. Según el informe 'Healthcare rallies for blockchain', en el cuidado de la salud, solo el 10 por ciento de los datos cubre factores clínicos. Un 60 por ciento se compone de factores exógenos al entorno clínico, como nutrición, hábitos de conducta y ejercicio físico. Este torrente de datos, recopilados por dispositivos portátiles, se está ya transmitiendo a la nube y a nuestros teléfonos inteligentes. Pero muchos de estos datos de salud generados por el paciente rara vez aterrizan en manos de un médico, y a veces ni siquiera llegan al paciente. Incluso los datos generados que sí llegan a los médicos generalmente no se almacenan en ningún sitio.

A pesar de las dificultades existen ya iniciativas de basadas en Blockchain para integrar, almacenar y consultar datos de dispositivos, como patrones de sueño, glucosa y frecuencia cardíaca combinados con información de visitas al médico, registros de salud, etc. pero habrá que superar importantes obstáculos. Al igual que los registros médicos, utilizar y confiar en estos datos depende de una robusta y homogénea gestión de la identidad, incluida la identidad de los dispositivos mismos. En casos donde los datos son menos precisos, como cuando se cuenta el número de pasos o un dispositivo funciona mal, las organizaciones necesitarán establecer nuevos protocolos y algoritmos para separar los datos correctos de los erróneos.

Otro ejemplo son los ensayos clínicos, que generan montañas de datos, y requieren del mantenimiento de registros de resultados, para permitir la revisión y validación por otros investigadores y apoyar el cumplimiento regulatorio. La tecnología Blockchain, en concierto con los sistemas de captura electrónica de datos (EDC), podría ser diseñadas para agregar, replicar y distribuir automáticamente los datos clínicos entre los investigadores y gestores, con mayor trazabilidad y control y más posibilidades de ser auditados fácilmente que con los complicados sistemas convencionales.

Al igual que otras industrias como la de consumo, Blockchain tiene una clara aplicabilidad en la cadena de suministro. Sistemas basados en Blockchain permiten trazar la fabricación y distribución de medicamentos en toda la cadena de suministro, registrando

que los medicamentos son adecuadamente almacenados y manipulados, y evitando que medicamentos falsificados puedan entrar en el mercado. Un ejemplo: Blockverify en el Reino Unido está ya trabajando en pilotos de procedencia de medicación que permiten profesionales y consumidores escanear píldoras para verificar su integridad, tal y como se explica en el informe 'Healthcare rallies for blockchain'.

Pero además de mejorar los procesos, simplificar operaciones etc, Blockchain está llamado a transformar la cadena de valor y el modelo de relaciones entre pagadores y proveedores de salud.

Por ejemplo. hoy en día resulta muy complicada la cuantificación del coste-beneficio de la atención y los tratamientos médicos, lo que dificulta la implantación de contratos basados en el reembolso por resultados (en lugar del tradicional reembolso por acto médico). Con la transparencia y auditabilidad que proporciona Blockchain, se podrían plantear contratos entre aseguradores (públicos y privados) y proveedores (de servicios, de medicamentos, etc.), que vinculen los reembolsos a los resultados clínicos, al tiempo que se reduce la complejidad de los registros.

Pero los cambios pueden ser mucho más transformacionales. En una plataforma Blockchain, las instituciones que una vez estuvieron integradas verticalmente pueden escalar lateralmente a través de otros socios. Y a medida que la transparencia se generaliza y se embebe en cada transacción, serán cada vez menos necesarios los terceros intermediadores (por ejemplo de información médica), reduciendo las barreras a la participación de organizaciones más pequeñas, dando lugar a posibles nuevas oportunidades. Puestos a imaginar, podríamos pensar en las situaciones siguientes:

- Plataformas abiertas de compraventa de servicios "on demand"
- Los pacientes recuperan el control de sus datos, lo que obligaría a los investigadores clínicos y la salud a competir por el acceso a sus datos
- Si pudiéramos compartir de manera eficiente los activos, incluidos los sofisticados y caros equipos médicos, los registros de salud y de resultados de los pacientes ¿qué valor aporta una autoridad de hospitalaria de control?
- Las camas y los muros de los hospitales no desaparecerán, pero ¿acaso no podría liberalizarse el acceso a los profesionales y a los activos?

Vemos por tanto que las soluciones Blockchain transformarán el ecosistema de la salud y aumentarán la calidad de la atención al permitir modelos de gestión innovadores y hacer evolucionar nuevos modelos de negocio. La información de salud almacenada en Blockchain cambiará no solo la forma en que almacena la información clínica, sino también cómo compartir información dentro de la organización, con socios de atención médica, pagadores, y lo más importante, con pacientes.

Son estos aspectos los que están haciendo que la tecnología Blockchain esté teniendo una buena acogida en las organizaciones de salud que se están moviendo rápidamente e incluso parecen estar tomando la delantera a la industria financiera, según apunta el nuevo estudio sobre blockchain en el sector sanitario realizado por el IBM Institute for Business Value, denominado 'Healthcare rallies for blockchain', que encuestó a 200 profesionales de la atención médica en 16 países.

El estudio desvela que el 16 por ciento de los encuestados no solo está experimentando con la tecnología blockchain sino que espera tener una solución comercial de Blockchain en breve, con 9 de cada 10 encuestados que afirman planear invertir para 2018 en varias áreas de su negocio. Según el estudio, en el momento actual se están probando aplicaciones en real, que esperan eliminar las fricciones que los detienen. Estás aplicaciones están sobre todo enfocadas en acceder a información fiable.

Los líderes del sector sanitario esperan que los mayores beneficios de Blockchain se obtengan de la reducción de los tiempos de las transacciones, el coste y los riegos, sobre todo en tres áreas: registros médicos, ensayos clínicos y cumplimiento normativo. También anticipan una innovación generalizada en los modelos de negocio tanto o más que en otras industrias que hemos encuestado hasta la fecha.

Pero a pesar de sus expectativas de innovación transformadora, las instituciones de salud, incluidos los líderes que están adoptando modelos de Blockchain, no prevén una disrupción significativa. Quizás algunos piensen que la densa red de restricciones regulatorias limitará la innovación a cambios incrementales en el status quo, retrasará la implantación de los nuevos modelos de trabajo y mantendrá a raya a los competidores.

Aunque es muy pronto para predecir cómo se desarrollarán las cadenas de bloques en el cuidado de la salud, la realidad es que los beneficios de blockchain son convincentes, aplican a múltiples aspectos de la asistencia sanitaria y son potencialmente muy disruptivos. Habrá que estar atentos a los acontecimientos a medida que las aplicaciones de la tecnología blockchain dejen de ser prototipos y se vayan acercando a su comercialización.

Sistema de Intercambio de Información Clínica basado en Blockchain

M. Ramos Naveira, J. Barros Castro, L. Carrajo García, G. Vázquez González
Avances en Telemedicina e Informática Sanitaria (ATIS). Instituto de Investigación Biomédica de A Coruña (INIBIC). 15006 - A Coruña. España

LA TECNOLOGÍA BLOCKCHAIN PERMITE LA CREACIÓN DE UN SISTEMA DE INTERCAMBIO DE INFORMACIÓN CLÍNICA (HIE POR SUS SIGLAS EN INGLÉS) ENTRE PROFESIONALES SANITARIOS, CENTROS MÉDICOS, INVESTIGADORES Y PACIENTES. DICHO SISTEMA PERMITIRÁ EL INTERCAMBIO DE INFORMACIÓN DE UN MODO QUE ES IMPOSIBLE O CONLLEVA UN ALTO COSTE A DÍA DE HOY. ADEMÁS, SE MEJORARÁ LA SEGURIDAD Y CONTROL EN EL USO DE DATOS SENSIBLES PORQUE SE PODRÁN REALIZAR FÁCILMENTE AUDITORÍAS DE LOS ACCESOS A CUALQUIER TIPO DE DATO.

Un caso de éxito en este sentido es el sistema de historia clínica electrónica de Estonia [1] (e-Health Record), que recopila datos de múltiples fuentes para ofrecer un repositorio común tanto a profesionales sanitarios como a pacientes. Dentro de este sistema, se emplea la tecnología blockchain para asegurar la integridad de los extractos clínicos, además de guardar un registro inmutable de los accesos a los mismos.

ALCANCE Y CASOS DE USO

La propuesta consiste en la creación de una blockchain privada, donde la entrada de nuevos nodos tiene que ser negociada y aprobada de antemano. Dichos nodos de la red se corresponden con proveedores de datos clínicos (es decir, centros clínicos), que los mantendrán almacenados en sus bases de datos locales, tal y como lo hacen en la actualidad. La red blockchain se utilizará sólo para el control y registro del acceso a dichos datos, ya que almacenarlos en la blockchain queda totalmente descartado por limitaciones técnicas debido al gran tamaño de los mismos.
Los centros médicos (nodos de la red) podrán registrar a cada profesional clínico individual como productor y consumidor de datos clínicos, con el objetivo de reducir la granularidad en los accesos a datos y por lo tanto permitir auditorías más precisas.
Las acciones que permitirá este sistema se pueden resumir en:

- Acceso por parte del paciente a sus datos médicos desde cualquier sitio y dispositivo conectado a Internet, a través de una aplicación móvil o web. Este acceso obtiene datos aunque estén segregados en diferentes nodos.
- Acceso por parte de cualquier consumidor de la red (centro médico o profesional sanitario) a los datos de cualquier paciente, siempre que este acceso haya sido permitido explícitamente y de antemano bien por el paciente o bien por el centro médico productor del dato. Estos permisos pueden concederse o revocarse en cualquier momento y se almacenan en la blockchain.
- Acceso a datos anonimizados de forma agregada para uso en investigación. Los diferentes centros investigadores pueden participar (si son incluidos en la blockchain privada) como consumidores para consultar datos. Los propios pacientes pueden otorgar y revocar el uso para investigación de sus datos, así como ver para qué fueron utilizados.

DISEÑO DEL SISTEMA

El sistema gira alrededor de varios conceptos:
- Paciente: el originario de los datos clínicos. Puede conceder y revocar permisos sobre ellos.
- Dato clínico: cualquier pieza de información clínica referente a un paciente. Puede tener cualquier granularidad, tamaño y formato, ya que no se almacenará en la blockchain.

- Creador: participante de la red que genera un dato de un paciente. Típicamente será un profesional sanitario adscrito a un nodo de la red, aunque esta definición puede extenderse a otros participantes (por ejemplo programas informáticos que generan información automáticamente, wearables, etc).
- Proveedor: un nodo (centro médico) de la red blockchain privada, que tiene almacenados localmente datos clínicos y permite (o no) el acceso a un consumidor tras verificar sus permisos registrados en la blockchain.
- Consumidor: participantes que pueden acceder a los datos clínicos que ofrecen los proveedores. Pueden actuar de consumidores tanto pacientes, como nodos, profesionales clínicos o investigadores.
- Consulta de datos: una petición de acceso a datos clínicos de un consumidor a la red. La respuesta puede provenir de múltiples proveedores, ya que los datos de un paciente pueden estar fragmentados en múltiples centros médicos (de hecho, este es uno de los problemas que busca resolver este proyecto). Las consultas pueden ser sobre un paciente concreto o agregadas sobre datos anonimizados.

Toda acción en la red (tanto consultas, como permisos de acceso, etc) queda registrada en la blockchain, constituyendo un log de accesos inmutable y facilitando por tanto las auditorías. Como estos accesos se registran en tiempo real, sería incluso posible el desarrollo de un sistema de alarmas para detectar accesos inusuales a datos. En este sentido, destaca el proyecto Verifiable Data Audit [2] de Google Deepmind.

Un requisito fundamental del sistema es el de permitir el anonimato de la información almacenada en la blockchain, ya que por definición está replicada en cada nodo.

Otro aspecto relevante a tratar en el proyecto es aquel referente a datos de los que el paciente no puede tener acceso debido a su naturaleza (por ejemplo información psiquiátrica). Este tipo de datos necesita más requisitos que simplemente los del paciente.

CONSIDERACIONES DE IMPLEMENTACIÓN

1.1. Elección de la implementación de blockchain

Respecto a la implementación, se utilizará una implementación blockchain existente, pero de manera privada. La implementación de blockchain debe permitir contratos inteligentes para registrar los permisos sobre los datos. Existen numerosas alternativas disponibles, de las cuales vamos a analizar las dos más ampliamente adoptadas por la industria: Ethereum [3] e Hyperledger [4].

1.1.1. Ethereum. El proyecto Ethereum está ampliamente apoyado por grandes compañías de multitud de sectores [5]. Aunque Ethereum es una red blockchain pública, su código se puede utilizar para implementar redes privadas.

Una de las decisiones más importantes es el método de consenso para la verificación de bloques de la red blockchain. ¿Cómo se asegura el sistema de que la información almacenada en la blockchain es válida y no ha sido manipulada?. ¿Cómo incentivar a los nodos para que mantengan el registro distribuido?. A continuación vamos a analizar la utilidad, desde el punto de vista del sistema propuesto, de los principales métodos de consenso disponibles en Ethereum:

- Proof of Work: en redes públicas se suele utilizar un método de recompensa a la capacidad de cómputo aportada (Proof of Work), que se emplea en resolver problemas matemáticamente complejos pero sin ninguna utilidad más que la de hacer difícil el proceso de creación de bloques (comúnmente denominado "minado"). En general, en redes privadas como la que proponemos esta solución no suele ser apropiada debido al coste computacional.
- Proof of Stake: Ethereum está en camino hacia este método de consenso, que resuelve algunos de los problemas presentes en Proof of Work. Un nodo que quiera participar en la red debe depositar un número de tokens en un contrato inteligente, que perderá si su comportamiento resulta ser malicioso. Para una red privada, Proof of Stake podría ser mejor que Proof of Work debido al menor consumo de recursos, pero resulta complicado el control sobre el comportamiento de los nodos.
- Proof of Authority: es un concepto novedoso, donde existe un número de nodos preestablecidos (denominados "sealers", que vienen a sustituir a los "mineros") que ostentan la autoridad sobre la red. Un nuevo nodo que quiera participar en la red debe ser aprobado por un conjun-

to de sealers. Como implementación podemos destacar Ethereum Clique [6], aunque la desventaja es que, al igual que el resto de soluciones Proof of Authority, la aproximación todavía no está lo suficientemente madura a día de hoy.

1.1.2. Hyperledger. Hyperledger es un proyecto de software libre creado para aportar soluciones blockchain que sirvan en cualquier industria. Dentro de Hyperledger podemos encontrar múltiples soluciones y herramientas, de las que podemos destacar para nuestro propósito Hyperledger Fabric, que permite construir una blockchain de manera modular.

Fabric permite crear redes blockchain privadas restringidas, que soporten contratos inteligentes y donde los participantes deben ser aprobados de antemano. Las transacciones se pueden hacer totalmente confidenciales, lo cual es una gran ventaja en nuestro caso dado el carácter sensible de la información clínica. El método de consenso es configurable, aunque lo habitual es usar un algoritmo Practical Byzantine Fault Tolerance (PBFT) o derivado, tecnología que hace a la red muy escalable y con un consumo de recursos relativamente bajo.

Hyperledger Fabric es una solución madura para crear redes blockchain privadas y consideramos que, debido a la falta de madurez de las posibles alternativas (Ethereum Clique) o a lo poco adecuado de usar una tecnología propia de blockchains públicas (Ethereum con Proof of Work o Proof of Stake), el sistema de intercambio de información clínica se implementará utilizando Hyperledger Fabric.

1.2. Ubicación dentro de un ecosistema blockchain de salud

El sistema de intercambio de información clínica puede implementarse como un contrato inteligente dentro de una red blockchain privada dedicada a la salud, donde coexista con otros contratos. En general, la mayoría de implementaciones blockchain que soportan contratos inteligentes permiten también la comunicación entre contratos. Esto nos permite implementar funcionalidad común a múltiples proyectos en un único contrato inteligente, que será invocado posteriormente por los contratos inteligentes de los proyectos que necesiten dicha funcionalidad.

En este sentido resulta conveniente la implementación de un sistema de gestión de identidad de los participantes en la red blockchain privada. Dichos participantes (que incluirá en principio a pacientes y a profesionales sanitarios, pero podría extenderse a otros actores de la red) serán creados por los nodos (centros médicos) de la red blockchain.

De esta manera, tanto el sistema de intercambio de información clínica como cualquier otro sistema dentro de la blockchain realizarán llamadas al contrato inteligente correspondiente al sistema de gestión de identidad, para verificar la identidad de pacientes y profesionales sanitarios.

De todos modos, en un estado de desarrollo posterior de todos estos sistemas, es posible que resulte conveniente ampliar el sistema de gestión para añadir a otros participantes, o incluso implementar contratos diferentes para otra funcionalidad común a múltiples proyectos.

CONCLUSIÓN

La tecnología blockchain tiene un gran potencial para mejorar la interoperabilidad y la seguridad en muchos procesos dentro de la informática sanitaria. El sistema propuesto en este trabajo se apoya en esta tecnología para permitir el intercambio de información clínica entre diferentes actores (profesionales sanitarios, centros médicos, investigadores y pacientes) de manera segura y auditable.

BIBLIOGRAFÍA

[1] *Sistema e-Health Record de Estonia.* Disponible en: https://e-estonia.com/solutions/healthcare/. Consulta: febrero 2018.

[2] DeepMind Technologies Limited. *Trust, confidence and Verifiable Data Audit.* Disponible en: https://deepmind.com/blog/trust-confidence-verifiable-data-audit/. Consulta: febrero 2018.

[3] Buterin, V. *A Next-Generation Smart Contract and Decentralized Application Platform.* Disponible en: https://github.com/ethereum/wiki/wiki/White-Paper. Consulta: febrero 2018.

[4] *Hyperledger.* Disponible en: https://www.hyperledger.org/. Consulta: febrero 2018.

[5] *Enterprise Ethrereum Alliance.* Disponible en: https://entethalliance.org/. Consulta: febrero 2018.

[6] *Clique PoA protocol & Rinkeby PoA testnet.* Disponible en: https://github.com/ethereum/EIPs/issues/225. Consulta: febrero 2018.

Una aproximación blockchain al ámbito de la salud

Francisco Javier Segura Entrena[1], Gorka Sánchez Nanclares[2]
1. Ingeniero Informático. Servicio de Coordinación y Aplicaciones Informáticas. Subdirección General de Tecnologías de la Información. Servicio Murciano de Salud.
2. Médico Especialista en M. Familiar y Comunitaria. Responsable de Innovación. Subdirección General de Proyectos e Innovación. Servicio Murciano de Salud.

DISTRIBUTED LEDGER TECHNOLOGY. CUALQUIER DESARROLLO BASADO EN BLOCKCHAIN (O DLT) OFRECE UN ENTORNO DISTRIBUIDO PARA AMPLIFICAR Y DAR SOPORTE A INFORMACIÓN SANITARIA HACIA UNA INFINIDAD DE PARTICIPANTES Y PROVEEDORES DE SERVICIOS. PODEMOS CONSIDERAR LA EXISTENCIA DE TRES PARTES DIFERENCIADAS:

1. SOFTWARE P2P
2. BLOCKCHAIN: REGISTRO, LEDGER O "LIBRO MAYOR"
3. INTERFAZ

SOFTWARE PEER-TO-PEER. El software p2p tiene preconfigurado el algoritmo que da forma al ecosistema, y se conecta con otros programas semejantes. Contiene las reglas de comunicación, emite transacciones, recibe nuevos bloques aprobados por la red, y los valída antes de incorporarlos a la blockchain. Tiene por tanto preestablecidas las reglas de validación y consenso.

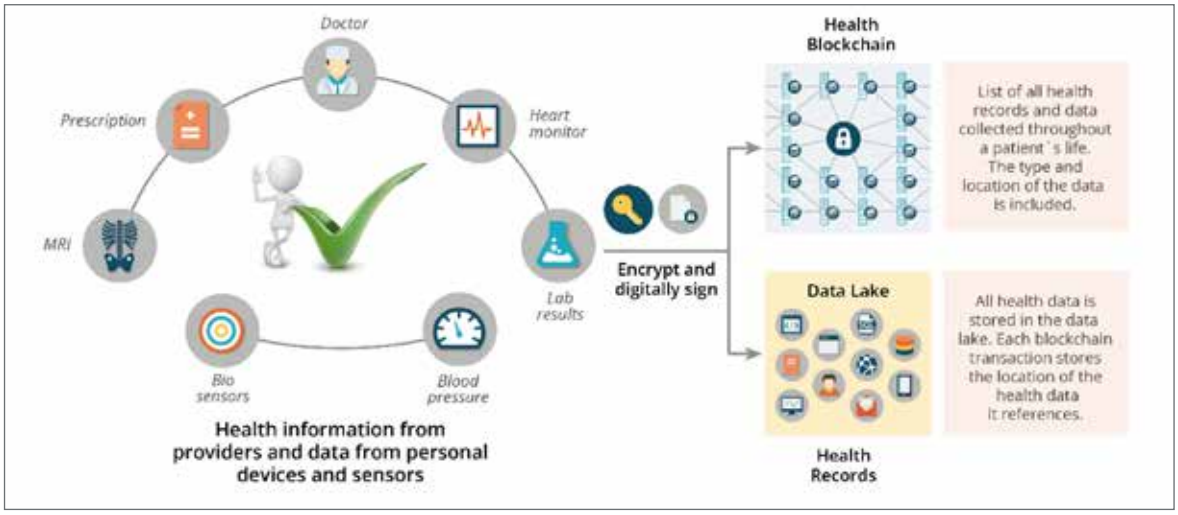
BLOCKCHAIN. También llamado *Distributed Ledger Technology*, es un registro incremental de transacciones agrupadas en bloques. Basado en criptografía, la integridad de cada bloque está garantizada. Si la red es pública y/o permisionada, cada bloque "se mina" -se añade- mediante un algoritmo de dificultad (se aplica una función Hash). La dificultad puede estar basada en algoritmos de cálculo computacional (PoW) o en algoritmos basados en participación (PoS). A menudo el minado sigue una política de incentivos. Si la red es privada, el/los nodos autorizados aprueban las transacciones, pero esto no la haría descentralizada.

INTERFAZ. Puede estar integrada en el software p2p o comunicarse con él. Emite transacciones que son procesadas y grabadas en la blockchain. Puede ser un aplicación web o móvil.

SOLUCIONES. Blockchain pone solución a los siguientes problemas:

- Establecer una red de confianza: Permitiendo desintermediación al no requerir un operador central, y proveer a cada participante de una copia de los datos y no requerir de un intermediario en el que confiar.
- Coste por transacción: Evitamos sistemas centrales y tecnología punta pudiendo usar hardware commodity y descentralización.
- Índice maestro de pacientes: Aportando un entorno distribuido que usa identificadores públicos y privados con claves de cifrado que mantienen la privacidad del paciente.
- Demasiados estándares: Ofreciendo datos actualizados en tiempo real y compartidos con toda la red mediante una interfaz común.
- Acceso limitado a los datos de salud: Ofreciendo acceso distribuido y seguro de los datos del paciente, que estarían grabados en la blockchain.

DATA LAKES. La blockchain no es escalable en capacidad, por lo que se usa de forma complementaria a los almacenes de datos llamados Data Lake. Los data lakes son escalables, y guardan eficientemente gran cantidad de información. Son buenos para mantener un archivo documental.
La información documental es un tema complejo de gestionar debido a lo difícil de mantener organizado y actualizado, por lo que la solución blockchain permitiría una fácil gestión.



BLOCKCHAIN

Almacena de forma indeleble las transacciones, guarda exclusivamente metadatos y datos precisos que puedan requerir los gestores en un momento dado. Enlazan a los documentos del data lake, que contienen digitalizados los informes generados por diversos prestadores de servicios sanitarios. La información del usuario se cifra con la identidad digital del mismo.

¿QUÉ APORTA BLOCKCHAIN A LA SANIDAD?

1. Blockchain aporta a diversos actores de sanidad leer información del paciente conservando su privacidad.
2. Estos actores pueden notificar a la red de sucesivos cambios o acciones y así tener un control total y actualizado de la información del paciente y de sus acciones con respecto al sistema de salud.
3. Permite actores públicos y privados, incluso da la posibilidad al usuario de acceder a su propia información según se va generando.
4. Permite la interacción de forma distribuida con otras aplicaciones que generen datos, con dispositivos conectados a internet (internet de las cosas), pudiendo recopilar datos obtenidos de dispositivos (aplicaciones y dispositivos de salud).
5. Cifrado que favorezca el secreto, y firma criptográfica que garantice quién ha emitido la información.
6. Descentralización, hardware asequible y funcionalidad distribuida.

Actores que pueden estar interconectados a la blockchain sanitaria

- Usuarios, nodos completos o apps ligeras
- Centros de salud
- Clínicas privadas
- Hospitales
- Farmacias
- Compañías de seguros
- Otros proveedores de la salud (ej fisioterapeutas, dentistas…)

UNA BLOCKCHAIN PROGRAMABLE PARA SANIDAD. Un posible prototipo para la industria de la salud, consistiría en una blockchain que permitiera un conjunto de Smart Contracts con diferentes funcionalidades.

Los Smart Contracts son un código ejecutable que puede ser guardado en la blockchain y ejecutado en diferentes ocasiones deslocalizadamente. Los smart contracts pueden almacenar valores y realizar funciones variadas, lo que los hace muy versátiles, al ser un lenguaje generalista para las interacciones con blockchain.

Por otro lado, los Smart Contracts podrían atender a información externa actualizada.

Conceptualmente, un usuario puede ser registrado por una autoridad. Si dicho usuario está en dicho listado, podría mediante criptografía, certificar su identidad y realizar acciones. Podría ser autorizado él mismo mediante su clave criptográfica (ej. su tarjeta inteligente, incluso su eDNI) y realizar acciones, o podría autorizar a un tercero (ej. una clínica) a realizar acciones que lo involucren, incluso ceder total o parcialmente sus datos.

Podemos ver un posible ejemplo funcionando con Smart Contracts (SC): Un SC podría tener la función de registro de usuarios, otro SC aportaría la funcionalidad de guardar relaciones entre identidades de pacientes y proveedores de servicios (lo que podemos entender como resumen de la HC del paciente), y un tercer SC se encargaría de conectar los niveles anteriores, gestionar los diferentes permisos y enlazar a documentos. El usuario y en general todas las entidades poseen un certificado criptográfico que le identifica y cifra la información. La aplicación de usuario (app) tiene el cometido de dar usabilidad eliminando la complejidad.

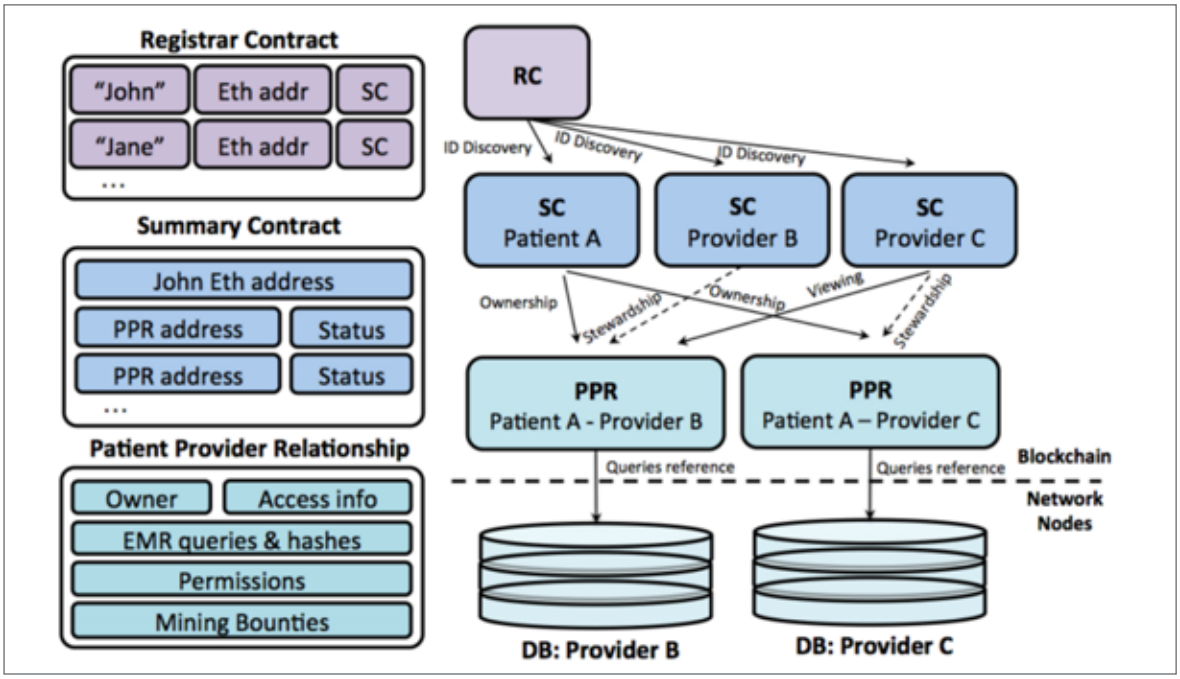
El Smart Contract almacena la identificación y los permisos, pudiendo restringir quién tiene derecho a acceder a los datos del mismo.

Posteriormente, cualquier otro usuario o entidad podría tener acceso a esa información si resulta autorizado por el sistema, pudiendo ser el proceso distribuido, salvo la gestión documental. Si bien están apareciendo nuevas soluciones tecnológicas para hacer esta parte distribuida.

FUNCIONAMIENTO DE GESTIÓN DOCUMENTAL. La blockchain almacenaría metainformación sobre los documentos, y donde están guardados. La interfaz aunque debe estudiarse en cada caso las necesidades de cada actor y su forma de gestionar la información, en esencia, sería relacionar el trabajo de manejo de bases de datos documentales, que unido a los permisos cedidos y grabados en la blockchain permitiría a un usuario u otra entidad acceder a los mismos, siempre con una base criptográfica, y por tanto segura. En definitiva, una blockchain de salud podría funcionar como un gestor de control de accesos y permisos para datos y registros de salud.

BIBLIOGRAFÍA

1. https://www.healthit.gov/sites/default/files/11-74-ablockchainforhealthcare.pdf
2. https://www.healthit.gov/sites/default/files/5-56-onc_blockchainchallenge_mitwhitepaper.pdf
3. https://www2.deloitte.com/content/dam/Deloitte/us/Documents/public-sector/us-blockchain-opportunities-for-health-care.pdf
4. Lorenzo Moreno (@rutrus) - Asociación murciana del Bitcoin y otras tecnologías
5. https://hbr.org/2017/03/the-potential-for-blockchain-to-transform-electronic-health-records
6. https://www.wired.com/2017/02/moving-patient-data-messy-blockchain-help/
7. https://www.coindesk.com/blockchain-healthcare-2017s-successes/
8. http://www.healthcareitnews.com/news/blockchains-potential-use-cases-healthcare-hype-or-reality
9. https://dminc.com/blog/blockchain-healthcare-hype-reality.



Blockchain, una oportunidad tecnológica para el Sector Salud

González Hernández, Mª Remedios[1]; Hidalgo Céspedes, Jose Fco[2]; Aparicio García, César[3]; Sánchez Nanclares, Gorka[4]

1. Ingeniera Informática, Analista/Programadora en el Centro Regional de Informática de la Región de Murcia, Vocal de formación en el COITIMUR, Co Founder de la plataforma blockchain CoinDataDesktop, Tecnóloga Blockchain.
2. Ingeniero Informático, Responsable de Infraestructura TIC para Investigación en la Universidad de Murcia, Coordinador de formación en CERTIC, Co Founder de la plataforma blockchain CoinDataDesktop, Tecnólogo Blockchain.
3. Ingeniero Informático, Responsable de Gestión Económica. Subdirección General de Tecnologías de la Información. Servicio Murciano de Salud.
4. Médico Especialista en M. Familiar y Comunitaria. Responsable de Innovación del Servicio Murciano de Salud.

LA BLOCKCHAIN ES UNA REALIDAD TECNOLÓGICA QUE LLEVA MADURANDO CERCA DE UNA DÉCADA, PERO HA SIDO RECIENTEMENTE CUANDO ESTE TÉRMINO SE HECHO FAMILIAR INUNDANDO LOS MEDIOS Y ASOCIADO MÁS ESPECÍFICAMENTE A LAS FINANZAS. EN LA PRODUCCIÓN DE SERVICIOS PÚBLICOS MANIFIESTA GRAN POTENCIAL PUESTO QUE VA A PERMITIR PLANTEAR SOLUCIONES DIFERENTES A LAS QUE HASTA AHORA HEMOS PODIDO PERMITIRNOS.

La sociedad hiperconectada y la tecnología blockchain, con todos sus peajes, nos están ofreciendo nuevas oportunidades de servicio y de negocio también en el ámbito sanitario. Las propiedades inherentes del acceso criptográfico de clave pública y privada, prueba de trabajo y datos distribuidos, crean un nuevo nivel de integridad para la información de atención médica.

El sector sanitario a través de servicios telemáticos ofrece mejoras de acceso a los ciudadanos aumentando con ello su satisfacción y percepción de calidad. Los esfuerzos dan sus frutos, pero es de sobra conocido que es mejorable en términos de interoperabilidad, de costes y de protección de datos. La tecnología blockchain puede ser el vehículo para mejorar y automatizar operaciones que ya se vienen realizando aunque sin una homogeneidad.

En el ámbito de la salud se están llevando numerosos avances, el uso selectivo de sensores biométricos será aconsejado en pacientes convalecientes, personas de avanzada edad, deportistas, recién nacidos o cualquier persona que lo desee. Actualmente algunos enfermos y muchos deportistas aficionados y profesionales ya están haciendo uso de este tipo de sensores por motivos dispares y comparten los resultados con profesionales o redes sociales como es el caso de los deportistas.

El uso intensivo de este tipo de sensores para la obtención de información da paso a la automatización de procesos y a la extracción de conocimiento. Estos tres aspectos caracterizan a la IoT[1] o Internet de las cosas (Internet of Things). IoT ha encontrado un aliado perfecto y casi inesperado en la blockchain. En primer lugar IoT presenta una topología descentralizada de sistemas autónomos que requieren conectividad y que ésta sea resiliente y flexible. Esa es la principal característica de la blockchain. Por otro lado, la recopilación de datos IoT y especialmente cuando éstos estén relacionados con la salud puede requerir de privacidad en los datos recopilados. En la blockchain, cada sensor puede depositar la información de forma periódica en el slot de su propietario preservando su anonimato en base a la posibilidad de cifrar criptográficamente y por el mismo hecho de que la información puede estar tan disociada de su identidad como ciudadano tanto como se desee mediante el uso de

diferentes direcciones de blockchain y la migración de los datos a conveniencia del usuario. En cuanto a la automatización y dado que la conectividad puede ser extrema, el dispositivo puede estar programado para medir y subir a la blockchain la información de salud del paciente o del deportista en los plazos previstos.

Todos esos datos recopilados podrían ser analizados sin conocer realmente con qué paciente están asociados ya que pueden estar disponibles en la red blockchain. Podrían usarse incluso para disparar alertas tempranas ante síntomas de enfermedades como la prevención de problemas circulatorios inminentes, secuelas por cambios en la reacción ante los tratamientos farmacéuticos y un largo etcétera. Un despliegue suficiente de sensores con conectividad blockchain podría ser la mejor arma para detectar precozmente epidemias o ver su evolución geográfica, poblacional o temporal.

Una vez que disponemos de este tipo de conocimiento y vista la utilidad del binomio IoT + blockchain, el siguiente paso es conectarlo con el médico y el sistema sanitario. El punto que une al paciente con el sistema IoT autónomo que hemos diseñado con la asistencia sanitaria puede ser la tarjeta sanitaria. El concepto de tarjeta va a ser deconstruido para reinventarse de nuevo. Será un pasaporte digital alojado en el móvil o en otro soporte que proporcionará un identificador a todo los sensores para que el almacenamiento de datos en la blockchain sea coordinado. El propio usuario del sistema podrá usarla para proporcionar acceso a ciertos agentes como una empresa privada de salud o un centro deportivo de alto rendimiento y éstos pueden personalizar su atención en base a los accesos proporcionados. También puede el usuario registrar su número de teléfono en un sistema de alerta temprana especializado de su elección, por ejemplo, en la detección de ictus. Bastaría con dar de alta su dirección de la blockchain y un teléfono para que él mismo o un familiar puedan ser advertidos de la inminencia del suceso o del nivel de riesgo.

Cabe preguntarse qué tipo de blockchain debemos desplegar para todo ésto. La blockchain pública tiene costes en cada operación que suponga añadir información o cambios de configuración en permisos. Sin embargo podemos

> ***"Todos esos datos recopilados podrían ser analizados sin conocer realmente con qué paciente están asociados ya que pueden estar disponibles en la red blockchain. Podrían usarse incluso para disparar alertas tempranas ante síntomas de enfermedades como la prevención de problemas circulatorios inminentes, secuelas por cambios en la reacción ante los tratamientos farmacéuticos y un largo etcétera"***

desplegar una blockchain privada con toda la funcionalidad de la pública pero cuyos costes de operación sean absorbidos por la administración sanitaria y las empresas de salud, de la misma manera que en la actualidad despliegan sistemas informáticos que requieren para su gestión empresarial. La diferencia entre que la blockchain sea pùblica o privada desaparece cuando todos los potenciales usuarios tienen habilitado el acceso. De esta manera una blockchain privada accesible a todos los usuarios del sistema público, empresas hospitalarias, farmacéuticas, rehabilitadores, etc... es en su contexto una red global. Es importante cuidar la descentralización de la red desplegada mediante la selección adecuada de la cantidad de nodos y su dispersión de manera que se garantice la supervivencia de la propia red ante un accidente o un ataque. La red de producción podría replicarse con los datos disociados para ser usada por grupos de investigación especializados en análisis de prevención de enfermedades, hacer seguimiento de sujetos con tratamiento específico, etc..

Las posibilidades solo encuentran límite en nuestra imaginación. Mediante el uso de contratos smart[2] se pueden crear tokens o moneda digital que representen un valor finalista empleado por usuarios del sistema sanitario o de la dependencia. Podría entregarse moneda digital para pañales, alimento específico, ciertas medicinas, ortopedia, sesiones de rehabilitación, etc... a personas concretas, solo usable en esos productos y con una duración de uso concreta de manera que si no se consume permanece en el sistema o lo pueda acumular para otros pe-

> ***La tecnología de Blockchain puede permitir que varias partes interesadas en la cadena de valor de la asistencia sanitaria compartan el acceso a sus redes sin comprometer la seguridad e integridad de los datos, permitiéndoles rastrear la procedencia de los datos y los cambios realizados"***

riodos. Esta nueva tecnología también puede ser el vehículo para el control y seguimiento en la cadena de suministro de los medicamentos evitando el fraude y falsificación, desde que se crean hasta saber cuáles son los destinos de estos productos o fármacos. Blockchain proporciona un vínculo inmutable y transparente a lo largo de cada etapa del proceso de producción, proporcionando un sistema fácil de auditar por parte de los organismos reguladores de manera que se puede proteger de una forma sencilla al consumidor final.

CASOS DE ÉXITO

Empiezan a surgir startups, *Saavha*[3] donde su propuesta aplica la integridad de la cadena de bloques a la verificación de las citas médicas, o *ScriptDrop*[4] que agiliza las operaciones entre farmacéuticos y pacientes en EEUU, a la vez que sirve como agenda a los pacientes para que no olviden sus prescripciones médicas, entregan las medicinas a domicilio y envían alertas con los horarios de toma de medicamentos o como pueda ser *Gero*[5] que promueve una iniciativa para mejorar la calidad de vida de los usuarios y "retrasar el envejecimiento" recopilando y procesando datos medioambientales, de costumbres de vida, etc. con el objetivo de diseñar medicamentos para prolongar la esperanza de vida.

En algunos países ya es una realidad el uso de la blockchain como eje principal en el ámbito de la salud como puede ser en Estonia[6] donde los pacientes que han visitado un médico mantienen un registro de su historial en lo que han denominado *KSI Blockchain*[7], o en el estado de Illinois[8] de los Estados Unidos donde mantienen un registro de todos sus funcionarios médicos usando la cadena de bloques.

Gran prueba de esta apuesta tecnológicaes como la mayor de las industrias tecnológicas y consultoras a nivel mundial también se están sumando a ella, como es el caso de IBM[9].

CONCLUSIÓN

Un mejor intercambio de datos entre los proveedores de servicios de salud y el paciente significa una mayor probabilidad de diagnósticos precisos, tratamientos más efectivos, sistemas de prevención autónomos y la mayor capacidad general de las organizaciones de atención médica para brindar atención más efectiva. La tecnología de Blockchain puede permitir que varias partes interesadas en la cadena de valor de la asistencia sanitaria compartan el acceso a sus redes sin comprometer la seguridad e integridad de los datos, permitiéndoles rastrear la procedencia de los datos y los cambios realizados. Con blockchain, las transacciones se pueden documentar en un registro descentralizado permanente, lo que reduce los retrasos, costes adicionales y errores humanos.

Es sin duda una oportunidad en los ámbitos público y privado desde el punto de vista sanitario pero también económico y de eficiencia.

1. http://searchdatacenter.techtarget.com/es/definicion/Internet-de-las-cosas-IoT
2. https://opensource.com/article/17/12/whats-blockchain-smart-contract
3. https://www.saavha.com/
4. https://www.scriptdrop.io/
5. https://de.decentral.news/gero-health/
6. https://e-estonia.com/solutions/security-and-safety/ksi-blockchain/
7. https://guardtime.com/technology
8. https://healthitanalytics.com/news/illinois-to-use-blockchain-for-healthcare-credential-management
9. https://www.ibm.com/blogs/blockchain/2017/10/blockchain-in-healthcare-patient-benefits-and-more/



XXIII PREMIOS NACIONALES DE INFORMÁTICA Y SALUD 2017

EL PASADO 18 DE ENERO TUVO LUGAR EL ACTO DE ENTREGA DE LA VIGESIMOTERCERA EDICIÓN DE LOS PREMIOS NACIONALES DE INFORMÁTICA Y SALUD. COMO VIENE SIENDO HABITUAL, SE CELEBRÓ EN EL SALÓN DE ACTOS DE LA FACULTAD DE MEDICINA DE LA UNIVERSIDAD AUTÓNOMA DE MADRID.

ACTO INSTITUCIONAL

El acto fue presentado por **Zaida Sampedro Préstamo,** vicepresidenta de Estrategia Digital de la SEIS, que se dirigió a los asistentes agradeciendo la asistencia. Se refirió especialmente a **Elena Andradas Aragonés**, directora General de Salud Pública, Calidad e Innovación del Ministerio de Sanidad, Servicios Sociales e Igualdad; **Juan Antonio Vargas Núñez**, decano de la Facultad de Medicina de la Universidad Autónoma de Madrid, "quien generosamente nos ofrece su hospitalidad y hace posible que estemos reunidos en este magnífico entorno académico y científico"; **Carmen Fernández Fernández**, directora de Diario Médico/Correo Farmacéutico; **Javier Olave Lusarreta**, vicepresidente de la Asociación de la Prensa de Madrid y **Mª José Marzal**, directora de ComputerWorld.

Tras dar la enhorabuena a todos los premiados, recordó que en el año 2017 la SEIS cumplió 40 años. "Si bien podríamos decir que son toda una vida, también podemos asegurar que nos gustaría verlos como los primeros 40 años de una vida que esperamos que sea muy larga. No quisiera dejar de hacer una mención especial, por su papel relevante, al presidente, Luciano Sáez Ayerra. Si 40 años es toda una vida, Luciano lleva capitaneando este barco más de media vida... más de 25 años. Gracias por tu dedicación y entrega a la SEIS", dijo.



A continuación intervino **Juan Antonio Vargas Núñez,** decano de la Facultad de Medicina de la Universidad Autónoma de Madrid. Dio la bienvenida a todos los presentes y comentó que es un honor para la facultad, como institución, poder albergar este acto. Felicitó a la SEIS por su 40 cumpleaños y a todos los premiados "por su esfuerzo continuado en busca de soluciones tecnológicas, un elemento clave que nos ayuda a mejorar nuestro sistema sanitario. Y debemos seguir avanzando en este sentido. Hoy se almacena todo tipo de datos de pacientes. El análisis y tratamiento de esta información será los que nos ayude a conseguir la medicina del futuro, más personalizada". Aludió también a la importancia de la historia clínica, que "contiene información que permitirá un análisis más preciso y profundo, para mejorar el tratamiento de las enfermedades".

Vargas Nuñéz se refirió además a la importancia de la imagen médica digitalizada, la genómica y a la necesidad de aunar esfuerzos con las CC AA y con las universidades, para mejorar la formación de los profesionales. Como decano, reiteró su agradecimiento a la SEIS "por seguir acudiendo a nuestro facultad y, en especial, a Luciano Sáez". Finalizó su intervención dedicando un recuerdo especial a José Luis Carrasco, felicitando a los premiados y deseando que el acto tuviera el mismo éxito de ediciones anteriores.

A continuación intervino **Luciano Sáez Ayerra,** presidente de la SEIS, que dio la bienvenida a todos a este acto y agradeció la presencia a autoridades y directivos del sistema sanitario y de la universidad, presidentes y representantes de asociaciones profesionales, científicas y empresariales, directivos y profesionales de la industria, representantes de los medios de comunicación, profesionales del sistema sanitario y tecnológico y compañeros socios de la SEIS.

"Bienvenidos un año más a este acto de reconocimiento a la labor de organizaciones, empresas y profesionales que trabajan día a día y desde hace muchos años por mejorar nuestro sistema de salud con la aportación de los avances tecnológicos. Muchas gracias decano, no solo por acompañarnos en este acto, sino por permitirnos realizar esta entrega de premios en tu casa, ya durante 23 años ya. Y especialmente gracias a Elena Andradas, directora general de Salud Pública, Calidad e Innovación del MSSSI, por poder contar con tu presencia. Agradezco también la colaboración y participación de los directivos de los medios de comunicación especializados en salud y en tecnología. Además, tengo que agradecer a Zaida Sampedro, vicepresidenta de Estrategia Digital de la SEIS, la coordinación general de los Premios Nacionales de Informática y Salud.

Hoy los protagonistas son los galardonados a los que felicitamos por su labor. Destacamos en esta edición al Servicio Extremeño de Salud, que lleva muchos años incorporando, de forma decidida, soluciones innovadoras tanto para sus profesionales como para los servicios que facilitan a los



ciudadanos. Como ejemplo reciente, la puesta en marcha del centro de salud on line, como instrumento que permite prestar servicios de salud al ciudadano desde cualquier lugar y dispositivo.

A Ibermática, que desde 1990 desarrolla soluciones específicas para nuestro sector y que cuenta con una importante división especializada en sanidad, basada en la innovación mediante la utización de tecnologías como procesamiento de lenguaje natural, o big data a través del Instituto Ibermática Innovación. Siempre hemos propugnado, desde nuestra Sociedad, la importancia de que la industria disponga de recursos y especialistas de este complejo mundo sanitario.

A dos profesionales con una larga trayectoria, impulsores de la investigación y la innovación mediante las TIC. Queridos Marcial y Fernando, habéis aportado mucho a nuestro sistema de salud y es una suerte poder seguir contando con vuestro conocimiento e iniciativas. Sois dos miembros destacados de nuestra sociedad.

Al Consejo General de Colegios Oficiales de Farmacéuticos, una organización profesional pionera en el uso de la TIC. Desde 1977 sus aportaciones a la informatización de la prestación farmacéutica han sido muchas y de relevante calidad. Es una organización innovadora y que difunde a todo su colectivo profesional servicios tecnológicos de alto nivel. Su apuesta por la trasformación digital es patente impulsando grandes proyectos como el vademecum digital, la receta electrónica y una plataforma digital que sustenta la red de farmacias. Muchas gracias presidente por asistir.

También al Servicio Andaluz de Salud, que independientemente de sus logros en materia de salud digital, apuesta cada año por transferir conocimiento a todos los profesionales involucrados en nuestro sector. No en vano es sede permanente de las Jornadas Nacionales de Innovación y Salud, donde se plantean y estudian nuevos retos a los que nos enfrentamos en nuestro sector. Muchas gracias, Juan Lucas, por asistir.

Y finalmente, destacamos a la Subdirección General de Tecnologías de la Información del MSSSI que, como pueden imaginar tiene para mí un alcance especial, ya que participe en su creación, allá por el año 1988. Son muchos años de trabajo detrás de los sistemas de información que dispone y ofrece el Ministerio. Y siempre con insuficiencia de recursos que solventan con su dedicación y entusiasmo. Como todos sabemos los profesionales que trabajan en las unidades tecnológicas viven siempre en una situación permanente de fuego graneado. Muchas gracias Juan Fernando por asistir.

Nuestra sociedad, está celebrando 40 años de trabajo. Una sociedad abierta a todos los profesionales, a todas las instituciones y entidades que se identifiquen con nuestra misión, que es promover la investigación, el desarrollo, la innovación, la implantación y buen uso de las TIC en el ámbito de la salud, siempre en beneficio de la sociedad y con pleno respeto a los derechos de las personas; en particular a su intimidad y privacidad.

Hoy iniciamos nuestro trabajo del año 2018. To-

das nuestras acciones seguirán trabajando con 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. Y también exponer los frenos existentes y realizar acciones para superarlos".
A las administraciones públicas, nuestros colaboradores tecnológicos, las entidades asociadas, las organizaciones sanitarias, los medios de comunicación y las asociaciones científicas y profesionales, nuestro reconocimiento por su apoyo y por el trabajo realizado. Sabemos que es un sobreesfuerzo a su labor profesional.
Para finalizar, quiero agradecer 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. Muchas gracias".

A continuación, pronunció unas palabras Elena Andradas, quien afirmó que "siempre es un placer y una gran satisfacción acompañar a la SEIS en actos como este". Para Andradas, las tecnologías se han convertido en una herramienta absolutamente imprescindible y clave para todas las actividades y en sanidad representan un fundamento estratégico para afrontar las mejoras que todos deseamos para el sistema sanitario. "El hecho de que 14 CC AA ya tengan receta electrónica está permitiendo que las oficinas de farmacia de nuestro país puedan realizar una dispensación más segura. A pesar de ello, queremos seguir avanzando para conseguir la plena implementación de la historia clínica y la receta electrónica". Tras referirse al reciente convenio firmado por el Ministerio de Sanidad, Servicios Sociales e Igualdad y la SEIS, finalizó con una felicitación a los premiados y a la SEIS.

Posteriormente Zaida Sampedro, dio lectura al Acta del Jurado:
Constituido el jurado de la Vigesimotercera Edición de los Premios Nacionales de Informática y Salud correspondientes al año 2017, formado por los miembros de la Junta Directiva de la Sociedad Española de Informática de la Salud, decide la concesión de los siguientes premios:

1. **Premio Nacional de Informática y Salud 2017, a la Entidad Pública o Privada que ha destacado en proyectos de transformación digital en el ámbito sanitario.**

Otorgado al Servicio Extremeño de Salud, por su apuesta decidida por la Salud Digital demostrada a lo largo de los años y, en especial, con la puesta en marcha del Centro de Salud on line, que presta servicios de salud al ciudadano desde cualquier lugar y dispositivo electrónico. El premio fue entregado por Elena Andradas y recogido por José María Vergeles Blanca, consejero de Sanidad y Políticas Sociales de la Junta de Extremadura.





El consejero agradeció a la SEIS y al Jurado la gentileza de haber reconocido la trayectoria del Servicio Extremeño de salud la incorporación de las TIC para mejorar la salud de la población. También felicitó a todos los premiados que han sabido incorporar las TIC para proporcionar un mejor servicio a los ciudadanos, gracias a la receta electrónica, después a la telemedicina y antes con la historia clínica electrónica única y dedicó el premio a todos los que componen el Servicio Extremeño de Salud y a la propia SEIS y su presidente, Luciano Sáez.

2. Premio Nacional de Informática y Salud 2017, a la Organización que ha realizado un mayor esfuerzo tecnológico para desarrollar soluciones en el sector sanitario.

Otorgado a Ibermática, por su contribución a la mejora de la atención sanitaria mediante el desarrollo de soluciones orientadas a diferentes necesidades del sector salud: desde gestión hospitalaria y de centros socio sanitarios, hasta plataformas para el desarrollo de nuevos modelos asistenciales, en los que se incluye su apuesta por la innovación mediante su Instituto Ibermática Innovación con tecnologías para el procesamiento de lenguaje natural, process Mining y Big Data.

Recogió el premio Juan Ignacio Sanz, consejero delegado de Ibermática y lo entregó Mª José Marzal, directora de Computer World. Sanz realizó una breve intervención para relatar que "nuestras aplicaciones permiten ayudar a médicos y a enfermeras y servicios de la salud a la mejora de la calidad asistencial. Consideramos que ha pasado la primera revolución de los Sistemas de Información, donde se centraban en la gestión y estamos ante una segunda revolución tecnológica que permitirá a los servicios asistenciales hacerlos sostenibles a través de la salud digital. La inversión en tecnologías en Sanidad es fundamental para desarrollar un nuevo modelo asistencial".

3. Premio Nacional de Informática y Salud 2017 al Profesional que, por su trayectoria y dedicación, ha colaborado especialmente en promover la transformación digital en el entorno sanitario.

Otorgado al Dr. D. Marcial García Rojo, por toda su carrera profesional y, especialmente, por sus aportaciones en Anatomía Patológica, los proyectos de investigación que ha desarrollado y su decidido impulso de acciones para promover la transformación digital de la atención sanitaria a través de sociedades científicas nacionales e internaciones, tanto en el ámbito de su especialidad como en el de la informática, primero como miembro de la SEIS y, posteriormente, de la Junta Directiva en la que llegó a desempeñar el cargo de vicepresidente y la Representación en las Asociaciones Internacionales.

Le entregó el premio Luciano Sáez Ayerra. García Rojo agradeció el premio a la SEIS, Sociedad



de la que "recibió mucho más de lo que pudo dar". Recordó su dedicación a la SEIS y dedicó el premio a su familia, especialmente a su mujer e hijos, recordando y agradeciendo la ayuda que siempre le habían prestado.

4. Premio Nacional de Informática y Salud 2017, al Trabajo realizado para difundir la implantación de las Tecnologías de la Información y la Comunicación en Salud.

Otorgado al Consejo General de Colegios Oficiales de Farmacéuticos de España, por su importante contribución a la transformación digital del mundo farmacéutico, especialmente a través de Portalfarma y sus opciones relativas a la información profesional para farmacéuticos, su repositorio de productos, la Información para ciudadanos, el aula de farmacia para estudiantes y como herramienta de comunicación entre todos los profesionales farmacéuticos; también por haber puesto a disposición de los profesionales sanitarios el mejor vademécum a nivel internacional como es el BOT PLUS, que ha favorecido de manera indudable el desarrollo de proyectos como la receta electrónica en el SNS y recientemente la receta electrónica privada y la que corresponde a los medicamentos de uso veterinario. Jesús Aguilar Santamaría, presidente del Consejo General de Colegios Oficiales de Farmacéuticos de España, recogió el premio que le entregó Carmen Fernández Fernández, directora de Diario Médico/Correo Farmacéutico. El premiado agradeció el reconocimiento a la SEIS y comentó que están trabajando día a día desde Farmacia en esta línea de la información y las telecomunicaciones. "Estamos trabajando cercanos al Ministerio en muchos proyectos y esperamos seguir avanzando, sobre todo en el proyecto de poner en red a todas las farmacias españolas", dijo.





5. Premio Nacional de Informática y Salud 2017, al esfuerzo institucional o personal de investigación o innovación en Proyectos para la utilización de las Tecnologías de la Información y la Comunicación en Salud.

Otorgado a Fernando Martín Sánchez, por su larga trayectoria en realizar proyectos de investigación en Bioinformática en España en el Instituto de Salud Carlos III y en la Universidad Francisco de Victoria, además de su importante labor en la Sociedad Española de Informática de la Salud y en IMIA donde fue Vicepresidente. Por su trayectoria internacional en la Universidad de Melbourne y en la Well Cornell University de Nueva York. Juan Antonio Vargas Núñez entregó el premio a Martín Sánchez. Tras agradecer el premio a la SEIS, recordó a mentores y amigos, como Juan Pazos de la Universidad Politécnica, a Luciano Sáez y a sus compañeros del equipo de investigación. Deseó que la Informática Médica sea reconocida y con un cuerpo de reconocimiento propio y con una estructura consolidada. Finalizó mostrando especial agradecimiento a toda su familia y en especial a su mujer e hijas.

6. Premio Nacional de Informática y Salud 2017, a la mejor aportación presentada en las actividades de la SEIS durante los últimos 12 meses.

Otorgado al Servicio Andaluz de Salud, porque las labores de promoción y difusión de proyectos de innovación mediante las TIC es demostrada a lo largo de los años, durante este año 2017 su contribución y apoyo institucional ha sido intensa tanto en las Jornadas Nacionales de Innovación y salud



en Andalucía como en la XIV Reunión del Foro de Seguridad y Protección de Datos en Salud celebrado en el Hospital Virgen del Rocío. Javier Olave Lusarreta, vicepresidente de la Asociación de la Prensa, entregó el premio a Juan Lucas Retamar Gentil, subdirector general de Tecnologías de la Información y Comunicaciones del Servicio Andaluz de Salud. Transmitió su agradecimiento a la SEIS y felicitó a García Rojo, médico muy querido y respetado en la sanidad andaluza, por el premio recibido. "El SAS y la SEIS hace muchos años que tienen una muy buena relación", dijo. Recordó que el próximo mes de junio se volverán a celebrar las Jornada de Informática en Andalucía, en la localidad de Torremolinos, que es una cita obligada para todos los profesionales del sector.

Premio Especial Informática y Salud 2017, otorgado a la Subdirección General de Tecnologías de la Información del Ministerio de Sanidad Servicios Sociales e Igualdad, por la labor destacada y continua que están realizando para desarrollar e implantar soluciones tecnológicas en el ámbito sanitario, que permiten avanzar en su transformación digital, haciendo especial mención a la implementación de un Nodo central de intercambio de información clínica que permite interoperabilidad de los sistemas de información de Historia Clínica Digital de las CC AA, receta electrónica etc., permitiendo que dicha información pueda ser accedida en el lugar y en el momento que se necesite, con los adecuados niveles de seguridad que la especial sensibilidad de esta información requiere y contando para ello con la certificación del Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001. Recogió el premio Juan Fernando Muñoz Montalvo, subdirector general de Tecnologías de la Información del Ministerio de Sanidad, Servicios Sociales e Igualdad, de manos de Elena Andradas Aragonés. Una vez recogido el premio, Muñoz Montalvo agradeció a la SEIS que reconozca "el trabajo que hacemos todos los días". Dijo sentir una ilusión muy especial "pensando en mis compañeros, en la administración pública y en el servicio público en general. Una de las pocas cosas que te enseñan es el reconocimiento de nuestros compañeros. Otra cosa es que es un premio real para todos, desde la secretaria, que es la cara amable, los más mayores, que nos enseñan experiencia, los jóvenes, que nos contagian de ilusión, de los que somos eternos, todos los que compartimos esas pizzas a las 12 de la noche". Tuvo un recuerdo especial para los tres últimos subdirectores que pasaron por la Sección, para Luciano Sáez, Francisco y Jesús García Marcos, y también para "nuestros colegas del Sistema Nacional de Salud, a los que reunimos a veces intempestivamente, sin ellos no existiría ninguno de estos proyectos". Y, finalmente, para los usuarios, "los que hacen que hagamos algo. Cuando empezamos no sabíamos nada de esto, podíamos hablar de bits y de bytes, pero ellos nos enseñaron el resto".

Entregados todos los premios, tuvo lugar el tradicional concierto de música de cámara a cargo de Rafael Domínguez (violonchelo) y Antonio Palmer (piano) y, para finalizar, un vino español.



XV FORO DE SEGURIDAD Y PROTECCIÓN DE DATOS EN SALUD

"RGPD: Qué nos exige a las Organizaciones Sanitarias"

LOS PASADOS 14 Y 15 DE FEBRERO TUVO LUGAR, EN EL AULA MAGNA DEL RECTORADO DE LA UNIVERSIDAD DE VALENCIA, EL XV FORO DE SEGURIDAD Y PROTECCIÓN DE DATOS EN SALUD. LA CITA, ORGANIZADA POR LA SEIS, EN COLABORACIÓN CON LA CONSEJERÍA DE SANIDAD UNIVERSAL Y SALUD PÚBLICA DE LA GENERALITAT VALENCIANA, SUPERÓ LA ASISTENCIA DE EDICIONES ANTERIORES.

ACTO INAUGURAL



El acto de inauguración contó con la participación de Ana Ávila Peñalver, directora general de Investigación de la Generalidad Valenciana; Luciano Sáez Ayerra, presidente de la Sociedad Española de Informática de la Salud y Mar España Martí, directora general de la Agencia Española de Protección de Datos.

Luciano Sáez fue el encargado de dar la bienvenida y agradecer su presencia a todos los asistentes, agradecimiento que hizo extensivo a la Consejería de Sanidad Universal y Salud Pública de la Generalitat Valenciana y a la Universidad de Valencia. "Hemos contado con la colaboración de la Agencia Española de Protección de Datos, la Autoridad Catalana de Protección de Datos, la Agencia Vasca de Protección de Datos y el Consejo de Transparencia y Protección de Datos de Andalucía", dijo. "Nuestra sociedad agradece a la directora general de Investigación, Innovación, Tecnología y Calidad, Ana Ávila Peñalver, su presencia. Es importante que se impulse este encuentro entre profesionales sanitarios, gestores, directivos, responsables tecnológicos y las autoridades de protección de datos.
Nuestro agradecimiento especial a Mar España, directora de la Agencia Española por impartir la conferencia inaugural de esta edición. Su presencia en el Foro, como máxima autoridad española en materia de protección de datos, demuestra la sensibilidad e importancia que concede a nuestro sector. Así mismo, nuestro

agradecimiento a todos los profesionales de la Consejería; a **Carmen Ferrer, Juan Miguel Signes** y **Miguel Chavarría,** delegado de la SEIS en Valencia, por su colaboración en la organización de esta reunión". No quiso olvidar a **Emilio Aced,** "secretario general de nuestra Sociedad y coordinador general e impulsor de este foro durante 11 años. Para nosotros siempre estará presente".

Sáez afirmó que "la SEIS tiene dentro de sus objetivos fundacionales organizar acciones que favorezcan el desarrollo y la implantación de las tecnologías de la información y las comunicaciones en el sector sanitario. Para ello pone en marcha diversas iniciativas que fomenten el desarrollo tecnológico en el ámbito de la salud con pleno respeto a los derechos de las personas y, en concreto, a su privacidad. En el año 2004, la SEIS creó el Foro de Protección de Datos de Salud, con la misión de disponer de un espacio de encuentro entre los profesionales que desarrollan su actividad en el ámbito sanitario, las autoridades de protección de datos y el sector tecnológico. El fin era compartir experiencias y conocimiento para asegurar una atención sanitaria de calidad y respetuosa, como ya he mencionado, con los derechos de los ciudadanos. Para cumplir esta misión se establecieron diversos objetivos que intentamos conseguir. Consideramos vital la colaboración de la Agencia Española y las Agencias Autonómicas, que con su sensibilidad hacia los temas de salud nos animan a seguir adelante. Agradecemos tanto a sus directores como a sus profesionales, el apoyo que se materializa año tras año, tanto en el propio diseño de las sesiones, como en su asistencia a la reunión anual.

Incorporamos la palabra 'seguridad' en nombre del Foro, ya que es un concepto vital en el diseño e implantación de los sistemas de información de salud. Por ello se constituyó la Red de Responsables de Seguridad del Sector Sanitario, con la denominación estatutaria de la SEIS: Comité Técnico de Seguridad de la Información de Salud. Este comité se puso en marcha para facilitar el establecimiento de canales de comunicación y de compartición de experiencias entre los profesionales del sistema sanitario". De hecho, "esta mañana han celebrado su undécima reunión para valorar sus actuaciones y necesidades y, en la primera sesión de este Foro, han presentado loss resultados", afirmó Sáez, que no dejó pasar la oportunidad de felicitar a **Juan Díaz** y **Juan Miguel Signes,** coordinadores del comité, por el trabajo realizado.

El presidente de la SEIS avanzó que el Foro se centraría en el nuevo reglamento general de protección de datos, que será de plena aplicación el 25 de mayo de 2018. "Este reglamento recoge cambios profundos y presenta nuevos enfoques para el abordaje de la protección de datos y, entre ellos, está el principio de responsabilidad activa. Este principio enmarca este Foro y, en concreto, cómo se traslada en sus diferentes aspectos a las organizaciones sanitarias y al personal que presta los servicios".

También hizo extensivo su agradecimiento a **M. Jesús Gemma Múgica Anduaga**, directora general de Osakidetza, así como a todas las empresas que, con su colaboración, hicieron posible el Foro: SIA, Panda Security, GMV y Philips Health System, no solo por su ayuda económica "sino por creer en nuestro proyecto y facilitarnos su conocimiento y tecnología". El capítulo de agradecimientos se cerró con la mención al trabajo de **Juan Díaz,** coordinador del Foro y a los miembros del comité organizador y del comité de programa: **Rosario Heras Carrasco, Manuel Medina Guerrero, Ramón Miralles López, Pedro Alberto González González, Juana M. Vegas Fernández, Carmen Ferrer, Juan Miguel Signes, Carlos García Codina** y **Francisco Martínez del Cerro.**

CONFERENCIA INAUGURAL

Mar España Martí fue la encargada de impartir la conferencia inaugural. Licenciada en Derecho por la Universidad Pontificia de Comillas, máster en Protección Internacional en Derechos Humanos por la Universidad de Alcalá y experta en gestión de entidades sin ánimo de lucro por la fundación Luis Vives, es funcionaria de carrera del Cuerpo Superior de Administradores Civiles del Estado en la especialidad jurídica desde 1989. En cuanto a su actividad académica, ha sido profesora del Máster de Protección Internacional de Derechos Humanos de la Universidad de Alcalá; profesora del Máster de Acción Política del Colegio de Abogados y la Universidad Rey Juan Carlos y profesora colaboradora de Derecho Administrativo en ICADE. Desde julio de 2015, es Directora de la Agencia Española de Protección de Datos.



Su conferencia puso de manifiesto que el Reglamento supone un planteamiento distinto con respecto al modelo que se ha venido aplicando tradicionalmente en protección de datos personales, sustituyendo el actual enfoque reactivo por uno preventivo y dinámico basado en el principio de responsabilidad proactiva. En este marco, realizó una presentación de las novedades que incorpora el Reglamento y de las acciones que la Agencia ha puesto en marcha para ayudar a cumplir con las nuevas exigencias.

Consideró importante mencionar las peculiaridades del sector sanitario que, "por su propia idiosincrasia, trata datos sensibles que pueden afectar a la esfera más íntima de las personas, y cuyo tratamiento o difusión para fines espurios puede tener consecuencias irreversibles en sus vidas. Es por ello que, en este sector, es imprescindible que los datos sean tratados garantizando la confidencialidad de la información y la intimidad de los pacientes por parte de todos aquellos profesionales, sanitarios o no, que tienen acceso a ella".

La directora de la Agencia señaló que "el gran avance de la tecnología ha permitido innovar en los métodos diagnósticos y en los tratamientos además de en los procesos de gestión. En el entorno sanitario, en los dos últimos años, la Agencia, en buena parte de los procedimientos sancionadores y de tutela de derechos que ha tramitado, se ha encontrado con incidencias relativas al acceso a la historia clínica. En el caso de los procedimientos de tutela, porque el paciente considera que la información facilitada por el centro está incompleta, porque no se le ha proporcionado el acceso a sus datos a través de un procedimiento sencillo y gratuito o porque le deniegan la cancelación de sus datos. Los procedimientos sancionadores tienen su causa, entre otros aspectos, en accesos indebidos a la historia clínica por falta de medidas de seguridad o quiebras de las mismas.

Centrándose en el RGPD, España informó de la pretensión del mismo para avanzar hacia una implantación única en todo el territorio de la Unión, así como afianzar la cultura de protección de datos preventiva y proactiva en todos los ámbitos, haciendo especial hincapié en la prevención por parte de las organizaciones que tratan datos, la llamada responsabilidad proactiva".

Actuar una vez se ha producido una infracción no es suficiente para mitigar el daño causado y, por ello, Mar España hizo referencia a la batería de medidas que incluye el Reglamento y que tienen por objeto que los daños no lleguen a producirse. Entre las medidas que puso de manifiesto cabe destacar el mantenimiento de un registro de actividades de tratamiento, implantar medidas de seguridad adecuadas en función del riesgo, realizar evaluaciones de impacto, nombrar un delegado de protección de datos, notificar las violaciones de seguridad de datos de carácter personal en caso de producirse o la promoción de códigos de conducta y esquemas de certificación.

De gran importancia es la interpretación que se está dando en algunos entornos sanitarios en rela-

ción a cómo puede afectar la aplicación del Reglamento y el contenido de la futura LOPD a la investigación. En este sentido, la directora de la Agencia afirmó con rotundidad que el marco legal de la investigación biomédica no ha cambiado, ya que el Reglamento contiene las mismas excepciones que se establecen en la legislación actual en cuanto a la compatibilidad del fin cuando es por motivos científicos. Así, recordó que el Reglamento, en su artículo 9.2 j), habilita el tratamiento de datos sensibles con fines de investigación científica de forma expresa. Incluso en el ámbito de la investigación pública podría invocarse el "interés público esencial" como causa legitimadora admitida por el artículo 9.2 g). Añadió que el artículo 58 de la Ley 14/2007, de Investigación Biomédica, regula la investigación con muestras biológicas y en su apartado 2 recoge que de forma excepcional podrán tratarse muestras codificadas o identificadas con fines de investigación biomédica sin el consentimiento del sujeto fuente, cuando la obtención de dicho consentimiento no sea posible o represente un esfuerzo no razonable. En estos casos se exigirá el dictamen favorable del Comité de Ética de la Investigación correspondiente.

En consecuencia el RGPD y el Proyecto de Ley Orgánica de Protección de Datos no sólo mantienen inalterado el régimen contenido en la Ley 14/2007 de investigación biomédica y el RD 1090/2015 sobre ensayos clínicos con medicamentos, sino que permiten realizar una interpretación más flexible del alcance que puede darse al consentimiento prestado de conformidad con la misma, superando, a título de ejemplo, la interpretación más restrictiva contenida en el artículo 60 de la Ley de Investigación Biomédica.

A partir de la aplicación del Reglamento no será necesario que la persona preste su consentimiento para una investigación concreta; ni siquiera para la realización de investigaciones en una rama muy delimitada, sino que, teniendo en cuenta la interpretación derivada directamente del RGPD, será suficientemente inequívoco y específico el consentimiento prestado en relación con una rama amplia de investigación como, por ejemplo, la investigación oncológica, o incluso para ámbitos más extensos.

Por otro lado, la Ley 14/2007 también contempla la posibilidad de realizar investigaciones sin consentimiento con un conjunto de garantías entre las que destacan que sean investigaciones de interés general y que las autoricen los comités de Ética de la Investigación. Sobre esta situación, la Agencia ha puesto de manifiesto que el RGPD permite una interpretación más amplia y flexible de los fines de investigación para los que debe prestarse el consentimiento o de los supuestos en que excepcionalmente la norma no lo exige.

Continuando con las medidas incorporadas en el RGPD, en la ponencia se destacó que estas se aplican también a responsables y encargados no establecidos en la Unión Europea siempre que realicen tratamientos derivados de una oferta de bienes o servicios destinados a ciudadanos de la Unión o como consecuencia de una monitorización y seguimiento de su comportamiento.

Se realizó una mención especial sobre la necesidad de realizar una evaluación de impacto cuando sea probable que el tratamiento previsto realizar entrañe un alto riesgo para los derechos y libertades de las personas; la responsabilidad de los directivos en las organizaciones sanitarias sobre los que se ha intensificado el foco desde la generalización de las normas de control (corporate compliance); y la obligación de nombrar un Delegado de Protección de Datos como figura esencial para la organizaciones y, especialmente, para las sanitarias debido a su cometido transversal, que lleva a exigir un perfil con elevada aptitud y un profundo conjunto de conocimientos jurídicos, tecnológicos y sobre la organización. En este último punto, la directora puso enfatizó el trabajo que está realizando la Agencia con los colegios profesionales para que estos puedan ofrecer servicios de delegado de protección de datos a sus colegiados, de tal forma que una pequeña consulta médica pueda utilizar los servicios del delegado nombrado por su colegio profesional.

El entorno sanitario es una prioridad en el Plan Estratégico 2015-219 establecido por la Agencia. En este sentido, la AEPD ha presentado las conclusiones del plan sectorial de oficio que realizó en el ámbito de la sanidad pública, pero las actuaciones van a continuar con dos nuevas actuaciones: la elaboración de guías para instituciones sanitarias y profesionales de la salud y un plan de inspección de oficio al sector socio-sanitario, ambos a desarrollar en el período 2018-2019.

En cuanto a otras actuaciones destacadas de la Agencia en relación con el impulso del Regla-

mento hay que mencionar el mantenimiento de reuniones estratégicas y talleres prácticos realizados con Unión Profesional y con los colegios profesionales, la presentación de materiales útiles entre los que se pueden destacar las guías de análisis de riesgos y evaluación de impacto, así como las jornadas celebradas con representantes de las distintas Comunidades Autónomas.
Finalmente, destacó el importante papel que desempeña la SEIS como piedra angular en la gestión sanitaria, concluyendo que, aunque el cambio normativo supone cambios en la manera de abordar la protección de los datos personales, esta transición debe ser abordada como una oportunidad de evolución y mejora.

A continuación, intervino la directora general de Investigación, Innovación, Tecnología y Calidad, Ana Ávila Peñalver. Puntualizó que "hablamos de datos, seguridad y protección, pero de datos de salud, que son los más sensibles y los que todos queremos preservar". En su opinión, las entidades sanitarias disponen de muchos datos y son un ejemplo de la necesidad y el manejo "de manera que podamos proteger estos datos".
Aludió a la referencia explícita de Mar España a los temas que contempla el reglamento de protección de datos y nos hemos asustado un poco pero se ha explicado que los cambios van a proporcionarnos oportunidades de mejora y que la supuesta moratoria que pensábamos que podría surgir a partir del 25 de mayo no se va a producir.
El objetivo fundamental del RGPD, como todos Vds. bien saben, es proteger a las personas físicas, sus derechos y libertades fundamentales. En el caso que nos ocupa, es decir, en el caso de los datos de salud, hay que mejorar la calidad asistencial al tiempo que se respeten escrupulosamente los derechos y libertades de las personas. Esto va a constituir un reto muy complicado y difícil que va a requerir mucho esfuerzo por parte de todos los agentes implicados y, aparte de esfuerzo, va a requerir grandes dotes de imaginación".
Ávila Peñalver dijo que el reto mencionado, tiene múltiples razones: "en primer lugar, por la naturaleza de los datos que tratamos, es decir, son datos de salud que es el bien más preciado y cuyo uso indebido puede ocasionar problemas



terribles y catastróficos. Ese uso inadecuado puede dañar seriamente los derechos y libertades de las personas. En segundo lugar, esto significa un reto por la naturaleza de los tratamientos a los que vamos a someter a los datos. Aquí me gustaría resultar dos aspectos: por una parte, la integración de la información sanitaria con los datos sociales. Quiero aprovechar para hacer referencia a un proyecto con el que pretendemos introducir los datos sociales, tan dispersos, en los sistemas de información que maneja la Consejería; introducir parte de la información que vaya a ser necesaria para la sanidad, en un sistema muy robusto que tenemos en la Consejería de la Sanidad Universal que utilizamos en la primaria. Se trata de un proyecto que además fue presentado hace unas dos semanas por la vicepresidenta del gobierno Valenciano. Se trata de un proyecto muy interesante que va a permitir la atención integral a las personas que pretendemos. Otra cuestión relativa al tratamiento de los datos y que forma parte de este reto es que, en la Consejería, tenemos una cantidad de datos imposible de imaginar que hay que tratar de otra manera. Tenemos un proyecto de big data que estamos lanzando gracias a la financiación Feder, que todavía debemos acabar de definir. Otra de las razones por las cuales los datos de salud representan un reto es por el tipo de infraestructuras que cada vez son más complejas, con equipos de todo tipo, que reclaman su conexión a internet. La cuarta razón es por las dificultades de las instituciones a adaptarse a las exigencia del RGPD y la quinta se debe la novedad estructural que introduce el RGPD".

PRIMERA SESIÓN



Estuvo dedicada a la "Seguridad y Privacidad, desde el diseño hasta el Producto". Actuó como moderadora **Carmen Ferrer Ripollés,** subdirectora general de Sistemas de Información para la Salud de la Dirección General de Investigación, Innovación, Tecnología y Calidad de la Consejería de Sanidad Universal y Salud Pública de la Generalidad Valenciana. Comenzó agradeciendo a la SEIS que hubiese elegido como sede a la ciudad de Valencia y a todos los presentes su interés por algo tan complicado como es la utilización de los datos en salud.

"La tecnología ofrece la posibilidad de proporcionar al ciudadano una cantidad de servicios antes impensables, pero también tiene ciertos riesgos, sobre todo, en lo relativo a la confidencialidad de sus datos personales. En esta primera mesa el foco lo vamos a poner fundamentalmente en dos temas. El primero, en la visión de las empresas que están generando gran cantidad de servicios y de herramientas que utilizamos en las instituciones sanitarias. También en aspectos de seguridad. Por otro lado, se presentarán las conclusiones de la Reunión del Comité Técnico de Seguridad de la Información en Salud". Tras preguntarse en qué punto nos encontramos con respecto al RGPD, dijo que "tendríamos que ir hacia atrás para comprender porqué estamos donde estamos. Hace mucho, en 1992, se publicó la ley orgánica que regulaba el tratamiento automatizado de datos. La 'a' de automatizado nos sigue haciendo daño, porque se sigue considerando y asumiendo que los asuntos de seguridad corresponden a la parte tecnológica, a la parte informática. Fue un decreto que no tuvo un reglamento en medidas de seguridad. En 1999 se publicó la LOPD que quitó la 'a' de automatizada para que nos tuviéramos que preocupar tanto de la información en soporte digital, como de la información en papel. En febrero de 2006 se desarrolló la ley. Así hemos trabajando hasta que, en mayo de 2016, apareció el RGPD que en el próximo mes de mayo alcanzará su vigencia plena. Será muy interesante conocer la opinión de las empresas del sector sobre el tema que nos ocupa".

En primer lugar, dio la palabra a **Jaime Martínez Sánchez,** responsable de Desarrollo de Negocio GRC & IT Legal Advisory de SIA Group. Su ponencia versó sobre "La privacidad como antesala del Tratamiento" y giró en torno a tres ejes fundamentales:

1. **Cultura de privacidad:** Fomentar y mantener una cultura de privacidad que se capilarice hacia todos los colectivos que forman parte de las organizaciones. En este punto, planteábamos la necesidad de establecer, en fase temprana, verificaciones relativas a privacidad sobre todos los nuevos supuestos (tratamientos, sistemas, servicios, iniciativas, proyectos…), a pesar de que no siempre resulte exigible realizar una evaluación de impacto a la privacidad (PIA), por no concurrir los presupuestos establecidos en el artículo 35 del RGPD.
2. **Cumplimiento integral:** Abordar el cumplimiento del Reglamento General de Protección de Datos (RGPD) desde una perspectiva in-

tegral. Precisamente, es en este punto donde SIA puede aportar un enorme valor a las organizaciones que se encuentren inmersas en el proceso de adaptación al RGPD, al proponer una visión global que muy pocas empresas están en condiciones de ofrecer, y que se proyecta a lo largo del ciclo de vida del tratamiento de los datos de carácter personal, a través de tres vectores principales:

- El consultivo: Grupo SIA cuenta con una solución modular que cubre, no sólo el proceso de adaptación a RGPD en sentido estricto, sino también los aspectos de formación, concienciación y comunicación, así como el soporte necesario para mantener vivo el modelo con posterioridad al 25 de mayo de 2018, fecha en la que resultará plenamente aplicable el texto reglamentario. Las soluciones consultivas de Grupo SIA están avaladas por una contrastada solvencia técnica, tanto empresarial, como de los equipos multidisciplinares con los que cuenta la División de Consultoría de SIA, con más de 20 abogados especializados en tecnologías de la información, y más de 50 ingenieros superiores, en posesión de certificaciones de reconocido prestigio en el mundo de la privacidad y la seguridad de la información.
- El de gestión: SIA es partner de OneTrust, tecnología líder a nivel mundial en la gestión de los programas de privacidad y avalada por una solvente comunidad de expertos (entre ellos, la IAPP). Dicha herramienta permite controlar y gestionar, a lo largo del tiempo, el cumplimiento del RGPD, especialmente en entornos organizativos complejos y distribuidos.
- El conocimiento tecnológico atesorado por Grupo SIA, en su rol de empresa integradora de tecnologías líderes provistas por diferentes fabricantes de reconocido prestigio internacional, lo que favorece la mejor aproximación tecnológica al cumplimiento de muchos de los requisitos técnicos o funcionales establecidos por RGPD, y aporte un enorme valor a lo largo del ciclo de vida del tratamiento de los datos.

3. **Racionalización y eficiencia:** La protección de datos de carácter personal no es, ni mucho menos, una nueva disciplina introducida por el RGPD. En España resulta exigible desde el año 1.992 y, en mayor medida, desde el año 1.999. A este respecto, se hace necesario identificar aquéllos elementos ya implementados con los que, en todo o en parte, se cumpla con diferentes requisitos del RGPD. A mayor abundamiento, la racionalización permitirá, no sólo, lograr dicho propósito, sino también evolucionar el cumplimiento de RGPD hacia un modelo GRC, identificando qué controles emanados de "otras normas" aplicables a una organización, permiten cumplir requisitos de RGPD, y qué controles emanados de RGPD permiten cumplir requisitos de esas "otras normas". A este respecto, Grupo SIA recomienda a las organizaciones dotarse de un Modelo Unificado de Controles (MUC) al que, previa racionalización, se incorporen un conjunto limitado de controles transversales, a través de los cuales poder gestionar, de una manera eficiente, el cumplimiento de diferentes regulaciones (entre ellas, RGPD).

Precisamente, uno de nuestros clientes, la Gerencia de Informática de la Seguridad Social (GISS), ha obtenido el premio 2017, concedido por la Agencia Española de Protección de Datos, a las 'Buenas prácticas en privacidad y protección de datos personales sobre iniciativas para adaptarse al Reglamento europeo de Protección de Datos", apoyando el cumplimiento del RGPD en el MUC, de la mano de SIA.

Vicente Martín García, director preventa de Panda Security, comentó a continuación que en Panda se hacen la reflexión de donde están realmente los datos. "Cuando pensamos en ello, a todos nos viene la idea de un gran data center, con grandes medidas de seguridad y donde todos los datos están protegidos, y también, una base de datos centralizada o nos viene la imagen de un pequeño servidor con una serie de permisos de accesos a la información que allí está contenida. Aunque allí haya datos, la gran mayoría son accesibles desde el puesto de trabajo, gracias a un equipo que tiene movilidad y que tiene acceso a los datos, porque tiene permiso para acceder a ellos". Recuerdó que el Índice SEIS dice que el 80% de los datos de este tipo de organizaciones se manejan de forma estructurada y en su gran mayoría están almacenados

en un PC y son accesibles. "Todo ello nos lleva a una situación en la que tenemos muchos datos dispersos y estructurados. Nosotros necesitamos trabajar con datos en local, es decir, accedemos a diferentes bases de datos y toda esa información la podemos consultar de manera directa con las aplicaciones que tenemos. Esto nos lleva a una situación en la que nos encontramos con datos dispersos, desestructurados y sensibles que llevan información con la que se puede identificar a los pacientes, por lo cual, hay que protegerlos y hay que saber dónde están y que tratamiento se está haciendo y, sobre todo, paliar las fugas de información que pudieran presentarse y, por supuesto, protegerlos de ciberataques". Citó varios ataques y robos de información relacionados con los datos sanitarios y finalizó afirmando que, "en Panda, disponemos de muchas medidas para la seguridad de los datos.

Rubén Villoria Medina, consultor de Sanidad y Project Manager en proyectos de Sanidad GMV, habló de las experiencias en Seguridad y Privacidad desde el diseño en el proyecto Harmony, en el cual se centró su intervención.

Harmony (Healthcare Alliance for Resourceful Medicines Offensive Against Neoplasms in Hematology), https://www.harmony-alliance.eu/, es un Proyecto IMI (Innovative Medicines Initiative), con el Consorcio público-privado más grande a nivel europeo centrado en el estudio de neoplasias hematológicas (53 partners de 11 países).

Este proyecto combinará datos clínicos de alta calidad con datos ómicos para optimizar y precisar los tratamientos en pacientes con enfermedades hematológicas. Para su diseño y ejecución abarca a todos los perfiles involucrados en estas enfermedades: Pacientes, Profesionales de la Salud, Asociaciones reguladoras, HTAs, Industria farmacéutica y Academias.

Los retos actuales y futuros del proyecto y de la plataforma que se ha construido son:

- Capacidad para evaluar las fuentes a injestar para medir el nivel de calidad de sus datos clínicos.
- Ser capaz de integrar múltiples fuentes de datos con información y tipos, muy heterogéneos utilizando un modelo de datos común.
- Obtener respuestas y conclusiones derivadas del análisis en conjunto de diversas fuentes de datos, cosa que no sería posible a partir de una única fuente.
- Definir flujos de datos cumpliendo la RGPD a través de la anonimización, con el soporte de comités éticos y expertos legales y cooperando con otros proyectos bajo el paraguas del BD4BO (Big Data For Better Outcomes).

En cuanto a los retos de privacidad y seguridad que se plantean están los de definir un marco ético legal para poder introducir y reutilizar los datos definiendo un proceso de anonimización de "Facto", que permita la utilización de datos de estudios ya finalizados.

Para la parte de cumplimiento de las regulaciones hay que tener en cuenta tanto el RGPD como las especificidades que se apliquen en cada uno de los países que participaran en el proyecto: España, Francia, Alemania, Italia, Reino Unido, Bélgica...

Para todo esto GMV, junto con el resto de partners del proyecto, empiezan definiendo las necesidades y objetivos del proyecto así como una exhaustiva revisión de todos los reglamentos que son aplicables. El punto de partida de este análisis es la realización de un PIA (Privacy Impact Assesment), en el cual se involucran a todos los perfiles del proyecto: Clínico, Ético, Legal, Técnico; proporcionando de esta manera una visión global de los riesgos y los objetivos, pudiendo establecer desde el diseño los controles necesarios para proteger la privacidad.

Desde el punto de vista técnico, el Hosting se aloja en un CPD que cumple con la ISO 27001 aplicando todos los controles identificados y necesarios en las cuatro capas de la plataforma: Físico, Red, Host y Servicios / Aplicaciones.

Además de los controles técnicos de seguridad se han definido en el proyecto en todos los niveles de accesos que roles y sobre que aplicaciones y datos se tendrá acceso: gobernanza de datos.

En nuestra experiencia, GMV como empresa líder en Seguridad y Privacidad, la clave está en incluir estas necesidades como requisitos en el diseño del proyecto e incluir a todos los perfiles implicados para detectar en esta fase de análisis los riesgos aplicables y poder aplicar los controles que los mitiguen.

Jorge Hernández de Sande, especialista en Servicios del Área de Monitorización y sistemas de Gestión Clínica, de Philips Health Systems, intervino con el tema "Malware: cuando los equipos no sólo se hacen viejos sino peligrosos".
En primer lugar, quiso llamar la atención sobre un tema relacionado con la electro medicina, que consiste en que no solo es importante la obsolescencia técnica de los productos sino su constante actualización. En su opinión, no solo hay que saber dónde está el dato, si no cómo lo adquirimos. Comentó que los dispositivos médicos "pertenecen a un mundo que cada vez está más interconectado y a la vez son ya incuestionables y se ha convertido en una prioridad para todo el sistema sanitario. Sin embargo, la mayor conectividad e integración con otros sistemas expone a los dispositivos médicos a vulnerabilidades de seguridad de las que estaban previamente protegidos. Por ello es preciso integrar estos dispositivos en los análisis de riesgos de la organización, prestando especial atención al impacto que supone su obsolescencia".
Enumeró lo que denomina los 10 riesgos más destacados de la tecnología de la salud según el Instituto ECRI y ofreció datos interesantes sobre el impacto de los ataques de ransomware y la obselescencia. Según FENIN, el 70% de los TAC, el 69% de los ecógrafos y el 81% de los equipos de soporte vital superaban, a finales de 2016, los 5 años de antigüedad.
En su opinión, "asusta la dimensión de lo que ha pasado estos últimos años respecto al número de ataques que se han producido en el entorno sanitario y cómo se han puesto en compromiso millones de pacientes con el coste, no solo desde el punto de vista del dato, sino también el impacto asistencial en las organizaciones".
Comentó como ejemplo del impacto que han tenido estos problemas en los dispositivos médicos los sistemas de monitorización. "En los sistemas de telemedicina observamos que hay una fuerte inversión inicial seguida de 8 o 10 años en el que el mantenimiento que aportamos es de tipo preventivo y correctivo", concluyó.

Juan Miguel Signes, coordinador del Comité Técnico junto a Juan Díaz García, presentó las conclusiones del Comité Técnico de Seguridad de la Información.

La reunión tuvo lugar como prólogo a las XV Jornadas de Seguridad y Protección de Datos de Salud y contó con la asistencia de representantes de casi todas las CC AA. Durante la reunión se hizo patente una vez más el interés y la necesidad de aumentar la colaboración y coordinación entre los agentes que tienen un papel destacado en estas materias en las distintas CC AA. En este sentido, resaltaron el acierto y esfuerzo de la SEIS al propiciar estos encuentros.
Todos los participantes coincidieron en la adecuación al nuevo marco normativo que regulará la protección de datos personales a partir del próximo 25/05/18. Los organizadores propusieron cuatro temas, uno fácil, otro resbaladizo, un tercero por el que se pasó de puntillas y un cuarto al que apenas dio tiempo para algunos comentarios.
El primero tuvo que ver con el cumplimiento del deber de información (RGPD Arts 12-14). Más concretamente con la necesidad de consensuar los conceptos y la iconografía que se utilizarán en la primera capa informativa. Sin ese consenso las diferencias entre las CC AA pueden dar al traste con el objetivo que persigue el RGPD, que no es otro que el de facilitar la comunicación a los interesados. En un momento posterior a la reunión, surgió la oportunidad de comentar este asunto con la directora de la AEPD, que recogió el guante y se ofreció a colaborar en la iniciativa.
El segundo asunto tuvo que ver con la gestión de los consentimientos (RGPD Art. 7), especialmente con el procedimiento de firma por parte de los interesados y con la digitalización de los documentos en papel. La validez de los sistemas basados en firma manuscrita sobre soporte electrónico fue objeto de discusión, comentándose los riesgos que algunos se han atrevido a asumir y otros no. Los informes en que se han basado esas actuaciones no son coincidentes y la situación genera inseguridad. Una solución podría venir de la mano de una regulación sectorial, que también podría terciar en otro asunto relacionado con la digitalización automática de las historias clínicas en papel. La creación de copias auténticas, tal como establecen las Normas Técnicas de Interoperabilidad, para grandes volúmenes de documentos resulta inviable dado que requieren una actuación por parte de un funcionario habilitado. A la espera de esta u otra

solución lo más prudente es realizar un análisis de riesgos y actuar en consecuencia.
El tercer asunto fue el nivel de detalle (granularidad) que hay que aplicar al concepto de tratamiento. La conclusión provisional fue que habría que considerar al menos dos niveles distintos. Uno más grosero para mantener el registro de las actividades de tratamiento (RGPD Art. 30), y otro más detallado para el control de tratamientos necesario para demostrar diligencia en aplicación del principio de responsabilidad proactiva (RGPD Art. 5.2).
El último asunto fue el problema organizativo que plantea el RGPD a las administraciones públicas con la creación de la figura del Delegado de Protección de Datos, la dotación de capacidades de análisis y gestión de riesgos, auditoría interna, etc. Para apreciar el problema en su justa medida hay que tener en cuenta la realidad de estas entidades (véanse los resultados del informe INES, en particular el nivel de cumplimiento del ENS y el nivel de madurez), las plantillas insuficientes y las todavía fuertes restricciones presupuestarias. Pese a todo, una conclusión que parece generar bastante consenso es la de dotarse de un DPD por servicio autonómico de salud asistido por un potente equipo multidisciplinar (ingenieros y letrados), con uno o más referentes en cada hospital con los que coordinaría todas las actuaciones.
La reunión finalizó reconociendo el interés de estos encuentros y la necesidad de encontrar vías que faciliten la colaboración (mensajería, reuniones virtuales a través de alguna plataforma de comunicación), la elaboración de recomendaciones y de informes, por ejemplo, para trasladarlos a las autoridades con capacidad para resolver los conflictos planteados. El interés y la necesidad fueron evidentes, sólo faltará que el día a día permita materializar esa voluntad en actuaciones reales.

SEGUNDA SESIÓN DEBATE



Bajo el lema "La Responsabilidad de los Directivos de las Organizaciones Sanitarias", la sesión fue moderada por **María Jesús Gemma Múgica Anduaga,** directora general de Osakidetza (Servicio Vasco de Salud) que, como directiva, comentó que ante la próxima fecha de entrada del cumplimiento del Reglamento General de Protección de Datos, tras dos años de transición para las adaptaciones tras su entrada en vigor, "va a llegar el 25 de Mayo y todos estamos un poco agobiados". Recordó que el nuevo marco normativo conlleva una serie de obligaciones y retos como la ventanilla única, la obligación de comunicar a las autoridades en el plazo de 72 horas incidentes graves como el acceso masivo indebido a datos protegidos o la nueva figura del delegado de protección de datos.

El primer ponente fue **Juan Fernando Muñoz Montalvo,** subdirector general de Tecnologías de la Información del Ministerio de Sanidad, Servicios Sociales e Igualdad, quien reconoció la dificultad de "hacer ver a los decisores esos elementos que están por debajo" que son obligaciones del nuevo reglamento como "la protección por diseño" y que "son difíciles y caros" de

implementar. Comentó que para las obligadas notificaciones a las autoridades por quiebra de seguridad, primero hay que darse cuenta del incidente y "esto a veces no es fácil".
Resaltó que adaptarse al nuevo reglamento exige un "cambio de forma de trabajar en la organización" y puede suponer una oportunidad "muy grande para permitir alinear dos enfoques, el de la protección de datos y el de la seguridad", lo que traerá claros beneficios.
En cuanto a su propia organización, citó como ejemplo de la dificultad de las adaptaciones, su experiencia de implantación de un esquema de certificación a la ISO 27000 que les costó 3 años pero que les ha facilitado el paso a la auditoría que exige el Esquema Nacional de Seguridad y lo mismo hará con algunos elementos que exige el nuevo RGPD. En cuanto a las CCAA, reconoció que "no hemos conseguido desde el Ministerio ayudar demasiado", si bien existe disposición en el Comité Técnico del Ministerio por carácter "autoorganizativo" y ante el algo grado de concienzación de los directivos de TI de alto nivel en el tema.

Ángel Serrano Cugat, secretario general técnico de la Consejería de Salud de la Junta de Andalucía, realizó un repaso de algunos aspectos del contenido del nuevo reglamento, advirtiendo los cuatro requisitos que impone:

1. Refuerzo de los derechos de los usuarios,
2. Refuerzo de las obligaciones de los que tratan los datos,
3. Refuerzo del poder de las autoridades de protección de datos,
4. Las infracciones conllevan más sanciones, continuando por las obligaciones de una de las figuras que sigue contemplando el reglamento en comparación a la LOPD actual: el responsable del tratamiento de datos, bajo los nuevos principios de "responsabilidad proactiva" o preventiva ("accountability") y el de "riesgo". Así, esta figura sobre la que recae la responsabilidad ante las autoridades (si bien recordó que a nivel de Historias Clínicas también recae la responsabilidad en las gerencias) está obligada por un lado a aplicar medidas organizativas eficaces para garantizar el cumplimiento del RGPD y la demostración de este cumplimiento, y por otro, a realizar un análisis de riesgos, que se debe tener en cuenta a la hora de decidir las medidas de cumplimiento que implantar.

Reconoció que en este momento existen serias dificultades por el hecho de que, a su juicio, el personal directivo y autoridades de las organizaciones sanitarias "no han recibido formación ni información suficiente" ni tampoco "se han asignado recursos adicionales para las nuevas tareas".

Ricard Martínez Martínez , de la Cátedra de Privacidad de la Universidad de Valencia, también apuntó que algunos retos "debíamos haberlos implantado hace tiempo", resaltando que el RGPD recoge normativamente el principio del "Privacy by design" (privacidad por diseño), del que ya se llevan décadas de investigación y hace tiempo que los desarrollos tecnológicos pueden realizarse de esa forma, con lo que no debería haber excusas para no haberlo implementado e incidió al respecto que las "leyes se publican para cumplirlas".
Comentó que no hay que perder de vista que "no protegemos datos, sino a los pacientes", que el medio ambiente en Salud es complejo, especialmente en el caso de los hospitales universitarios con investigación, y la nueva figura obligatoria por el reglamento, el Delegado de Protección de Datos, que debe "estar emponderado" en la organización y ante el debate de si debe ser una figura interna o externa, destacó que lo importante es que sea eficaz, "que cace ratones".

Manuel Vilches Martínez, director general de la Fundación IDIS, comentó las dificultades añadidas que tiene el sector sanitario privado para adaptarse a las obligaciones del nuevo reglamento, ante su mayor interrelación de agentes relevantes, como la dispersión de clínicas y profesionales que pueden prestar la atención sanitaria, o las aseguradoras, que para la facturación deben recibir información de los tratamientos sanitarios realizados sobre sus clientes.
Alertó de los riesgos de menor eficacia en la propia asistencia sanitaria que puede conllevar el nuevo reglamento, como el aumento de listas de espera ante las nuevas disposiciones sobre el Consentimiento Informado, que "va a exigir más de 20 minutos a la admisión", y la necesidad de

"definir circuitos tremendamente complicados para poder cumplir con la normativa", así como de los cambios informáticos y las necesidades de más personal, que implicarán un coste económico adicional.
Comentó que, por otro lado, el propio paciente no le da tanta importancia a la privacidad de sus datos como le dan las autoridades que han realizado la norma y opinó que las sanciones son "absolutamente desorbitadas" resaltando la discriminación que supone que las multas correspondientes no se apliquen a los servicios de salud público ante las mismas infracciones.

Ramón Martín Miralles López, coordinador de Auditoría y Seguridad de la Información de la Autoridad Catalana de Protección de Datos, comenzó citando la broma extendida en el sector: "hay dos tipos de leyes, las de obligado cumplimiento y las de protección de datos"; y aseguró que "con el RGPD esto se ha acabado", avisando del papel sancionador que se refuerza con el nuevo reglamento. A su juicio, las organizaciones deben implantar Sistemas de Gestión de Protección de Datos que se integren en la gestión ordinaria de las actividades del centro, de tal forma que la protección de datos no tenga que ser algo especial. al igual que en la gestión de un restaurante no se preocupan solamente por disponer de buenos cocineros sino también de que la propia cocina sea saludable; y resaltó que en ese esquema la nueva figura del Delegado de Protección de Datos debe contar con una relación "muy fluida y de confianza" con la directiva.

SESIÓN TERCERA



"Casos prácticos. La experiencia de las autoridades de protección de datos" fue el título de la sesión moderada por Pedro Alberto González González, responsable del Registro y Auditoría de Ficheros de la Agencia Vasca de Protección de Datos. González explicó que los ponentes de la mesa eran miembros de las autoridades de protección de datos nacional o autonómicas y se han repartido una larga serie de casos que han seleccionado de experiencias reales, que se presentan por orden de temas o principios del reglamento.

Los ponentes fueron Cristina Gómez Piqueras, inspectora – instructora de la Subdirección General de Inspección de Datos de la Agencia Española de Protección de Datos; Carles San José i Amat, jefe del Área de Inspección de la Autoridad Catalana de Protección de Datos y Juana María Vegas Fernández, letrada de la Asesoría Jurídica de la Agencia Vasca de Protección de Datos.

En primer lugar se presentaron casos relacionados con el principio de "Calidad", es decir, de casos de tratamiento excesivo de datos, ante la

normativa que fije que los "tratamientos" de datos deben ser "pertinentes, adecuados y limitados a lo necesario":

- Petición de certificado de asistencia al hospital por visitar a un familiar ingresado para presentarlo en el trabajo y que resulta en un certificado expedido en el que se indica el motivo de hospitalización: es una infracción del hospital por declaración de situación personal, tras comunicarla al hospital cambió el procedimiento.
- El informe completo de asistencia médica, con sus antecedentes personales incluidos, de un detenido tras un forcejeo en la detención se entrega a la Policía Local: la APD catalana estimó que el informe completo debió haberse entregado al paciente, sin perjuicio de que se enviara otro documento estrictamente de informe de los daños recientes y sin antecedentes personales de salud al juzgado, y abrió infracción a la Policía Local.
- Parte de interconsulta del médico de cabecera a Urología en el que figura la relación completa de todos los episodios previos del paciente de todos los ámbitos y tipos: el parte debe hacer constar solamente los antecedentes relevantes para la consulta, y si no hay ninguno, "sin antecedentes relevantes".

Principio de deber de secreto:

- Una clínica utilizó para la publicidad de un tratamiento la imagen de una paciente real sin el consentimiento de ésta: sanción a la clínica.
- La hija de un paciente se ofrece a pagar la factura y la clínica entrega una factura con el detalle de todos los tratamientos sin el consentimiento del paciente: es una infracción.
- A una paciente le llegan los datos de pruebas con información adicional de otra paciente por error del hospital, denunciando la primera paciente al hospital por mal sistema: se abrió proceso de infracción que ha acabado en un mejor procedimiento de comunicación del hospital.

Derecho de acceso:

- Persona cree ser un caso de bebé robado y solicita datos al hospital de cuando nació: el hospital se la deniega al conllevar datos protegidos de su posible, tras instrucción de la Agencia Vasca se estimó que tenía el derecho a este acceso.
- Persona en situación de acogimiento familiar reclama la Historia Clínica de su madre biológica tras su fallecimiento: fue desestimado el derecho.
- Petición de estado de las células madre del cordón umbilical cedido a un centro privado para investigación: no se estima el derecho.

Acceso a los accesos de los profesionales

- Un paciente solicita la relación de profesionales que han accedido a sus datos en un hospital: caso abierto en estudio, en principio no tiene derecho por protección de datos a saber la identidad de los profesionales pero posiblemente sí si llega como petición por la ley de transparencia.

Accesos indebidos a la Historia Clínica

- Condena a 1 año y 6 meses de prisión a un médico por acceder y entregar a la historia clínica de un paciente de forma reiterada tras la solicitud de un amigo del paciente.
- Condena de prisión a un médico por el acceso diario y reiterados a la historia clínica de una mujer para obtener información para su amigo, ex-marido de la mujer.

Rectificación y cancelación de datos

Generalmente se deben a casos no bien visto socialmente. Cristina opina que los médicos son los que deben determinar si los datos son "viejos" y se pueden cancelar tras la petición de un paciente.

- Un paciente solicita borrar de la historia su trastorno bipolar "del pasado": el hospital pregunta a los médicos, que dictaminaron que se mantenga la información en la HC porque puede ser necesaria al entender que dicho trastorno o sus efectos no ha caducado.

Falta de medidas de seguridad

- Una organización sanitaria tiene un sistema informático para el acceso desde internet a los pacientes a su Historia clínica, pero resulta que permite a cualquier persona sin autentificarse conocer la relación de usuarios con HC, y a los usuarios pacientes del sistema consultar la HC de otros pacientes simplemente cambiando unas cifras de la dirección web: se multó con 30 mil euros a la organización sanitaria.

CUARTA SESIÓN DEBATE



"El Delegado de Protección de Datos" fue el tema de la sesión moderada por Juan Domene García, gerente del Departamento de Salud Valencia-Arnau de Vilanova-Llíria, quien comenzó recordando la obligación de contar para el próximo 25 de mayo con la figura del Delegado de Protección de Datos para muchos casos, entre ellos los servicios públicos y repasó sus principales cometidos:

1. Informar y asesorar al responsable y encargados de los tratamientos de datos.
2. Supervisar el cumplimiento, viniendo a jugar el papel una auditoría interna reforzada.
3. Es complementario al responsable de seguridad, ayudando en la implementación de las políticas de privacidad desde el diseño.
4. Debe establecer los registros de cumplimiento.
5. Mantener los planes de auditoría y formación.

La primera ponente, Carmen Casado Seoane, de la Junta Directiva de la Asociación Profesional Española de Privacidad [APEP], presentó una "hoja de ruta" para el establecimiento del Delegado de Protección de Datos [DPD] en la organización en la forma de respuesta a estas preguntas:

- ¿DPD sí o no? Sí, donde obliga la ley como es el caso de las Administraciones Públicas. Hay empresas que no están obligadas, como es el caso de las de Desarrollo de Sofware, pero les puede convenir para los trabajos antes sus clientes estar asesoradas con un DPD.
- ¿Cómo: interno/externo?Más conveniente que sea interno si es un sector crítico como el de los servicios de salud, pudiendo ser tanto una responsable como un órgano colegiado que cuente con recursos.
- ¿Quién?La norma exige solamente que tenga conocimientos jurídicos de Protección de Datos. Es conveniente que sepa de normativa de Salud, conozca la institución y la tecnología y tenga dotes de comunicación.

Rosario Heras Carrasco, responsable de la Unidad de Evaluación y Estudios Tecnológicos de la Agencia Española de Protección de Datos [AEPD], habló sobre la cuestión de si externalizar la figura, avisando que hay publicidad de empresas que ofrecen el servicio de DPD por costes de pocos centenares de euros al año que no son fiables, aconsejando que si se externaliza sea en una empresa de reconocida profesionalidad y contratando suficiente dedicación, pudiendo ser conveniente solicitar algún tipo de certificado (no lo exige el RGPD). A este respecto, informó que la AEPD ha diseñado un esquema de certificación con el que pretende formar y certificar buenos profesionales como DPD. Así oferta unos cursos de formación conducentes a la obtención de dicho certificado con este reparto: 50% normativa de PD y sectorial, 30% principio de responsabilidad y 20% conocimientos de auditoría; y para varios perfiles, de más horas (80) para gente sin experiencia previa en el ramo.

José Manuel Laperal González, responsable de Seguridad de Sistemas de Información de la Dirección General de la Información del Servicio Madrileño de Salud [SERMAS], comentó que en el caso del SERMAS han visto la figura del Delegado de Protección de Datos, además de obligada, como algo muy útil, y que han estado valorando si contar con un DPD en cada centro sanitario, pero ante la imposibilidad de tanta nueva plantilla y el esfuerzo adicional de coordinación que requeriría, avanzó, aunque todavía no es oficial, que van a optar por disponer de un único DPD centralizado, que sería del tipo colegiado, un Comité Delegado transversal muy reducido, en un comienzo reducido a dos personas fijas, un cargo de segundo nivel y un técnico de apoyo personal interno, y varios representantes de la Atención Especializada, Primaria, etc.

Opinó que es fundamental que esté refrendado por la más alta dirección del SERMAS y que tenga capacidad de acción en los centros.

Desde la sala se comentó que la reciente encuesta de madurez en implementación de políticas de seguridad según el Esquema Nacional de Seguridad, INES, ha mostrado que la mayoría de los hospitales están en un nivel 2, mientras que lo exigido por el RGPD se situaría en un nivel 4, lo que hace suponer que el cumplimiento del RGPD será en un principio imposible.

El responsable de seguridad del SERMAS comentó al respecto que, efectivamente la situación en centros es mejorable, aunque se ha mejorado bastante últimamente a raíz de los incidentes de seguridad por ataques informáticos, y, precisamente, la figura de un DPD centralizado puede ayudar a avanzar lo necesario.

QUINTA SESIÓN



"RGPD: ¿En qué nos afecta a los profesionales? fue el lema de la quinta sesión. Por ausencia de Jesús Rubi (adjunto a la directora de la AEPD), moderó la mesa Cristina Gómez Piqueras, que comentó que la sesión iba a tratar de cómo la RGPD va a afectar a los profesionales, que en realidad son los que van a trabajar los datos.

Juan Lucas Retamar Gentil, subdirector de Tecnologías de la Información y Comunicaciones en el Servicio Andaluz de Salud, comentó que hace algo más de un año, la Junta de Andalucía comenzó a impartir unas breves sesiones de formación a la alta dirección como consejeros, viceconsejeros, secretarios y directores generales que, en su opinión, fueron muy positivas. "Implicar a la dirección en estas cuestiones es fundamental porque, además, desde hace años hemos interiorizado que las nuevas medidas, los nuevos proyectos, se abordan sin recursos adicionales, por lo que hace tiempo se alcanzó un nivel de saturación".

Refirió que, dentro de los perfiles del sistema sanitario, hay un gran desconocimiento de lo

que esto va a representar y cómo puede afectarles, por lo que "estamos haciendo mucho hincapié en la formación y tendremos que hacer modificaciones para adaptarlas al nuevo reglamento". Consideró que el nuevo reglamento no va a tener mucho impacto en el día a día.
Respecto a la concienciación, dijo haber notado un cambio importante cuando se empezaron a abrir expedientes de investigación o sancionadores en mayor número de los que se presentan en muchas ocasiones. "Hemos modificado las alarmas y las alertas que ahora tenemos con la puesta en marcha del nuevo reglamento. Si pensamos en la investigación creo que podemos encontrarnos con más diferencias. El investigador no comprende que no le podamos proporcionar toda la investigación que necesitan". Diferenció dos situaciones. En el ensayo clínico clásico se investiga de forma regulada, con un comité de ética, con un consentimiento tácito por parte del paciente. En el nuevo reglamento se va a percibir como más y más elementos adicionales a dar.
Luego está la base de datos poblacional, en la que se añade información desde el año 2002. "Tenemos varios miles de millones de registros que, para el investigador, son una auténtica mina de oro, pero no hemos aún moderado, de manera clara, cuál es la gobernanza de esa información y bajo qué condiciones se entrega esa información, a quién y cómo".
Asumió que hay otros colectivos de profesionales, como son los de gestión, con los que tendrían que revisar los procedimientos de acceso y derecho. Mencionó a los profesionales de la informática, con los que habrá que abrir varias líneas de trabajo para adecuarse a la nueva situación.

El segundo ponente fue **Iñaqui Pariente de Praga,** abogado y profesor de la Universidad de Deusto.
Comenzó refiriéndose a comentarios que afirman que la nueva Ley General de Protección de Datos paraliza la investigación biomédica y que un buen número de asociaciones profesionales sanitarias están su contra. Tras leer el Considerando 159, sentenció que la realidad es todo lo contrario, ya que muchos fines y prioridades del nuevo reglamento están orientados a su aplicación en la investigación médica.
En relación a quién lidera la adhesión al reglamento en el ámbito interno, afirmó que "nos estamos encontrando de todo".
Consideró que, a la hora de aplicar el reglamento y trasladarlo a la organización, hay que seguir un modelo y definir roles y responsabilidades. "No podemos pensar en el delegado exclusivamente si no pensamos quién va a ser el responsable del tratamiento. Esto es lo más importante, saber si los hospitales o las consejerías van a ser los responsables. Habrá que ir rellenando los huecos, trabajando con eso e involucrando a la organización a base de ir descendiendo y el descender es la formación; difusión, formación y aceptar que trabajamos en el ámbito de la seguridad de los datos.
Es importante tener una estrategia que nos lleve al punto que queremos llegar. Si definimos adecuadamente al responsable definiremos también adecuadamente el tratamiento de los datos. Ayer lo trabajamos en la reunión que tuvimos en el comité. Nombraremos al delegado y veremos quién es el que va a establecer un conjunto de obligaciones. Hay que definir todos los roles y todos los responsables y eso nos llevará a definir correctamente el tratamiento de los datos. Por lo tanto, hay que comenzar a configurar el registro de tratamientos y, a partir de ahí, revisar sobre todo la legitimación de los tratamientos".
También comentó que los consentimientos informados ya no valen: "cada vez tienen menos importancia y lo que necesitamos es aplicar títulos que están en el reglamento y que necesariamente hay que concretar". En su opinión, crear leyes es factible y, por lo tanto, debemos desarrollar normativas e ir al tema. Es necesario añadir garantías de confidencialidad.
Finalizó su intervención incidiendo en que hay que documentarse y adelantarse a lo que pueda pasar. "Hay que tener todo pensado y acreditado. Hemos hecho muchas cosas y nos quedan otras muchas por hacer".
Insistió en la importancia de definir roles, definir responsabilidades y modificar, en su caso, los aspectos jurídicos que tenemos hasta ahora. Y terminó diciendo que el tema de buenas prácticas va a ser bien recibido incluso más allá de los aspectos legales.

Hermelinda Vanaclocha, subdirectora general de Epidemiología, Vigilancia de la Salud y Sanidad Ambiental de la Dirección General de Salud Pública de la Comunidad Valenciana comenzó su intervención preguntándose qué problemas puede tener el personal sanitario de cara a un reglamento nuevo. "Podemos encontrar mermadas las actividades que tenemos que hacer debido a la LGPD y a que a una legislación detrás exige que tengamos que desarrollar una serie de funciones y si no podemos acceder a una serie de datos a nivel individual no lo podremos hacer. Entre los profesionales de salud pública hay mucho consenso sobre cuáles son sus objetivos y sus funciones. Todo el mundo tiene claro que, desde el punto de vista asistencial, si vemos a un enfermo, hay que acceder a sus datos. Pero hay casos en los que no hacemos eso. Por ejemplo, si trabajamos en salud pública. Nosotros no actuamos sobre la población en su conjunto y, hasta ahora, con la ley de proyección de datos actual, en muchas CC AA se han presentado muchos problemas, como por ejemplo, que una persona que trabaja en epidemiología tenga acceso a la historia clínica. El problema ha llegado a tal punto que, en alguna de estas CC AA, se ha sacado legislación específica para que estos profesionales pudieran tener acceso. Con lo que ahora aparece no tenemos nada claro qué legislación va a ir detrás. El problema fundamental es que ni siquiera nos vamos a poner de acuerdo en lo que entendemos por salud pública, cuál es nuestra misión, cuáles son los servicios que tenemos que prestar, qué actividades tenemos que realizar y cuáles son los resultados que tenemos que alcanzar. Partiendo de esa base, en protección de datos resulta más difícil entender por qué tenemos que acceder a datos individuales en determinadas ocasiones. Trabajar con datos agregados es importante, ya que en alguna ocasión te facilita la toma de decisiones aunque en otros casos esto no es posible.

Pone el ejemplo de enfermedades infecciosas transmisibles. Si tenemos un caso de meningitis en un niño, como no sepamos el nombre del niño y a qué colegio va es imposible que podamos romper la cadena de transmisión. Tenemos que acceder a esos datos. Igualmente es necesario poder tener acceso a los datos en el cáncer de mama y en el cáncer de colon. Si tenemos que llevar a cabo una campaña de vacunación que, por cierto, es la medida existente –en relación al coste– más eficaz en el sistema sanitario, no podremos llevarla a cabo sin datos. Necesitamos que el reglamento tenga en cuenta estas líneas de actuación. Algunas sociedades científicas han tenido un posicionamiento conjunto y piden al gobierno que se comprometan a enviar a las Cortes una propuesta que intente paliar estas dificultades".

Finalizó considerando que una sanidad moderna se basa en la gestión inteligente de información.

Seguidamente, Carmen Espinós, que se dedica a la investigación, comentó que el término 'paralizar' es dramático y que 'dificultar' le parecía más aceptable. Al investigar sobre enfermedades raras no valen los datos anónimos. "Hago genética y la cantidad de información que recibo del genoma de un paciente es increíble, de ahí que, en mi día a día, me encuentre con dos problemas. El primero es que al transmitir la información a los hospitales con los que colaboramos y con el médico de la especialidad que toque, por ejemplo, a través de la unidad de genética, ellos tienen que interpretar la información que nosotros facilitamos. Muchas veces, si no estamos ante un especialista en genética nos encontramos con que no entienden la información que les facilitamos. Ahora trabajamos con mucha más información, ya que trabajamos con el genoma. Para trabajar mejor, los que hacemos genética nos tenemos que entender perfectamente con los que hacen clínica. Por ese motivo tenemos que conocer al paciente y necesitamos tener acceso a esa información sensible.

El otro problema está relacionado con el consentimiento informado. Cada hospital tiene sus normas y tiene su modelo del consentimiento informado. Como muchos trabajos los realizamos con 4 o 5 hospitales, tenemos que pasar por 4 o 5 comités éticos. Además, el comité ético de la Consejería de Sanidad. El paciente tiene que firmar muchos consentimientos informados y al final termina muy cansado de todos nosotros y no quiere firmar más ni hacer más viajes. La carga burocrática es extraordinariamente complicada de entender", dijo.

CLAUSURA



El acto de clausura estuvo presidido por **Narcís Váquez,** secretario autonómico de Salud Pública y del Sistema Sanitario de la Consejería de Sanidad Universal y Salud Pública de la Generalidad Valenciana.

En primer lugar, intervino **Juan Díaz,** coordinador general del Foro que hizo un excelente resumen del Foro, destacando los puntos más importantes de cada una de las mesas celebradas.

Seguidamente intervino **Margarita Uria Etxebarria,** directora de la Agencia Vasca de Protección de Datos, que agradeció a la SEIS la labor que vienen realizando. "Este Foro, como lugar de encuentro de todos los actores interesados, ha demostrado ya su consolidación. Todas las mesas me han parecido extraordinariamente acertadas", dijo.

Por su parte, **Manuel Medina Guerrero,** director del Consejo de Transparencia y Protección de Datos de Andalucía, hizo referencia a la calidad didáctica del Foro, que había permitido tomar el pulso a la problemática de la protección de datos del sector. "En Andalucía asumiremos la competencia a partir del 25 de mayo. Nacimos en 2016 coincidiendo con la aparición del Reglamento Europeo", recordó.

Isabel González Álvarez puntualizó que, dada la importancia del tema tratado, echaba en falta a muchos gerentes. "Es importante saber, conocer y también saber cómo trasladar todo esto. Hay que trabajar para conseguir una cultura de la protección de datos, porque es algo sagrado", dijo. Tras dar las gracias a los organizadores y a todos los participantes, dio por clausurado el XV Foro de Seguridad y Protección de Datos de Salud.





AGENDA 2018

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

- **FORO DE ENFERMERÍA**

  Lugar: Tomelloso (Ciudad Real)

  Fechas: 12 y 13 de Abril de 2018.

- **VIII REUNIÓN DEL FORO DE INTEROPERABILIDAD EN SALUD**

  Lugar: A Coruña

  Fechas: 9 y 10 de Mayo de 2018

- **XXV JORNADAS NACIONALES DE 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

FORO DE
SALUD CONECTADA

Coordina: **Óscar Moreno**



Valoración del documento de reflexión y orientación sobre los Smart Wearables

En diciembre de 2016 la Comisión Europea realizó una consulta y publicó el documento *Reflexión y Orientación sobre smart wearables* que recogió las contribuciones de más de cuarenta interesados principales de la UE (organizaciones y expertos): de organizaciones públicas de investigación y tecnología, de grandes y medianas empresas, de asociaciones profesionales, organismos de normalización, organizaciones de innovación y diseño y de alianzas y regiones.

En las respuestas al documento *Reflection and orientation paper on smart wearables* de diciembre de 2016 se plantearon cuestiones importantes en el dominio de los *Smart Wearables* (por ejemplo, relacionadas con pruebas, estandarización y protección de datos) y ofrecieron sugerencias sobre las acciones necesarias para respaldar el desarrollo tecnológico, la innovación y la implementación.

Según los encuestados, para desencadenar todo el potencial de los "wearables inteligentes" en Europa se necesita un esfuerzo bien coordinado de Investigación e Innovación. Debe apuntar a:

1. Alcanzar niveles de preparación en alta tecnología, incluyendo la demostración viable y la fabricación de componentes básicos de tecnología y de prototipos integrados.
2. Construir plataformas abiertas para *weareables* conectados y ponerlos a disposición de los interesados
3. Desarrollar aplicaciones y fomentar ecosistemas relacionados.
4. Fomentar el desarrollo de normas a tiempo y proporcionar un marco regulatorio claro y adecuado.
5. Desarrollar y fomentar la confianza y la aceptación de los *weareables* inteligentes por parte de los Usuarios en un contexto de innovación social.
6. Incrementar el conocimiento y las habilidades por medio de programas educativos.

Desde entonces, la Comisión ha publicado el Programa de trabajo 2018-20 de las TIC y la digitalización de la industria y los servicios europeos ocupan un lugar importante en dicho programa. Los Centros de Innovación Digital en electrónica de *weareables* buscan ayudar a las empresas a madurar, innovar y validar sus productos con tecnologías y objetos *weareables* y flexibles.

Los *weareables*, como facilitadores para la implementación de algunos de los objetivos políticos perseguidos por la CE y, en particular, la DG CONNECT (por ejemplo, IA, big data, cloud computing, e-Salud), también se beneficiarían del trabajo normativo emprendido sobre el Mercado Único Digital –Digital Single Market- (por ejemplo, el lanzamiento de 5G, asignación de espectro, regulaciones de datos y ciberseguridad) y de la iniciativa Digitalización de la industria europea, que respalda la investigación y la innovación.

Para aprovechar todo el potencial de los *wearables* inteligentes en la Unión Europea y beneficiarse de este campo emergente para la creación de crecimiento industrial, de nuevas empresas y empleo, es esencial adoptar un enfoque personalizado y coordinado. Un buen paso en esta dirección sería el diseño y la implementación, consultándolo con los actores privados y públicos, de una ambiciosa agenda de investigación e innovación con una hoja de ruta asociada, que fomente las asociaciones interdisciplinarias e intersectoriales.

Más información:

- Artículo de consulta a los actores implicados (Dic. 2016) https://ec.europa.eu/digital-single-market/en/news/european-commission-seeks-input-reflection-and-orientation-paper-smart-wearables
- Informe final Reflection and orientation paper on smart wearables - http://ec.europa.eu/newsroom/dae/document.cfm?-doc_id=50020
- Reflection and orientation paper on smart wearables - https://ec.europa.eu/digital-single-market/news-redirect/50786
- Programa de Trabajo 2018-20 ICT - https://ec.europa.eu/programmes/horizon2020/en/h2020-section/information-and-communication-technologies.

FORO DE
INTEROPERABILIDAD

Coordina: **Adolfo Muñoz Carrero**

UNE –EN ISO13940 – Planificación sanitaria

Continuamos con la exposición de los conceptos definidos por la Norma. En esta entrega se van a tratar los conceptos relacionados con la planificación sanitaria. Las descripciones aparecen con el término del concepto en negrita. 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 A LA PLANIFICACIÓN SANITARIA

- **Plan asistencial:** plan personalizado y dinámico que incluye la *actividad sanitaria necesaria identificada,* los *objetivos* y las *metas sanitarias*, en relación con uno o más temas de salud en un proceso sanitario. Un proceso sanitario no tiene por qué estar limitado a una unidad organizativa.
- **Plan asistencial uniprofesional:** *plan asistencial* limitado a aquellas *actividades de proveedor sanitario* realizadas por *profesionales sanitarios* que tienen la misma *titulación del profesional sanitario.*
- **Plan asistencial multiprofesional:** *plan asistencial* que abarca las *actividades de proveedor sanitario* realizadas por *profesionales sanitarios* que tienen diferentes *titulaciones de profesional sanitario.*
- **Plan asistencial básico**: contenido y estructura reutilizable para un *plan asistencial* potencial para un conjunto especificado de circunstancias. Normalmente está basado en el conocimiento de *guías clínicas y protocolos.*
- **Guía clínica:** conjunto de declaraciones desarrolladas sistemáticamente para asistir a la toma de decisiones realizadas por los actores sanitarios acerca de *actividades sanitarias* que han de realizarse en relación con *temas de salud* específicos. Suelen ser genéricas sin incluir indicaciones para sujetos de la asistencia específicos. Deben contener criterios normalizados e indicadores para su medición.
- **Protocolo:** *guía clínica* adaptada. Son más precisos que las guías clínicas y a menudo se presentan de manera formal con respecto a los comportamientos y roles esperados de los *actores sanitarios.*
- **Vía clínica:** vía para las *actividades sanitarias* que informan el contenido de los *planes asistenciales básicos.* Proporcionan una orientación detallada para cada etapa en la gestión de un paciente.
- **Objetivo de salud:** logro último deseado de un *proceso sanitario* que aborda *necesidades sanitarias.*
- **Meta sanitaria:** logro deseado de una o más *actividades sanitarias,* que se consideran como un paso operativo intermedio para alcanzar un objetivo de salud específico.
- **Conjunto de actividades sanitarias:** conjunto de *actividades sanitarias.*
- **Actividad sanitaria necesaria:** conjunto de *actividades sanitarias* que incluye aquellas *actividades sanitarias* valoradas como necesarias para abordar una *necesidad de salud* específica. Puede ser identificada por cualquier *profesional sanitario* que realiza la valoración de las necesidades de salud para un *sujeto de la asistencia*. Se gestiona en un *plan asistencial.*

SEGURIDAD Y PROTECCIÓN DE **DATOS**

Coordina: **Juan Diaz**

El **Análisis de Riesgo** y la **Evaluación de Impacto**

El Reglamento General de Protección de Datos (RGPD), que comenzará a aplicarse el 25 de mayo, establece que las organizaciones que tratan datos personales deben realizar un análisis de riesgos con el fin de establecer las medidas que sean necesarias para garantizar los derechos y libertades de las personas. En aquellos casos en los que los tratamientos impliquen un riesgo alto para la protección de datos, el RGPD dispone que esas organizaciones están obligadas a realizar una evaluación de impacto.

El RGPD supone un cambio del modelo tradicional hacia un modelo más dinámico, adaptado a la transformación tecnológica que se está produciendo en el ámbito del tratamiento de la información personal y enfocado en la gestión de los riesgos potenciales asociados al tratamiento. Con esta finalidad, el Reglamento incorpora el principio de responsabilidad activa de quienes tratan datos personales, de forma que puedan determinar qué medidas son adecuadas para proteger los datos y los derechos y libertades de las personas.

La Agencia Española de Protección de Datos ha presentado recientemente las Guías de Análisis de Riesgo y Evaluación de Impacto en la Protección de Datos Personales como herramienta de ayuda para el cumplimiento del RGPD. Para entidades que tratan datos de escaso riesgo, la Agencia ofrece Facilita_RGPD, un cuestionario online gratuito con el que empresas y profesionales pueden obtener los documentos mínimos indispensables para ayudar a cumplir con el Reglamento.

Análisis de riesgos en la protección de datos. Las organizaciones que no puedan utilizar Facilita_RGPD deben llevar a cabo un análisis de riesgos. En este sentido, la Guía de Análisis de Riesgos recoge una metodología adecuada para evaluar el nivel de riesgo en relación con los tratamientos de datos personales que realizan. Esta guía también incluye plantillas y anexos de gran utilidad para empresas y profesionales.

El análisis y la gestión de riesgos son procedimientos que permiten a las organizaciones hacer un diagnóstico sobre los riesgos para los tratamientos de datos personales y, en ocasiones, aportar información suficiente para decidir si es necesario o no llevar a cabo una Evaluación de Impacto en Protección de Datos.

La Evaluación de Impacto en la protección de datos. La Evaluación de Impacto es un proceso que permite a las organizaciones identificar los riesgos que un sistema, producto o servicio puede implicar para los derechos y libertades de las personas y, tras haber realizado ese análisis, afrontar y gestionar esos peligros antes de que se materialicen. La Guía de Evaluación de Impacto en la Protección de Datos ayudará a las organizaciones a identificar las actividades que conllevan un alto riesgo y a establecer las medidas de control más adecuadas para minimizar el mismo antes de iniciar el tratamiento. Al igual que la Guía de Análisis de Riesgos, ésta también incluye plantillas y anexos que serán útiles para llevar a cabo la evaluación.

En el proceso, la organización debe conocer para qué y cómo se van a utilizar los datos, identificar, evaluar y tratar los riesgos potenciales y elaborar un plan de acción donde se incluyan las medidas de control para garantizar los derechos y libertades de las personas.

Con estas guías, la Agencia busca promover una cultura proactiva de la privacidad, proporcionando una ayuda a las organizaciones que contribuya, a la vez, a fortalecer la protección de los derechos y libertades de las personas.

INFORMÁTICA **MÉDICA**

Coordina: **José Sacristán**



¿Cuáles serán las tendencias en **Big Data** para 2018?

Te mostramos lo que opinan las 13 compañías más innovadoras del sector en uno de los temas más candentes de los próximos meses. ¿Quieres saber qué nos han contado? Atento a este artículo.

Solo en 2015 se generaron nada menos que 145 Zettabytes, con la previsión de que las personas, máquinas y objetos conectados a Internet hagan lo propio con 600 Zettabytes de datos en 2020. La inmensa mayoría de esos 600 ZB, adelantados en un informe de Cisco, serán datos efímeros por naturaleza, y que nunca serán almacenados ni procesados. Igualmente, una gran mayoría de estos datos no son útiles. Se calcula que aproximadamente el 10% son datos útiles (es decir, 60 Zettabytes en 2020). Y, de ese total solamente otro 10% de datos (es decir, 6 Zettabytes) serán procesados y convertidos en valor de negocio mediante analítica de Big Data.

¿Cómo afrontar este desafiante escenario con la tecnología actualmente disponible? ¿Qué recursos o aproximaciones deben plantearse las compañías para abordar con éxito los desafíos presentes y futuros del Big Data? En TICbeat hemos preguntado a 13 de las principales compañías de este segmento para conocer cuáles son las opiniones más extendidas al respecto arrojando algo de luz a este incipiente y dinámico entorno.

"Los datos son 'el nuevo petróleo', se están convirtiendo en pieza clave de la sociedad y la economía", afirma Antonio Conde, Director de IoT y Transformación Digital en Cisco España. "Durante 2018 las organizaciones utilizarán cada vez más la analítica de Big Data para optimizar procesos operativos, mejorar la experiencia de servicio a los clientes y la atención a los ciudadanos y generar nuevas fuentes de ingresos, principalmente mediante ofertas personalizadas. Pero la analítica de Big Data tendrá su mayor potencial en el análisis en tiempo real. Y aún más si el análisis se realiza en el extremo de la red, donde los datos conservan su valor".

Más información: *http://www.ticbeat.com/tecnologias/tendencias-en-big-data-para-2018/*

El Proyecto **TANGO** busca arquitecturas para tecnologías como IoT y Big Data

Entornos fundamentales en el marco de las ciudades inteligentes, como Internet de las Cosas (IoT), Big Data y Computación de Alto Rendimiento, entre otras tecnologías, se verán beneficiados con los hallazgos del proyecto europeo de I+D+i TANGO, centrado en la creación de un nuevo modelo de programación y en el desarrollo de herramientas de modelado de software que pueden utilizarse en diferentes arquitecturas y configuraciones de hardware heterogéneas.

https://www.esmartcity.es/2018/01/17/proyecto-tango-busca-nuevas-arquitecturas-para-tecnologias-iot-big-data

SECTOR
ENFERMERÍA

Pablo Sánchez Ballesteros
Enfermero del Consorcio Hospitalario Provincial de Castellón y editor del blog "Enfermería Tecnológica"

Coordina: **Azucena Santillán**

Smartphone ¿Herramienta de trabajo o peligroso distractor para las enfermeras?

De acuerdo con los datos del informe Digital In 2017 Global Overview llevado a cabo por We Are Social y Hootsuite , España es el país con mayor proporción de usuarios de teléfono móvil, con una tasa de penetración del 88%(1). La mayoría de los teléfonos móviles que se adquieren en la actualidad son smartphones (teléfonos inteligentes) con conexión a internet.

Por esto, día a día utilizamos esta herramienta en el desempeño de la profesión enfermera. El Smartphone puede ser un poderoso aliado a la hora de llevar un control del trabajo a turnos, buscar información para mejorar el desempaño de nuestras tareas o incluso estar en contacto con otros profesionales con similares inquietudes.

Existen múltiples Apps en el mercado que nos pueden facilitar el trabajo como son:

- NandaNocNic: Aplicación que permite realizar la consulta de los Diagnósticos de enfermería, los Resultados de los pacientes y las Intervenciones enfermeras (Nanda, Noc, Nic).
- Aturnos: Permite simplificar y optimizar la gestión de los turnos de trabajo.
- Guía Terapia Intravenosa: Una App desarrollada por enfermeras de Menorca y que es una gran ayuda a la hora de revisar aspectos relacionados con la terapia intravenosa.
- AempsCIMA: Creada por la Agencia Española de Medicamentos y Productos Sanitarios. Permite el acceso al prospecto de 15.000 medicamentos y unos 1.600 principios activos.
- HealthScience: Una App con múltiples fuentes de información, agenda de eventos científicos, podcasts y buscadores de evidencia científica.
- UniversalNurses: Una App destinada a derribar las barreras idiomáticas a la hora de atender a pacientes extranjeros.
- Guía Salud: Una App para consultar Guías de Práctica Clínica del Sistema Nacional de Salud.

Éstas y muchas otras Apps pueden hacer que el trabajo de las enfermeras sea más eficiente, pero el uso del Smartphone durante la jornada laboral no está exento de riesgos. Utilizar el teléfono móvil durante la jornada laboral supone un riesgo, ya que la mayoría de éstos se encuentran contaminados con algún patógeno relacionado con el medio hospitalario. Hay estudios que demuestran que un 80% de los teléfonos móviles de las enfermeras se encuentran contaminados con bacterias(2).Según un estudio de USA, el 78,1 % de las enfermeras reconoció haber usado el Smartphone para asuntos personales durante la jornada laboral (sin tener en cuenta los posibles descansos). La mayoría de enfermeras lo utilizó para enviar mensajes, leer mails, leer noticias, revisar las Redes Sociales, comprar e incluso para jugar(3).

Entonces, ¿cómo sabemos cuándo una enfermera está utilizando el Smartphone para aspectos relacionados con el trabajo o para asuntos personales? Buena pregunta que habrá que dilucidar cuanto antes. Hay que establecer algún tipo de norma para fomentar el adecuado uso de éstos, así como evitar las distracciones y problemas que el uso para otros menesteres pueda ocasionar.

BIBLIOGRAFÍA

1. **We are Social, Hootsuite.** Digital in 2017 Global Overview [Internet]. 2017 [consultado 30 enero de 2018]. Disponible en: https://www.slideshare.net/wearesocialsg/digital-in-2017-global-overview?ref=https://thenextweb.com/insights/2017/01/24/digital-trends-2017-report-internet/
2. **Morioka I, Tabuchi Y, Takahashi Y, Oda Y, Nakai M, Yanase A, et al.** [Bacterial contamination of mobile phones shared in hospital wards and the consciousness and behavior of nurses about biological cleanliness]. Nihon Eiseigaku Zasshi [Internet]. 2011 Jan [Consultado 30 enero del 2018];66(1):115–21. Disponible en: http://www.ncbi.nlm.nih.gov/pubmed/21358142
3. **McBride DL, LeVasseur SA, Li D.** Non-work-related use of personal mobile phones by hospital registered nurses. JMIR mHealth uHealth [Internet]. JMIR mHealth and uHealth; 2015 Jan 13 [consultado 30 enero del 20180];3(1):e3. Disponible en: http://mhealth.jmir.org/2015/1/e3/

SECTOR
FARMACIA

Coordina: **Alberto Gómez Lafón**

La **farmacia** y los **medicamentos** en **Inforsalud** 2018

En consonancia con los datos generales de Inforsalud, esta edición de 2018 presentó un gran número de comunicaciones de carácter general, más de 60, aproximadamente 18 posters y 12 proyectos de innovación. Pero es que además, en lo que respecta al área del medicamento y de la farmacia, la cifra fue de 11, de los cuales 10 provinieron de CC.AA y una de los servicios centrales del MSSSI, a las que podrían añadirse algunas otras que podrían estar incluidas en este apartado.

Por su naturaleza, los proyectos relacionados con la prestación farmacéutica y por tanto con la prescripción electrónica, ganaron por mayoría absoluta.

Desde una perspectiva general, los resultados sin embargo enmascaran una pequeña decepción. Considerando que Inforsalud se dirige a todo un sector que engloba; Oficinas de Farmacia, Farmacia Hospitalaria, Administraciones Públicas, Industria Farmacéutica, etc., y que su objetivo primordial es el de mostrar los avances y la evolución en la que estamos inmersos, cabe pensar que o bien determinados subsectores no encuentran en Inforsalud el escenario mas idóneo para divulgar sus nuevos proyectos TIC, o bien no se están promoviendo proyectos novedosos en beneficio del ciudadano en determinadas áreas, fáciles de detectar. En cualquier caso y como muestra de adonde se dirige el sector, les describo las tendencias, en forma de comunicaciones, que este año han sido presentadas y que se podrán conocer a través del libro de comunicaciones del congreso:

- Guia farmacoterapeutica semfyc: herramienta de ayuda a la prescripcion integrada en OMIAP.
- Visado electrónico: cómo lo hacemos en el paraíso.
- Sistema web para el plan de contingencia del proyecto de interoperabilidad de la receta electrónica.
- Herramienta web para el sistema de auditoría de vigilancia de productos sanitarios (no medicamentos).
- Ontología sobre la adherencia al tratamiento en pacientes crónicos complejos polimedicados.
- Fecha de seguimiento: funcionalidad de e-receta que potencia el control en polimedicados.
- Prescripción electrónica hospitalaria. Implantación en el Complejo Hospitalario Universitario de Vigo.
- Optimización del Vademecum personal de prescripción por el médico en receta electrónica.
- Introducción a blockchain y su uso en la informática de la salud.
- Beneficios percibidos de un sistema de prescripción electrónica asistida.
- Certificado electrónico del SESCAM: de la tarjeta a la nube.

Como se puede observar un panorama completo en lo que respecta a la prestación farmacéutica, en el que abundan las incorporaciones de herramientas de ayuda a la prescripción, con el objeto de aumentar los niveles de seguridad del paciente especialmente en el ámbito hospitalario y también relacionado con este objetivo, los proyectos que pretenden medir, vigilar y en su caso corregir la adherencia a los tratamientos con medicamentos, especialmente en pacientes crónicos y polimedicados. Tal vez es digna de resaltar por novedosa, la comunicación que hace referencia al fenómeno Block Chain y su aplicación en el mundo del medicamento y de la Farmacia, si bien, el futuro nos aclarará si esa tecnología es apropiada o no en este campo.

NOTICIAS DEL SECTOR

Coordina: **Diego Sáez**

- **El Servicio Andaluz de Salud ha desarrollado un nuevo 'Navegador Único de la Historia Clínica' que sustituye a la anterior 'Historia de Salud Única'.** El objetivo de este cambio es que los profesionales del ámbito asistencial, tanto de Atención Primaria como Hospitalaria, cuenten con una visión global de la historia clínica del ciudadano a través de una única interfaz, dotándolos así de una herramienta más manejable e intuitiva. De esta manera, el personal sanitario accederá a todos los elementos de la historia clínica de sus pacientes sin necesidad de emplear diferentes herramientas, ni distintas formas de acceso.

- **En marcha la tercera edición de cursos de formación en TIC dirigidos a facultativos, personal de enfermería y farmacéuticos** organizados por el Servicio Andaluz de Salud, en colaboración con la línea IAVANTE de la Fundación Pública Progreso y Salud. Esta oferta formativa es gratuita y está acreditada por la Agencia de Calidad de Andalucía (ACSA) y tiene como objetivo facilitar el uso de las TIC que utilizan los profesionales del Servicio Andaluz de Salud en el desempeño de su trabajo diario. La metodología empleada es la teleformación mediante una herramienta, denominada Massive Open Onlice Course (MOOC) que permite al alumnado acceder a una formación virtual de calidad, abierta y gratuita. En las ediciones de 2015-2016 se matricularon algo más de 7.000 alumnos y obtuvieron un buen grado de satisfacción.

- **InterSystems anuncia la disponibilidad de InterSystems IRIS Data Platform, la primera plataforma de datos que ofrece gestión de datos multi-modelo y multi-workload** (carga de trabajo múltiple), interoperabilidad nativa y una plataforma abierta de análisis en un único producto. InterSystems IRIS es una plataforma de datos completa y unificada para construir aplicaciones ricas en datos más fácil y rápidamente. Permite a las organizaciones combinar los datos de eventos y de transacciones con grandes conjuntos de datos históricos y de otros tipos, con el fin de captar oportunidades de negocio sin explotar y mejorar la eficiencia operativas. InterSystems IRIS capacita a los negocios digitales actuales para ser más inteligentes, rápidos y más flexibles.

- **El Hospital General Universitario de Ciudad Real es el primero de la región que ha completado el proceso de implantación del programa e-Delphyn BB** con el que el Servicio de Salud de Castilla-La Mancha (Sescam) va a centralizar en un registro telemático único la gestión los servicios y datos de los Bancos de Sangre de los catorce hospitales y tres centros de transfusión de la región. Se trata de un nuevo sistema de gestión de la donación, procesado de los componentes sanguíneos, análisis de las donaciones, distribución, almacenaje, transfusión, estudios gestacionales, estudios inmunohematológicos, recogida de progenitores hematopoyéticos y hemovigilancia a lo largo de toda la cadena de transfusión.

- **Castilla-La Mancha (SESCAM) va a iniciar el diseño de un Plan de Optimización de Uso de los Antimicrobianos propio,** adaptado a la realidad de la Comunidad Autónoma, a su perfil de prescripción y a su propio perfil de resistencias antibióticas, asegurando una plena implantación entre todos los profesionales y los centros en los que desarrollan su actividad. Así lo afirmó la directora gerente del Servicio de Salud de Castilla-La Mancha, Regina Leal, durante la inauguración de una Jornada sobre el Programa de Optimización de Antibioticoterapia (PROA) en Castilla-La Mancha.

- **El Servicio de Salud de Castilla-La Mancha (Sescam) ha dotado al servicio de Microbiología del hospital general universitario de Ciudad Real de tecnología avanzada para la identificación de microorganismos en un plazo de tiempo muy reducido.** Se trata de un equipo basado en tecnología conocida como MALDI-TOF que realiza el análisis por espectrometría de masas para identificar microorganismos con mayor exactitud y rapidez. Con esta

tecnología "se puede informar de manera más rápida qué bacteria u hongo tiene el paciente, con el género y su especie, lo que significa un gran avance para el diagnóstico de infecciones microbianas permitiendo ajustar los tratamientos antibióticos".

- **TICH Consulting ha desarrollado una aplicación para pacientes que permite al usuario identificarse y pedir cita con su médico a través de su móvil,** registrar su llegada al centro, consultar los resultados de analíticas, pruebas radiológicas o informes de alta. La ventaja más notoria de la nueva APP de Green Cube es la disminución de colas y tiempos de espera, sin costes de adquisición ni mantenimiento. Diseñada para smartphones y tabletas, está disponible para Android y IPhone, y el paciente puede descargarse la aplicación de Green Cube automáticamente y sin coste de las tiendas de Apple o Google, tanto en su terminal telefónico como en su Tablet, con los mecanismos de identificación para el cumplimiento de la ley de protección de datos.

- **El equipo provincial TIC de Jaén del Servicio Andaluz de Salud, dentro de la iniciativa 'Tecnolab Salud', ha puesto en marcha un primer proyecto de impresión de modelos 3D para intervenciones quirúrgicas.** Hasta el momento, se han realizado modelos para siete especialidades distintas, participando en más de 40 intervenciones y teniendo cada vez más demanda por parte de los equipos quirúrgicos. Los modelos que realizan son de venas y arterias, huesos y órganos, siendo los primeros los que tienen mayor demanda, ya que se utilizan en intervenciones relacionadas con el cáncer de pulmón. En cuanto a órganos, imprimen riñones, laringes, bronquios y cráneos. Estas impresiones sirven para que los cirujanos tengan una mayor certeza sobre la anatomía del individuo que van a intervenir, así como para adelantar ciertos trabajos que normalmente se realizan cuando el paciente está siendo operado. 'Tecnolab Salud' nace, en el equipo provincial TIC de Jaén, como un laboratorio de iniciativas innovadoras que tengan como objetivo generar una transformación tangible en la organización.

- **Las infecciones relacionadas con la asistencia sanitaria (IRAS) y en concreto las causadas por bacterias multirresistentes (BMR), constituyen un grave problema de salud pública, porque los tratamientos con antimicrobianos quedan limitados y su capacidad de diseminación es amplia.** El equipo provincial TIC de Sevilla del Servicio Andaluz de Salud ha desarrollado un sistema informático de alertas para la detección e identificación precoz de pacientes infectados o colonizados por algunos de estos microorganismos y que cuentan con sucesivos ingresos en el mismo centro o con cualquier otro hospital del Sistema Sanitario Público de Andalucía. El sistema, denominado Health Alert Monitor (HAM), permite a los profesionales sanitarios adoptar rápidamente las medidas de control de infecciones oportunas y evitar la diseminación del microorganismo a otros pacientes susceptibles. Hasta el momento, este sistema se ha implementado en todos los centros hospitalarios de la provincia de Sevilla y en el Hospital Universitario Reina Sofía de Córdoba, habiéndose comenzado su extensión por toda la región, de manera que a finales de 2018 esté funcionando en todos los hospitales de Andalucía.

- **El Centro Médico Colón confía su gestión a Info33+.** Ubicado en el centro de Bilbao, el Centro Colón es un ambulatorio multidisciplinar perteneciente a IMQ que cuenta con 52 profesionales médicos que ofrecen un servicio de atención primaria y 17 especialidades médico-quirúrgicas y diagnósticas, siendo las principales la medicina general, pediatría, traumatología, otorrinolaringología, cardiología, endocrinología, alergología, radiología, análisis clínicos y urgencias. Se trata de un centro caracterizado por la calidad y servicio a los pacientes, reconocido con la acreditación ISO 9001. A fin de continuar en esta senda de excelencia, ha adoptado como herramienta de gestión Info33+, la solución desarrollada conjuntamente por IMQ e Ibermática para dar una respuesta global e integrada a las necesidades del centro, mejorando su productividad y eficiencia. Con Info33+, el Centro Médico Colón espera dar un salto adelante tanto en su gestión interna como en la atención a sus más de 150.000 pacientes anuales.

VIII Reunión del Foro de Interoperabilidad en Salud

TRABAJANDO POR LA INNOVACIÓN TIC EN SALUD 40 AÑOS

Síguenos en Twitter:

@SEISeSalud

"Interoperabilidad, Internet de las cosas y Salud Integrada"

Organiza

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

A CORUÑA
9 y 10 mayo de 2018

Complejo Hospitalario Universitario A Coruña
As Xubias, 84, 15006 A Coruña

COLABORADORES TECNOLÓGICOS

Atos · Fujitsu · Getronics · gmv · Ibermática · indra · Informática El Corte Inglés · InterSystems · Microsoft · Philips · Siemens Healthineers