NÚMERO
145

I+S

JUNIO
2021

REVISTA DE LA SOCIEDAD ESPAÑOLA DE INFORMÁTICA Y SALUD

ESPECIAL

SEGURIDAD Y PROTECCIÓN DE DATOS EN TIEMPO DE PANDEMIA



ENTIDADES ASOCIADAS

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD





















































AÑO 2021 NÚMERO 145 **SUMARIO**

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

Directora
Zaida Sampedro

Comité Editorial
Luciano Sáez
Jesús Galván
Alberto Gómez Lafón
Francisco Martínez del Cerro
Guillermo Vázquez

Comité de Redacción
José Luis Monteagudo
Juan Fernando Muñoz
José Quintela
José Sacristán
Carlos García Codina
Mercedes Alfaro
José Manuel Pastora
Angel Blanco Rubio
Gregorio Gómez
Martin Begoña Oleaga
Juan Diaz
Lola Ruiz
Luz Fidalgo
Juan Ignacio Coll
Inmaculada Moro
Javier López Cavero
Fco. Javier Francisco Verdu
Carlos Gallego Pérez,
Fernando Martín, Mercedes Alfaro
Adolfo Muñoz Carrero
Carlos Parra Calderón
Elvira Alonso Suero
Miguel Chavarría
Santiago Thovar
Miguel Angel Benito Tovar
Fernando Martín Sánchez
Inmaculada C. Castejón Zamudio

Colaborador Técnico
Diego Sáez

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

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

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

5 **EDITORIAL**

6 **ESPECIAL** SEGURIDAD Y PROTECCIÓN DE DATOS EN TIEMPO DE PANDEMIA

6 Cesión voluntaria de datos personales de salud para investigación clínica
12 Una conectividad segura y sin fisuras, claves para los entornos sanitarios
15 Retos del Delegado de Protección de Datos en la Investigación en Salud. Oficina del Delegado de Protección de Datos - Fundación TIC SALUT SOCIAL
18 Securización de la Gobernanza del dato
20 Ningún dato sensible vale una vida
22 Tribunal Supremo y Agencia Española de Protección de Datos: Accesos indebidos a la historia clínica y derecho del afectado a conocer la identidad del infractor
24 Equipamiento médico electrónico: ¿puede la certificación del dispositivo garantizar un alto nivel de seguridad?
26 Hospitales y centros de salud aceleran la adopción de nuevas soluciones tecnológicas
29 La seguridad sanitaria en la era COVID-19
32 Identificación y gestión de vulnerabilidades en el Servicio de Salud de las Illes Balears (Ib-Salut)
36 Impulsar la Ciber-colaboración

38 **ACTIVIDADES DE LA SEIS**

38 XI REUNIÓN DEL FORO DE INTEROPERABILIDAD EN SALUD 2021
47 XVIII FORO DE SEGURIDAD Y PROTECCIÓN DE DATOS DE SALUD
64 XXIV CONGRESO NACIONAL DE INFORMÁTICA DE LA SALUD

66 **FOROS Y SECTORES**

66 Foro de Salud Conectada
68 Foro de Gobernanza
70 Foro de Interoperabilidad
71 Sector de Informática Médica
72 Foro de Enfermería
73 Sector de Farmacia

75 **AGENDA**

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

ENTIDADES
COLABORADORAS

SOCIEDAD ESPAÑOLA DE
INFORMÁTICA DE LA SALUD

COLEGIO OFICIAL DE FARMACÉUTICOS DE CÁCERES

COLEGIO OFICIAL DE FARMACÉUTICOS DE BADAJOZ

CONSEJO GENERAL DE COLEGIOS OFICIALES DE FARMACÉUTICOS

EMERGRAF, S.L. CREACIONES GRÁFICAS

HOSPITAL CLINIC. SISTEMAS DE INFORMACIÓN

I.C.P. INGERNIEROS, S.A.

IDCSALUD

MUTUAL CYCLOPS–CENTRE DOCUMENTACIÓ

OSAKIDETZA - SERVICIO VASCO DE SALUD

SOCIOS TECNOLÓGICOS PRINCIPALES

SOCIOS TECNOLÓGICOS COLABORADORES

Interoperabilidad, Seguridad y Protección de Datos de Salud

La Sociedad Española de Informática de la Salud promueve activamente el impulso de una visión corporativa del Sistema Nacional de Salud, de tal forma que las múltiples organizaciones y profesionales que trabajan en ellas se vean dentro de una única gran organización, al servicio de la salud que tiene unos objetivos y funciones comunes.

Para difundir esta visión corporativa es esencial incorporarla en la formación de los profesionales sanitarios que, en nuestro caso, se realiza a través del Máster en Dirección de Sistemas y TIC para la Salud y en Digitalización Sanitaria, a través de nuestras actividades, que permiten los contactos personales de los profesionales y directivos para que puedan compartir conocimiento y experiencias, algo muy difícil de conseguir en una organización tan dispersa como la sanitaria.

Debido a la situación sanitaria que sufrimos en este último año, hemos tenido que relacionarnos solo a través de formatos virtuales y, gracias a la tecnología, hemos conseguido avanzar en todas las acciones, aunque el formato totalmente virtual no sea el óptimo. Sin embargo, nos hemos acostumbrado al teletrabajo y a la participación virtual, extremo que debemos seguir aprovechando, ya que permite la participación y asistencia de aquellos que por diferentes motivos no podrían hacerlo.

En este número de la revista tratamos dos temas que consideramos esenciales para el Sistema Sanitario. El primero es un resumen de la reunión del Foro de Interoperabilidad en Salud, desarrollado íntegramente en formato virtual. Y el segundo es un resumen del Foro de Seguridad y Protección de Datos, desarrollado en formato híbrido, presencial y virtual. Este tema se refuerza, además, con los artículos del "Especial", que abordan cuestiones relacionadas.

Quisiera destacar la importancia del Comité Técnico de Interoperabilidad en el Sistema Sanitario de la SEIS, por los trabajos que están desarrollando y que conforman un importante avance para impulsar y favorecer el desarrollo de proyectos tecnológicos innovadores, que permitan su fácil y rápida integración.

Por otra parte, hay consenso absoluto sobre que la seguridad y la protección de datos es un concepto fundamental en la construcción e implantación de los sistemas de información de salud. La SEIS creó en 2013 el Comité Técnico de Seguridad de la Información de Salud y, desde entonces, está desarrollando importantes trabajos colaborativos para avanzar de una forma coherente y conjunta en las diferentes organizaciones sanitarias, compartiendo soluciones y acordando criterios en materia de seguridad y protección de datos.

No obstante, de acuerdo al ÍNDICE SEIS 2020, la inversión en seguridad en los sistemas de información del SNS es mucho más baja que la realizada en cualquier otro sector con el que se pueda comparar. En el año 2020 únicamente se han invertido 16 M€, lo que corresponde a un 2% del gasto total TIC, que implica una disminución del 20% respecto al año anterior. La inversión en seguridad es una asignatura pendiente, que es imprescindible abordar con urgencia, ante la necesidad de conocer y tener visibilidad de las amenazas existentes en las organizaciones, y de las que ha habido malas experiencias últimamente en todo el mundo. Es crítico garantizar la disponibilidad y seguridad de los sistemas asistenciales si queremos mantener un Sistema Sanitario de calidad.

Cesión voluntaria de datos personales de salud para investigación clínica

Juan Díaz García[1], Rafael Marín Jiménez[2]

1. Delegado de Protección de Datos del Sistema Sanitario Público de Andalucía
2. Oficina de Delegado de Protección de Datos del Sistema Sanitario Público de Andalucía

1. RESUMEN

La cesión voluntaria de datos personales relativos a la salud como mecanismo facilitador del cumplimiento de la normativa de protección de datos para la investigación clínica, se enfrenta a varios retos: sensibilizar a la población al mismo nivel que lo está con la donación de órganos, adaptar su filosofía "pre-RGPD" a los nuevos cambios normativos, alcanzar carácter legal, superar los riesgos de seguridad en el tratamiento de los datos, etc. Distintas iniciativas está contribuyendo a satisfacer estos retos, bajo otras denominaciones pero con el mismo objetivo, destacándose en este artículo las llevadas a cabo desde el ámbito público, tanto a nivel andaluz, como nacional e incluso internacional. Sin embargo, es preciso reflexionar sobre el grado de madurez en el que se encuentran las instituciones públicas para erigirse como adalid de la confianza de la ciudadanía y garantizar así el éxito de la cesión voluntaria de datos.

2. INTRODUCCIÓN

A) ORÍGENES Y PROMOTORES

La protección de datos personales es una de esas "fuerzas de la naturaleza" que no deja indiferente a nadie, suscitando interesantes controversias entre sus defensores y detractores. En la sociedad de la información, su omnipresencia se hace más evidente a medida que su objeto protegido se perfila como sensible, alcanzando su máxima expresión en el contexto de la salud ciudadana. Este hecho a dado lugar a filosofías o movimientos que amparándose en el logro de loables objetivos como sociedad, permitan flexibilizar los límites normativos entorno a este derecho fundamental. Entre estos objetivos se encuentra el descubrimiento de mejores maneras de tratar, prevenir, diagnosticar y comprender las enfermedades a través de la investigación clínica.

La cesión voluntaria de datos personales relativos a la salud surge como un intento de equiparar la investigación médica a la asistencia sanitaria estableciendo un paralelismo con la donación de órganos, potenciando así la autonomía del paciente respecto de otras bases de legitimación para el tratamiento de sus datos personales. También tiene un alto componente de empoderamiento ciudadano, hasta el punto que algunos de los autores que han tratado este movimiento afirman su necesidad debido a que *"la experiencia, los recursos y las tecnologías para la producción de investigación relacionada con la salud han sido secuestrados dentro de los marcos profesionales, regulatorios y de mercado de la medicina clínica y la salud pública"*.

B) CONCEPTO. OBJETIVO

Una aproximación al concepto de cesión voluntaria datos para investigación en salud está expresada en el ensayo "Data Donation as a Model for Citizen Science Health Research"[1]. Se trataría por tanto de llevar a cabo investigación científica en el ámbito de la salud en base a los datos personales aportados voluntariamente por sus titulares y que fueron generados con otro propósito formando una colección.

Su objetivo no es otro que prever futuras necesidades de datos para líneas de investigación a fin de que llegado el momento no sea preciso llevar a cabo un proceso de "reclutamiento" de ciudadanos, reduciendo, sino eliminando, el tiempo de identificación de casos, localización de personas, información, registro o descarga de datos, estructuración..., lo que en la actualidad choca frontalmente con el principio de minimización de datos del Reglamento Europeo de Protección de Datos (RGPD).

Otra aproximación a este concepto, en contraposición a la filosofía "opt-in" anterior, podría ir en la línea de adquirir la obligación legal de nacimiento de ceder los datos personales relativos a la salud por defecto con la única aunque extensa finalidad de contribuir altruistamente a la investigación clínica, tal y como ocurre en España con la donación de órganos. En este caso sería el principio de privacidad por defecto del RGPD con el podría surgir conflicto, contando con la existencia de un marco normativo que legitimara el tratamiento.

3.ESTADO DEL ARTE

No cabe duda que el objetivo de la cesión voluntaria de datos personales es compartido por otras filosofías, que sin entrar en detalles sobre las mismas, merecen ser referidas para ofrecer una panorámica básica del terreno en el que se mueve la investigación en salud.

El "yo cualificado" (Qualified Self or Self-Tracking), como parte de la denominada ciencia ciudadana, es un movimiento que incorpora tecnología, como sensores y dispositivos portátiles, para adquirir datos sobre diversos aspectos de la vida de una persona, especialmente la salud y el estado físico, con el objetivo de mejorar la autodetección, la autoconciencia y el rendimiento humano dentro de la industria de la salud digital. Implementado a través de plataformas como Open Human[2].

Los "datos abiertos" (Open Data) es una filosofía y práctica que persigue que determinados datos estén disponibles de forma libre a todo el mundo, sin restricciones de copyright , patentes u otros mecanismos de control. Los datos deben publicarse en bruto (sin procesar), bien estructurados y en formatos conocidos que faciliten la reutilización. En la actualidad, abrir al mundo los datos personales de los ciudadanos europeos requiere de procesamiento previo para conseguir anonimizar o al menos seudonimizar los mismos, salvo que hayan sido cedidos mediante consentimiento libre.

Precisamente en el marco del consentimiento, se están pilotando tecnologías[3] basadas en blockchain, destinadas a informar a los pacientes en relación con los tratamientos médicos que requieren su firma y que como no, igualmente son útiles para la formalización de la cesión de datos.

También se han creado repositorios públicos que articulan y conectan la información dispersa entre diferentes sistemas de salud para ponerla al servicio de la investigación médica, garantizando la seguridad de los datos y el respeto a la privacidad de los usuarios, o así se presentan; este es el caso de Health Data 29[4].

Apple han introducido un marco de código abierto denominado ResearchKit ("primo hermano" de HealthKit) que permite a los investigadores y desarrolladores crear aplicaciones para la investigación médica, creando flujos de consentimiento visual, tareas activas dinámicas en tiempo real y encuestas.

4.I NICIATIVAS PÚBLICAS

A) PLATAFORMA DE CESIÓN DE DATOS MÉDICOS[5]

Se trata de una idea avanzada desde la Vicepresidencia de Investigación del Centro Superior de Investigaciones Científicas (CSIC) y cuya propuesta técnica ha sido elaborada por el Grupo de Computación Avanzada y e-Ciencia (IFCA).

La idea subyacente de esta plataforma está nuevamente basada en trasladar el modelo de la donación de órganos a la cesión de datos personales relativos a la salud, manteniendo los mismos bajo el control íntegro de la administración pública.

1. https://theoryandpractice.citizenscienceassociation.org/articles/10.5334/cstp.178/
2. https://www.openhumans.org/
3. https://www.blockchaineconomia.es/donar-datos-covid-19/
4. https://www.healthdata29.org/
5. https://digital.csic.es/handle/10261/194943

Al margen de los desafíos técnicos y temáticos, los beneficios y motivaciones, el pilotaje, etc. que se documentan en el proyecto, a los efectos del presente artículo interesa resaltar los aspectos considerados sobre la cesión de datos como fuente:

- Programa voluntario mediante el cual los usuarios del Sistema Cántabro de Salud puedan "ceder" sus datos para su uso en investigación biomédica.
- Los datos serán "desidentificados", no anonimizados para el depósito.
- Los usuarios podrán retirar su consentimiento en cualquier momento y los datos dejarán de utilizarse a partir de ese momento.
  - Por supuesto no se pueden retirar los datos de estudios pasados o cuando hayan sido agregados o anonimizado dejando de ser datos personales.

B) REGISTRO ANDALUZ DE DONANTES DE MUESTRAS [Y DATOS] PARA INVESTIGACIÓN BIOMÉDICA

Una iniciativa novedosa fue el Registro de Donantes de Muestras para la investigación Biomédica de la Consejería de Salud de la Junta de Andalucía para fomentar la investigación biomédica, facilitando la participación altruista de la ciudadanía, en un entorno que proteja los derechos de las personas donantes.

El Registro quedó constituido en la "Orden de 15 de junio de 2015, por la que se crea en el ámbito de la Consejería de Igualdad, Salud y Políticas Sociales el fichero de datos de carácter personal denominado «Donantes de Muestras para la Investigación Biomédica en Andalucía»", y que fue publicada en el Boletín Oficial de la Junta de Andalucía, el 23 de junio de 2015.

El registro permite disponer de una base de datos que incluye la información suficiente que permita activar las donaciones cuando éstas fueran necesarias de manera concreta, constituyendo la nueva fuente de obtención de muestras para investigación. Recoge la información básica de identificación y salud (datos) de personas interesadas en participar de manera voluntaria en investigación. El órgano responsable del Registro es la Secretaría General de Investigación, Desarrollo e Innovación en Salud de la Consejería de Salud y Familias, y el Biobanco del Sistema Sanitario Público de Andalucía es el encargado de su gestión.

Cerca de 2000 personas se han inscrito, en diferentes tipos de patologías o líneas de investigación, como Neoplasias, Parkinson, Esclerosis, etc. Desde todas las provincias de Andalucía como desde otras Comunidades Autónomas. Fundamentalmente se usa este registro en proyectos que requieren información o muestras con bajo riesgo para el donante, como son muestras de cabello, uñas, saliva, orina, heces o sangre.

Aunque la iniciativa lleva algunos años, su acogida no ha sido generalizada ya que es bajo porcentaje de su penetración que se ha conseguido. Siendo una población estimada de 8 millones, con un 80% de población potencialmente donante (excluido menores) de aproximadamente 6,4 millones, solo ha participado un 0,03% de la población.

C) UK- NHS - CEDENTES DE DATOS UNIVERSALES

El manejo de los datos de salud en el Reino Unido es un caso especial por su complejidad de actores, alcances definidos y su trasformación para conseguir un marco de confianza del ciudadano hacia su Sistema Nacional de Salud. Su marco de cumplimiento legal y la iniciativa de los Principios Caldicott para la protección de la confidencialidad de las personas fueron los pilares iniciales para tener un marco de compartición de información clínica entre los actores de Sistema de Salud.

Basado en la Medicina Primaria y Hospitalaria se desarrolló la necesidad de integrar dichas fuentes, siendo aceptado de pleno en el ámbito de la asistencia sanitaria, y con dudas en el ámbito SocioSanitario, Gestión o Investigación.

En las dos últimas décadas se ha regulado el Reglamento del Servicio de Salud (Control de la Información del Paciente) de 2002 y la Ley del Servicio Nacional de Salud de 2006 que permiten que se levante temporalmente el deber de confidencialidad del derecho común, de modo que la información confidencial de los pacientes pueda ser transferida a un solicitante sin que quien la divulgue incumpla el deber de confidencialidad del derecho común. En enero de 2012, el Foro del Futuro del NHS identificó un problema relacionado con la información de salud y recomendó una revisión: "para asegurar que haya un equilibrio

adecuado entre la protección de la información del paciente y el uso y el intercambio de información para mejorar la atención al paciente".

El National Data Guardiań s emitió en 2016 un informe sobre la Seguridad de los Datos, Consentimiento y Modelo de exclusión, donde se recogía la necesidad de elaborar un modelo de consentimiento/exclusión voluntaria que dejara absolutamente claro a los pacientes/usuarios de la asistencia cuándo se utilizará la información de asistencia sanitaria y social sobre ellos y en qué circunstancias pueden optar por la exclusión voluntaria. Recogiendo que la información es esencial para una atención sanitaria y social de alta calidad: para apoyar el funcionamiento del sistema de atención sanitaria y social; para mejorar la seguridad y la calidad de la atención, incluso mediante la investigación; para proteger la salud pública; y para apoyar la innovación. El intercambio de datos es esencial para identificar la atención deficiente. Es evidente que un intercambio de datos más eficaz podría haber permitido identificar y abordar antes algunos de los recientes fracasos en la prestación de una atención adecuada a los pacientes.

En septiembre de 2013 el Secretario de Estado de Salud dijo: "Cualquier paciente que no quiere compartir los datos personales que se encuentran en el registro de su médico de cabecera con el HSCIC tendrá su objeción respetada". Dos "Exclusiones" fueron introducidos posteriormente: uno para los datos personales confidenciales que salen de la práctica de Medicina Primaria para propósitos más allá del cuidado directo (Tipo 1), y el otro para los datos personales confidenciales que son difundidos desde el HSCIC (Health and Social Care Information Centre) con fines más allá de su cuidado directo (Tipo 2).

El 25 de mayo de 2018 se introdujo la opción de exclusión de los datos nacionales, que permite a los pacientes no utilizar sus datos con fines de investigación o planificación, de conformidad con las recomendaciones formuladas por el National Data Guardian en su Review of Data Security, Consent and Opt-Outs.

Marco General: Si entrar en detalle del marco regulatorio específico y su adecuación al Reglamento General de Protección de Datos si se recogen los principios fundamentales de manejo de la información de salud basada en el Consentimiento, Tratamientos dentro de las Obligaciones Legales y Salud Publica, etc. También se recoge la Anonimización y controvertida Des-Identificación de los datos de Salud, que sería necesario una revisión en profundidad de los riesgos que conlleva.

Y en especial nos interesa el ser cedente de datos por defecto para la integración de datos de salud relacionado con la asistencia directa, para la gestión sanitaria y la investigación. Así como la regulación de la "Exclusión" para que pueda ser entendida y realizada por el paciente.

La cláusula de exclusión de los datos nacionales se aplica a la divulgación de información confidencial de los pacientes para fines que van más allá de la atención individual en todo el sistema de salud y de atención social de adultos de Inglaterra. En términos generales, la opción de exclusión de los datos nacionales se aplica a menos que exista un requisito legal obligatorio o un interés público superior para que los datos se compartan. La exclusión voluntaria no se aplica cuando la persona ha consentido en compartir sus datos o cuando los datos son anónimos de acuerdo con el Código de Prácticas de Anonimización de la Oficina del Comisionado de Información (ICO).

Detalle del Modelo de Exclusión: La cláusula de exclusión de los datos nacionales se aplica a los datos que se originan en el sistema de atención social de la salud y de adultos en Inglaterra y que aplican las organizaciones de salud y de atención que posteriormente procesan esos datos para fines que van más allá de la atención individual. La exclusión voluntaria no se aplica a los datos divulgados por los proveedores de servicios de salud y atención fuera de Inglaterra o a los servicios de atención social para niños. En este caso se permite el acceso a datos de contacto de los pacientes para obtener el consentimiento a participar en la investigación.

Un paciente puede establecer una exclusión voluntaria a través de una serie de canales que incluyen canales en línea, asistidos digitalmente y no digitales. Cualquier persona registrada en los Servicios Demográficos Personales (PDS) y que, por consiguiente, tenga un número del Sistema Nacional de Salud (NHS), puede establecer una exclusión voluntaria de datos nacionales. La exclusión voluntaria se almacena en

un registro central con su número del NHS que sirve de apoyo a la infraestructura de TI para la atención sanitaria y social en Inglaterra.

En los casos en que los investigadores necesiten identificar a personas para participar en estudios de investigación, puede aplicarse a este proceso la cláusula de exclusión de los datos nacionales, dependiendo del mecanismo utilizado para identificar a los posibles sujetos de la investigación.

La exclusión voluntaria se aplica independientemente del formato de los datos, lo que incluye los datos electrónicos estructurados y no estructurados y los registros en papel. Cuando se aplique la cláusula de exclusión, todo el registro (o registros) asociado con esa persona deberá ser eliminado completamente de los datos que se están divulgando. El número del NHS se utiliza como identificador para la eliminación de los registros. NHS Digital y Public Health England están aplicando la opción de exclusión de los datos nacionales a todas las publicaciones de datos de alcance y cumplen con esta política. Se exige a otras organizaciones pertinentes que cumplan con la exclusión voluntaria para marzo de 2020.

Por defecto aplica la siguiente clausula a todos los pacientes: "Mi información puede ser usada para gestionar el NHS y la Asistencia Social, así como apoyar la investigación para mejorar tratamiento y cuidado para todos. Su información será utilizada para comprobar la calidad de su cuidado, para pedirle su opinión sobre el cuidado que ha recibido, y para ayudar a los investigadores a mejorar el tratamiento de enfermedades como el cáncer y su prevención."*

La Exclusión (Escenario Limitado): "Mi información puede ser usada para gestionar el NHS y la Asistencia Social, pero no para la investigación. Su información será utilizada para comprobar la calidad de su cuidado y pedirle su opinión sobre los cuidados que has recibido. Su información no será utilizada por los investigadores para mejorar la forma en que las enfermedades como el cáncer son tratados y prevenidos."*

La Exclusión (Escenario Restringido): "Mi información sólo será utilizada por las personas que proporcionen directamente mi cuidado. La gente que le cuide podrá ver la información que necesite. El NHS y la asistencia social no podrá utilizar su información para comprobar la calidad de la atención que recibe, ni tampoco los investigadores la usarán para mejorar la forma en que las enfermedades como el cáncer se tratan y se previenen."*

El Control de la Base de Datos Central: Los registros médicos contienen información confidencial, de modo que cualquier divulgación a una persona determinada sin consentimiento para apoyar actividades como investigaciones médicas importantes o planes de atención sanitaria debe ser de interés público más amplio y estar sometida a un riguroso escrutinio para mantener la confianza del público.

Para ello se creó el Grupo Asesor de Confidencialidad (CAG), establecido por la Autoridad de Investigación Sanitaria el 1 de abril de 2013 para evaluar las solicitudes con respecto al Reglamento del Servicio de Salud (Control de la Información del Paciente) de 2002. Proporciona asesoramiento de expertos independientes al Organismo de Investigación Sanitaria y al Secretario de Estado de Salud sobre si debe o no aprobarse una solicitud para procesar información de pacientes sin consentimiento.

El CAG actúa como una salvaguarda a través de la provisión de garantías de que las solicitudes son examinadas independientemente por un grupo imparcial antes de que se tome una decisión final. Aplicando tanto para fines de investigación como de no investigación.

La Autoridad de Investigación Sanitaria toma la decisión final de aprobación de todas las solicitudes de investigación en las que la información pertinente se haya generado en Inglaterra. El Secretario de Estado de Salud (a través del Departamento de Salud) toma la decisión final de aprobación para todas las demás solicitudes relevantes.

Datos Actuales: De los 66 millones de habitantes del Reino Unido en 2019, aproximadamente menores de edad son un 20% = 14 millones. Quedando una población de 52 millones candidata a participar en registro central de pacientes, de los cuales han ejercido su derecho de "Exclusión" unos 1.5 millones desde que entró en vigor hasta junio de 2020.

Esto supone que un 2.8 % de la población ha optado por estar fuera de los posibles usos en la gestión y/o investigación, lo que significa que el Sistema de Sa-

(Traducción libre de los autores)

lud dispone de una base de datos potencial de más de 50 millones de ingleses que admiten la gestión y la investigación con sus datos de salud, demostrando una alta confianza en el sistema y sus garantías.

5. PARA REFLEXIONAR

No cabe duda que las intenciones subyacentes a la cesión de datos personales relativos a la salud con destino a la investigación clínica son, en un plano teórico, más que admirables. Pero la ciencia también requiere de una mirada crítica que no sólo tome en consideración el modelo objeto de estudio sino que además analice sus riesgos. El derecho fundamental a la protección de datos ofrece un amplio abanico de posibilidades a la investigación científica en salud, pero a cambio también exige una rigurosidad y unas condiciones al entorno del investigador que no por repetidas han de darse por cumplidas.

Para empezar, el contexto en el que se originó el movimiento en favor de la cesión de datos ya no existe; la derogada LOPD 15/99 giraba entorno al consentimiento del afectado como premisa fundamental para el tratamiento de los datos, dejando poco margen a excepciones más allá de las recogidas formalmente en normas con rango de ley. ¿Y qué es la cesión de datos sino una forma de consentimiento? Afortunadamente para la investigación, en la actualidad la LOPDGDD 3/2018, bajo la redacción de la disposición adicional decimoséptima, permite tratar datos seudonimizados sin contar con el consentimiento del afectado.

Claro que las siguientes preguntas son obligadas, ¿tienen las organizaciones que gestionan los historiales clínicos de los pacientes la madurez suficiente para ofrecer datos seudonimizados? ¿se han producido los cambios organizativos necesarios para segregar a los equipos de investigación de los proveedores de datos (responsables del tratamiento)? ¿los consabidos Comités de Ética de Investigación Biomédica han incorporado a sus filas expertos en protección de datos?

No tenemos un marco nacional de uso compartido por los Servicios de Salud o el Ministerio de Sanidad de la información asistencial para la gestión o la investigación, tenemos 17 + 1 islas de información. Lo que conlleva a no tener bases de datos consolidadas a nivel nacional que permitan un acceso a grandes volúmenes normalizados. En cambio, tenemos una marco poco regulado y controlado de las decisiones distribuidas de los comités de éticas de la investigación de los centros, o autonómicos que controlen las garantías de los procesos de accesos a datos. Y tampoco tenemos un órgano superior que analice o controle el marco de la aplicación de las habilitaciones recogidas en la Disposición adicional decimoséptima de la LOPDGDD 3/2018.

Volviendo al pasado, sin ánimo de perseguir unicornios pero si de apostar por la mejora continua, conviene volver la vista al Plan de Inspección Sectorial de Oficio de Hospitales Públicos[6] de la Agencia Española de Protección de Datos y revisar sus recomendaciones respecto del modelo de gestión de datos en el ámbito de la investigación médica. En él se sacaban a la luz "posibilidades de mejora" tanto respecto del consentimiento, como de la implementación de los registros de acceso, las salas de lectura de historias clínicas de hospitales,... Por tanto, la pregunta en este caso es ¿los pacientes, titulares de sus historias clínicas, deberían confiar en los servicios sanitarios públicos cediendo sus datos para investigación de cara a preservar su privacidad?

Los defensores a ultranza de la investigación por encima de todas las cosas sugieren que los ciudadanos españoles tienen la suerte de tener garantizada su información personal en poder de la Administración, puesto que llevan una década disfrutando de la seguridad que les ofrece el RD 3/2010 por el que se regula el Esquema Nacional de Seguridad (ENS). Si bien ciertamente es una norma cuyo cumplimiento ofrece serias garantías, la seguridad absoluta no existe, convendría saber cual es el nivel de cumplimiento de dicha norma, no a través del Informe de Resultados Generales Anual del Estado de la Seguridad (Encuesta INÉS) sino de forma pormenorizada por sectores poniendo el foco en el sanitario. Aún así, para el 2019, este informe muestra en la tabla 59 que tanto el índice de madurez como el índice de cumplimiento para sistemas de categoría media y alta es deficiente. Toca recordar que las medidas de seguridad aplicables a los tratamientos de datos personales, conforme a la disposición adicional primera de la LOPDGDD 3/2018 son las recogidas en el ENS.

6. https://www.aepd.es/es/media/planes/plan-de-inspeccion-hospitales-publicos.pdf

Una conectividad segura y sin fisuras, claves para los entornos sanitarios



José Luis Laguna
Director Systems Engineering Fortinet España y Portugal

UNA DE LAS CONSECUENCIAS DE LA PANDEMIA HA SIDO LA ACELERACIÓN DEL PROCESO DE TRANSFORMACIÓN DIGITAL EN TODOS LOS ÁMBITOS, SIENDO LA INDUSTRIA DE LA SALUD UNA DE LAS QUE MÁS HA AVANZADO EN ESTE SENTIDO. EL CONFINAMIENTO Y EL COLAPSO DEL SISTEMA ASISTENCIAL PROVOCADO POR LA PRIMERA OLA IMPULSÓ LA ATENCIÓN MÉDICA *ONLINE*, LO QUE GENERÓ UNA GRAN DEPENDENCIA TECNOLÓGICA POR PARTE DE LAS TI DE LOS CENTROS SANITARIOS Y POR LA NECESARIA TRANSMISIÓN DE DATOS CRÍTICOS AL PERSONAL MÉDICO O A LOS LABORATORIOS.

La atención sanitaria online y las consultas virtuales han permitido a los pacientes acceder, en un momento muy complicado, a los servicios médicos, de tal manera que el personal sanitario ha podido seguir realizando sus tareas y atender a sus pacientes en un ecosistema sin fronteras. Además, la tecnología digital ha sido vital a la hora de aunar esfuerzos entre organizaciones sanitarias que, gracias a esta coordinación, han podido agilizar su labor.

Lógicamente todos estos avances no están carentes de peligros, ya que implican una gran complejidad, fragmentación y más riesgos para las redes hospitalarias.

Para hacer frente al aumento de los casos de COVID-19 y mantener al mismo tiempo los servicios esenciales de urgencias, muchos hospitales han abierto urgencias independientes o temporales, incluso en tiendas de campaña, para realizar pruebas a los pacientes de COVID-19 y llevar a cabo la administración de vacunas de forma independiente a la atención a la hospitalaria habitual. Cada uno de estos espacios necesita tener las mismas soluciones de conectividad y colaboración rápidas, seguras y fiables que el propio hospital. Es necesario registrar la información del paciente, verificar la información de la seguridad social, acceder a los historiales médicos online, compartir los registros de laboratorio y de vacunas con otros médicos, publicar y comprobar los protocolos de atención, controlar los signos vitales e informar sobre el estado del paciente a los familiares.

La disponibilidad de nuevas tecnologías digitales, como la red definida por software (SD-WAN), permite a los hospitales y clínicas establecer rápidamente centros satélites de atención y tener acceso inmediato a recursos críticos. Pero si bien esta tecnología puede proporcionar la información necesaria para resolver problemas médicos urgentes y mejorar los resultados de los pacientes, también hacen que las redes sanitarias distribuidas sean mucho más complejas y, por tanto, más vulnerables a los ataques.

La conectividad es una cuestión crítica. Los equipos de TI del sector sanitario pueden tener que gestionar cientos de conexiones de clínicas remotas, oficinas, redes domésticas de trabajadores y pacientes al mismo tiempo. Y si alguno de ellos se cae eso conlleva graves consecuen-



cias para la salud y la seguridad de los pacientes, puesto que el sector sanitario no puede tolerar tiempo de inactividad o lentitud en los procesos.

En este contexto, las soluciones SD-WAN, que permiten un despliegue rápido, son de gran utilidad si bien la SD-WAN tradicional no incluye el componente de seguridad necesario. Esto implica que los equipos de TI tienen que diseñar e implementar una solución de seguridad superpuesta que puede requerir tiempo y recursos para su configuración, y no puede adaptarse fácilmente a los cambios que se están produciendo en el sector Sanitario sin afectar a la operativa normal de los usuarios. Por todo ello, se puede retrasar considerablemente la capacidad de un hospital para desplegar una clínica satélite de urgencias.

Otro de los vectores de ataque a los que se enfrenta el sector es el desarrollo y despliegue de dispositivos de Internet de las Cosas Médicas (IoMT) y nuevas aplicaciones de atención al paciente para proporcionar atención *online*. A ello se une la explosión de nuevos *endpoints*, que deben ser fiables, resistentes, interconectados y seguros. De hecho, el número de aplicaciones médicas descargadas durante la pandemia de COVID-19 aumentó un 30% en Estados Unidos en 2020, y un asombroso 134% en Corea del Sur. Y para 2022, se espera que el número de enfermeras y médicos que utilizan dispositivos móviles supere el 90%, según el estudio *The Future of Healthcare: 2022 Hospital Vision Study* realizado por Zebra Technologies.

El IoMT tiene muchas ventajas pero amplía enormemente la superficie de ataque. Las redes sanitarias actuales se ven expuestas a riesgos sin precedentes. Los sistemas informáticos obsoletos combinados con protocolos de ciberseguridad inadecuados y la falta de personal informático, contribuyen a poner en peligro los datos sensibles. Como resultado, en enero de 2021, el *ransomware* fue responsable del 46% de las filtraciones de datos sanitarios, según el análisis de los investigadores de ciberseguridad de Tenable.

Además de la ampliación de la superficie de ataque, las organizaciones del sector sanitario deben seguir cumpliendo con leyes nacionales muy reguladas, lo que supone una gran responsabilidad a la hora de gestionar de forma segura la información médica privada de los pacientes.

> ***Una solución Secure SD-WAN proporciona visibilidad avanzada, conectividad flexible, seguridad de nivel empresarial y protección avanzada para las redes sanitarias actuales, que se expanden y evolucionan rápidamente"***

EL RETO DE SIMPLIFICAR Y ASEGURAR UNA RED DISTRIBUIDA

Para hacer frente al factor agravante de la ampliación de las superficies de ataque de la red y el correspondiente aumento del volumen de amenazas, las empresas del sector sanitario necesitan simplificar y asegurar sus infraestructuras de red ampliamente distribuidas. En concreto, las conexiones con ubicaciones fuera de las instalaciones, como consultorios médicos, clínicas y centros emergentes, deben funcionar y cooperar con una latencia mínima, máxima visibilidad y seguridad absoluta.

La SD-WAN aprovecha la WAN corporativa, así como la conectividad multi-cloud, para ofrecer un rendimiento de aplicaciones de alta velocidad en el perímetro de la WAN. Una de las principales ventajas de la SD-WAN es que proporciona una selección dinámica de rutas entre las opciones de conectividad -MPLS, 4G/5G o banda ancha-, de modo que los hospitales, las clínicas y los médicos siempre tienen una ruta optimizada para la consulta online y otras aplicaciones en la nube.

Pero la conectividad es sólo la mitad de la historia. La seguridad y el cumplimiento son igualmente importantes. El reto es que las soluciones tradicionales de seguridad superpuestas que ofrecen la mayoría de las tecnologías SD-WAN simplemente no pueden adaptarse a los entornos de conectividad dinámicos de los que dependen la mayoría de los entornos sanitarios. En su lugar, la seguridad debe integrarse en cada dispositivo SD-WAN, permitiendo que los médicos en remoto, las ubicaciones dispersas y el centro de datos se adhieran a un conjunto común de políticas de seguridad y criterios de aplicación. A diferencia de las soluciones SD-WAN tradicionales, una solución Secure SD-WAN integra las capacidades de red y seguridad, proporcionando conectividad y protección sin fisuras en el perímetro de la WAN, la capa de acceso y los *endpoints*.

Secure SD-WAN incorpora la seguridad directamente en la conexión con *firewalls* de nivel empresarial totalmente integrados y funciones de red privada virtual (VPN), así como funciones de seguridad adicionales, como el cifrado, el sistema de prevención de intrusiones, el antivirus, la seguridad y el filtrado web y el *sandboxing*. También ofrece despliegues intuitivos y sin intervención, lo que permite ahorrar valiosos recursos de TI en el sector sanitario. Y la orquestación centralizada de VPN automatiza la conectividad dinámica en la red más compleja con flujos de trabajo intuitivos, la priorización de las aplicaciones críticas y las conexiones WAN de auto-reparación.

Una solución secure SD-WAN se compone de un firewall de nueva generación (NGFW), acceso seguro por cable e inalámbrico, conexión a la nube, acceso acelerado a las aplicaciones y una conectividad consistente, junto con una gestión centralizada y análisis e informes completos. De esta manera, los equipos de TI consolidan las funciones esenciales en una solución unificada para ayudar a solucionar los problemas y responder más rápidamente a los ciberincidentes.

En definitiva, una solución Secure SD-WAN proporciona visibilidad avanzada, conectividad flexible, seguridad de nivel empresarial y protección avanzada para las redes sanitarias actuales, que se expanden y evolucionan rápidamente. La implementación de una solución Secure SD-WAN es imprescindible para las redes sanitarias que requieren establecer una conectividad rápida, escalable y flexible en todos los entornos de red. Permite la rápida implementación de una solución de seguridad sanitaria ideal, segura, resistente, fiable y con capacidad de respuesta, al igual que los profesionales que la necesitan.

Retos del Delegado de Protección de Datos en la Investigación en Salud

Oficina del Delegado de Protección de Datos - Fundación TIC SALUT SOCIAL[1]

Robert Rubió Ochoa[1]; Miriam Mendez Garcia[2]; Sara Hernández Corbacho[3]
1. Director oficina DPD
2. Responsable Área de Investigación oficina DPD
3. Responsable Área de Organización oficina DPD

PALABRAS CLAVE: Comités de Ética de Investigación (CEI), proyectos de investigación, recursos y herramientas, DPD

La aplicación de la normativa de protección de datos en el ámbito sanitario reviste una complejidad que se ve aumentada cuando hablamos de investigaciones con datos de salud. Como ejemplo de esta complejidad encontramos el actual debate existente entorno la definición de roles en el marco de los ensayos clínicos, o del uso de herramientas de inteligencia artificial en el ámbito sanitario. Las normas propias de cada país, que desarrollan el *Reglamento UE 2016/679, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos* (RGPD), han realizado varias previsiones específicas en relación a la investigación en salud.

En este sentido la *Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos digitales* (LOPD-GDD), a través de la letra h, apartado segundo de la disposición adicional 17a, estableció una previsión por la que resultaba obligatoria la incorporación en todos los Comités de Ética de Investigación (en adelante CEI) de un Delegado en Protección de Datos Personales (en adelante DPD), o en su defecto, a un experto con conocimientos suficientes del RGPD.

El objeto de esta previsión era conseguir que todos los proyectos de investigación evaluados por un CEI cumplieran con los requerimientos establecidos por la normativa de protección de datos.

Si bien a partir de esta previsión, los CEI han ido incorporando al DPD, o en su defecto, a especialistas en protección de datos, el objetivo perseguido por esta norma requiere cambios más allá de la participación en el CEI de esta figura y que implican acciones a nivel institucional, debido a que el desarrollo de las funciones del DPD o experto en el CEI, reviste varias dificultades.

¿QUÉ ELEMENTOS DIFICULTAN EL EJERCICIO DEL DPD EN LOS CEI?

En primer lugar, los DPD de cada CEI deben revisar en cada sesión un elevado número de proyectos, la mayoría incorporan el uso de tecnologías emergentes como la inteligencia artificial, el Big Data, la biometría y la realidad virtual, entre

1. https://ticsalutsocial.cat/dpd-salut/

otras, así como el desarrollo de dispositivos y aplicaciones de salud (Apps), y que deben comprender para valorar los riesgos desde el punto de vista de la privacidad.[2]

En este sentido, y en relación a la necesidad de evaluar los protocolos que se presentan en los CEI, se hace necesario que el proyecto incorpore toda la información relativa al ciclo de vida de los datos y que describa para cada etapa todas las actividades u operaciones de tratamiento que se llevaran a cabo sobre los datos de carácter personal con el objetivo de entender los posibles riesgos a los que se pueden ver expuestos los mismos. De lo contrario, no se disponen de unos elementos mínimos para el análisis y se dificulta la tarea de analizar las implicaciones que desde la perspectiva de protección de datos pueda tener el proyecto. Esto ocurre, en parte por desconocimiento del investigador de aquellos elementos en protección de datos que debe tener en cuenta en el diseño del proyecto y que debe incorporar en el protocolo y, en parte, por la percepción errónea de que el dictamen favorable del CEI ya es una base de legitimación suficiente para el tratamiento de datos del proyecto.

¿EN QUÉ DIRECCIÓN DEBEMOS TRABAJAR PARA SOLVENTAR ESTÁS DIFICULTADES?

De acuerdo a lo indicado, parece que la simple incorporación del DPD en los CEI no es suficiente para garantizar que los proyectos que se evalúan cumplan con los requerimientos mínimos de protección de datos, por lo que se hace necesario crear una serie de herramientas y metodologías que ayuden a los centros al cumplimiento de esta normativa y faciliten la evaluación de los proyectos por parte del CEI.

Desde la Oficina de Delegado de Protección de Datos de la Fundación TICSALUTSOCIAL se han establecido diferentes líneas de trabajo con agentes clave del sistema de salud y fundaciones de investigación para cubrir las necesidades detectadas, homogeneizar y estandarizar los criterios en protección de datos, y proporcionar herramientas y materiales que faciliten la evaluación de los proyectos en este ámbito.

1. FORMACIÓN

La herramienta básica para garantizar el cumplimiento de la normativa de protección de datos es la formación de los investigadores y los miembros de los CEI, de forma que conozcan sus obligaciones a nivel de protección de datos, específicamente en el ámbito de la investigación. Los proyectos deben diseñarse teniendo en cuenta la privacidad como un elemento más del proyecto. En este sentido, se ha elaborado para los investigadores un módulo específico de formación en protección de datos en el ámbito de la investigación, para que todos los profesionales que participan de alguna forma en la elaboración o evaluación de los proyectos dispongan de una sólida base para el desarrollo de su tarea.

2. MATERIAL DE APOYO

Esta formación debe acompañarse simultáneamente de materiales que faciliten la aplicación de criterios de protección de datos en el ámbito específico de la investigación. Por ejemplo, establecer modelos indicando los apartados que debe incorporar un protocolo desde el punto de vista de protección de datos, modelos de hoja de información y de consentimiento, con la información mínima de protección de datos. Así como, infografías y otras herramientas de consulta práctica.[3]

3. HERRAMIENTA EVALUACIÓN DE IMPACTO

Uno de los elementos que genera más dificultad, y que a la vez es más necesario en el ámbito de la investigación, es la evaluación de impacto. Es una herramienta que generalmente, se utiliza poco en el ámbito de la investigación, y que debe implantarse como una parte más del proyecto, viendo su utilidad para la gestión del mismo, y no como un "simple trámite legal" al que debe dar cumplimiento la normativa de protección de datos. Para conseguir este fin, se ha trabajado

2. Lecuona Ramírez, I. et al (2020, noviembre). Pautas para evaluar proyectos de investigación e innovación en salud que utilicen tecnologías emergentes y datos personales. http://diposit.ub.edu/dspace/handle/2445/171978

3. https://ticsalutsocial.cat/wp-content/uploads/2020/07/avaluacio-dels-aspectes-derivats-de-la-normativa-de-proteccio-de-dades-en-projectes-de-recerca-versiofinal.pdf

conjuntamente con el Observatorio de Bioética y Derecho de la Universidad de Barcelona en una herramienta de fácil uso con lenguaje claro, con definiciones y ejemplos, que permite una autoevaluación para detectar riesgos en el tratamiento de datos personales y ayuda a mitigarlos a partir de propuestas automatizadas, así como establecer un plan de acción. Esta herramienta está en tres idiomas (Catalán, Castellano e Inglés) y es de acceso abierto[4].

4. RECURSOS TÉCNICOS

Además de estos recursos o metodologías, existen otros elementos que a nivel institucional pueden ayudar al cumplimiento de la normativa, como la disposición de recursos técnicos que los investigadores precisan para el tratamiento de los datos y que han de ser conformes a los requerimientos de seguridad del RGPD, a fin que no acudan a elementos externos que no disponen de unos requerimientos de seguridad mínimos, como el uso de *clouds* públicos. Por lo que se hace necesario proporcionar herramientas de gestión y programas con las garantías del Esquema Nacional de Seguridad.

5. COLABORACIÓN

La coordinación entre los diferentes participantes en el proyecto de investigación y los expertos también es una herramienta fundamental. En este sentido por ejemplo se debe garantizar la colaboración en el CEI de otros profesionales de la institución, ya que la aplicación de la normativa de protección de datos no sólo requiere un conocimiento jurídico, sino también nociones de tecnologías y sistemas de información y conocimientos científicos, por lo que resulta imprescindible colaborar juristas, técnicos y científicos para evaluar los proyectos de manera integral.

Es necesario llevar a cabo una armonización de criterios y herramientas que venga dada a nivel de sistema de salud, de forma que todos los CEI puedan evaluar los aspectos de protección de datos de los proyectos de investigación bajo unos mismos criterios. Por ejemplo, resultan útiles iniciativas como la de la Agencia Española del Medicamento y Productos Sanitarios (AEMPS), que ha creado un grupo de trabajo para elaborar un memorándum para que los CEI evalúen los Estudios Observacionales con Medicamentos, con unos mismos criterios, incorporando la perspectiva de protección de datos y donde se incorpore a los DPD a participar.

> ***El trabajo del DPD en los CEI debe darse acompañada de las herramientas institucionales que apoyen su función, con la colaboración de investigadores y técnicos, y de forma coordinada a nivel de sistema de salud y de acuerdo con los criterios establecidos por las autoridades internacionales en materia de protección de datos"***

Esta colaboración debe coordinarse también a nivel europeo siguiendo los criterios establecidos por el Comité Europeo de Protección de Datos (CEPD) y el Supervisor Europeo de Protección de Datos (SEPD). En este sentido se deberá prestar especial atención a la guía que se espera que publique este año el CEPD relativa al ámbito de la investigación, y que vendrá a dar respuesta a los diferentes roles y bases legitimadoras que pueden utilizarse en investigación.

En definitiva, el trabajo del DPD en los CEI debe darse acompañada de las herramientas institucionales que apoyen su función, con la colaboración de investigadores y técnicos, y de forma coordinada a nivel de sistema de salud y de acuerdo con los criterios establecidos por las autoridades internacionales en materia de protección de datos. Nos enfrentamos a retos complejo y globales, que debemos resolver con herramientas y criterios comunes para garantizar el progreso y el avance de la ciencia con pleno respeto a los derechos de nuestros conciudadanos

4. https://ticsalutsocial.cat/dpd-salut/avaluacio-dimpacte-relativa-a-la-proteccio-de-dades-aipd-en-salut/

Securización de la Gobernanza del dato

Francisco Leal Usero
Head of Southern Area, Cybersecurity BU Inetum

LOS DATOS SE HAN CONVERTIDO EN UN ACTIVO FUNDAMENTAL PARA TODO TIPO DE ORGANIZACIONES, DE HECHO, HAY LIBROS CUYO TÍTULO NOS DAN UNA IDEA LO QUE REPRESENTA EL DATO, DE LA VITAL IMPORTANCIA DEL MISMO Y LA ESPECIAL NECESIDAD DE PROTECCIÓN QUE REQUIEREN. PRUEBA DE ELLO ES LA OBRA DE JUAN MANUEL LÓPEZ ZAFRA: "ALQUIMIA: CÓMO LOS DATOS SE ESTÁN TRANSFORMANDO EN ORO".

Efectivamente, los datos son el nuevo oro y como tal su valor está en alza, y se ha convertido en un codiciado objeto y es por todos de sobra conocido que la seguridad 100% no existe, que todo es atacable y vulnerable que solo es cuestión de tiempo, incorrectas configuraciones o actuaciones negligentes.

El dato requiere de una especial protección y prueba de ello es el acervo comunitario que viene a establecer obligaciones en la protección del dato conforme a lo establecido por el RGPD o la Directiva NISD y circunscritos al ámbito sanitario, estos datos requieren de medidas de protección adicionales.

Los procesos de Transformación Digital o en algunos casos la acelerada digitalización llevada a cabo tras la pandemia, han facilitado las cosas para los ciberdelincuentes y han complicado las tareas de securización de los datos sanitarios, prueba de ello es el número de ataques a organizaciones sanitarias, siendo la propia OTAN la que denunciaba una ola de ataques contra Hospitales. Ante semejante panorama no nos queda otra, incluyo aquí a las organizaciones privadas que colaboramos con las entidades sanitarias en su adecuada, correcta y efectiva securización de los datos, que adoptar soluciones eficaces para garantizar los parámetros de seguridad que requieren los datos en los entornos sanitarios.



No estoy siendo alarmista al afirmar que es vital mantener a salvo los datos sanitarios, dado que, ante un ataque exitoso por parte de cibercriminales lo que se halla en juego son vidas humanas.

Como indicaba en párrafos anteriores, tras el proceso de digitalización al que se han visto obligadas las entidades e instituciones sanitarias, el perímetro de la ciberseguridad ha sufrido una abrupta difuminación, siendo necesario convertir al usuario final en la primera barrera de seguridad, en un *firewall* humano a través de la concienciación y la formación, acompañado de sistemas integrales que garanticen el ciclo seguro de la información sin restringir el acceso a la misma



que imposibilite su uso de forma extremada pues tan perjudicial es una excesiva protección como la ausencia de la misma, sin desdeñar un factor decisivo en el proceso de digitalización y transformación, lo que se denomina sobreexposición.

Este inusitado incremento en la superficie de exposición de las entidades sanitarias y la obligada interconexión y facilidad de acceso a la información es un reclamo para los malhechores, cuyo objetivo es apropiarse de forma indebida de los datos sanitarios. Para corroborar esto último, existe una tendencia alcista y un inusitado interés en la Dark Web por obtener bases de datos en general, siendo de especial interés bases de datos de entidades sanitarias al tratarse de un suculento, en términos económicos, botín. Las entidades sanitarias deben hacer frente, en lo que respecta a la securización de los datos, a tres problemas principales, siendo estos los datos de especial sensibilidad que manejan , la heterogeneidad de las infraestructuras que albergan los Sistemas de Información y las Infraestructuras de Seguridad y, por último, el control y securización de dispositivos OT/ IoT.

Para abordar proyectos que implementen soluciones globales y desde una perspectiva cibersegura desde el inicio, ENISA ha publicado una guía para la seguridad de los servicios sanitarios bajo el nombre "Directrices sobre contratación para la ciberseguridad en los hospitales" altamente recomendable.

¿A qué cuestiones deben dar respuesta los proyectos de securización de los datos sanitarios? Estimamos que son ¿Qué? ¿Para qué? ¿Cómo? El resultado no es otro que acometer proyectos que, sin mermar la visibilidad de los datos, estén cibercontrolados.

1. **¿Qué?:** Soluciones globales de Seguridad Física, Seguridad Lógica, Identidad Digital y Cumplimiento Normativo. Es preciso tener visibilidad sobre todos los eventos del mundo físico que ocurren en los sistemas hospitalarios, con especial énfasis en los dispositivos IoT y OT. El perímetro sigue siendo una pieza fundamental para la securización de infraestructuras por las que los datos sanitarios discurren.
2. **¿Para qué?** Para cumplir con la normativa, pues al tratarse de infraestructuras críticas (véase el Anexo II de la Directiva NISD) y servicios esenciales están sujetos a medidas de seguridad reforzadas. Esto tiene una especial transcendencia pues lo que está en juego son vidas humanas como aludíamos en párrafos anteriores.
3. **¿Cómo?** Mediante las mejores practicas y la experiencia en la implementación de soluciones integrales con visión 360º, somos capaces de abordar grandes proyectos donde se conjugan el Gobierno de la Red a través del control de la actividad que transita por esta, sin obviar el Gobierno del Endpoint mediante el control de la actividad en el puesto de trabajo, poniendo énfasis en el Gobierno del Dato supervisando y controlando toda actividad que sobre ellos se lleva a cabo y finalizando por el Gobierno de la Identidad y los accesos, es decir, a través del control de la actividad del usuario.

Ningún dato sensible vale una vida

MEDIGATE

MANTENER EL FUNCIONAMIENTO HOSPITALARIO ANTE CUALQUIER CIBERATAQUE ES UNA DE LAS PRIORIDADES DEL SECTOR SANITARIO. LA ESTRATEGIA ZERO TRUST AYUDA A ALCANZAR LOS OBJETIVOS EN MATERIA DE SEGURIDAD CLÍNICA.



Desde que comenzó la pandemia por la Covid-19, los profesionales sanitarios se han situado en primera línea de defensa para proteger y atender a los pacientes, mientras que los actores maliciosos están aprovechando esta situación para conseguir que más personas caigan en sus redes. El entorno sanitario se ha convertido en uno de los objetivos principales de los ciberdelincuentes y el coronavirus en su gancho más popular.

Para mantenerse a salvo y evitar ciberataques, los responsables del sector sanitario deberían focalizarse en invertir en herramientas que puedan ayudarles a ser capaces de detectar y responder frente a cualquier anomalía que ocurra en el sistema, incluso antes de que pueda producirse. De acuerdo con Stephon Goldberg, Vicepresidente de Ingeniería de Sistemas de Medigate: "La creación y aplicación de políticas sobre dispositivos médicos son medidas preventivas que darán sus frutos a largo plazo, pero el presente requiere de soluciones de detección y respuesta para que las organizaciones continúen operando y ofreciendo una atención de calidad a los pacientes".

En este sentido, mantener el funcionamiento de las organizaciones sanitarias ante cualquier ciberincidente debe ser la principal prioridad de todo responsable de seguridad, ya que ningún dato sensible vale una vida. Y, una vez se haya hecho frente a las amenazas más inmediatas, el siguiente paso es llevar a cabo una revisión de las prácticas de seguridad.

¿CÓMO IMPLEMENTAR UNA ESTRATEGIA ZERO TRUST EN EL SECTOR SANITARIO?

No existe una única solución para adoptar fácilmente una estrategia de Zero Trust en el sector sanitario. De hecho, es necesario un conjunto de personas, procesos, herramientas y tecnologías trabajando juntas en todo el sistema de salud para crear y desarrollar continuamente una estrategia efectiva. A diferencia de los entornos tradicionales de oficina, la mayoría de los dispositivos en el ámbito clínico no están asociados a ningún usuario o dato específico, por lo que no se pueden aplicar los principios tradicionales de Zero Trust. Por ejemplo, las bombas intravenosas, los monitores, los endoscopios o las resonancias magnética, entre otros dispositivos, no están vinculados a una persona concreta, es decir, no existe ningún usuario conectado o registrado desde una perspectiva digital, aunque haya una persona físicamente conectada a los mismos.

Por otra parte, estos dispositivos no son herramientas estáticas, se mueven constantemente –ya sea con un paciente o de uno a otro– en el trascurso de la atención sanitaria. Por lo tanto, el concepto de Zero Trust debe adaptarse a los requisitos específicos del entorno clínico para proteger la continuidad de la atención sanitaria. En



este sentido, el modelo Clinical Zero Trust garantiza que el paciente es lo primero, por ello, la estrategia debe diseñarse con el objetivo de proteger la atención al paciente y no a los dispositivos. "¿Se imagina lo que supondría que se bloqueara el acceso a un ventilador? La estrategia de Clinical Zero Trust ayuda a los sistemas sanitarios a implementar controles de seguridad efectivos sobre los protocolos asistenciales para mantener su integridad y fluidez, sin obstaculizar la atención al paciente", señala Jamison Utter, Director Evangelizador de Producto de Medigate.

Para implementar esta postura de seguridad, se deben tener en cuenta todos los dispositivos y procesos que intervienen en la prestación de la asistencia sanitaria, lo que en última instancia puede ayudar a los sistemas sanitarios a optimizar la eficiencia y mejorar los resultados. Esto es fundamental para permitir las transformaciones operativas y eficaces que los sistemas de salud buscan a medida que avanzan hacia una medicina más conectada. Los hospitales y sistemas de salud inteligentes sólo son posibles si están protegidos y Clinical Zero Trust puede ser un facilitador, permitiendo que los protocolos de atención se entreguen de manera segura para satisfacer tanto las necesidades de los pacientes como las del personal y las del propio negocio.

Medigate, líder en seguridad IoT para el sector sanitario

Medigate ha sido reconocida como mejor compañía dentro de la categoría 'Seguridad IoT en Sanidad', por KLAS Research, analista independiente sobre tecnologías IT dirigidas al sector sanitario, en su informe 'Best in KLAS 2021: Software & Services Report'. La compañía se ha focalizado desde el primer día en resolver los desafíos de seguridad a los que se enfrentan las organizaciones sanitarias. Este reconocimiento es especialmente gratificante porque se basa, en gran parte, en la información práctica aportada por clientes reales del sector sanitario.

El fabricante proporciona tres capacidades esenciales para una seguridad TI efectiva: visibilidad de todos los dispositivos conectados a la red, detección de amenazas potenciales y prevención automatizada de ataques. "Nuestra plataforma brinda a los líderes de seguridad, biomedicina y negocio los datos necesarios para tomar mejores decisiones de seguridad y gestión de activos que permitan reducir los riesgos y conduzcan a mejores resultados para los pacientes. Con un gran conocimiento de la identificación de dispositivos y del flujo de trabajo del sector, nos esforzamos en proporcionar a las organizaciones la información y las herramientas necesarias para acelerar su transformación hacia un sistema sanitario inteligente y conectado, a la vez que ofrecemos una atención basada en el valor", afirma Jonathan Langer, CEO y cofundador de Medigate.

Medigate es también líder en Seguridad de Dispositivos Médicos Conectados, según Forrester, que lo sitúa como uno de los ocho proveedores principales en esta categoría.

Tribunal Supremo y Agencia Española de Protección de Datos: Accesos indebidos a la historia clínica y derecho del afectado a conocer la identidad del infractor

Vicente Lomas Hernández
Jefe de Servicio de Coordinación Jurídica del SESCAM.
Vocal del Comité Técnico de Seguridad de la Información. Delegado de Protección de Datos.

RESUMEN:

En este breve artículo se analizan, a raíz de una reciente STS y el posterior informe de la Agencia Española de Protección de Datos, las implicaciones del acceso indebido a la historia clínica tanto desde la perspectiva penal, como desde la perspectiva de la legislación de protección de datos personales.

I. INTRODUCCIÓN

Recientemente el Tribunal Supremo -STS de 25-09-2020, nº 476/2020, rec 366/2019-, y la Agencia Española de Protección de Datos después – Informe del Gabinete Jurídico de la AEPD nº de ref 0003/2021- han analizado desde perspectivas distintas cuestiones conexas relacionadas con el derecho a la protección de datos personales en el ámbito sanitario y, en particular, sobre los accesos indebidos de profesionales sanitarios a la historia clínica de otro compañero igualmente sanitario. (STS)

II. TRIBUNAL SUPREMO: ACCESOS INDEBIDOS DE PROFESIONALES SANITARIOS A LA HISTORIA CLÍNICA DE OTRO COMPAÑERO SANITARIO

Entre los meses de mayo a julio de 2013, dos enfermeros, Ruperto y Emma, ésta última enfermera interina en sustitución del afectado, también enfermero, Teodulfo, accedieron durante el período en el que éste se encontraba en situación de baja laboral a su historia clínica.

Para ello, y siendo conscientes del compromiso de confidencialidad contraído, accedieron con sus claves informáticas personales, sin el consentimiento ni conocimiento de Teodulfo, y sin que mediara entre éste y los infractores relación asistencial que pudiera justificar el acceso.

Por tales hechos ambos enfermeros fueron condenados por la comisión de un delito de descubrimiento y revelación de secretos. La sentencia de instancia fue recurrida por considerar que la forma de proceder de Teodulfo para averiguar si se accedió indebidamente a su historia clínica, no se habría ajustado al protocolo establecido para este tipo de casos.

En definitiva lo que se discute no es que el denunciante accediera a su historia clínica (aspecto que por otra parte la sentencia de instancia considera irrelevante), sino que accediera al historial para conocer las personas que habían

consultado o visualizado su historia clínica, sin que exista derecho alguno al conocimiento de esos datos, y sin observar los requisitos procedimentales establecidos por la Gerencia.

El TS da validez a las pruebas así obtenidas en atención a las siguientes razones:

a) El hecho de conocer o identificar a las personas que han consultado una historia clínica no supone lesión alguna del derecho a la protección de datos.

b) La actuación del denunciante fue previa al inicio de las investigaciones policiales, y absolutamente desconectada de éstas ya que estaba orientada simplemente a obtener información.

c) A lo anterior añádase, según recoge la Sentencia, que "*tampoco apreciamos la existencia de un riesgo cierto de propiciar, con la admisión de la prueba controvertida, prácticas que comprometan pro futuro la efectividad del derecho fundamental en juego en el ordenamiento jurídico español*".

Finalmente la Sala declara que en tanto que los hechos probados describen accesos no consentidos a la historia clínica de un tercero, éstos son legalmente constitutivos del delito previsto en el artículo 197.2 del Código Penal.

III. AEPD: DERECHO A CONOCER LA IDENTIDAD DE LA PERSONA/S QUE HA ACCEDIDO INDEBIDAMENTE A SU HISTORIA CLÍNICA.

La consulta planteada a la AEPD versa sobre si desde la perspectiva del Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD) y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, (LOPDGDD), y teniendo en cuenta la Sentencia del Tribunal Supremo nº 476/2020 de 25 de septiembre, el contenido del derecho de acceso a la historia clínica, comprende la información sobre quién ha accedido a la misma.

1. NORMATIVA APLICABLE.

En primer término la AEPD aclara que para dar respuesta a este tipo de consultas, la normativa de referencia debe ser la sanitaria, en concreto "*la LAP por ser la norma que, por razón de la materia y especialidad, se aplica al derecho de acceso a la historia clínica*".

2. LA LEGISLACIÓN BÁSICA ESTATAL NO PREVÉ EL DERECHO A CONOCER QUIÉN HA ACCEDIDO A LA HISTORIA CLÍNICA.

La AEPD constata que de la lectura de la LAP "no se infiere que incluya la relación de las personas que han accedido a la misma", lo que no impide que existan normas autonómicas en las que sí se prevé que el contenido del derecho de acceso a la historia clínica comprenda también, conocer quien ha accedido a la misma.

3. EL CRITERIO DE LA AEPD

La AEPD reitera su criterio manifestado en informes anteriores, contrario a que el derecho de acceso a la historia clínica pueda comprender conocer la información sobre quién ha accedido a la misma, "*pues ni forma parte de la historia clínica y además hace referencia datos personales de terceros*".

A continuación la Agencia toma en consideración la STS de 25 de septiembre de 2020, que a su juicio no permite llegar a una conclusión distinta, pues "la Sentencia analiza un caso concreto desde la perspectiva de la legalidad de la obtención de las pruebas y su afección al proceso judicial y a los derechos de los acusados llegando a la conclusión indicada. Lo que no significa que con la Sentencia se esté legitimando o "legalizando", desde el punto de vista de la LAP, ni de la LOPDGDD, que dentro del derecho de acceso a la historia clínica, deba comprenderse también, conocer quién ha accedido a la misma".

Por todo ello la conclusión final a la que llega la AEPD es que:

"*No debe entenderse incluido dentro del derecho de acceso a la historia clínica al amparo del artículo 18 de la LAP, la información referida a si ha habido accesos y a la identidad de las personas que han accedido, salvo que en la normativa autonómica aplicable o en otras normas se prevea expresamente esa posibilidad.*"

Equipamiento médico electrónico: ¿puede la certificación del dispositivo garantizar un alto nivel de seguridad?

Los responsables de la atención sanitaria con exceso de trabajo no deberían tener que preocuparse también por los ciberataques

José Battat
Director General de Trend Micro Iberia

EN LOS ÚLTIMOS MESES, ESPAÑA HA ACABADO SIENDO UNO DE LOS CENTROS DE ATENCIÓN A NIVEL MUNDIAL POR SER LA SEGUNDA NACIÓN OCCIDENTAL AFECTADA POR LA EPIDEMIA DE COVID-19. EN TÉRMINOS DE CIBERCRIMEN, ESPAÑA TAMBIÉN OCUPA POSICIONES DESTACADAS EN EL RANKING MUNDIAL DE ATAQUES QUE SE APROVECHAN DE LA PANDEMIA, TANTO PARA CORREOS ELECTRÓNICOS DE PHISHING COMO PARA ATAQUES DIRIGIDOS A INSTALACIONES SANITARIAS.

Los hospitales y otras instalaciones de salud trabajan siempre bajo presión para atender a sus pacientes, situación que ha llegado a límites insospechados durante la emergencia sanitaria. Sin embargo, además de esto, lamentablemente también tienen que hacer frente a numerosos ataques contra sus sistemas informáticos, ataques que en muchos casos han aprovechado la situación actual para apoderarse de los sistemas a través del *ransomware* y que incluso pueden llegar a cerrar redes y equipos médicos electrónicos. En el sector de la seguridad estamos constantemente monitorizando estos ataques para proveer la mayor cantidad de información posible y reaccionar a estos ataques de la manera más apropiada.

Por desgracia, tanto en la sanidad como en la industria, a menudo nos enfrentamos a situaciones algo controvertidas. La mayoría de las veces, estos ataques no comprometen a los ordenadores o servidores tradicionales, sino a toda una serie de dispositivos especializados que son esencialmente computadoras en un "paquete" diferente. Es este "paquete" (compuesto por ejemplo, por máquinas de tomografía computarizada, escáneres de ultrasonido, cardiógrafos, etc.) lo que hace que tengan certificaciones que a menudo prohíben la instalación de cualquier tipo de software de seguridad.

Debido a la certificación del dispositivo y a las garantías en cuanto a su rendimiento, no es posible instalar ningún tipo de protección de seguridad. Pero, ¿los organismos de certificación, o los propios fabricantes del dispositivo, certifican que el rendimiento es válido incluso en caso de *malware* dentro del dispositivo? Esta es una cuestión que deben considerar las administraciones sanitarias y los fabricantes de dispositivos.



A veces, y especialmente en el caso de los dispositivos médicos electrónicos, la certificación impide la instalación de parches para sistemas operativos obsoletos. No es posible controlar el flujo de datos sin el riesgo de que la producción deje de estar certificada. ¿Pero sobre qué base se preparan estas certificaciones? ¿Se han tenido en cuenta las situaciones en las que los dispositivos pueden garantizar su rendimiento incluso en presencia de *malware* dentro del dispositivo o en la red a la que están conectados?

Es necesario revisar la certificación de los dispositivos industriales en general, y de los equipos médicos electrónicos en particular, y debe convertirse en un aspecto crucial desde el comienzo del proceso de adquisición.

Como ya se ha mencionado, al supervisar el tráfico de Internet en las últimas semanas, hemos observado una serie de ataques a hospitales y centros sanitarios, y la mayoría de ellos han puesto en peligro específicamente a los dispositivos médicos electrónicos (por ejemplo, escáneres CT, escáneres de ultrasonido, cardiógrafos, etc.) que, debido a su certificación, no pudieron actualizarse ni instalar un software de seguridad.

Los hospitales deben exigir a sus proveedores que certifiquen sus dispositivos o validen las garantías incluso en caso de *malware*, una garantía que también cubre el resto de la red, porque si el *malware* entrara en uno de estos dispositivos, sería como si un Troyano se infiltrara en toda la infraestructura, con lo que aumentaría exponencialmente el riesgo de un cierre total. Si bien es cierto que podemos limitar el daño protegiendo la infraestructura, también es cierto que los controles específicos dentro de los dispositivos actuales reducirían aún más ese riesgo.

Hospitales y centros de salud aceleran la adopción de nuevas soluciones tecnológicas

Antonio Pérez Vicente[1], **Raúl Gómez**[2]
1. Zebra Technologies España. Healthcare Sales Specialist
2. Zebra Technologies España. Senior Healthcare Sales Engineer

ZEBRA TECHNOLOGIES CORPORATION, EMPRESA INNOVADORA CON SOLUCIONES ORIENTADAS A LA MEJORA DE RENDIMIENTO EMPRESARIAL, SEÑALA QUE, AUNQUE HOSPITALES Y CENTROS DE SALUD DE TODO EL MUNDO LLEVAN DÉCADAS ESFORZÁNDOSE POR DIGITALIZAR Y AUTOMATIZAR POR COMPLETO SUS PROCESOS, LA SITUACIÓN DE PANDEMIA ACTUAL HA SIDO EL CATALIZADOR PARA QUE SE ACELERE SU TRANSFORMACIÓN DIGITAL.

La gran mayoría de los centros de salud ha hecho ya progresos significativos y está sacando un mayor provecho de la tecnología, pero la velocidad a la que se necesita el cambio sigue superando la velocidad a la que se está produciendo.

"La tecnología necesaria ya está disponible y puede implementarse ahora mismo, produciendo un impacto inmediato de mejora en muchos procesos sanitarios. Las tecnologías móviles se han ido desplegando en un tiempo récord para mejorar las tareas de admisión y diagnóstico de pacientes, mitigar la escasez de suministros y fundamentar las decisiones para conseguir mejores tratamientos, abordando algunos de los problemas sistémicos del sector", explica Antonio Pérez, especialista en Sanidad en Zebra Technologies.

> ***Dotar a los profesionales sanitarios de dispositivos móviles profesionales, incorporando software colaborativo, les ayuda a comunicarse en tiempo real con otros compañeros a través de mensajes de texto, voz, e intercambio de datos, mejorando la eficiencia en procesos de colaboración"***

Entre las diferentes aplicaciones de la tecnología que ya estamos viendo en la comunidad sanitaria destacan las siguientes:

- Distribución y Administración de medicamentos. Profesionales y pacientes de todo el mundo están preocupados por el mantenimiento de la cadena de frío durante las campañas masivas de distribución de vacunas. Este reto es extensivo a una gran variedad de productos farmacéuticos, sensibles a las variaciones de temperatura. Por ello, las mejores prácticas, recomiendan disponer de varios niveles de tecnologías de control de la temperatura, en función de si los activos se transportan en palés o neveras y se almacenan en frigoríficos, congeladores o salas de temperatura controlada. Los métodos de recogida de información manuales sólo pueden captar la temperatura de un artículo en un momento determinado y no permiten conocer si se produjo alguna alteración importante durante todo el proceso de distribución y almacenaje. De ahí la importancia de contar con registradores electrónicos de datos, que puedan controlar continuamente la



temperatura ambiental y alertar sobre posibles cambios. Es posible también, poner etiquetas de detección de temperatura en los propios viales, para que quienes administran la medicación sepan si se ha mantenido la temperatura adecuada, hasta el mismo momento de la inyección.

- Movilidad, comunicaciones y software colaborativo. Disponer de sistemas de comunicaciones colaborativos, es fundamental para mejorar la eficiencia y el trabajo en equipo. Dotar a los profesionales sanitarios de dispositivos móviles profesionales, incorporando software colaborativo, les ayuda a comunicarse en tiempo real con otros compañeros a través de mensajes de texto, voz, e intercambio de datos, mejorando la eficiencia en procesos de colaboración. Los dispositivos móviles profesionales, unidos a las herramientas de comunicaciones colaborativas, permiten, por ejemplo, acceder a los historiales de los pacientes mientras se les atiende, pudiendo actualizarlos en tiempo real sin necesidad de desplazarse a un puesto de control fijo.
- Identificación positiva de pacientes. La entrega de pulseras con código de barras en el momento del ingreso garantiza una identificación correcta de los pacientes durante todo el tiempo que permanezcan en el centro de salud. Esta identificación permite una trazabilidad completa y una disminución de errores, en procesos tan importantes como la administración de medicamentos o la recogida de muestras. Si queremos ir un paso más allá, podemos colocar en las pulseras etiquetas de identificación por radiofrecuencia (RFID), que nos permitirán, tanto la identificación tradicional, como la monitorización y localización de los pacientes en todo el recinto sanitario.
- Gestión de inventarios. La gestión del inventario es desde hace tiempo una preocupación en el ámbito sanitario. Disponer de un inventario preciso, facilitará la tarea del personal sanitario, redundando en una mejor calidad de servicio al paciente. La combinación de diferentes tecnologías, como Wifi, RFID, Bluetooth etc., unida a dispositivos profesionales diseñados para usos específicos, como lectores de código de barras, terminales móviles, *tablets* etc. y software adecuado, nos permitirá disponer de una trazabilidad completa de los artículos de uso habitual. Conocer las cantidades disponibles de medicamentos, saber dónde está ubicado un equipo médico para realizar un diagnóstico, gestionar la ropa de cama o uniformas del personal sanitario, son sólo algunas de las aplicaciones que ya podemos implementar con tecnologías actuales.

Más información sobre la aplicación de la tecnología al sector sanitario
www.zebra.com/healthcare

ACERCA DE ZEBRA

Zebra hace posible que la primera línea de negocios en *retail/ecommerce,* fabricación, transporte y logística, sanidad y otras industrias puedan alcanzar un rendimiento óptimo. Con más de 10.000 partners en 100 países, Zebra proporciona soluciones *end-to-end* adaptadas a cada sector para permitir que cada activo y trabajador sea visible, esté conectado y sea totalmente eficiente. Nuestras soluciones líderes mejoran la experiencia de compra, la gestión y el seguimiento del inventario, así como la eficiencia de la cadena de suministro y la atención al paciente. En 2020, Zebra ha entrado en Forbes Global 2000 por segundo año consecutivo y ha sido incluida en la lista de las Mejores Empresas para Innovadores de Fast Company.

Contacto:
Antonio Pérez Vicente
Zebra Technologies España
Healthcare Sales Specialist
antonio.perez@zebra.com

Raúl Gómez
Zebra Technologies España
Senior Healthcare Sales Engineer
raul.gomez@zebra.com



La seguridad sanitaria en la era COVID-19

Más de 102 millones de datos sanitarios expuestos en 2020 tras ciberataques: el *ransomware* fue la causa principal de la mayoría de las brechas analizadas

TENABLE

SØREN KIERKEGAARD, EL FILÓSOFO DANÉS, ESCRIBIÓ QUE "LA VIDA SÓLO PUEDE SER ENTENDIDA A POSTERIORI" PERO "DEBE SER VIVIDA HACIA ADELANTE". EN EL MISMO ESPÍRITU, TENABLE®, LA EMPRESA DE CYBER EXPOSURE, LLEVÓ A CABO, A TRAVÉS DE SU EQUIPO DE RESPUESTA DE SEGURIDAD (SRT, SECURITY RESPONSE TEAM), UNA RETROSPECTIVA DEL PANORAMA DE LAS AMENAZAS EN 2020, EN LA QUE SE EXAMINARON LAS PRINCIPALES INFORMACIONES SOBRE VULNERABILIDAD Y CIBERSEGURIDAD DEL AÑO PARA OBTENER UNA VISIÓN GLOBAL Y ELABORAR UNA GUÍA PARA LOS PROFESIONALES DE LA CIBERDEFENSA.

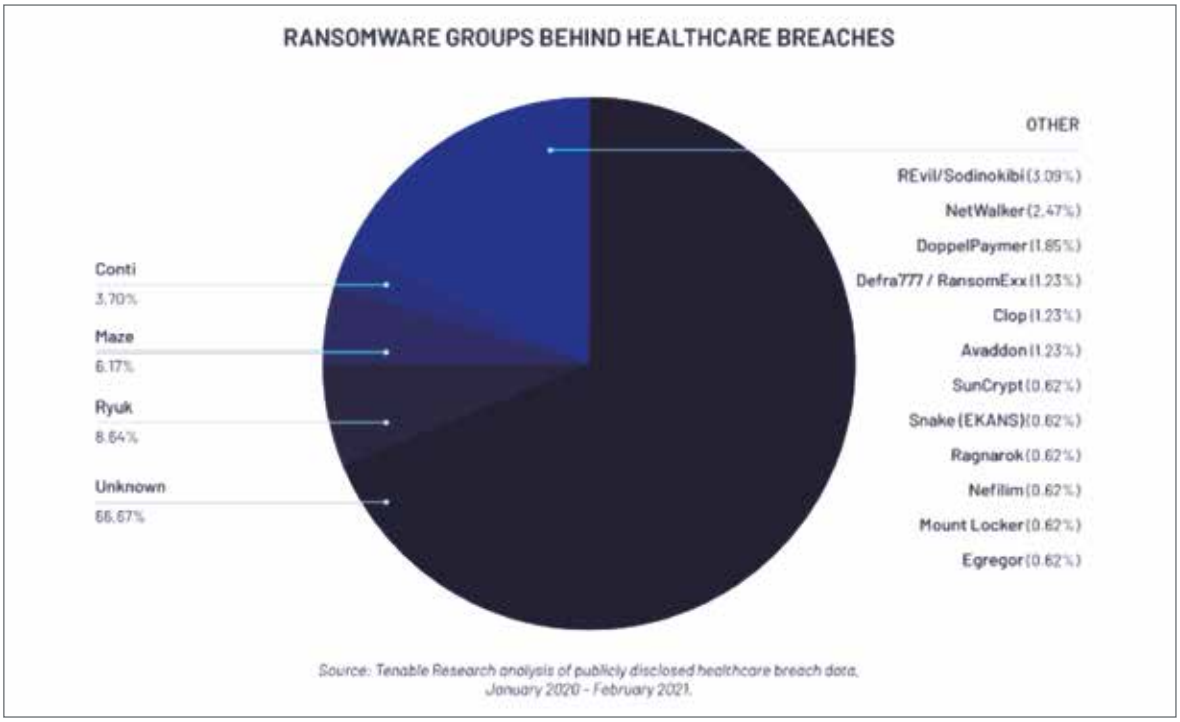
El SRT de Tenable supervisa la inteligencia sobre amenazas y vulnerabilidades para contribuir a crear y priorizar los *plugins* para los productos de Tenable, y también para ayudar a los clientes a estar informados de los riesgos asociados a las vulnerabilidades. El equipo también supervisa y sigue las infracciones divulgadas públicamente para determinar cómo y cuándo las vulnerabilidades han sido un factor de riesgo.

La retrospectiva del panorama de amenazas de 2020 reveló un total de 22.000 millones de datos expuestos como consecuencia de 730 infracciones divulgadas públicamente, y el sector sanitario fue, con mucha diferencia, el más afectado. Esto no es una sorpresa, si se considera el crítico rol que han tenido las infraestructuras sanitarias a causa de la pandemia de COVID-19.

El análisis realizado por el SRT de Tenable ha determinado que más de 102* millones de datos sanitarios estaban expuestos en 2020 como resultado de brechas de datos. Y casi tres* millones de datos sanitarios ya han sido expuestos en los dos primeros meses de 2021. La amenaza a la asistencia sanitaria y los sistemas de salud era previsible dada la creciente demanda de consultas en telesalud, materiales médicos y por la competición internacional para el desarrollo y distribución de vacunas.

Al examinar la causa de estos ataques, el *ransomware* fue, de lejos, el más prominente, representando la impresionante proporción de 54,95% de las brechas. Ryuk destacó por delante del resto, apareciendo repetidamente en las divulgaciones de brechas y representando 8,64% de las brechas relacionadas con el ransomware, seguido de Maze (6,17%), Conti (3,7%) y REvil/Sodinokibi (3,09%)

El análisis de SRT descubrió que las brechas a través de terceros representaron más de un cuarto de las brechas rastreadas y casi 12 millones de datos expuestos. Otras causas principales de las brechas de datos fueron el compromiso del *email/phishing* (21,16%), amenazas internas (7,17%) y bases de datos no seguras (3,75%).



Mientras la actual pandemia de COVID-19 sigue ejerciendo una presión sin precedentes sobre la infraestructura sanitaria mundial, los atacantes descubren que lo que ya era un objetivo atractivo es todavía más tentador", explica Rody Quinlan, director de respuesta de seguridad de Tenable. "Estos ataques no van a desaparecer a corto plazo, y por eso es urgente que las organizaciones, especialmente las que están en el punto de mira en el sector sanitario, entiendan las amenazas contra ellas y se doten de los recursos necesarios para reducir sus riesgos cibernéticos."

El *ransomware* Ryuk, principal culpable de los ataques de *ransomware* contra el sector sanitario, es conocido por favorecer una serie de vulnerabilidades, entre las cuales se encuentra Zerologon, una de las más prominentes de 2020.

Para reducir el riesgo de ataque, las organizaciones sanitarias deben:

- Priorizar las vulnerabilidades: identificar y remediar las vulnerabilidades de mayor impacto empresarial.
- Abordar la causa originaria: una vez identificadas y priorizadas las vulnerabilidades con mayor probabilidad de introducir riesgos para el negocio, remediarlas y continuar con un control periódico de mantenimiento.

CÓMO TENABLE AYUDA A LAS EMPRESAS A PRIORIZAR LAS VULNERABILIDADES Y A ABORDAR LAS CAUSAS ORIGINARIAS

Tenable® ofrece una plataforma de "Gestión de Cyber Exposure" que ayuda a los líderes de seguridad alineados con el negocio a responder a sus preguntas clave de ciberseguridad con confianza:

Ver todo. Predecir lo que importa. Actuar para abordar el riesgo.

Más de 30.000 organizaciones de todo el mundo confían en Tenable para comprender y reducir los riesgos cibernéticos. Como creador de Nessus®, Tenable amplió su experiencia en vulnerabilidades para ofrecer la primera plataforma del mundo que permite ver y proteger cualquier activo digital en cualquier entorno informático.

La gestión de Cyber Exposure es una disciplina emergente que ayuda las empresas a ver, predecir y actuar para abordar el riesgo cibernético a lo largo de toda su superficie de ataque. Fundamentadas en la gestión de vulnerabilidades ba-

> ***Tenable.ep, es la primera plataforma del sector de gestión de vulnerabilidades basada en el riesgo, todo en uno, diseñada para escalar a medida que los requisitos informáticos dinámicos cambian"***

sada en el riesgo, las mejores prácticas de gestión de Cyber Exposure introducen un idioma común enfocado en los riesgos y basado en métricas que todo mundo comprende — desde las áreas de operaciones de seguridad y de TI, hasta la dirección ejecutiva y los participantes clave.

Tenable.ep, es la primera plataforma del sector de gestión de vulnerabilidades basada en el riesgo, todo en uno, diseñada para escalar a medida que los requisitos informáticos dinámicos cambian. Tenable.ep reúne en una sola plataforma los productos líderes del sector -Tenable.io® Vulnerability Management, Tenable.io Web Application Scanning, Tenable.io Container Security y Tenable Lumin-, lo que permite a los clientes ver todos sus activos y vulnerabilidades en un único cuadro de mandos junto a las principales amenazas, *exploits* y métricas de priorización.

La capacidad de poner en marcha y conectar rápidamente los activos modernos al entorno corporativo es fundamental para la transformación digital y las iniciativas de trabajo desde casa.

Los atacantes no diferencian entre tipos de activos y tampoco deberían hacerlo los defensores. Por ello, Tenable.ep se diseñó para dar a las organizaciones el poder de identificar cada activo y exposición, predecir qué vulnerabilidades tienen más probabilidades de ser explotadas y actuar para abordar los riesgos críticos. Tenable.ep ofrece una gestión de vulnerabilidades basada al riesgo dentro de una única solución unificada sin necesidad de comprar productos separados y gestionar diferentes modelos de licencia.

Tenable tiene un historial de innovación para elevar el nivel de la ciberseguridad. Con Predictive Prioritization, Tenable ayudó a las organizaciones a pasar del intento de resolver todo lo que tuviera una puntuación CVSS crítica, a adoptar una estrategia basada en el riesgo que se centra en resolver lo más importante. Frictionless Assessment eliminó las barreras a la visibilidad unificada de los activos en el *cloud*. Y ahora, con Tenable.ep, la empresa ha reunido estas innovaciones y ha simplificado la forma de evaluar activos dispares de manera que las organizaciones puedan abordar sus programas de gestión de vulnerabilidades holísticamente.

Para saber más sobre Tenable y Tenable.ep la plataforma de cyber exposure visite: www.tenable.com.

* NOTAS

- Las divulgaciones públicas pueden ocurrir días, meses o incluso años después del propio evento
- Las cifras se han extrapolado a partir de 293 violaciones de datos divulgadas públicamente entre enero de 2020 y febrero de 2021.
- De las 293 brechas que se sabe que expusieron datos en el periodo de 14 meses analizado, 57,34% revelaron públicamente cuántos datos fueron expuestos.
- En 2020 se expusieron 102.907.137 datos sanitarios, y 2.864.677 se han revelado durante este año (en enero).

Una entrada de blog con más información está disponible aquí.

https://www.tenable.com/blog/healthcare-security-ransomware-plays-a-prominent-role-in-covid-19-era-breaches

Identificación y gestión de vulnerabilidades en el Servicio de Salud de las Illes Balears (Ib-Salut)

Miguel Ángel Benito Tovar[1]; Eva Quintana Pozo[2]; Jaime Borrás Guerrero[3]
1. Jefe de Servicio de Protección de Datos en el Servicio de Salud de las Illes Balears
2. Ingeniero Superior de Tecnologías de la Información en el Servicio de Salud de las Illes Balears
3. Senior Security Consultant en EY

PALABRAS CLAVE
Riesgo, vulnerabilidades, análisis periódico, activos, Tenable, OTRS, motor integrador.

INTRODUCCIÓN

Uno de los principales objetivos del Servicio de Seguridad de la Información del Servicio de Salud de las Illes Balears, es establecer un proceso de identificación de activos y de gestión sus vulnerabilidades maduro que permita a las Gerencias territoriales tener un mayor control sobre los riesgos de seguridad de sus activos, así como definir un mecanismo ágil y sencillo para la reducción de dichos riesgos.

CONCEPTOS CLAVES

Antes de empezar, a hablar de lo que supone un ciclo completo de identificación y gestión de vulnerabilidades es importante repasar los principales conceptos a tener en cuenta para lo que tomaremos como referencia las definiciones definidas en el "Glosario de Términos de Ciberseguridad" elaborado por el INCIBE:

Vulnerabilidad: Podríamos definir una vulnerabilidad como un fallo técnico o deficiencia de un programa que puede permitir que un usuario no legítimo acceda a la información o lleve a cabo operaciones no permitidas de manera remota. Se trata de un "agujero" que puede ser producido varias razones. Entre ellas, destacaríamos una debilidad en el *hardware*, carencias en los procedimientos, errores de configuración, errores en los sistemas de validación o debilidades en el software. Estas vulnerabilidades (virus, gusanos, *ransomware*, troyanos, *keyloggers*) pueden ser explotadas y pueden poner en peligro nuestros sistemas, así como el acceso a datos e información sensible.

Gestión de vulnerabilidades: proceso continuo que consiste en la identificación, evaluación y corrección de vulnerabilidades en los sistemas de información y las aplicaciones de un organismo. Generalmente, esta gestión se realiza en tres pasos:

1. Obtención de un inventario (y categorización por nivel de criticidad) de los activos de una entidad, lo que incluye servidores, infraestructura de redes, estaciones de trabajo, impresoras y aplicaciones.
2. Detección de las vulnerabilidades existentes mediante escáneres de redes, escáneres de vulnerabilidades, software de pruebas de penetración automáticas y determinación de los niveles de riesgo.
3. Reparación de sistemas y dispositivos vulnerables y presentación de informes sobre las medidas correctivas adoptadas.

OBLIGACIONES LEGALES

Al hablar de la importancia que tiene la ges-

tión de vulnerabildiades es necesario sin duda recordar que dicha gestión es una obligación a la cual tenemos que dar cumplimiento las Administraciones Públicas según establece el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad a través de su artículo 20 y las medidas referentes a Mantenimiento [op.exp.4] y Protección frente a código dañino [op.exp.6] las cuales son aplicables a todos los sistemas de información:

Artículo 20. Integridad y actualización del sistema.

1. Todo elemento físico o lógico requerirá autorización formal previa a su instalación en el sistema.
2. Se deberá conocer en todo momento el estado de seguridad de los sistemas, en relación a las especificaciones de los fabricantes, a las vulnerabilidades y a las actualizaciones que les afecten, reaccionando con diligencia para gestionar el riesgo a la vista del estado de seguridad de los mismos.

Mantenimiento [op.exp.4].

c) Se dispondrá de un procedimiento para analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la aplicación o no de la actualización.

Protección frente a código dañino [op.exp.6].

Se dispondrá de mecanismos de prevención y reacción frente a código dañino con mantenimiento de acuerdo a las recomendaciones del fabricante.

GESTIÓN DE VULNERABILIDADES EN IB-SALUT

Para la gestión de las vulnerabilidades del Organismo se ha optado por utilizar la solución Tenable Security Center (de aquí en adelante, "Tenable.SC"), la cual ha sido diseñada para que los activos pudieran ser analizados de acuerdo con la política de gestión de vulnerabilidades organizativa. Con ella es posible gestionar las vulnerabilidades basadas en el riesgo, disponiendo de una visibilidad inmediata hacia nuestra red. Asimismo, permite disponer de información clara y procesable con tableros de control, informes y flujos de trabajo, identificando y priorizando las vulnerabilidades instantáneamente, mediante inteligencia de amenazas y puntuaciones de riesgo incorporadas. Por último, permite acelerar la respuesta ante incidentes con alertas de configuración, notificaciones y emisión de tickets personalizables.

Debido a la naturaleza de la red de IB-Salut, los usuarios y roles, así como las Políticas de escaneo y el conjunto de dispositivos que conforman la totalidad de la red son repartidos siguiendo dos criterios fundamentales: Características del dispositivo y de la gerencia analizada. En Tenable.SC tenemos la posibilidad de definir grupos que otorgan los permisos de acceso de los usuarios, los cuales se corresponden con los que aparecen en sistema de Gestión de Identidades del organismo.

En IB-Salut, Tenable.sc está configurado para lanzar escaneos de descubrimiento y vulnerabilidades al menos cada 35 días en cada una de las gerencias. La finalidad de esto es mantener un control rutinario y garantizar que las Gerencias sean analizadas periódicamente. Estos escaneos siguen el siguiente patrón:

- **Paso 1:** Se realiza un escaneo de descubrimiento, para encontrar nuevos dispositivos dentro de la subred de la Gerencia.
- **Paso 2:** Se realizan dos escaneos de vulnerabilidades, uno para las máquinas Windows y otro para las máquinas UNIX (Linux, BSD y Solaris).
- **Paso 3:** Se realiza un tercer escaneo, esta vez para las máquinas en las que se ha detectado la presencia de tecnología VMware (máquinas virtuales, etc).
- **Paso 4**: Se realiza un cuarto escaneo, esta vez para el resto de los dispositivos (*Firewalls*, DNS's, IOT's, etc). En este último no se incluye el análisis de equipo personales.

En cuanto a la presentación de resultados, tras la finalización del ciclo de escaneo de vulnerabilidades de cada Gerencia, se genera un informe ejecutivo que permite conocer el sumario de las vulnerabilidades y sistemas analizados. Éste



Ejemplo reporte ejecutivo

se envía periódicamente a los responsables de Seguridad de cada gerencia. En este informe generado automáticamente por Tenable.SC, podremos encontrar un resumen global de la gerencia, que incluirá las vulnerabilidades actuales y las vulnerabilidades ya mitigadas. También contamos con gráficos de evolución en los que se puede observar, por ejemplo: el top 20 vulnerabilidades explotables.

Por otro lado, existe la posibilidad de realizar escaneos manuales, los cuales pueden utilizar cualquiera de las políticas y ejecutarse en cualquier momento. Los análisis no tienen por qué realizarse sobre la totalidad de una gerencia, sino que se puede escanear un activo o conjunto de activos concretos.

> ***Para la gestión de las vulnerabilidades del Organismo se ha optado por utilizar la solución Tenable Security Center (de aquí en adelante, "Tenable.SC"), la cual ha sido diseñada para que los activos pudieran ser analizados de acuerdo con la política de gestión de vulnerabilidades organizativa"***

ROLES Y RESPONSABILIDADES

Los actores principales con responsabilidades dentro del procedimiento de gestión de vulnerabilidades e identificados en procedimiento interno de "Análisis y gestión periódica de vulnerabilidades con Tenable Security Center" son:

- Responsable de seguridad: Determina las medidas necesarias para asegurar el nivel de seguridad de los sistemas del Servicio de Salud ubicados en IslaLink y en los CPD de las Gerencia territoriales. Estas medidas se materializarán en el impulso de la realización de los análisis de vulnerabilidades por parte del personal especializado en dicha tarea.
- Responsable del sistema: En el caso de los sistemas corporativos centralizados, esta figura recaería en el jefe del servicio correspondiente de la Subdirección de Tecnología y en el caso de otros centros y unidades, en quien ostente la coordinación del área técnica (jefes de servicio de informática).

Son los responsables de garantizar que se gestionan adecuadamente las vulnerabilidades detectadas en el sistema del cual es responsable, e informa al Responsable de seguridad de los avances y problemas que puede encontrarse en el trascurso de la solución de las vulnerabilidades.

- Tercero o Proveedor: Colabora con el Responsable del sistema de información y el Respon-

sable de seguridad en las tareas de corrección de las vulnerabilidades de los sistemas que provee al Servicio de Salud.

- Oficina de Seguridad de la Información: Configura la plataforma, programa los análisis de vulnerabilidades, realiza escaneos puntualmente y evalúa los resultados obtenidos de dichos análisis. Presenta los resultados a los responsables de seguridad y del sistema de información. Evalúa las métricas y los indicadores que se reportan al Responsable de seguridad.
- Administradores de Sistemas: equipo responsable de garantizar una correcta gestión y administración de los sistemas de información del Servicio de Salud, con principal foco en la gestión del correcto funcionamiento de estos, además de aplicar las guías de bastionado referidas por el Servicio de Seguridad del Servicio de Salud.

PRÓXIMOS PASOS

Paralelamente se está llevando a cabo la integración entre Tenable.SC, Trend Micro Deep Security y la herramienta de Gestión de Ticketing de IB-Salut (OTRS), la cual permitirá que todas las vulnerabilidades recogidas por Tenable.SC pasen al sistema OTRS por medio de tickets, obteniendo así más control y seguimiento sobre el ciclo de vida de las vulnerabilidades.

La arquitectura que se ha definido es el resultado de integrar Tenable.sc, OTRS y un sistema encargado de poder recoger la información de ambas plataformas y realizar las acciones pertinentes:

- Sistema integrador: recogerá las vulnerabilidades descubiertas por Tenable.sc, las almacenará en una base de datos y generará o actualizará el pertinente ticket en el sistema OTRS.
- Tenable.sc: recogerá todas y cada una las vulnerabilidades detectadas. Se establecerá la comunicación con el sistema integrados gracias a su API.
- Trend Micro Deep Security: A través de la integración prevista entre Tenable.sc y deepsecurity se gestionarán los riesgos de las vulnerabilidades disminuyendo el riesgo de aquellas que estén parcheadas individualmente.
- OTRS: gracias a su API, se podrá establecer la comunicación con el sistema integrador para la creación/actualización de tickets.

> ***"La arquitectura que se ha definido es el resultado de integrar Tenable.sc, OTRS y un sistema encargado de poder recoger la información de ambas plataformas"***

Los casos de uso que se han definido en esta primera fase inicial, son los siguientes:

1) Creación de tickets: Se creará un ticket por activo. Dicho ticket incluirá el acumulado de vulnerabilidades detectadas en el activo. Este ticket, se irá actualizando tras cada ciclo de análisis, incluyendo aquellas nuevas vulnerabilidades que se detecten y suprimiendo las ya mitigadas.
2) Reescaneo: La generación de reescaneos de las vulnerabilidades para aquellos tickets que hayan sido cerrados es otra de las funcionalidades que deben implementarse. Cuando el sistema examine qué tickets están en estado "cerrado", Tenable.SC generará un reescaneo automático para determinar si dicha vulnerabilidad se ha solucionado correctamente. De haberse mitigado, mantendrá el ticket en estado "cerrado", por lo contrario, lo actualizará a estado "abierto".

REFERENCIAS

Soporte de vulnerabilidades CCN-CERT: Resumen de vulnerabilidades. Análisis, notificación y seguimiento de aquellas vulnerabilidades más críticas. Disponible en: https://www.ccn-cert.cni.es/seguridad-al-dia/vulnerabilidades.html

Glosario de términos de Cibserguridad. INCIBE. Disponible en: https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_metad.pdf

Impulsar la Ciber-colaboración



Laura Prats Abadía
Cyber Risk Manager Sham en España (Grupo Relyens)

EL PASADO MES DE MAYO, DESDE SHAM (GRUPO RELYENS) TUVIMOS LA OCASIÓN DE PARTICIPAR EN EL XVIII FORO DE LA SEGURIDAD Y PROTECCIÓN DE DATOS DE LA SALUD ORGANIZADO POR SEIS EN OVIEDO. SIN DUDA, UN ESPACIO PRIVILEGIADO PARA CONOCER LAS ÚLTIMAS TENDENCIAS Y PERSPECTIVAS DEL SECTOR, ESPECIALMENTE, EN LO RELATIVO A LOS RIESGOS VINCULADOS A LAS TECNOLOGÍAS SANITARIAS.

Desde Sham quisimos exponer nuestro punto de vista acerca de la gestión de riesgos, objetivo íntimamente ligado a la misión de la compañía. Aunque Sham, como mutua aseguradora, es un nuevo actor en el entorno de la ciberseguridad de nuestro país, la gestión de riesgos está en el corazón de la compañía. Sham siempre ha tenido muy presente un enfoque preventivo y de acompañamiento al sector sanitario para mejorar la gestión del riesgo, prevenir incidentes y mejorar la seguridad del paciente.

Sham es consciente de las oportunidades que se abren con las nuevas tecnologías en la sanidad, pero también de los nuevos riesgos que pueden incluso afectar directamente a la seguridad del paciente. Por lo tanto, Sham inició un proceso de transformación para acompañar al sector en la gestión y prevención de estos riesgos, incluyendo, como no podía ser de otra forma, soluciones tecnológicas específicas.

Analizando los nuevos riesgos tecnológicos, la ciberseguridad destaca por su efecto sobre los servicios sanitarios. Cuando los tratamientos y servicios al paciente descansan sobre las redes de comunicación y los sistemas de información, es la propia seguridad del paciente la que se ve comprometida si un *hacker* consigue hacerse con el control de los sistemas.

Para proteger las redes hospitalarias y corporativas encontramos en el mercado un buen número de soluciones enfocadas a cada una a las diferentes necesidades en la prevención y la respuesta a un incidente. Sin embargo, desde Sham consideramos que hay un aspecto específico del sector sanitario que necesita de un tratamiento propio. Nos referimos a la protección de los Dispositivos médicos (DM) conectados a las redes hospitalarias.

La conexión de los dispositivos médicos a las redes corporativas facilita el flujo de información del paciente mejorando los procesos de atención sanitaria. Sin embargo, estos dispositivos tienen su propia problemática que los hace uno de los puntos más vulnerables de la red. Veamos algunos ejemplos.

- Son equipos que, en general, no incorporan seguridad desde el diseño ya que no ha sido una exigencia hasta que la interconexión lo ha revelado como una necesidad.
- Su alto coste impide una rápida renovación del parque, por lo que hay dispositivos conectados con sistemas obsoletos y vulnerables.
- Su actualización depende del proveedor e implica normalmente unos tiempos elevados para las exigencias de la ciberseguridad

- La variabilidad de sistemas y protocolos, dificulta el análisis y conocimiento de los dispositivos, aumentando el número de posibles vulnerabilidades.
- La necesidad de pruebas exhaustivas y certificaciones, hace en la mayoría de los casos no se pueda instalar software específico para su control, lo que impide la instalación de software específico de terceras partes.

Por todo ello, Sham propone la solución CyberMDX para cubrir estos vectores de riesgo sobre los dispositivos médicos. Esta solución, diseñada específicamente para el sector sanitario, permite detectar todos los equipos conectados de forma automatizada, analizar sus riesgos y vulnerabilidades, estudiar su comportamiento y alertar de cualquier anomalía detectada en la red. Esto lo hace sin instalar código en los dispositivos, sino analizando el tráfico de la red e inspeccionando los paquetes para detectar y recoger la información de cada dispositivo y su comportamiento. Como funcionalidades clave podemos destacar:

Inventario y trazabilidad. CyberMDX cuenta con una base de conocimiento específico en equipamiento médico. Esto le permite identificar claramente cada equipo conectado, sean dispositivos médicos de tratamiento (DM), equipos que dan soporte o conectividad (IoMT-IoT) o tecnologías de información (TI) de propósito general. Este inventario se genera de forma automática, añadiendo una gran variedad de información sobre el propio dispositivo, sus protocolos, conectividad, etc.

Evaluación de riesgos. CyberMDX permite detectar las vulnerabilidades de los equipos y sus fallos de configuración o de aplicación de políticas. Con esta información y el conocimiento de la criticidad de cada dispositivo sanitario (su conexión con el paciente, su papel en el entorno hospitalario, etc), proporciona una clasificación de riesgos que nos permiten identificar los puntos más críticos y priorizar las acciones del equipo de seguridad.

Detección y respuesta. La solución CyberMDX, analizando el tráfico de la red, es capaz de detectar comportamientos anómalos y conexiones indebidas, tanto dentro de la red como hacia el exterior de la misma. Los datos obtenidos de la red se tratan con el apoyo de inteligencia artificial (IA) y el conocimiento de las redes hospitalarias. Esto permite un grado muy alto de acierto en sus avisos, permitiendo una rápida reacción en caso de incidentes. Además, CyberMDX permite un gran número de integraciones con otras soluciones de seguridad, lo que potencia la capacidad del sistema en su conjunto para detectar y responder a un ciberataque.

Informes cumplimiento. CyberMDX permite generar de forma dinámica controles sobre los dispositivos y el comportamiento de la red. Estos controles permiten disparar acciones de las soluciones integradas para actuar sobre los sistemas o enviar mensajes predefinidos. De esta forma, se pueden establecer controles rápidamente que detecten incumplimientos o ataques en sus primeros estadíos.

Informes soporte biomedicina. CyberMDX proporciona datos al equipo de biomedicina o electromedicina para la optimización del parque de dispositivos médicos. La información sobre la utilización de los dispositivos, su localización o los errores detectados, es de utilidad para gestionar el mantenimiento y mejorar la eficacia del uso de los equipos médicos.

A pesar de todo, desde Sham somos conscientes que la seguridad total no existe y las organizaciones necesitan estar cubiertas cuando el riesgo se ha materializado. Por ello, ofrecemos un ciber-seguro especializado, Sham CyberProtection®, que cubrirá cualquier incidencia que no se haya podido atajar.

Como conclusión general a este Foro cabe destacar la necesidad de la colaboración e integración entre todos los actores involucrados en la ciberseguridad del sector sanitario-. Para una disciplina como la ciberseguridad en constante evolución, contar con un espacio de intercambio y diálogo específico del sector sanitario, supone un impulso importantísimo para la colaboración y el aprendizaje conjunto en el sector. Se dice que el nivel de seguridad lo da el eslabón más débil: reforcemos la ciberseguridad entre todos para proteger a los pacientes, que es el fin último de las organizaciones de la salud.

XI REUNIÓN DEL FORO DE INTEROPERABILIDAD EN SALUD 2021

El acto inaugural del Foro de Interoperabilidad 2021 se celebró de manera virtual, al igual que el resto del foro, debido a la situación de pandemia. Estuvo presidido por Gotzone Sagardui Goikoetxea, consejera del Departamento de Salud del Gobierno Vasco, y contó con las intervenciones de Juan Fernando Muñoz, director general de Salud Digital del Ministerio de Sanidad, y del presidente de la SEIS, Luciano Sáez Ayerra.





En su primera intervención, el presidente de la SEIS recordó que estaba previsto realizar el encuentro de forma semipresencial en Vitoria, pero la situación sanitaria obligó a realizarlo exclusivamente en formato virtual.

Luciano Sáez señaló que el "foro de interoperabilidad en salud es una acción imprescindible en un escenario tan heterogéneo como el sanitario, en el que cada día es más importante la convergencia de los sistemas de información y de las soluciones tecnológicas" y destacó la "presencia fundamental" de las TIC en el País Vasco, así como la exitosa gestión general de la pandemia con todas sus implicaciones; la automatización de la gestión global de las PCR; la implantación y despliegue de los sistemas de teletrabajo; la aplicación de la analítica de los datos de la pandemia y el inicio de proyectos para la aplicación de inteligencia artificial en la práctica clínica.

Al mismo tiempo aprovechó la presencia del director general de Salud Digital y Sistemas de Información del SNS, a quien reiteró el "compromiso con el Ministerio para colaborar tal y como figura en el convenio marco que tenemos suscrito para impulsar la transformación digital del sistema nacional de salud".

También resaltó la "importancia" del Comité Técnico de Interoperabilidad en el sistema sanitario –que mantuvo una reunión en el marco del Foro–, del que destacó los trabajos que están desarrollando y sobre los que recordó que su objetivo general era servir de plataforma a los responsables de interoperabilidad de las diversas organizaciones del sistema sanitario con el fin de intercambiar ideas, experiencias, elaborar propuestas, concienciar a los directivos de salud sobre la importancia de la interoperabilidad y promover acciones para la mejora de los sistemas de información en el sector sanitario.

El presidente de la SEIS aseguró que la disponibilidad de acuerdos para la interoperabilidad de los sistemas de información de salud no solo era necesario para el ciudadano, sino que "es imprescindible para impulsar y favorecer el desarrollo de proyectos tecnológicos innovadores que permitan su fácil y rápida integración en los sistemas de salud", y puntualizó que "nos encontramos actualmente en un escenario en el que se están definiendo proyectos fundamentales en el marco de una transformación digital promovida por la financiación de los fondos

de reestructuración y resiliencia, lo que justifica el lema de esta edición del foro: La interoperabilidad como herramienta tractora de la transformación digital del sistema nacional de salud". Finalmente avanzó que existía un nuevo trabajo iniciado por la Sociedad para conocer el grado de implantación de los proyectos de medicina de precisión en el sistema de salud y aseguró que "por su enorme repercusión en los proyectos TCI, esperamos poder ofrecer sus resultados en el último trimestre del año".

A continuación, intervino Juan Fernando Muñoz, titular de la Dirección General específica de TI en el Ministerio de Sanidad, quien recordó la apuesta del ministerio en una estrategia de transformación digital del SNS. En cuanto al estado de la interoperabilidad, afirmó que ya "contamos con un buen desarrollo de sistemas interorperables", como la HCE o la receta electrónica, entre otros, y también con un "ecosistema favorable", debido a varios factores: el impulso de los organismos internacionales, como la OMS y la UE con múltiples programas; una serie de estrategias nacionales como la de España Digital 2025, la de Ciencia y Tecnología, la de Inteligencia Artificial y la estrategia de medicina personalizada; "de forma muy excepcional", un "amplio consenso político" a través del comité de reconstrucción, que considera urgente aumentar los recursos humanos y económicos; también "de forma excepcional", los recursos financieros de la iniciativa *NextGenerationUE*, los fondos de recuperación por la Unión Europea tras el covid-19, donde la sanidad y especialmente los recursos digitales van a ser una de las líneas financiadas; y finalmente pero "no menos importante", ese "marco de Gobernanza consolidado" que no es otro que el Consejo Interterritorial del Sistema Nacional de Salud.

Sobre la estrategia de Salud digital en el SNS, destacó que actualmente se encontraba en proceso de



elaboración interna y anunció que en breve se dará a conocer una primera versión, con cuatro objetivos estratégicos: capacitar e implicar a las personas en el propio cuidado de salud; crear procesos de valor; desarrollo de la información interoperable y de un espacio de datos para la generación de conocimiento científico y, por último, adecuar el progreso a las exigencias de la sociedad actual. Muñoz afirmó que esta estrategia "configurará el espacio común, pero no se quedará en un diagnóstico y en las líneas de actuación", sino que definirá, en colaboración con las CC. AA. las áreas de actuación específicas, como el *datalake* sanitario, la historia de salud digital, la imagen médica o el centro de salud digital.

Por último, interveno Gotzone Sagardui Goikoetxea, consejera del Departamento de Salud del Gobierno Vasco, que, tras recordar los objetivos del foro, citó el programa de recuperación y resiliencia "NextEsukadi 2021-2026" que pretende garantizar la capacidad asistencial en el propio domicilio, o el proyecto de la historia sociosanitaria de Euskadi. También señaló que "es positivo adoptar estándares de código abierto de intercambio de datos buscando sistemas reutilizables" y concluyó que "la clave está en el trabajo en común, en la cogobernanza".

PRIMERA SESIÓN: "RESULTADOS DE LOS TRABAJOS DEL COMITÉ TÉCNICO DE INTEROPERABILIDAD DEL SISTEMA SANITARIO"

La mesa estuvo presidida por Mercedes Alfaro Latorre, subdirectora general de Información Sanitaria de la Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud del Ministerio de Sanidad, quien explicó que el Comité Técnico de Interoperabilidad del Sistema Sanitario de la SEIS intenta contribuir a afrontar los retos en comunicación e intercambio de información entre los sistemas desde hace diez años: el antiguo Comité de Normalización ha devenido en el actual comité de Interoperabilidad que está coordinado por Adolfo Muñoz Carrero, también Secretario del Comité 139 de UNE y representante español en varios comités.





La subdirectora general concluyó que la interoperabilidad nos tiene que llevar a "funcionar" de una manera coordinada, concepto que desde este Comité de la SEIS "se tiene muy asumido".

Adolfo Muñoz, jefe de la Unidad de Investigación en Salud Digital del Instituto de Salud Carlos III y coordinador del Comité Técnico de Interoperabilidad, fue el primer ponente que intervino, con la exposición de algunos trabajos del Comité, no sin antes recordar que la idea es tener representantes de los responsables en interoperabilidad de todas las CC. AA. para intercambiar la experiencia y poder reutilizar en el resto los desarrollos e investigaciones que se hacen.

A continuación, mostró el Maestro Interoperable de Personal Sanitario [MIPS], que el comité quiere adoptar como uno de sus trabajos, y que surgió del máster que realiza la SEIS con el Instituto de Salud Carlos III, para el que se tiene el objetivo de poder acabar desarrollando una norma que sea aplicable en el SNS. Los autores de este trabajo de fin de máster son Alejandro Filoso Rosas, del Servicio Extremeño de Salud, y Carmelo Justiniano Godoy y Enrique Pérez, del Servicio Canario de Salud.

Su objetivo en primer lugar consiste en identificar los requisitos, tanto funcionales como de datos, extraídos de los siguientes ámbitos: las definiciones de la norma UNE-EN ISO13940-2016 que sirvió de marco conceptual; de toda la legislación de normativa sanitaria con sus diferentes tipos de vinculaciones profesionales (funcionario, estatutario y laboral), organizaciones (pública, privada), relación económica (trabajador por cuenta ajena, propia, no remunerado, etc.); del conocimiento de estándares como FHIR de HL7, y de registros que ya existen, como el registro nacional de profesionales para, a continuación, especificar el área conceptual de dominio, creando este Maestro con elementos no redundantes con los tipos, propiedades y relaciones que definen los conceptos de personal sanitario, profesión sanitaria, formación, régimen jurídico, etc… y construir el arquetipo, para lo que se ha utilizado la herramienta LinkEHR basada en la nueva revisión de la norma ISO 13606, rechazándose la posibilidad de fusiones para hacer una interoperabilidad semántica de calidad.

Como mejoras que pueden conllevar el MIPS, Muñoz citó "aumentar el repositorio para ampliar más allá del profesional sanitario, normalizar términos y relaciones, entre la historia de salud electrónica con la gestión de recursos humanos, una clasificación de roles sobre la Historia Clínica del SNS con términos definidos con la terminología SNOMED-CT, mayor especificación de los subcomponentes de segmentos de estándares HL7 que implican datos de profesionales, etc.". Finalmente concluyó que le corresponde al Ministerio estudiar si tiene interés para el Sistema Nacional de Salud.

A continuación, Javier Quiles del Río, subdirector de Sistemas y Tecnologías y Estructura de Gestión Integrada del Área Sanitaria de Ferrol, del servicio Gallego de Salud, realizó un repaso a varios de los puntos tratados en la reunión del Comité de Interoperabilidad que tuvo lugar esa misma mañana, recordando que comenzó su andadura en 2018 y mantiene reuniones semestrales, haciendo coincidir una de ellas con este Foro.

Quiles del Río anunció que una de las conclusiones fue que la frecuencia de reunión aumentaba e informó de que "además de una puesta al día y foto de la situación de la interoperabilidad, se ha estado evaluando un trabajo de mayo de 2020: un documento de consenso de todo el Comité sobre cómo establecer la mejor forma de integrar el equipamiento electromédico con los SSII del hospital". De esta manera, puntualizó que "no hay un modelo 100% consensuado entre todos los fabricantes, y con el objetivo de facilitar la compra de este tipo sistemas se elaboró una guía que ya está publicada en la página web de la SEIS, que aporta indicaciones valiosas para incluir en los pliegos de contratación como condiciones y requisitos para la compra de estos equipamientos".

En este sentido, señaló que "cuando se elaboró esta guía ya se propuso mantener una actualización de este documento, adaptándose y recogiendo nuevos estándares y nuevas capacidades de estos equipos, para no limitar tampoco la capacidad de asistencia sanitaria. Así, toca ahora dicha actualización, para la que sería necesario incluir dos tipos de equipamientos: de oftalmología gracias a la evolución en estándar DICOM en esta área, que ha llegado a generar miniPACS oftalmológicos, mientras que la guía actual aborda solo los retinógrafos; y digitalización de imágenes de cristales de anatomía patológica, con alguna experiencia previa de las CC. AA., cuatro de ellas con un proyecto sobre la mesa pendiente de lanzamiento.

También comentó que se había tratado la idea de que haya una norma derivada de este documento en el comité de normalización 139, subrayando que se valoraría esa posibilidad.

Por último, resumió otros temas tratados en la reunión: la necesidad de normalizar la información y equipos de laboratorio, especialmente tras un año tan activo con las pruebas de PCR; la necesidad de un modelo de integración de dispositivos médicos que utiliza un paciente en su casa o en el centro, pero sin estar hospitalizado, ante la cada vez más habitual situación de que los datos generados por el dispositivo acaban en un repositorio del proveedor con acceso por un SSII o página web diferente por cada proveedor y la necesidad de mayor coordinación con el comité de Seguridad de la SEIS.

SEGUNDA SESIÓN: DEBATE "LA INTEROPERABILIDAD COMO HERRAMIENTA TRACTORA DE LA TRANSFORMACIÓN DIGITAL DEL SISTEMA NACIONAL DE SALUD"





El debate estuvo moderado por **Carlos Gallego Pérez,** coordinador general de la XI Reunión del Foro de Interoperabilidad en Salud, y contó con la participación de **Nicolás Francisco González López**, jefe de servicio del Área de Tecnología de OSAKIDETZA - Servicio Vasco de Salud; **Benigno Rosón Calvo**, subdirector general de Sistemas y Tecnologías de la Información del Servicio Gallego de Salud y **Juan Ignacio Coll Clavero,** director general de Transformación Digital, Innovación y Derechos de los Usuarios del Servicio Aragonés de Salud.

Acerca de la cuestión general sobre: "¿Qué tenemos aprendido?", **Nicolás González** se centró en la reciente experiencia de la pandemia y, tras afirmar que hay cambios de modelos asistenciales, señaló que ya se ha demostrado que "somos operativos desde las TI, tras conseguir en muy

poco tiempo la flexibilización del puesto de trabajo, la consolidación de las plataformas de telemedicina o los tratamientos virtuales hasta el punto de que ya se puede afirmar que combinamos consulta presencial con virtual". Ahora, continuó, "nos toca acompañar, no convencer", dado que "ya se ha convencido" y "podemos provocar desde las áreas TIC". En cuanto a las herramientas de interoperabilidad destacó que las ve más como "conductoras" que como "tractoras".

Por su parte, Benigno Rosón matizó que "la interoperabilidad no es tractora, es necesaria" y afirmó que por un lado "hemos avanzado estos 19 años en este campo y ahora hay más herramientas de interoperabilidad y más fáciles que nunca", pero por otro, "sigue costando años lograr interoperar, como por ejemplo sucede ahora con los proveedores de sistemas en la nube". En su opinión, para avanzar en ese último punto, "falta dar un puñetazo en la mesa y decir: esto se acabó".

Juan Ignacio Coll argumentó que "la interoperabilidad es absolutamente necesaria para la transformación digital", que debe entenderse como "una metamorfosis". Para alcanzarla es necesario que se "salga de la parte estrictamente técnica para llegar a la parte funcional, porque ahí es dónde está la parte estratégica". En su opinión "se ha hecho poco, pero tenemos casos de éxito claros: como la receta electrónica". Además, incluyó nuevos retos "como la medicina 5P o un mundo que está a punto de ser 100% digital, tanto en su equipamiento como en la forma de tomar sus decisiones por parte de los profesionales, siendo necesario normalizar y saber qué hacer con toda esa información".

Nicolás González coincidió en la conveniencia de un esquema nacional de interoperabilidad en salud, y afirmó que "tecnológicamente estamos preparados para que sean los profesionales los que elijan qué información guardar".

En esa línea, Benigno Rosón comentó algunos problemas que dificultan la alineación: "Quien compra tiene claro que el sistema tiene que ser interoperable, pero luego le cuesta establecer los catálogos homogéneos; ya se dice que si un sistema no es interoperable pues 'fuera del concurso' o que si interopera pero luego no interopera, pues 'penalización', pero luego por inmediatez y la premisa de que 'el fin justifica los medios', se acaba asumiendo; y por último, los marcos no se acaban aplicando porque las estructuras de los organismos normalizadores 'están enormemente debilitadas' concluyendo que esta necesidad de la interoperabilidad tenemos que entenderla todos y ser rigurosos".

Juan Ignacio Coll aseveró que "si nos lo creemos realmente" se logrará la transformación digital y afirmó que "se ha detectado desde la propia industria que las organizaciones deberían adoptar más estándares, lo que efectivamente facilitaría su trabajo".

A continuación, el moderador dio paso a las preguntas y comentarios de los asistentes. Uno de ellos comentó que en otros países como EE. UU. "forzaron con una ley y fondos para implantar el estándar preguntando "¿No podríamos hacer una ley que obligue a la interoperabilidad y se acompañe con financiación?". Ante esta consulta, Nicolás González reconoció el impulso que supondría tal medida y apuntó que "por ahora es en el pliego dónde se deben poner las condiciones, debiéndose exigir un dosier técnico de cómo las implementa, citando el problema de las integraciones 'ocultas', las que llegan en el propio proyecto y la falta de información de los SSII que se contratan, que generan costes y variaciones en el alcancen final del proyecto: necesitamos identificarlos y hace falta que sean transparentes, siendo necesario una institución nacional que nos pueda ayudar".

Otro de los asistentes señaló la importancia de "incluir a los funcionales en la estrategia de la interoperabilidad", ante lo que el moderador coligió que "hay un riesgo en la línea de dejar el peso en los funcionales" y citó como ejemplo: "un patólogo puede pedirte una solución propietaria concreta porque así se lo indica la industria". Juan Ignacio señaló que solo ahora la "parte de negocio" está empezando a entender la necesidad de la interoperabilidad y que la transformación "es más que desplegar un SW, es refundar la organización".

Después de otras preguntas, el moderador concluyó el debate, resumiéndolo en las dos grandes ideas tratadas por los ponentes: "es necesario un consenso tras el diálogo entre todos los actores; es necesario un gobierno de la interoperabilidad".

TERCERA SESIÓN: "LA NORMALIZACIÓN Y LA INTEROPERABILIDAD PARA LAS INFRAESTRUCTURAS DE INFORMACIÓN EN SALUD"

La sesión estuvo moderada por **Marisa Merino Hernández,** directora gerente de la Organización Sanitaria Integrada Tolosaldea de OSAKIDETZA - Servicio Vasco de Salud, y contó con cuatro ponencias de expertos.

Salvador Capella, miembro de la Unidad de Coordinación del Instituto Nacional de Bioinformática en el Departamento de Ciencias de la Vida del Centro de Supercomputación de Barcelona (BSC), comenzó explicando que el BSC es mucho más que un supercomputador. Cuenta con cuatro departamentos de investigación además del de operaciones, entre ellos el de Ciencias de la Vida que se dedica a medicina personalizada y que implica genómica, *machine learning*, infraestructuras de datos y *text mining* o cómo extraer información del texto.

También colideran con el IACS (Instituto Aragonés de Ciencias de la Salud) un proyecto a nivel europeo sobre cómo entender la explotación del uso del dato de salud de forma distribuida, y recordó que hace poco se ha puesto en marcha el Espacio Europeo de Datos en Salud, siendo el objetivo del proyecto generar una agenda estratégica. Así se pretende disponer de *data hubs* o infraestructuras que sirvan el dato cumpliendo con lo legal y las características de datos, y apuntó que a veces hay soluciones tecnológicas que sobre el papel están muy bien pero que "luego no funcionan".

Capella puntualizó que "a nivel español tenemos IMPACT, infraestructura para la medicina personalizada asociada a las ciencias de la salud, que se puso en marcha el año pasado por el Instituto de Salud Carlos III, coordinado por los Ministerios de Ciencia y de Sanidad y que tiene tres programas, de medicina de datos, de medicina genómica y el de ciencia de datos. Otro proyecto relacionado es el de extracción de información no estructurada en lenguaje natural para conseguir información estructurada. También participan en varias iniciativas mundiales sobre estándares y tecnologías de federación de infraestructuras de datos".

Por último, destacó las iniciativas española y europea de portales de datos sobre el covid-19, en las que participan desde el BSC; y relacionado con este, participan en otro proyecto sobre si fuera posible extraer el conjunto de datos estándar directamente de la HCE de hospitales.



A continuación, **Carlos Luis Parra Calderón**, jefe de Sección de Innovación Tecnológica del Hospital Universitario Virgen del Rocío y subdirector general de Sistemas y Tecnologías de la Información del Servicio Gallego de Salud, dedicó su ponencia a las historias digitales de salud como fuentes de datos para las infraestructuras de información, usando los principios FAIR y estándares de interoperabilidad como FIHR. En este sentido subrayó que "estamos en un momento histórico en el que vamos a disponer de una gran financiación" y pidió que "no montemos cada comunidad su chiringuito de *big-data,* dado que el mundo científico ya no funciona así".

Pero ¿Qué son los principios FAIR? Se publicaron en una revista en 2016 y son aplicables a cualquier trabajo científico que recoge datos y que en resumen establece que el dato debe ser: F: Localizable; A: Accesible; I: interoperable; R: reutilizable.

"Las historias de salud [HDS] tienen información que no está preparada para la investigación y existen diferentes opciones de especificaciones estándares a nivel internacional para extraer datos de la HDS, pero no cumplen los principios FAIR, estando sólo orientados a dar respuesta a la interoperabilidad. Es conveniente por tanto un proceso de 'FAIRificación' sobre extracciones de datos de la HDS a falta de que los datos de la propia HDS sean '*FAIR by design*' para un uso secundario, por ejemplo, de investigación", argumentó.

Parra Calderón señaló que "con ese objetivo se ha

lanzado el proyecto multinacional FAir4Health, en el que participan, y que pretende aplicar los principios FAIR a diferentes colecciones de datos de forma federada, entre ellas la de dos hospitales: de Sevilla y de Ginebra, de pacientes crónicos de Aragón, etc., a varios casos de uso, como de investigación epidemiológica y un servicio digital de riesgo de rehospitalización a treinta días. Una de las ventanas de los principios FAIR es que conseguimos datos preparados para la inteligencia artificial". También reconoció que "aunque con una federación de datos funciona, nunca va a funcionar igual que con datos centralizados en un supercomputador".

Además, puntualizó que "uno de los socios de Fair4Health es la propia HL7, y con su ayuda se está realizando una guía del estándar FHIR para aplicar los principios FAIR, en el que hay un interés 'tremendo' por parte de la industria: FHIR4FAIR, que pueden descargarse de confluence.hl7.org" y aclaró que "FHIR no implica que los datos sean FAIR pero puede ayudar a FAIRificar datos".

Por su parte, **Joaquín Dopazo**, miembro del Área de Bioinformática Clínica de la Fundación Progreso y Salud de la Junta de Andalucía, comenzó su intervención indicando que "entre los usos primarios de los datos genómicos se encuentra el uso por parte de grupos de bioinformáticos o bioestadísticos expertos que manejan estos datos y es 'complicado' que sea interoperable" y señaló que "las soluciones interoperables pasan por un software corporativo que debe ser transparente al usuario de genética". También señaló que "ya tienen un proyecto piloto en Andalucía que proporciona ayuda al diagnóstico automático y que estos datos deben quedar bien guardados, así como la vinculación entre los datos clínicos y los genómicos".

Dopazo afirmó que "el logro más interesante, y que sería extensible al resto del país, es el circuito clínico de secuenciación del coronavirus, realizado con 14 hospitales y que empezó con más de mil genomas de la primera ola, donde ahora hay una centralización en bioinformática de la secuenciación de las muestras recibidas desde varios centros, cuyo resultado se envía al proyecto nacional y al europeo y se guarda además localmente vinculado con las historias clínicas".

En este sentido señaló que se está ampliando el concepto de uso primario de los datos: ahora cuando aparece una variante nueva se mira los pacientes que había antes a ver si tenían esa variante y se puede llegar a dar un diagnóstico que antes no se podía hacer sin una investigación, siendo también un uso primario de datos gracias a la tecnología. Así estudios secundarios de toda la vida han pasado a ser un uso primario de datos, gracias a implementar unas buenas herramientas que permiten la interoperabilidad. Para finalizar, aseveró "no tenemos que darnos de cabeza contra las leyes, lo que tenemos que hacer es replantear el uso que esas leyes nos permitan".

Por último, **Gloria González Gacio,** PhD consultora clínica y Health Data Standards Specialist de BITAC, empresa con experiencia en interoperabilidad semántica, habló sobre la interpretación de datos genotípicos y genómicos en la historia clínica utilizando estándares como SNOMED-CT y LOINC.

González Gacio indicó que "uno de los grupos de trabajo de la asociación BioInformátics Barcelona (BIB), donde participan con otras empresas, universidades, hospitales y centros de investigación, es el grupo de integración de datos genotípicos con genómicos, siendo una de sus recientes propuestas en ese campo, la elaboración de una guía para las HCE; otra el estudio de terminologías como SNOMED-CT en la genómica clínica, que concluyó que los estándares para presentar el fenotipo están fuertemente ligados al dominio".

Continuó explicando que "a partir de estos estudios preliminares, realizaron un estudio con casos reales en Cataluña, con dos centros sanitarios: el Hospital Clínic y el Instituto Oncológico, viendo que en la actualidad para capturar información fenotípica en la clínica no se utilizan estándares mientras que es generalizado en la investigación".

También explicó su participación en el grupo de referencia de genómica clínica y de medicina de precisión de SNOMED-CT, "con la idea de colaborar con terminologías existentes de dominios específicos involucrados en la medicina genómica, donde la secuenciación del exoma se está volviendo cada vez más popular, detallando la forma de trabajo: es el fenotipo el que desencadena el estudio en el laboratorio, se utiliza la codificación LOINC para la codificación automática de los genotipos, se identifican los datasets, tanto en la petición como en el

informe de genómica, y se utiliza un módulo SNOMED-CT para identificar. Para cada variable se ha identificado el código LOINNC más adecuado".

Ante la pregunta ¿Cómo integran los datos genotípicos que están en el HIS con los datos genómicos del LIS?, contestó que "partiendo de subconjuntos de términos SNOMEd-CT para trastornos de la especialidad y del catálogo de pruebas del LIS codificado en LOINC y de los servicios web del servidor terminológico CTMAG para consultar los contenidos en SNOMED-CT, se crea una tabla de relación".

Por último, afirmó que están trabajando en un prototipo de lenguaje natural para extraer toda la información fenotípica del paciente para el proceso crítico de selección de las variantes, de tal forma que pase a ser parte del *datalake* sanitario.

Como conclusión a la sesión, la normalización de los datos clínicos y genómicos con estándares globales como SNOMED-CT; estándares de laboratorio como LOINC y estándares relevantes en genómica, es esencial para permitir una eficiente medicina de precisión, así como el uso de herramientas de inteligencia artificial sobre el datalake del hospital.

CUARTA SESIÓN: EL PAPEL DE LA INTEROPERABILIDAD EN LOS PROYECTOS *NEW GENERATION EU*



La sesión estuvo moderada por **Martín Begoña Oleaga,** subdirector de Informática y Sistemas de Información OSAKIDETZA – Servicio Vasco de Salud, y contó con los ponentes: **Carlos Royo Sánchez,** presidente de la Comisión de Salud Digital AMETIC; **Pol Pérez Sust,** coordinador general de las TIC en el Departament de Salud de la Generalitat de Catalunya; **Pablo Serrano Balazote,** director de planificación del Hospital Universitario 12 de Octubre y **Raúl Pérez Antón,** miembro de Healthcare Informatics Philips Ibérica.

El hilo conductor del moderador planteó la interoperabilidad como un tema recurrente tratado durante años en este foro y en su predecesor. En su intervención, **Carlos Royo Sánchez** presentó los macroproyectos tractores trabajados por AMETIC para impulsar la transformación digital en diferentes sectores clave, con un objetivo claro y marcado: Mejorar la sostenibilidad del Sistema Nacional de Salud, la innovación y el empleo, mediante la colaboración público-privado en proyectos tecnológicos. Estos ambiciosos proyectos están, además, muy alineados con el Plan de Resiliencia presentado por el Gobierno.

"Se plantea la necesidad de un fuerte liderazgo mundial y la participación de España en ese papel con un buen uso de los fondos disponibles a nivel europeo, entre los cuales se estima un gasto aproximado de 21.000 millones en planes de transformación digital y aproximadamente 1.000 millones dedicados en exclusiva al sector sanitario", destacó. En este aspecto, subrayó "el proyecto 'El ciudadano español', gestor de su salud y donante de conocimiento, el cual sitúa como centro del proceso de salud al usuario y busca situar a España a la cabeza del liderazgo digital e innovador mediante el fortalecimiento del Sistema Nacional de Salud mejorando la eficiencia y productividad".

A continuación, **Pol Pérez Sust** expuso diferentes iniciativas trabajadas en la Generalitat de Catalunya, todas ellas relacionadas con la Interoperabilidad y la digitalización de la salud: Monitorización domiciliaria del paciente, empoderándole en la gestión no solo de su salud si no de su información médica; Potenciar la vigilancia epidemiológica de enfermedades con alto impacto como el covid-19 mediante la interoperabilidad de sistemas de información, ya que el control epidemiológico está actualmente muy centrado en enfermedades de menor impacto social por sus diferentes características de propagación; Mejor aprovechamiento de los datos ómicos (aquellos obtenidos por tecnologías genómica, la transcriptómica, la proteómica, la metagenómica, la metatranscriptómica, la metabolómica, etc.) mediante la recopilación e integración de estos

datos en una plataforma tecnológica que permita su disponibilidad y uso en diferentes investigaciones y proyectos; Dentro del marco del Plan de Salud 2016-2020 del Departament de Salud se creó la plataforma SIMDCAT para la digitalización y estandarización de las imágenes de Patología Digital aprovechando el potencial del cloud computing. Esta plataforma será utilizada en 450 centros y por parte de todos los profesionales del SISCAT; Como punto final, expuso la utilización de un modelo de datos y gobernanza mediante un estándar abierto que permite independizar los sistemas de información y la capa de persistencia subyacente, proporcionando una gran flexibilidad al sistema.

Durante la siguiente intervención, Pablo Serrano Balazote presentó de manera general los diferentes proyectos en desarrollo por parte del Hospital Universitario 12 de Octubre. La exposición no estuvo tan centrada en sus propios proyectos, sino en las diferentes tecnologías utilizadas para realizar una normalización en el registro de datos e información. Esto les permitió iniciar proyectos compartiendo información de forma sencilla y eficiente: modelo H7 para el intercambio electrónico de información clínica; el estándar de transmisión de imágenes médicas y datos conocidos como DICOM; o terminologías clínicas comunes como SNOMED-CT, CIAP-2 o CIE-10.

"El uso de este tipo de estándares y tecnologías posibilita alcanzar un alto grado de interoperabilidad, aportando flexibilidad y robustez a una organización en un ámbito tan clave como la salud. Esta capacidad les está siendo de gran ayuda para enfrentarse a la actual pandemia por covid-19, al permitir una rápida integración de información entre proyectos y fuentes, y facilitar la atención al paciente e investigación", señaló.

Finalmente, y como un factor para tener en cuenta, Raúl Pérez Antón trajo a colación el problema de la privacidad de la información, su seguridad, los derechos del paciente y las obligaciones a nivel de organización. Expuso la evolución del archivo médico en papel hasta el archivo digital, –usando como ejemplo el descubrimiento de la identidad de una momia por los restos de su dentadura– y planteó la innegable posibilidad de identificar, tarde o temprano, a un paciente por su información médica aun encontrándose de forma aislada en un sistema.

Pérez Antón subrayó diferentes necesidades y soluciones en la identificación de usuarios, tanto internos como externos a una organización, mediante el acceso a la información de un paciente, así como la obligación de integrar al paciente en la toma de decisiones sobre la disponibilidad de su información médica. Siguiendo la línea del resto de ponentes, expuso la posibilidad de uso de estándares reconocidos y existentes para normalizar y agilizar los procesos.

Como conclusión sobre esta sesión, y tras la diferente ronda de conclusiones de cada ponente, es evidente que la Interoperabilidad de Sistemas de Información no puede seguir siendo un objetivo para alcanzar sin la base de la innovación y progreso en el tratamiento de la salud de los usuarios del Sistema Nacional de Salud. Y con ese planteamiento, el desarrollo o uso de estándares normalizados y reconocidos es clave para compartir la información clínica, principio y fin de todos los procesos de tratamientos de la salud.

QUINTA SESIÓN



SESIÓN DE CLAUSURA



XVIII FORO DE SEGURIDAD Y PROTECCIÓN DE DATOS DE SALUD

"Protección de Datos y Seguridad de la Información en tiempos de pandemia"

El XVIII Foro de Seguridad y Protección de Datos de Salud, celebrado en Oviedo los días 19 y 20 de mayo de 2021, giró en torno al impacto que ha tenido la pandemia del covid-19 desde la perspectiva de la seguridad de la información y la protección de datos personales.



BIENVENIDA Y CONFERENCIA DE APERTURA: "ESTRATEGIA NACIONAL DE CIBERSEGURIDAD"

Javier Candau, jefe del Departamento de Ciberseguridad del CCN y director general de Seguridad y Estrategia Digital presentó y explicó la Estrategia Nacional de Ciberseguridad (ENC), cuyo objetivo es "lograr que España haga un uso seguro de los sistemas de información y telecomunicaciones, fortalezca las capacidades de prevención, defensa, detección y respuesta a los ciberataques, garantice el uso seguro y fiable del ciberespacio, proteja los derechos y libertades de los ciudadanos y promueva el progreso socio económico".

La ENC está basada en cinco objetivos con siete líneas de acción, entre los que se destacaron:

- [Ob_1] Seguridad y resiliencia de las redes y sistemas de información y comunicaciones del sector público y de los servicios esenciales:
  - [LA_1] Reforzar las capacidades ante las amenazas provenientes del ciberespacio, cuyas principales medidas son:
    - Potenciar la colaboración de los centros de excelencia e investigación.
    - Asegurar la coordinación y operación de los organismos responsables en ciberseguridad.
    - Potenciar las capacidades de ciberdefensa y de ciberinteligencia.
    - Promover la participación de las empresas en plataformas sectoriales.
    - Potenciar y promover los desarrollos realizados en la red de CSIRT española.
    - Garantizar la coordinación, la cooperación y el intercambio de información, fomentando la prevención y la alerta temprana.
    - Implantar medidas de defensa activa en el sector público para mejorar las capacidades de respuesta.

Pero la más destacada, por encima del resto de medidas es:

- Impulsar el desarrollo de plataformas de notificación, intercambio de información y coordi-

nación la mejora de la ciberseguridad sectorial.

- [LA_2] Garantizar lae seguridad y resiliencia de los activos estratégicos para España, cuyas principales medidas son:
  - Asegurar la plena implantación del ENS, del Sistema de Protección de Infraestructuras Críticas y el cumplimiento y armonización que las soportan.
  - Reforzar la implantación de infraestructuras y servicios de telecomunicaciones y sistemas de información horizontales comunes, y compartidos por las AA. PP.
  - Desarrollar catálogos de productos y servicios cualificados y certificados.

Destacan las siguientes medidas:

- Potenciar la progresiva implantación y creación de infraestructuras de ciberseguridad en las CC. AA., ciudades autónomas y entidades locales y en sus órganos vinculados o dependientes que cooperarán y se coordinarán con las estructuras nacionales en pro de la mejora de la ciberseguridad nacional.
- Desarrollar el Centro de Operaciones de Ciberseguridad de la AGE que mejore las capacidades de prevención, detección y respuesta, e impulsar el desarrollo de estos centros en el ámbito autonómico y local.
- Reforzar las estructuras de seguridad y la capacidad de vigilancia de los sistemas de información que manejan la información clasificada.
- Asegurar la protección de infraestructuras científico-técnicas singulares.

El siguiente punto tratado fue el desarrollo de la Red Nacional de SOC's, cuyo objetivo es "dar una respuesta eficiente integrando todas las capacidades nacionales a través de la plataforma Nacional", mediante cinco líneas:

- [L1_NYCCSS] Cumplimiento y análisis de riesgos.
- [L2_COCS] Operación de la Ciberseguridad.
- [L3_VIGILANCIA] Superficie de exposición (CCN – cert).
- [L4_CICS] Detección.
- [L1_RESPUESTA] Respuesta inmediata (CCN – cert).

Los principios de actuación de un SoC deben ser:

- Revisión de la seguridad de la entidad teniendo en cuenta sus sistemas, infraestructuras, aplicaciones y páginas web.
- Análisis de los registros y evidencias generadas por diferentes fuentes de la entidad al objeto de automatizar procesos y presentar alertas de seguridad.
- Revisar y completar las medidas de seguridad basada en dispositivos de punto final (endpoint) y dispositivos perimetrales para asegurar las conexiones y el contenido de estas.
- Vigilancia constante de la superficie de exposición a la ciberamenaza.
- En su caso, colaboración con la entidad para resolver los incidentes detectados u ocurridos.

Además, deben integrarse con los CSIRT's de referencia. El Plan de digitalización de las AA. PP contempla como una medida de protección la constitución de un SoC y el cumplimiento del ENS. Por otra parte, la Red Nacional de SOC's se coordinará con la Unión Europea.

También añadió que la gestión de una crisis se debe basar en la "voluntad de vencer", la "capacidad de ejecución" y en la "libertad de acción". Para ello, la Guía de Buenas Prácticas BP/20, Gestión de Cibercrisis indica estos puntos:

- Liderazgo:
  - BP. 1 Liderazgo, valores y control.
- Preparación:
  - BP. 2 Planes y protocolos estructurales.
  - BP. 3 Comité de Crisis. Configuración.
  - BP. 4 Control permanente de la superficie de exposición.
  - BP. 5 Gestión adecuada de grupos de interés. Stakeholders.
- Respuesta:
  - BP. 6 Diagnóstico inicial y escenarios posibles.
  - BP. 7 Coordinación.
  - BP. 8 Iniciativa y proactividad.
- Comunicación:
  - BP. 9 Discurso unificado y fuente oficial de información.
  - BP. 10 Transparencia, empatía y asunción de responsabilidades.
  - BP. 11 Puesta en valor de las acciones adoptadas.
- Cierre:
  - BP. 12 Cierre formal de la crisis.
  - BP. 13 Implementación de lecciones aprendidas.

Para finalizar concluyó que "la Estrategia Nacional de Ciberseguridad del 2019 tiene nuevos objetivos, pero no se sabe los objetivos que se han cumplido de la estrategia del 2013. Son necesarios

fondos e impulso político para el sector público. Los fondos de Recuperación y resiliencia deberían impulsar la Red Nacional de SOC's y su Plataforma Nacional. También deberían impulsar una actuación en conjunto desde la parte defensiva. España tiene actividades avanzadas en los campos de gestión de riesgos (PILAR), medidas de seguridad (ENS) y notificación de incidentes (LUCIA)". Como recomendación dijo que se debía solicitar e instalar mCLAUDIA.

PRIMERA SESIÓN: "SOLUCIONES DE SEGURIDAD ANTE EL TRATAMIENTO DE DATOS DE SALUD"



Durante el transcurso de la sesión se expusieron las soluciones de seguridad ante el tratamiento de los datos de salud que tiene cada empresa para los diferentes ámbitos. Víctor Egido, de Tenable, expuso su estrategia: "Gestión de la ciberexposición en entornos sanitarios. Casos prácticos" y señaló que "el aumento de los ataques cibernéticos ha ido en aumento durante la pandemia en todos los sectores, en el sector sanitario ha crecido un 45%. En la mayoría de las ocasiones, los ataques son debidos a que no se han tratado las vulnerabilidades conocidas".

Como conclusión la estrategia de Tenable era clara: "Monitorizar para ver todo lo que sucede en nuestro entorno; predecir lo realmente importante; y actuar sobre el riesgo, mediante 'vacunas'".

José de la Cruz, miembro de Trend Micro, intervino con el tema: "Inmunidad de grupo frente al Ransomware". Destacó que debe ponerse en valor la importancia de los sistemas de información y los riesgos asociados: "si no hay disponibilidad de los sistemas, la asistencia sanitaria actual puede no producirse de la forma adecuada".

Remarcó que los ataques de Ransonware son la principal táctica que se está utilizando: "Es una táctica muy lucrativa, que genera innumerables pérdidas a la organización. En la actualidad, se busca el eslabón más débil de la cadena de suministro para realizar el ataque". Aunque también se realizan ataques de Phishing, para el robo de datos y credenciales, que poseen mucho valor actualmente. Los equipos sanitarios actuales, son víctimas de muchos ataques, ya que suelen llevar software, sistema operativo… desactualizados u obsoletos en la mayoría de los casos. Para ello, la solución de Trend Micro se basa en 3 pilares:

- *Stellar One*: protege dispositivos uno a uno.
- *Vision One*: si tenemos visibilidad, es todo mucho más fácil y rápido. Control y corrección, debemos tener una visibilidad global.
- *Cloud One:* mitigar las vulnerabilidades es muy importante y, en ocasiones, no se pueden instalar los parches. El parcheo virtual, "soluciona" el problema de forma temporal.

La visibilidad es lo más importante, saber lo que pasa para poder encontrar soluciones

Laura Prats, miembro de Sham, introdujo el tema: "Cómo evitar un ciberataque en dispositivos mé-

dicos y datos de salud". Sobre este aspecto indicó que "la transformación digital es imparable y los dispositivos médicos deben adaptarse a la constante evolución de los riesgos que conlleva. Se debe tener muy en cuenta la visibilidad y gestión del inventario, la gestión de riesgos, así como la seguridad de las aplicaciones y de los datos".

La solución propuesta por Sham es CyberMDX. "Se basa en la identificación, evaluación, prevención, detección y análisis de la red de la organización, ya que suele ser difícil directamente desde cada dispositivo. Ofrece un descubrimiento continuo y en tiempo real de los dispositivos médicos conectados y en la red de la organización, proporcionando una visibilidad necesaria para aplicar inteligencia artificial y evaluar los riesgos de cada dispositivo, teniendo en cuenta las exposiciones conocidas, el potencial de ataque y la criticidad operativa. Controlando el flujo de la red se controlan los riesgos asociados de las redes sociales, entrega de resultados por Internet, securización conexión con el paciente, etc.", destacó.

Ernesto Sanz, miembro de S2 GRUPO, expuso el tema: "Monitorización de pacientes: más que constantes vitales". En su opinión existen muchos más sistemas de información, el mundo IoT cada vez toma más protagonismo.

S2 Grupo utiliza la solución GLORIA, del CCN, para la detección y gestión de amenazas, detectando equipos no inventariados o conexiones no permitidas, mediante alertas que permiten una mayor rapidez de actuación. Para la detección se utiliza inteligencia artificial que permite recoger parámetros de cada servicio, aprendiendo el patrón normal de comunicaciones, de tiempo, etc.

Por su parte, Alfonso Ríos, miembro de SIA, trató el tema: "Protegemos los datos de salud en los procesos de identificación digital: Digital Onboarding". Apuntó que "el creciente número de clientes digitales exige un entorno seguro para sus operaciones. Se debe aprovechar la tecnología de identificación y el uso de elementos biométricos. La identidad digital y la firma electrónica permiten que la acreditación de la identidad sea usable, flexible y segura de forma garantizada, generando evidencias seguras, confiables y con validez jurídica".

El proceso digital Onboarding se basa en: Los medios de captura y evaluación de credenciales (documentos y medidas biométricas), deben disminuir los riesgos de fraude (Orden Ministerial ETC/465/2021 de certificados digitales cualificados); y las medidas biométricas pueden usarse como doble factor de autentificación.

En este sentido, SIA propone una solución completa que cumple con la normativa vigente: Identificación remota y verificación de la documentación; el cliente debe dar un consentimiento informado y, al mismo tiempo, se le dan una serie de recomendaciones: Firma electrónica y custodia de evidencias. De esta manera, esta tecnología permitiría enviar información al paciente, con servicios mayores a un acuse de recibo.

Posteriormente los asistentes intervinieron con preguntas, entre las que destacaron: ¿Se puede entender una captura de datos como un dato personal? La respuesta fue que el RGPD sí considera los datos biométricos como datos personales. En este caso, SIA tiene el rol de encargado de tratamiento.

Otra pregunta cuestionó cuáles eran los retos que debería abordar el sector de salud en este aspecto, cuya respuesta indicó que se debería diferenciar el enfoque entre paciente y personal sanitario, ya que los requisitos son totalmente distintos. Los servicios de salud deben potenciar los servicios telemáticos a los pacientes y poner los mecanismos necesarios para su uso.

SEGUNDA SESIÓN: "VISIBILIDAD Y CIBERCONTROL EN ENTORNOS HOSPITALARIOS"

En la segunda sesión se expusieron las soluciones de seguridad ante el tratamiento de datos de salud que cada empresa tiene en los diferentes ámbitos de tratamientos.

Por su parte, Francisco Leal, miembro de Inetum expuso su estrategia: "Segurizando el gobierno del dato". Señaló que "el aumento de los ataques al sector salud ha puesto de manifiesto la importancia de segurizar los procesos, las políticas y las medidas de seguridad para proteger los datos. La pandemia y la transformación digital han transformado el perímetro de la organización y el perímetro se encuentra donde se encuentre el trabajador".

En este sentido, subrayó que "los datos se han



convertido en oro, en especial los sanitarios, por lo que el RGPD y la directiva NIS han puesto énfasis para su protección. Las brechas de seguridad cuestan una media de 5,9 millones de euros a la organización, pero el mayor impacto no es el económico, sino la falta de disponibilidad de los datos, que puede llevar al coste de vidas humanas".

Las directrices de ENISA son muy ambiciosas en el sector sanitario y pretenden responder a las siguientes preguntas:

- ¿Qué debe protegerse? Debe protegerse la seguridad física, la seguridad lógica y la identidad digital.
- ¿Por qué deben protegerse los anteriores aspectos? Para el cumplimiento normativo.
- ¿Cómo deben protegerse? Se podrán proteger de múltiples formas: monitorización y correlación (SIEM), *Threat Hunting*, SOC, ...

Por esta razón, desde Inetum se puso énfasis en los siguientes aspectos:

- Gobierno de la red.
- Gobierno del *endpoint*.
- Gobierno del dato.
- Gobierno de la Gestión de Identidades y Gestión de Accesos.

Por otro lado, la solución de ProTego trató los anteriores aspectos y sus características son: concienciación, el factor humano ahora es el perímetro y nuestro primer *firewall*; los riesgos: monitorización y análisis, y la protección de datos en sus tres estados: en reposo, en tránsito y en uso, mediante el cifrado de los mismos.

Otro aspecto para destacar fue que la imagen médica se ha convertido en el foco de los ataques porque todos los dispositivos son difíciles de actualizar, por ello se protege el tráfico de estos dispositivos.

Javier Pérez, miembro de Fujitsu, expuso su estrategia: "Soluciones de ciberseguridad para el hospital del futuro". Añadió que "las tecnologías están totalmente embebidas en el sector sanitario (inteligencia artificial, biometría, etc.), por lo que han aumentado los ataques al sector. Las tendencias actuales son la asistencia remota y la telemedicina. Por tanto, se debe dotar a los sistemas de los mecanismos adecuados de protección. El principal mecanismo de protección es el Esquema Nacional de Seguridad (ENS), con sus principios y medidas de seguridad. El problema es que no está demasiado implantado".

La solución propuesta por Fujitsu se basó en los siguientes aspectos:

- En Seguridad Física, se apuesta por la biometría.
- Ciber protección tecnología sanitaria.
- Cifrado de datos.
- Control de la desinformación, ya que puede alterar las tendencias.
- Externalización de servicios, con el consiguiente peligro de NO verificar qué medidas de seguridad implementan dichos servicios externos.
- Planes de continuidad y resiliencia, importantísimos en sanidad.
- Controles de seguridad en el uso de la tecnología *Big Data*.
- Cloud en salud.

Las principales tecnologías de ciberseguridad que han posibilitado la transformación digital del sector sanitario han sido: el uso de la biometría, no solo para accesos a zonas determinadas, sino también para la identificación de los pacientes; *Blockchain* /IoT, y comunicación de transacciones e identificación electrónica de pacientes.

Las recomendaciones de Fujitsu para el sector sanitario fueron:

- Adecuación y certificación ENS.
- Disponer entendimiento nivel ciber-resiliencia ante un *Ramsomware*.
- Disponer de planes de concienciación.
- Soluciones de visibilidad de la red y control de acceso.
- Gestión de identidades y cuentas privilegiadas.
- Protección de tecnología sanitaria.
- Uso de biometría.

Por otro lado, Lluís Planas, miembro de Fortinet expuso su estrategia: "Cómo proteger los datos de salud en un entorno SmartHospital". Explicó que "debido al covid-19 la telemedicina en España ha sufrido un fuerte aumento repentino, lo que ha puesto a prueba a las tecnologías y a las organizaciones. Aunque la misma permite mejores resultados, conlleva riesgos asociados que deben asumirse, tanto en los dispositivos como en el flujo de información. El espacio de ataque a proteger en el entorno sanitario es cada vez mayor y los ciberataques evolucionan cada vez más".

En este sentido, se consideró que los retos de la ciberseguridad tenían que ser: Encontrar y retener a profesionales con conocimientos específicos; monitorizar y proteger los entornos distribuidos para mitigar los efectos de la descentralización; los silos tecnológicos son un reflejo de la organización y sus sistemas de comunicación interna; el coste es una lucha que no depende de los técnicos y exigir el cumplimiento de la normativa vigente. Sin embargo, "la solución es más bien una estrategia, un único punto amplio, integrado con otras soluciones y automatizado, ya que no tenemos suficientes recursos", admitió.

El objetivo pasaba por dar seguridad a las personas, los datos y los dispositivos basándose en tres pilares: protección de la infraestructura perimetral; autenticar usuarios y definir permisos de acceso y control sobre las transmisiones.

En este sentido, "la regulación es muy estricta y cumplirla cada vez es más complejo. La descentralización de la sanidad tiene sus cosas buenas y sus puntos débiles. Aunque 'Internet of Medical Things (IoMT)' es el futuro, deben gestionarse correctamente estos dispositivos y sus repositorios: Debemos recordar que el mayor enemigo es el factor humano, ya que es incontrolable, pero se tiene la tecnología para minimizar estos errores (control de los permisos, control de los accesos, etc.); además los repositorios suelen estar en la nube, pero debemos tener una visibilidad de toda la información y de su flujo, siendo capaces de reaccionar delante de lo que vaya sucediendo", subrayó.

Santiago Lagóstena, miembro de Ingecom expuso su estrategia: "Clinical Zero Trust". La solución propuesta por Ingecom para la protección de los dispositivos médicos es Medigate, que garantiza la protección de datos de los pacientes, mediante sus diferentes certificaciones.

Lagóstena destacó que "los dispositivos médicos pueden no estar incluidos en dominio, tener sistemas operativos propios, etc. Son dispositivos que no están preparados para segurizar, suelen ser 'móviles', no suelen utilizarse con efectividad, etc. Y todo esto, ocasiona costes adicionales.

Los retos para dar seguridad a los dispositivos médicos son: Retos técnicos: aumento de la conectividad sin seguridad por diseño adecuada, equipos no inventariados, diversidad de fabricantes y dispositivos; retos organizacionales y riesgos asociados a los equipos.

La solución propuesta permite descubrir e identificar de forma automatizada dispositivos médicos conectados a la red; el análisis de protocolos de comunicación únicos de dispositivos médicos (Dicom y HL7) para detectar anomalías; la prevención de ataques automatizada con microsegmentación y la interacción con los principales *players* de seguridad del mercado.

El grado de madurez es la clave diferenciadora, no se puede proteger lo que no se conoce y la integración con muchos fabricantes es complicada.

Durante su intervención, Albert Cabré, miembro de Olympus transmitió su estrategia: "Seguridad y GDPR del contenido multimedia y de retransmisiones en el entorno hospitalario". Señaló que "la situación actual es la de seguridad basada en la infraestructura de red, debido a la nula o baja

seguridad de los equipos médicos. En el caso del contenido multimedia y de retransmisiones en el entorno hospitalario, las grabaciones no están cifradas y los equipos permiten que la exportación y transmisión sea de forma directa y sin control. Además, no se aplican parches de seguridad ni actualizaciones, o resultan demasiado costosas, por tanto, se incumple con el RGPD, que indica que debe realizarse un control de la información y los accesos deben ser sólo los permitidos".

Para solucionar este incumplimiento del RGPD, Olympus propuso una solución con las siguientes características: No tener grabadores inconexos e inseguros, sino un sistema centralizado virtualizado y segurizado, así se sabe quién accede a la información (mediante LDAP), las transmisiones son seguras (desde la captura hasta el repositorio) y se dispone de un único punto de conexión; Seguridad en el propio terminal de captura mediante discos encriptados, protección ante caída de tensión y LAN, automodificaciones con envío de informes sin necesidad de técnico e ir dispositivo a dispositivo; y funcionalidades adaptadas a las necesidades de los equipos médicos mediante acceso seguro vía web, que permite librerías personalizadas y ordenadas por etiquetas, edición de vídeos y comparación para quedarse con lo que se necesite y no haya duplicidades, así como captura segura desde un dispositivo móvil que se transfiere vía wifi a la solución y no deja rastro en los dispositivos móviles de la captura.

Por otro lado, comentó el aspecto de las retransmisiones (tele-colaboración) que no requieren sistemas de videoconferencia o herramientas de mercado no médico, sustentado en dos cuestiones: Un modelo basado en la nube, seguro mediante control de acceso a través del LDAP y envío de invitaciones con doble factor de autentificación y por tiempo limitado; y funcionalidades adaptadas a las necesidades de los equipos médicos: selección de fuentes, anotación bidireccional, enmascarado del paciente, grabación segura de la sesión, etc.

TERCERA SESIÓN: "INAUGURACIÓN OFICIAL: SESIÓN AUTORIDADES DE CONTROL"



Jesús Jiménez, miembro del Consejo de Transparencia y Protección de Datos de Andalucía, señaló que su principal preocupación era garantizar el derecho de la ciudadanía a relacionarse con los servicios asistenciales, a través de las nuevas herramientas proporcionadas por la pandemia y en especial a la protección de los datos personales, conociendo los riesgos asociados.

"La Inteligencia Artificial requiere toda la atención necesaria para garantizar el cumplimiento de privacidad de los datos, así como los derechos fundamentales de las personas, evitando sesgos y discriminaciones", puntualizó.

Por su parte, **Margarita Uría,** de la Agencia Vasca de Protección de Datos, destacó que las autoridades de control han realizado una actividad muy especial debido a la situación de pandemia. "En 2020 ha habido una crisis sanitaria, pero también humana, en el aspecto social y económico. La lucha contra esta pandemia ha provocado la toma de medidas que podrían afectar a la privacidad de las personas con lo que se han tenido que tomar medidas y sancio-

nes para que se respetara la privacidad de los datos. Se ha tenido que dar formación a colectivos con las premisas de las autoridades de control, ya que ninguna normativa ni legislación suspende el derecho fundamental de la protección de datos que tienen en su tutela. Hace falta humildad para afrontar situaciones difíciles y colaboración con todas las partes implicadas.", indicó.

Además aseguró que el tratamiento de datos de salud siempre ha sido una prioridad. La pandemia había supuesto importantes retos como los intercambios de información entre autoridades y organizaciones públicas y privadas; se había tenido que garantizar los derechos de privacidad; el teletrabajo y otros aspectos también habían tenido que vigilarse y se habían multiplicado las consultas de los ciudadanos.

En este sentido, los principios del RGPD permitieron afrontar los retos anteriores. Además, el inicio de la pandemia coincidió con la presentación de una Guía dirigida a los pacientes, que abordaban las principales acciones en datos de salud. También se aprobó una Guía de Evaluación de Impacto y el Código de conducta para el tratamiento de datos personales en el ámbito sanitario.

Mar España, directora de la Agencia Española de Protección Datos (AEPD), subrayó que el derecho a la protección de los datos no quedó suspendido por la situación de pandemia. Se redactó un informe con criterios específicos para que no sucediera, sin que supusiera un obstáculo para el correcto tratamiento de la pandemia.

No obstante, los dos grandes temas que habían surgido por la pandemia fueron, por un lado, el certificado de vacunación: "tiene su base jurídica en las directivas europeas sobre la libre circulación de las personas. Solo deberá contener los datos de la fecha de vacunación o la fecha de superación del covid-19, dando alternativas para las personas no vacunadas, para no ser discriminadas. Deberá verificarse mediante un código de barras", puntualizó.

Por otro lado, la investigación científica: "se está procediendo a una planificación estratégica. Ya se dispone de un borrador para una guía y el Comité Europeo ha señalado que la base reguladora debería ser el interés público, con consentimiento del interesado y permitiendo las transferencias internacionales de datos. Se quiere impulsar un modelo de consentimiento en este ámbito. La Fundación 29 de febrero aboga por una base de datos común para salvar vidas, con datos anonimizados, ya que existe la base jurídica para ello", destacó.

Pablo Fernández, consejero de Salud de Asturias lanzó la siguiente reflexión: "la pandemia no ha acabado y no se debe bajar la guardia, sobre todo hasta que no esté erradicada en los países más pobres".

CUARTA SESIÓN: "RETOS PARA EL DESARROLLO DE SOLUCIONES TECNOLÓGICAS EN LA LUCHA CONTRA EL COVID-19"



Durante su intervención, Santiago Graña, subdirector general del Impulso de la Digitalización de la Administración (SGAD /SEDIA/MAETD), explicó que "los fondos europeos dan una idea de la importancia de la digitalización del sector público. Impulsan el plan 'España Digital', pensando en la digitalización de la industria y del sector público, con una inyección del plan de recuperación,

dando especial importancia a la formación. La pandemia ha convertido en oportunidad la digitalización, aunque haya sido en modo de crisis, pero se ha respondido de forma satisfactoria, a pesar del aumento del volumen que ha supuesto". También destacó que gracias a los fondos se implementó la aplicación Radar Covid que se hizo con un enfoque diferente a la geolocalización, siendo mucho más respetuosa con la privacidad por defecto y desde el diseño; se importó de los países asiáticos, pero se adaptó para respetar la privacidad y se hizo un piloto que funcionó muy bien porque confirmó que duplicaba la eficacia frente al seguimiento manual.

Sobre Radar Covid también se debatió si debía ser descentralizada o centralizada, y se optó por la parte descentralizada por lo que los datos quedaban en los móviles y no se subían a ningún servidor. Además, para que la aplicación funcione, debe existir colaboración entre la ciudadanía y las autoridades sanitarias; y "nunca se planteó que fuera obligatoria, ni se podía instalar en el 100% de móviles. Tiene un efecto red y se pretendía que al menos llegará a un 20% de la población como objetivo. Se han conseguido 7'3 millones de descargas, pero no significa que estén activas", puntualizó.

Inmaculada Moro, subdirectora de Enfermería de OSAKIDETZA: Rastreadores en el País Vasco, señaló que el planteamiento inicial fue entender los rastreos como un único sistema para cualquier zona o persona. El rastreo se basó en el diagnóstico de los positivos y debía ser lo más rápido posible, para cortar las cadenas de transmisión.

Destacó que se hizo un gran esfuerzo para el diagnóstico (unos 13.000 PCR diarios), que se comunicaban de forma rápida al afectado para cortar la cadena de transmisión. "Primero solo se notificaba si era positivo, hasta que pudieron asignarle un código de la aplicación Radar Covid para tenerlo rastreado. Los rastreadores se coordinan con los servicios de salud laboral, medicina preventiva, centros sociosanitarios, etc., para tener cubierto el mayor ámbito posible. Se han identificado un 6'3 % de positivos, detectados a través de la aplicación Radar Covid", indicó.

En el caso de las vacunaciones "se han ido haciendo en función de las que han ido llegando, poniendo los medios. Pero lo más importante es que la ciudadanía participe y se refleja la información de las personas que se han 'negado' a vacunarse. Se recoge en la historia clínica cuando la negativa es clara", subrayó.

Algunas de las preguntas de los asistentes versaron sobre si los rastreadores habían venido para quedarse. Cuestión a la que Moro respondió que "el aprendizaje de esta pandemia es que hay cosas que son más ágiles y fáciles para la ciudadanía, pero deben regularse y desarrollarse, cumpliendo algún criterio más, dotando de medios y formación a los profesionales".

Ignacio Lage, responsable de Área de Desarrollo Software y Proyectos (STIC – SAS), intervino con el tema "La visión desde una perspectiva tecnológica en Andalucía".

Sobre este aspecto explicó que "la pandemia ha hecho evolucionar a todos los ámbitos y cambiar en la medida que surgían nuevas necesidades y expectativas. La primera fase fue garantizar la continuidad del servicio, mediante el teletrabajo desde prácticamente cero. Se consiguió y se dio solución a la situación. Era una situación histórica que se solucionó en tiempo récord. Debían mantenerse los principios de legalidad, con la usabilidad, ante los riesgos inherentes que conllevaba".

Por otro lado, señaló que "la capacidad de respuesta ha sido eficaz porque los sistemas y la interoperabilidad, entre otros, estaban mejor preparados de lo que posiblemente se creía. Se han implantado nuevas herramientas, pero el cambio inmediato fue posible gracias a que ya se disponía de una base. También ha sido muy importante la colaboración entre organismos públicos y privados. Pero todo ello no tendría que quedarse en papel mojado, debería seguir avanzando. Se han tenido que cambiar cuadros de mandos, movilidad, portales del paciente, telemedicina, video-consultas así como compartir datos con los nuevos parámetros necesarios para la situación y todo ha funcionado".

Así mismo destacó que desde el Área de Desarrollo de Software y Proyectos se ha implementado una herramienta para compartir información con el paciente llamada Mercurio. "La clave fue todo el trabajo que se había realizado anterior a la pandemia. La conclusión es que no se estaba tan mal, a pesar de lo que se pudiera creer", admitió.

Entre las preguntas de los asistentes se hizo hincapié en si la protección de datos durante la pan-

demia había supuesto algún problema. La respuesta fue que en algunos casos sí, pero en otros se han planteado retos, como el pasaporte pandémico. Lage concluyó que "la lección aprendida es que se debe colaborar más y llegar a un equilibrio entre privacidad y uso".

Alfredo Díez, responsable de CC de Ciberseguridad de Oesia intervino con una charla sobre la empresa privada ante la situación de pandemia. En este sentido, señaló que había dos opciones: cancelar contratos o aprovechar recursos humanos para superar las adversidades.

Oesia inició doce campañas en diferentes ámbitos, algunas de las cuales fueron: Los ataques al sector sanitario aumentaron y se lanzaron escudos a los sistemas, segurizando los centros sanitarios en tiempo récord, mediante sondas para monitorizar las redes; también tuvieron mucha importancia los sistemas de Alerta temprana, mediante los servicios de vigilancia digital, que monitorizaba lo que pasaba en Internet y en la web oscura; se participó en aplicaciones de rastreo de pacientes ingresados en hospitales, para poder detectar de forma más rápida y se creó una aplicación para tener seguimiento y contacto con sus familiares y sanitarios, mediante un código QR. En el supuesto caso de que se perdiera el código QR, no se podía acceder a los datos de los pacientes, ya que era el propio familiar el que tenía que poner los datos.

La intervención de Antonio José Álvarez Gamero, de Baxter S.L., giró en torno a la especialidad en salud digital basada en interconectar las líneas de la empresa aplicadas a las nuevas tecnologías para facilitar el acceso al paciente.

Señaló que "Baxter ya tenía experiencia en otro tipo de pandemias, por lo que disponía de herramientas de rastreo que se adaptaron a la situación actual, con especialización en asistencia domiciliaria, que ha facilitado la optimización de los recursos, por ejemplo, dejando de ocupar camas y los enfermos permanecen aislados en su entorno de control con una mínima exposición, al ser pacientes de riesgo".

Juan Díaz, coordinador del Comité Técnico de Seguridad de la Información de Salud, explicó que el Comité se creó para la coordinación interterritorial de protección de datos y la seguridad de la información en el sector sanitario y debido a la pandemia, se reúnen mensualmente por videoconferencia. Cuenta con la participación de todas las CC. AA.

En la reunión del foro se debatió sobre: El certificado digital ¿cómo se va a categorizar, uso de autentificación, gestión del certificado y alternativas?; Los diferentes roles que pueden darse en ensayos clínicos (DPD, promotor, investigador principal, monitorización, etc.); Los fondos europeos para financiar un SOC sectorial y los servicios con terceros que asumen el papel de responsable de tratamiento.

Además, añadió que se quiere abordar a corto plazo: La identidad digital sin registro físico; El uso generalizado de Clave Permanente, no solo para temas de salud; la explotación masiva de los datos en Investigación e Internet of Medical Things (IoMT).

QUINTA SESIÓN: "CASOS PRÁCTICOS: LA EXPERIENCIA DE LAS AUTORIDADES DE PROTECCIÓN DE DATOS"

Los ponentes que dieron voz a la experiencia de las autoridades de Protección de Datos fueron: José Luís Falcón del Consejo de Transparencia y Protección de Datos de Andalucía; Lourdes Hernández, de AEPD; Eva García, de Autoridad Catalana de Protección de Datos y Juana Vegas, de la Agencia Vasca de Protección de Datos. En la quinta sesión se compartieron varios casos prácticos que demostraron que la protección de datos personales, y en especial de las categorías especiales de datos, sigue siendo un derecho fundamental aun en tiempos de pandemia.

La sesión de debate quedó dividida en ocho grandes bloques:

1. Teletrabajo

El teletrabajo ha supuesto un riesgo a nivel del tratamiento de datos personales. En este sentido las autoridades de control aportaron las siguientes recomendaciones:

- Recomendaciones para los responsables:
  - Definir política de protección de la información.
  - Identificación de los riesgos asociados a los recursos tecnológicos.
  - Difundir la citada política y las buenas prácticas en el ámbito del teletrabajo a través de protocolos documentados.
  - Elegir prestadores de confianza.



- Configurar equipos para situaciones de movilidad.
- Revisar los accesos producidos sobre los recursos tecnológicos.

– Recomendaciones para los trabajadores:
- Respetar la política de protección de la información definida por la organización.
- Proteger los dispositivos (mantener el software actualizado, no acceder a redes públicas, etc.).
- Garantizar la protección de la información (no hacerla visible a otros).
- Si la información se ve comprometida, comunicarlo al responsable de tratamiento.

2. Tratamiento de los datos de contacto de los ciudadanos

En este hilo de debate las autoridades de control presentaron algunos de los casos relacionados con el tratamiento de los datos de contacto de los ciudadanos con fines ulteriores para lo que fueron recabados:

– Uso de datos de padrón con fines asistenciales

Tras la llegada de la pandemia se planteó la posibilidad de utilizar los datos del padrón (nombre de los ciudadanos y número de teléfono relacionado) para contactar con los ciudadanos en caso de urgencia y prestar una asistencia sanitaria en caso de ser necesario.

La finalidad del tratamiento de los datos del padrón municipal es la de acreditar la residencia de los ciudadanos y se basa en las condiciones establecidas por el artículo 6. 1. d) y 6. 1. e) del RGPD (proteger los intereses vitales del interesado y para el cumplimiento de una misión realizada en interés público).

Tras realizar el test de compatibilidad establecido por el artículo 6. 4 del RGPD se determinó que la nueva finalidad del tratamiento de los datos de padrón (asistencial) no era compatible con el fin para el que se recogieron inicialmente (acreditar la residencia). En este sentido, y con el objetivo de encontrar una alternativa para poder prestar una correcta asistencia a la ciudadanía sin vulnerar sus derechos de privacidad y protección de datos, se propuso la siguiente solución: remitir avisos de zonificación. De tal modo, los residentes pertenecientes a un barrio podrían ser avisados acerca de la necesidad de llevar a cabo alguna acción de carácter asistencial (PCR, pruebas de antígenos, confinamiento perimetral, etc.).

– Cesión de datos de padrón municipal para ofrecer servicios sociales y evitar situaciones de aislamiento.

En la línea del caso anterior, la cesión de datos del padrón municipal con la finalidad de prestar servicios sociales a personas en situación de aislamiento no era compatible con el fin para el que se recogieron inicialmente. En este sentido, la AEPD propuso la alternativa de que fueran los ayuntamientos quien, por el ejercicio de sus competencias, contactaran con los ciudadanos y ofrecieran los datos de contacto de los servicios sociales ofrecidos por distintas organizaciones sin ánimo de lucro.

3. Toma de temperatura

La toma de temperatura fue otro de los grandes dilemas en lo que respecta al tratamiento lícito de los datos personales de las personas. Se plantearon preguntas como: ¿cuándo se puede? ¿quién puede? ¿qué pasa si un ciudadano tiene la temperatura elevada? ¿qué dispositivos son los adecuados?

Según la AEPD, la aplicación de estas medidas requiere de las exigencias previstas por las autoridades sanitarias y estas solo deben aplicarse atendiendo a los criterios establecidos por estas autoridades de control. Algunos de estos criterios podrían ser:

- Establecer rangos de fiebre según evidencia científica.
- La base jurídica nunca podrá ser el consentimiento del interesado, puesto que el mismo, puede negarse.
- Analizar si es posible realizar este tratamiento por otros medios menos intrusivos.

Toma de temperatura en el ámbito laboral: La toma de temperatura en el ámbito laboral queda legitimada por la condición de licitud de tratamiento establecida en el artículo 6.1.c) del RGPD. Según la Ley de Prevención de Riesgos Laborales (LPRL) los empleados tienen derecho a la salud en el trabajo y los empleadores tienen la obligación de cumplir con tal derecho. Dichas tomas de temperatura en el entorno de trabajo deben ir acompañadas de protocolos y procedimientos.

Toma de temperatura en el ámbito escolar: La toma de temperatura en el ámbito escolar también queda legitimada por el cumplimiento de una obligación legal y debe ir acompañada de protocolos relacionados. En este sentido, los centros educativos disponen de un protocolo transversal que refleja las medidas de prevención (en las que se encuentra la toma de temperatura) y medidas de actuación en caso de detección.

4.Tratamiento por los empleadores de los datos de salud de sus trabajadores

En relación con el tratamiento de los datos de salud de los trabajadores por parte de sus empleadores, las autoridades de control compartieron algunos de los casos y preguntas más frecuentes acontecidas desde el inicio de la pandemia:

- ¿Puede la empresa saber si una persona está infectada o no?
  La empresa podrá saber si una persona está infectada o no para definir líneas de actuación y prevención internas. Para ello, una vía legítima es mediante el uso de cuestionarios de salud limitados en los que solicite la presencia de ciertos síntomas (y no de su estado de salud) y del estado domiciliario de los trabajadores.
- ¿Puede la empresa comunicar que una persona está contagiada?
  La empresa únicamente podrá informar a aquellos trabajadores con los que la persona infectada ha estado en contacto. No se puede publicar, por ningún medio (correo electrónico, muros de redes internas laborales, etc.), que una persona está infectada.
- ¿Puede el personal de seguridad de una empresa realizar tomas de temperatura?
  Solo en casos excepcionales y bajo estrictos protocolos, la toma de temperatura podrá realizarse no exclusivamente por personal sanitario (incluido el personal de seguridad de una organización).
- Aun estando de vacaciones, ¿el trabajador, en caso de estar infectado, tiene la obligación de informar a su empleador?
  Si el trabajador presenta síntomas durante sus vacaciones, y si antes de entrar en dicho periodo ya presentaba síntomas y ha estado en contacto con otros trabajadores, tendrá la obligación de comunicárselo a la empresa (y la empresa tendrá el derecho de saberlo).

5. Uso de la mascarilla

El no uso de la mascarilla por razones y motivos de salud obligaba a las personas afectadas por tal condición a tener que presentar documentos justificativos que acreditasen su estado de salud.

6. Investigación y análisis de aplicaciones

La situación de la pandemia ha permitido habilitar legítimamente el acceso remoto para la monitorización de datos en los proyectos de investigación sanitaria. En estos casos siempre deberán quedar claros los roles y responsabilidades de cada una de las partes involucradas, siendo el promotor el responsable de tratamiento y el monitor el encargado.

En cuanto a las APPs y webs de autoevaluación se determina que la aportación de datos es un acto meramente voluntario (bajo consentimiento). Los datos recabados por el GPS solo se tratan con el fin de saber si una persona está en un municipio.

7. Homenajes a personas fallecidas por covid-19

Con motivo de realizar un homenaje a las personas fallecidas por covid-19, surge la necesidad de consultar los datos de contacto de sus familiares o seres queridos.

Puesto que el RGPD no aplica al tratamiento de datos personales de personas fallecidas no existe una base legal que habilite la posibilidad de comunicar estos datos. En este sentido, se propuso como alternativa que, todos aquellos familiares que quisieran homenajear a sus seres queridos se apuntasen a un listado específico.

8. Vacunación

Con relación al tratamiento de los datos de vacunación, las autoridades de control compartieron algunos de los casos y preguntas más frecuentes acontecidas desde el inicio de la pandemia, una de ellas era si los empleadores podían tener acceso a la información de si sus trabajadores estaban vacunados. La respuesta que se dio es que las empresas únicamente podrán saber si una persona ha decidido no vacunarse y por qué motivos (razones genéricas). Dicho dato siempre deberá estar analizado en función de para qué y por qué necesita la empresa ese dato.

SEXTA SESIÓN: "INTERCAMBIO DE DATOS DE SALUD EN TIEMPOS DE COVID"



Santiago Farré, de la Autoridad Catalana de Protección de Datos explicó que la pandemia había supuesto una prueba de fuego para diferentes sectores de la protección de datos. "Se han gestionado los riesgos, siendo de alta probabilidad y alto impacto, de forma satisfactoria, gestionando la información de forma proporcionada y garantizando las medidas adecuadas para la protección de datos", señaló.

Mercedes Alfaro, de la Secretaría General de Salud Digital, Información e Innovación del SNS (Ministerio de Sanidad), intervino con el tema: "Sistemas de vigilancia epidemiológica". Comenzó hablando sobre el sistema de vigilancia de enfermedades de declaración obligatoria. "Tras la llegada de la pandemia, se vio que dichos sistemas de información no estaban preparados para acompañar esta situación y que se debía implantar un sistema que diera una respuesta más rápida y eficiente a los ya existentes. Por ello, se tuvo que implantar un sistema de información nuevo en dos partes: una primera, de pruebas diagnósticas con laboratorios. Los laboratorios debían enviar diariamente los resultados de las me, ya que las pruebas PCR se hacían en sitios preparados para ello, que debían enviar cada día las muestras analizadas con una demora máxima de 12 horas y georreferenciadas por código postal para tener los indicadores útiles en las CC. AA., pero no tenían los datos de otras CC. AA. Limítrofes; y otra segunda, en los laboratorios. Estos debían tener datos unívocos para identificar a las personas y en el Ministerio se cruzaban con la base de datos de la Seguridad Social, que es la mayor de España (incluidos los menores, indocumentados, MUFACE, etc.), explicó.

Posteriormente, Alfaro aclaró que "al cruzarse con esta base de datos se obtenía el código postal, y se hacía un *hash* para anonimizar. Este ha sido un sis-

tema de información muy útil, ya que incluso se podía ver la movilidad de las personas. Otro sistema de información fue el de ingresos y altas de cada hospital, que luego se agrupaba por municipio, provincia y finalmente por CC. AA. de forma mensual. Semanalmente, se mandaba por el mismo sistema el material disponible de EPIS, con un consumo semanal para la previsión de compras y sus picos".

En el turno de preguntas se cuestionó cuáles habían sido las lecciones aprendidas durante la pandemia, a lo que Alfaro respondió que "muchas, pero por encima de todas, que los sistemas a los que no se les da importancia toman valor en estas situaciones. La BD con código unívoco y vitalicio por paciente, por ejemplo. Respecto a la protección de datos, el principio de proporcionalidad es fundamental incluso a todos los niveles de la vida. El uso de *hash* unívocos e irreversibles también son fundamentales".

Ángel Cabal, miembro del Consorcio Asturiano de Servicios Tecnológicos, partió de la base de que las administraciones locales pequeñas debían tener los mismos servicios que un gran ayuntamiento. "Para ello se creó el Consorcio Asturiano de Servicios Tecnológicos, para dotar de servicios tecnológicos a las pequeñas administraciones locales mediante recursos compartidos (CPD, comunicaciones, aplicaciones de gestión, DPD, ...), para ser más eficientes", puntualizó.

En este sentido subrayó que "el consorcio es el Encargado del tratamiento de todos los datos y han conseguido que todos sus proveedores de servicios firmen su contrato de sub-encargado de tratamiento. Tener una política común ha permitido contar con un intercambio de datos igual, con los mismos criterios para todos, lo que ha facilitado el intercambio. Todo el personal municipal pudo hacer uso del teletrabajo con seguridad, con lo que los ayuntamientos han seguido siendo operativos, con guías, procedimientos y códigos de buenas prácticas comunes".

Según Cabal, "la principal lección aprendida fue en el ámbito social, ya que los servicios sociales son multisectoriales, multirecurso, multiadministración y tecnológicamente dispersos ya que cada sector tiene sus soluciones. Se está trabajando para conseguir el expediente social único, para evitar estas diferentes aplicaciones, pero se tiene que estudiar muy bien cómo hacerlo, sobre todo en cuanto al tema de los intercambios de información", señaló.

En el turno de preguntas se abordó qué era más conveniente la historia social unificada o desagregada, y se concluyó que era mucho más fácil proteger los datos en sistemas desagregados. Con la tecnología Big data se podían tratar de forma conjunta y solo los datos que fueran necesarios.

Maider Urroz, de la Unidad Delegada de Protección de Datos del Gobierno de Navarra trató el tema: El intercambio de información de casos covid-19 en el ámbito educativo. Explicó que "se comprobó que no se estaba atendiendo bien a los niños, al estar en casa con videoconferencias. Se crearon comités técnicos para establecer diferentes escenarios para la vuelta presencial, siempre con la incertidumbre del avance de la pandemia. También se crearon los grupos estables de convivencia, no burbuja, con protocolo de actuación en caso de un positivo. Para que los servicios de salud accedieran a los datos por ser contacto estrecho, se permitió el acceso a la base de datos de educación con la base legitimadora de interés público, aunque se dieron cuenta de que los sistemas de información no estaban preparados. Por último, se tuvo que crear un sistema de información conjunto entre Educación y Salud para la detección y notificación de positivos, para cortar la cadena de propagación lo más rápido posible. Este sistema creó una pasarela para que los rastreadores accedieran a los contactos del grupo estable de un positivo. Los datos estaban actualizados al día y se aplicaba el protocolo establecido (el rastreador según criterios médicos informa del confinamiento de la clase y se notifica a todos por SMS de forma inmediata, con la consecuente ganancia de tiempo). También se aplicaron los principios de protección de datos".

David de Falguera, de E&Y intervino con el tema: Intercambio de información con entidades privadas y certificados de inmunidad (pasaportes de vacunación). Indicó que "se debe poner en valor los servicios de prevención de riesgos laborales de las compañías del sector privado, al colaborar en la información de las autoridades sanitarias, legitimados como base de interés público. Se debe definir e identificar correctamente el flujo de información en el intercambio de datos. Ha sido un reto para cumplir con la protección de datos, importante sobre todo por la pluralidad de intervinientes como podría ser una compañía multinacional (departamentos internos, proveedores, autoridades sanitarias autonómicas y estatales)".

Añadió que para garantizar que se realizaba el intercambio correctamente, se debían tener en cuenta los principios de la protección de datos:

- Minimización (la tendencia es recoger demasiada información y esto debía evitarse).
- Transparencia (el flujo de datos no quedaba suficientemente claro).
- Deber de información (los destinatarios tampoco quedaban demasiado claros).
- Confidencialidad (complicada por el uso de diferentes canales de intercambio que dificultaron, a su vez, el análisis de riesgos para ver el canal más adecuado).

En cuanto al pasaporte verde, señaló que "para garantizar el derecho de libre circulación de las personas en la UE, el intercambio de datos se está definiendo en un reglamento que no constituye una base legal para que el receptor retenga la información (garantizando el plazo de conservación) y deja una puerta abierta a la realización de transferencias internacionales de datos con el objetivo de garantizar la corrección de los datos y las medidas de seguridad para garantizarla".

En la ronda de preguntas se habló sobre si resultaban adecuados los canales de mensajería gratuita, a lo que Falguera respondió que "se ha priorizado la agilidad y es un riesgo, ya que pueden no cumplir las medidas de seguridad adecuadas". Respecto al flujo de datos entre las entidades privadas y públicas señaló que "fue un aprendizaje continuo a medida que se iba avanzando y cada CC. AA. tenía su propio sistema".

SÉPTIMA SESIÓN: "EXPERIENCIAS DE LOS DELEGADOS DE PROTECCIÓN DE DATOS EN LOS COMITÉS DE INVESTIGACIÓN"



Jorge Prado, de DPD SERGAS, destacó que "la pandemia ha tenido gran impacto en la investigación biométrica y ha acelerado lo que se tenía previsto en este campo, aprovechándose el avance de forma eficiente. La pandemia se ha combatido con datos. El responsable (SERGAS) asumió como propias todas las investigaciones derivadas de la pandemia. Cualquier profesional que hacía un estudio relacionado con el Covid, se ha visto respaldado por la base legitimadora del interés público".

Recalcó que "no va a ser fácil volver a la normalidad, porque los estudios dejarán de verse amparados por la base legitimadora del interés público. Ningún estudio ha sido rechazado con el argumento de la protección de datos, sino por otros motivos. Hay que utilizar los datos, pero de forma anonimizada. Se ha evidenciado la necesidad de la explotación de los datos sanitarios, pero se debe ir con cuidado, porque es un tema muy complejo. Muchos promotores no son conscientes de los riesgos que asumen como responsables de un tratamiento".

El equilibrio de intereses es un reto y es muy fácil que se rompa

Francisco Campoamor, presidente del Comité de

Ética de Investigación Illes Balears puntualizó que "anteriormente la confidencialidad de las investigaciones era relativamente fácil de conseguir. Con la aparición de las nuevas tecnologías, la protección de datos ha ido complicando su cumplimiento. La mayoría de los investigadores tienen un perfil clínico, con apoyo legal, pero sin formación en la parte tecnológica. Es un reto para los investigadores con perfil clínico 'entender' el lenguaje legal o técnico". También comentó que la presencia del DPD en los Comités de Ética había reforzado la protección de datos y aportado conocimientos en la parte tecnológica, facilitando el entendimiento legal y técnico.

"Los avances tecnológicos han sido especialmente perjudiciales para los investigadores independientes, los cuales también conllevan otros peligros, como la frustración, ya que no tienen claros los conceptos legales, no tienen conocimientos respecto a la anonimización de los datos, las medidas de seguridad para protegerlos, etc. Por tanto, es fundamental la formación, así como que se faciliten las herramientas y aplicaciones con las medidas de seguridad adecuadas para cumplir con la legislación vigente en materia de protección de datos", indicó.

Hay que facilitar la vida a los investigadores

Miriam Méndez, de la Oficina DPD del Departamento de Salut de la Generalitat de Cataluña, señaló que los contenidos de los protocolos de investigación, eran difíciles de "entender" para los DPD, ya que no tenían los conocimientos clínicos adecuados. "La inquietud que se tiene en Cataluña es cómo se puede ayudar a los Comités de Investigación y/o Ética, así como a los investigadores de forma fácil y que se pueda evaluar. Han trabajado en la elaboración de unas fichas de datos que deben contener un protocolo, intentando entenderse cada uno en su "idioma", con las guías de conceptos de protección de datos, así como los procedimientos a utilizar".

Por otro lado, explicó que se había elaborado una herramienta de evaluación de impacto de Protección de Datos y también se estaba trabajando en la formación. "No se puede exigir, sin antes haber facilitado los recursos necesarios", afirmó.

"El objetivo es que los investigadores presenten al Comité de Ética proyectos con todos los elementos de cumplimiento necesarios para facilitar el trabajo al investigador. Es muy importante que el centro se dote de los recursos necesarios de almacenamiento. Por tanto, el DPD debe ser un elemento coordinativo entre el centro, el investigador, los grupos de trabajo, las autoridades, etc", explicó. Por último, advirtió que "se ha trabajado para que se tenga un criterio común en todo el territorio español, y no que cada CC. AA. tenga unas restricciones o reglas".

Vicente Lomas, de SESCAM, comentó que "la seudonimización es un reto para el investigador principal, por lo que ha diseñado un procedimiento para que realice desde los servicios de Tecnologías y Comunicación del centro responsable de los datos. Se ha elaborado un único modelo propio de contratos de ensayos clínicos, a pesar de que los laboratorios intentan incluir sus propios clausulados. El principal punto de conflicto con los laboratorios es que el centro sea el encargado del tratamiento y no el responsable del tratamiento. También resulta problemático en la transferencia de datos a otras empresas y fuera de la Unión Europea".

Joaquín Gimeno, del DPD del Servicio Aragonés de Salud, señaló que "debido a la pandemia ha sido difícil contactar con participantes de los estudios de forma presencial, por lo que se han utilizado herramientas gratuitas de Internet, con formularios en los que deben aceptar políticas de privacidad de la plataforma por parte del participante. Por ejemplo, GOOGLE te hace aceptar navegador, SO, IP, teléfonos…". Por esta razón, continuó: "se ha redactado una lista de recomendaciones para los investigadores, para que sean conscientes de los peligros (contraseñas fuertes, encriptación archivos correos electrónicos, SO y antivirus actualizados… así como un Código de Buenas Prácticas. En Aragón se está haciendo un proyecto big data de historias clínicas, anonimizadas, con la finalidad de que no accedan a datos personales, aparte de otras utilidades económicas, de gestión, etc.". Por último, argumentó que era imprescindible exigir formación a los investigadores, para que fueran conscientes de la importancia de lo que tienen entre manos.

Finalmente, tuvo lugar la Charla Magistral de Ricard Martínez con el tema "Lo que realmente importa". Durante su intervención admitió que "la analítica de datos ha venido para quedarse, van a ser comunes los estudios retrosprectivos con grandes cantidades de datos, ya que los investiga-

dores se han dado cuenta de que, con más datos, la aproximación al resultado final es más fiable. Se tienen carencias en la formación, pero no se tiene que criminalizar a los investigadores. Normalmente, los equipos de investigación bien financiados tienen un project manager y técnicos, que sería a los que habría que formar". También se debería concienciar al equipo directivo y político, para que sean conscientes de la relevancia que tienen las investigaciones. Por tanto, la formación debe ser a todos los niveles y de forma obligatoria".

También destacó que "la carencia de recursos a los que se enfrenta un investigador es un gran problema. Además hay carencia a la apertura de otros investigadores, que provoca que los investigadores hagan estudios por su cuenta. Existe una preocupación irreal por los datos que se tratan del paciente, ya que cuando nos hacen falta los datos de los pacientes, se cogen sin problemas".

Además, invitó a la reflexión, "¿quién debe cumplir con la normativa vigente de protección de datos, el centro o el investigador? El soporte legal y, sobre todo tecnológico, debe facilitarlo el centro, ya que es el responsable de los datos. A los investigadores se les debe dotar de medios. No hay criterios para escenarios por el interés común y diferentes derechos a nivel europeo. La Directiva decimoséptima permite definir repositorios controlados y garantizar ciertas condiciones con datos pseudoanonimizados, pero se tiene que sincronizar con el art. 184 del RGPD. Se dice que el paciente controla sus datos, pero ¿se ha pedido si quieren que sus datos sean utilizados para la investigación? ¿existe algún programa de donantes de datos correctamente implementado?".

CLAUSURA



Las conclusiones derivadas del Foro fueron las siguientes: en primer lugar, el sector sanitario debe afrontar muchos y diversos retos. Para ello debe haber una estrategia, pero es necesario tener los recursos necesarios. En este sentido, los fondos de recuperación son muy importantes.

Los equipos directivos de los centros se dieron cuenta de la importancia de la ciberseguridad. Por esta razón, hay que ver a la pandemia como una oportunidad, pero no hay que actuar a causa del miedo, sino porque es necesario.

También es crucial compartir información y estar coordinados con las plataformas nacionales de intercambio y los SOC's sectoriales. Además, la visibilidad en la organización es importante para poder combatir y protegerse ante los incidentes. En este proceso es imprescindible la colaboración público-privada.

En el foro se pusieron de manifiesto los retos y deberes para los DPD en investigación. Se concluyó que la seguridad debe verse como un medio de transformación, no como un medio de defensa. Por último, se incidió en la necesidad de formar a los usuarios, equipos directivos, investigadores, etc.

XXIV Congreso Nacional de Informática de la Salud

Infors@lud 2021

Lema "La Evolución del ecosistema digital en Salud"

MADRID, 21, 22 Y 23 DE JUNIO

HOTEL NH COLLECTION MADRID EUROBUILDING



INTRODUCCIÓN Y OBJETIVOS

El XXIV Congreso Nacional de Informática de la Salud bajo el lema "La evolución del ecosistema digital en Salud".

Durante el último año hemos sido todos actores y espectadores de un nuevo escenario mundial ante la situación creada por la pandemia reduciendo el contacto físico y teniendo que aumentar la capacidad de prestación servicios sanitarios , ante una demanda urgente desbordada. Esto ha cambiado radicalmente la forma de trabajo de todos los profesionales y la relación con los pacientes.

Los procesos de gestión de los Servicios de Salud intentan dotarse con un soporte digital lo más amplio posible que garantice la disponibilidad de toda la información y la integración de todos ellos. Actualmente hemos aterrizado en el "teletrabajo" y en soportes para las nuevas necesidades de los profesionales tanto en el ámbito de la gestión como en el ámbito clínico. Otro de los puntos fuertes del cambio en nuestro "ecosiste-

ma digital" es el vuelco que se ha dado en el ámbito sociosanitario con la transformación digital de sus servicios que pasan a estar directamente conectados con los servicios sanitarios propiamente dichos.

Los comités organizador y científico aceptamos la responsabilidad de poner en valor todo lo anterior y hemos trabajado para ofrecer un Congreso donde compartir, formar, desarrollar y acompañar a todos los profesionales en este nuevo escenario en que nos movemos.

El programa del Congreso incluye sesiones de debate con relevantes ponentes implicados en este cambio. Además, se considera imprescindible recoger las experiencias de los investigadores y profesionales, en sesiones específicas para su participación, en forma de comunicaciones (orales o en formato poster) y proyectos innovadores. Dentro del Congreso se recogen también sesiones dedicadas a las TIC en Farmacia (INFORFARMA) y en Enfermería. También se destaca la atención que se presta a las fuentes de financiación para salud digital y las sesiones de la Plataforma de Innovación.

Por todo ello, INFORSALUD 2021 es una cita imprescindible para todos los interesados en el sector de las TIC en Salud y en su contribución a la transformación sanitaria para la mejora de la calidad y a la eficiencia de los sistemas sanitarios.

PROGRAMA PRELIMINAR

Lunes 21 de junio	16.00 - 16.30	Recogida de Documentación		
		SALA 1	SALA 2	SALA 3
	17.00 - 18.00	Sesión de Apertura de Autoridades Sanitarias		
	18.00 - 18.30	Visita Oficial Área Exposiciones		
	18.30 - 19.30	Sesión Debate "La evolución del ecosistema digital en Salud"		
	19.30 - 20.00	Inauguración Oficial		
Martes 22 de junio	09.30 - 11.00	Sesión Debate 1 "Una nueva era digital en la Salud Pública"	Sesión Tecnológicas 1	Sesión de Comunicaciones 1
	11.00 - 11.30	Café y VisitaÁrea de Exposiciones		
	11.30 - 13.00	Sesión Debate 2 "La transformación Digital en la coordinación entre servicios sanitarios y servicios sociales"	Sesión Tecnológicas 2	Sesión de Comunicaciones 2
	13.00 - 14.30	Sesión Debate 3 "Los recursos humanos sanitarios y las nuevas necesidades digitales"	Sesión Tecnológicas 3	Sesión de Comunicaciones 3
	14.30 - 16.00	Descanso		
	16.00 - 17.30	Sesión Debate 4 "Poniendo el foco en el ciudadano"	Sesión Tecnológicas 4	Sesión de Comunicaciones 4
	17.30 - 18.00	Presentación de Posters Área de Exposiciones		
	18.00 - 19.30	Sesión Debate 5 "Financiación y gobernanza de los proyectos de salud digital en España "	Sesión Tecnológicas 5	Sesión de Comunicaciones 5
	20.00	Cocktail Área de Exposiciones		
Miércoles 23 de junio	09.30 - 11.00	Mesa Redonda Plataforma de Innovación "Financiación de la Innovación"	Sesión Tecnológicas 6	Sesión de Comunicaciones INFORFARMA
	11.00 - 11.30	Café y visita Área de Exposiciones		
	11.30 - 13.00	Mesa Redonda INFORFARMA "Adaptaciones tecnológicas en farmacia a raiz del COVID19"	Mesa Redonda Enfermería	Sesión Tecnológicas 7
	13.00 - 14.30	Sesión de Autoridades	Sesión Debate INFORFARMA "Avances en los sistemas de información de farmacia"	
	14.30 - 16.00	Descanso		
	16.00 - 17.30	Sesión Debate 6 "Haciendo realidad el valor de los datos"	Proyectos Innovadores 1	Sesión de Comunicaciones 6
	17.30 - 19.00	Sesión Debate 7 "¿Cómo integrar la antención no presencial en los modelos asistenciales?"	Panel Inteligencia Artificial	Proyectos Innovadores 2
	19.00	Clausura y Entrega de Premios		

FORO DE
SALUD CONECTADA

Coordina: **Óscar Moreno**

Acuerdo sobre la propuesta de la Comisión relativa al Certificado COVID Digital de la UE

El 17 de marzo de 2021, la Comisión Europea presentó una propuesta para crear un certificado COVID de la UE con el que facilitar la circulación libre y segura de la ciudadanía dentro de la UE durante la pandemia de COVID-19. A petición de la Comisión, el Parlamento votó a favor de la activación del procedimiento de urgencia para las dos propuestas el 25 de marzo. El Consejo adoptó su posición de negociación el 14 de abril, y el Parlamento lo hizo el 29 de abril.



Imagen de NakNakNak en Pixabay

Paralelamente al proceso legislativo, ya se estaban realizado avances importantes en los aspectos técnicos. La pasarela de la UE, que permite verificar los certificados a través de las fronteras, está lista y empezará a funcionar en junio. Durante las dos últimas semanas de mayo se han llevado a cabo pruebas piloto en diecisiete Estados miembros e Islandia, y otros cinco Estados miembros realizarán pruebas la última semana de mayo.

La Comisión también proporciona software de referencia de código abierto para ayudar a los Estados miembros a desarrollar su solución nacional para expedir certificados, escanear y comprobar los códigos QR, así como una cartera de referencia para su almacenamiento.

Anteriormente, el 21 de abril, los representantes de los Estados miembros habían adoptado unas directrices de especificaciones técnicas en la red de

sanidad electrónica, una red voluntaria que conecta a las autoridades nacionales responsables de la sanidad electrónica. Dichas directrices son el producto de la estrecha labor de la Comisión con los Estados miembros, que dio lugar a unas primeras directrices adoptadas en enero y actualizadas el 12 de marzo, y a un marco de confianza acordado el 12 de marzo de 2021. Además, en la red de sanidad electrónica se desarrolló una plantilla de diseño común.

La información más reciente facilitada por los Estados miembros sobre las medidas contra el coronavirus y las restricciones de viaje está disponible en la plataforma Re-Open EU.

Pero a 20 de mayo la Comisión acoge con satisfacción el acuerdo político provisional alcanzado entre el Parlamento Europeo y el Consejo sobre el Reglamento que regulará el Certificado COVID Digital de la UE. Esto significa que el certificado (anteriormente denominado «certificado verde digital») podría estar listo a finales de junio, según lo previsto. Este acuerdo se ha alcanzado en un tiempo récord, solo dos meses después de la propuesta de la Comisión.

Según palabras de la presidenta Ursula von der Leyen: «*Estamos cumpliendo nuestro compromiso de poner en marcha el Certificado COVID Digital de la UE antes del verano. La ciudadanía de Europa está deseando volver a viajar de nuevo, y el acuerdo alcanzado hoy les permitirá hacerlo en breve con total seguridad.*

El Certificado COVID Digital de la UE es gratuito, seguro y accesible a toda la población. Abarcará la vacunación, los tests y la recuperación, ofreciendo diferentes opciones a la ciudadanía y respetando plenamente sus derechos fundamentales, incluida la protección de los datos personales.

Toda la ciudadanía de la Unión tiene el derecho fundamental a la libre circulación en la UE. El Certificado COVID Digital de la UE, disponible en papel o en formato digital, facilitará los desplazamientos en Europa para que las personas puedan ir a ver a sus familias y a sus seres queridos o para que puedan disfrutar del merecido descanso».

Las principales características del Certificado COVID digital de la UE son:

- abarcará la vacunación, los tests y la recuperación;
- estará disponible en formato digital y en papel, dependiendo de la elección de cada persona destinataria, e incluirá un código QR firmado electrónicamente;
- será gratuito, fácil de obtener y también podrán disponer de él las personas vacunadas antes de la entrada en vigor del Reglamento que lo regule;
- los Estados miembros también lo podrán utilizar con fines nacionales, en función de sus respectivas legislaciones;
- los Estados miembros se abstendrán de imponer restricciones adicionales de viaje a las personas titulares de un Certificado COVID Digital de la UE, a menos que dichas restricciones sean necesarias y proporcionadas para salvaguardar la salud pública;
- la Comisión también movilizará 100 millones de euros para proporcionar tests asequibles a los Estados miembros.

El Parlamento Europeo y el Consejo deben adoptar ahora formalmente el acuerdo político. El Reglamento entrará en vigor el 1 de julio, con un período de introducción progresiva de seis semanas para la expedición de certificados en aquellos Estados miembros que necesiten más tiempo.

Paralelamente, la Comisión seguirá apoyando a los Estados miembros a la hora de ultimar sus soluciones nacionales para la expedición y verificación de los Certificados COVID Digitales de la UE, y prestará apoyo técnico y financiero a los Estados miembros para que se integren en la pasarela de Internet

Más información:

- Comisión Europea – Noticias – Certificado Digital Verde (Marzo) - https://ec.europa.eu/commission/presscorner/detail/en/ip_21_1181
- COVID-19: Certificado Digital Verde – https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/covid-19-digital-green-certificates_en
- Comisión Europea – Noticias - https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2593
- Plataforma Re-Open EU - https://reopen.europa.eu/en

Uso de la IA en las Enfermedades más Recurrentes

Pilar Ruiz Ayuso
Consultora en Transformación Digital e Inteligencia Artificial en Ibermática Digital

INTRODUCCIÓN

En el artículo anterior, se explicó cómo la IA, juega un papel importante para la detección del cáncer de mama, y que se presentan ciertos retos tecnológicos importantes, que habrá que tener en cuenta, y serían los siguientes:

- El uso de herramientas como por ejemplo ontologías, árboles de decisión, etc, son clave para estructurar bien el know-how, debido a que el conocimiento que un patólogo posee sobre un diagnóstico es difícilmente transferible.
- La intervención humana genera demoras de tiempo, que podrían evitarse en gran medida si se dispusiese de una arquitectura orientada a servicios interoperables orquestada de forma conveniente.

Cardiopatía isquémica en cifras

Según la OMS (Organización Mundial de la Salud), las Estadísticas Sanitarias Mundiales de 2019, apuntaba que actualmente, la cardiopatía isquémica, es la principal causa de muerte a nivel mundial, y ahora está ocasionando más muertes que nunca. Las cifras se han incrementado exponencialmente en 20 años, de 2 millones de muertes a casi 9 millones.

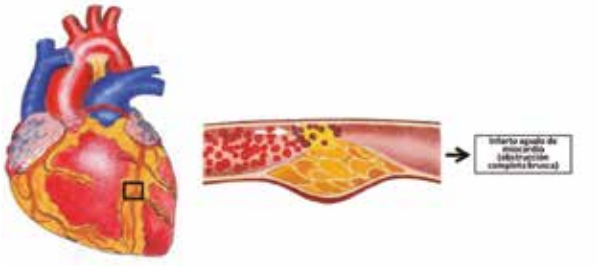
Actualmente, el dolor torácico no traumático, es uno de los motivos más frecuentes de ingreso en las urgencias generales a nivel mundial con cifras superiores al 35%. Siendo además un síntoma que suscita inquietud entre los profesionales sanitarios, por el amplio abanico de posibilidades diagnósticas que conlleva.

¿Qué son las cardiopatías isquémicas y de qué medios se disponen para su detección?

La cardiopatía isquémica es producida cuando la sangre tiene dificultad para pasar por las arterias coronarias, y por lo tanto, oxígeno y alimento al corazón, y la consecuencia en la mayor parte de las ocasiones, es debido a una obstrucción del paso de la sangre a través de las arterias coronarias debido a unas placas de grasa llamadas ateromas, que se producen en enfermedades como la arteriosclerosis.

La dificultad en el diagnóstico de este síntoma, radica en que el dolor torácico puede deberse a una enfermedad banal o ser la expresión de un proceso potencialmente mortal. Además, la intensidad del dolor y su expresión es totalmente subjetiva y los síntomas son percibidos de maneras muy diferentes por los pacientes.

Una gran parte de los esfuerzos diagnósticos realizados por los profesionales para el dolor torácico en el servicio de urgencias, se encamina a detectar síndromes coronarios agudos (SCA), ya que tiene consecuencias muy diferentes en relación al tiempo necesario para diagnosticarlas y tratarlas. En cuanto a esta patología es vital tratarla en los primeros 90 minutos para disminuir su mortalidad y consecuencias fatales posteriores al infarto.



Síndrome coronario agudo

Actualmente la determinación del riesgo y el diagnóstico se realiza siguiendo unas guías clínicas, como por ejemplo las desarrolladas por el American College of Cardiology (ACC). Estas guías se crearon para dar solución a un entorno de urgencias donde el tiempo es muy limitado, y por ello, en el triaje inicial con el paciente, se preguntan ciertas cuestiones, y se complementa con ciertas pruebas básicas para determinar un diagnóstico.

Lamentablemente, al tener un número acotado de parámetros a los que referenciarse, y al perder una perspectiva comparada, ya que el diagnóstico de un paciente es hecho de manera individual y es el profesional sanitario quien en base a las variables y mediante su juicio clínico global basado en su experiencia personal, es el que realiza un diagnóstico comparativo con situaciones en la que él ha estado involucrado en el pasado, pueden pasar inadvertidos casos que si no tienen una atención primaria urgente, hay un alto riesgo de mortalidad.

Aplicando la Inteligencia Artificial en casos de uso reales

Ante la situación en la que únicamente se pueden utilizar un numero acotado de variables, y ya que en la Historia Clínica Electrónica (HCE) del paciente, se almacenan múltiples informaciones, potencialmente importantes, pero que, en la actualidad, aunque cubren la inmensa mayoría de casuísticas, dejan fuera algunos casos, y en esos casos, se desconoce si hay variables importantes que no se están usando, por lo cual, no se están utilizando.

Actualmente, se están desarrollando proyectos de investigación enfocadas al uso de ciertas variables subjetivas, donde mediante la aplicación de algoritmos de IA, ayuden tanto a la objetivación de información, como a descubrir conocimiento oculto en los datos (como por ejemplo qué variables, rangos dentro de ellas o correlaciones ofrecen un mejor diagnostico).

Estos sistemas de apoyo al diagnóstico clínico en urgencias, serán la base para:

- Explotar la información de la Historia Clínica Electrónica (HCE) de los pacientes, que mediante los modelos de extracción de conocimiento a través de técnicas de machine learning, que establecerán reglas de predicción diagnóstica (RPD) de EAC (Enfermedad Arterial Coronaria),y tratamiento de las imágenes patológicas, podrán predecir los diferentes posibles diagnósticos cardiacos, ofreciendo así un Soporte a la Decisión Clínica *in situ,* pudiendo reducir los tiempos en hospitales de primera línea hasta de un 20%. Actualmente, las cifras son cercanas a las 7 horas, ya que en aquellos casos que no existe certeza, tienden a quedarse los pacientes en observación, destinando una serie de recursos y esfuerzos que finalmente no lo van a necesitar.
- Explorar la información obtenida mediante sistemas de Visual Analytic, que permitirán, mediante modelos de *machine Learning,* buscar como optimizar el proceso asistencial con mejores prácticas. Gracias a estos sistemas, se podrá ofrecer información que permita adecuar los ingresos hospitalarios, buscando minimizar tanto los falsos negativos (pacientes con patología no detectada), con el riesgo consecuente reduciéndolos a niveles entre el 0-1% y los falsos positivos (pacientes ingresados que no debieron serlo), ya que el coste promedio un día de ingreso en la planta de cardiología, sin la solicitud de pruebas complementarias es bastante elevada.

Retos tecnológicos para el desarrollo de soluciones aplicados a la cardiopatía isquémica

Para asumir los retos tecnológicos a los que nos enfrentamos en el desarrollo de diagnóstico de una patología isquémica aguda, hay que tener en cuenta varios puntos:

- Para hacer uso de algoritmos y modelos de *machine learning* que permita agilizar el diagnóstico de la cardiopatía isquémica se necesita desarrollar soluciones con una arquitectura, bajo el paradigma *Big Data*, que busque cubrir los gaps que las actuales plataformas de Historia Clínica Semántica tienen, como problemas con el tratamiento de las imágenes patológicas, el texto escrito en lenguaje natural, o modelos matemáticos eficientes en un área con tanta diversidad como la de la salud humana.
- En la actualidad la interpretación de los electrocardiogramas (ECGs) se hace por profesionales altamente entrenados, que no siempre se encuentran disponibles en la urgencia. Por otro lado, la tarea de clasificación de señales ECG es una tarea de alta complejidad, ya que existe variabilidad de formas de latido de un mismo tipo entre dos pacientes, por lo que es una tarea que requiere mucho tiempo para realizar un diagnóstico basado en los patrones que caracterizan los latidos normales o anormales, por lo que habrá que desarrollar algoritmos de *DeepLearning* y redes neuronales para ofrecer un soporte al diagnóstico que complemente la experiencia de los profesionales de la urgencia, minimizando el nivel de falsos positivos.
- Gran parte de la información almacenada en la Historia Clínica Electrónica (HCE), como los antecedentes personales, el evolutivo, etc. está escrita en lenguaje natural y por lo tanto ni codificada, ni explotable por los sistemas de *Machine Learning.* Esta práctica hace que cuando se requieran más datos para realizar una investigación, sea necesario una codificación manual. Para poder extractarla, hay que aplicar tecnologías del Procesamiento del Lenguaje Natural (NLP) para extractar la información relevante de los historiales clínicos disponible en la HCE, de una forma automática para hacer factible su uso en proyectos de analítica de datos en el sector salud.

En conclusión, vemos que urgencias, es un ámbito muy especial, con múltiples especialidades, distintos tipos de experiencia, y en el que el tiempo es un factor determinante, con lo que no se pueden emplear de manera extensiva estrategias de comités que decidan de los casos diferentes, por ello, es vital hacer uso de sistemas de apoyo que mediante la IA, realicen una predicción diagnóstica en aquellos casos que sean más dudosos, y se sumen a las habilidades de los humanos, para poder mejorar la asistencia y la confianza en los programas de detección de dicha patología.

FORO DE
INTEROPERABILIDAD

Coordina: **Adolfo Muñoz Carrero**

Arquetipos de referencia definidos en la parte 3 de **UNE-EN ISO 13606:2020** (I)

Según la norma UNE-EN ISO 13606, un arquetipo, algunas veces conocido como modelo clínico, especifica un patrón para representar un aspecto de la documentación clínica (un concepto). Para ello, define restricciones al modelo de referencia (estableciendo cardinalidades, nombres y códigos) de las clases del modelo de referencia. Ante la infinidad de posibilidades que existen, en la parte 3 de la norma se especifican algunos arquetipos, llamados "de referencia" para modelar partes de un extracto de la HSE con el fin de proporcionar cierta previsibilidad en cuanto a la forma en que la información de salud está representada en el extracto. Estos arquetipos de referencia pueden actuar como base de partida para crear conjuntos de arquetipos más especializados y dependientes de cada entorno, pero al estar basados en esta base común, es más probable que estén alineados semántica y estructuralmente, lo que facilitaría la interoperabilidad semántica.

En una anterior entrega de esta sección (ver el número 143) se presentaron algunos de esos arquetipos relacionados con la información demográfica, pero la parte 3 incluye varias categorías más:

- Arquetipo para *Null_flavor (ELEMENT)*: debe ser incluido en cualquier arquetipo para el que se prevea que algunas de sus instancias puede tener información faltante o no disponible. Se complementa con la lista de términos (sin información, inválido, desconocido, enmascarado, no aplicable) para describir la falta de un dato.
- Arquetipo para la política de acceso (*COMPOSITION)*: debe usarse para comunicar las políticas de acceso a los datos de acuerdo con la parte 4 de la norma.
- Arquetipos de referencia para entidades demográficas (que ya se vieron en esta sección en el número 143 de la revista)
- Arquetipos de referencia para medicamentos: identificación de los elementos de datos y de datos descriptivos de medicamentos basados en la norma ISO IDMP (compuesta por las normas ISO, 11238, 11239, 11240, 11616 y 11615). La especificación del arquetipo de referencia en este caso se deriva del correspondiente modelo clínico detallado y está compuesto por el arquetipo raíz para el medicamento (*Medicinal Product)* y las 4 secciones que lo componen: ingrediente *(Ingredient)*, producto farmacéutico *(PharmaceuticalProduct)*, medicamento regulado *(RegulatedMedicinalProduct)* y medicamento empaquetado *(PackagedMedicinalProduct)*.
- Arquetipos de referencia para la especificación de la información clínica: los arquetipos definidos en esta categoría (*Health Condition, Healthcare Activity Element, Clinical Context, Activity Management, Association, Consideration, Dosage y Method)*, se basan en las estructuras de información clínica de referencia que se describen en otro apartado de la norma y que se han desarrollado basándose en la definición de estos conceptos que se dan en la norma UNE-EN ISO 13940 (CONTSYS), añadiéndose, además, algunos atributos adicionales para la armonización con recursos FHIR.

Dada la utilidad que pueden tener para la el desarrollo de los arquetipos clínicos, en una entrega posterior de esta sección se analizarán las estructuras de información clínica de referencia que se definen en el apartado 12 de la parte 3 de la norma.

Los arquetipos de referencia pueden descargarse en **http://en13606.org/specifications.html**.

INFORMÁTICA **MÉDICA**

Coordina: **José Sacristán**

Obtención de certificados electrónicos cualificados sin necesidad de personación física en una oficina de registro

Se ha publicado en el BOE del 14 de mayo, la Orden ETD/465/2021, de 6 de mayo, por la que se regulan los métodos de identificación remota por vídeo para la expedición de certificados electrónicos cualificados.

Esta Orden, en aplicación del artículo 7.2 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza(Abre en nueva ventana) , determina las condiciones y requisitos técnicos de verificación de la identidad a distancia y, si procede, de otros atributos específicos de la persona solicitante de un certificado cualificado, mediante otros métodos de identificación como videoconferencia o vídeo-identificación que aporten una seguridad equivalente en términos de fiabilidad a la presencia física.

Se dota así al ordenamiento jurídico español, de una norma específica que permitirá a los prestadores de servicios electrónicos de confianza utilizar esta ventaja competitiva en la provisión de sus servicios, y que les habilitará a identificar de forma remota por vídeo a los solicitantes de certificados cualificados, de forma que puedan seguir expandiendo su actividad y competir con los prestadores establecidos en otros países que ya disponen de una normativa nacional a tal efecto.

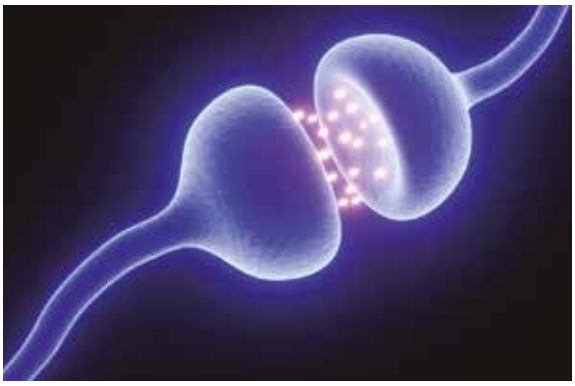
El sistema de identificación remota por vídeo empleado en el proceso deberá incorporar los medios técnicos y organizativos necesarios para verificar la autenticidad, vigencia e integridad de los documentos de identificación utilizados, verificar la correspondencia del titular del documento con el solicitante que realiza el proceso, mediante tecnologías como el reconocimiento facial, y verificar que este es una persona viva que no está siendo suplantada; debiendo quedar todos estos requisitos acreditados, en los términos que establece el anexo F11 de la Guía de Seguridad de las TIC CCN-STIC-140(Abre en nueva ventana), del Centro Criptológico Nacional mediante la certificación del producto.

https://administracionelectronica.gob.es/pae_Home/pae_Actualidad/pae_Noticias/Anio2021/Mayo/Noticia-2021-05-14-Obtencion-certificados-electronicos-cualificados-sin-necesidad-de-personacion-fisica.html#.YKyTfTztb3g

Crean el primer cerebro electrónico que aprende como el humano

Por primera vez en la historia, un grupo de científicos ha logrado crear una máquina que aprende como el cerebro humano, utilizando unos nuevos componentes que actúan igual que las sinapsis.

Este descubrimiento supera las limitaciones de los ordenadores actuales para procesar información compleja y abre la puerta a una revolución en el mundo de la computación neuromórfica, donde el objetivo es emular la increíble capacidad de proceso del cerebro humano con el mismo bajo coste energético.



https://www.elconfidencial.com/tecnologia/novaceno/2021-04-30/cerebro-neuronas-ciencia-computadoras_3059171/

SECTOR DE
ENFERMERÍA

Coordina: **Inmaculada Moro**

Gestión del Cuidado Basada en Datos

Lucia Garate Echenique
Coordinadora Líneas Estratégicas Subdirección de Enfermería. Dirección General de Osakidetza.

Los centros sanitarios son organizaciones de gran complejidad. Generalmente, las instituciones sanitarias son grandes en cuanto a lo geográfico y lo humano. Atienden una gran variedad de procesos, y de una altísima especificidad. Deben responder de modo preciso, diligente y eficaz a la importante demanda, y su hacer tiene un enorme impacto en la economía, calidad de vida y resultados en salud de la sociedad.

Estas características nucleares hacen que cualquier decisión, respecto de su orientación o funcionamiento, tenga importantes consecuencias que deben ser adecuadamente previstas, medidas y evaluadas.

Clásicamente las organizaciones sanitarias se han evaluado de acuerdo a indicadores de actividad. Estos indicadores son herramientas muy válidas para medir la producción, respondiendo bien a preguntas de cuánto hacemos (nº de consultas, nº de altas, nº de partos, nº urgencias, nº de domicilios, nº de vacunas…). Su combinación con un enfoque poblacional que evalúe la actividad destinada a grupos específicos (mujeres, pacientes crónicos complejos, con índices socioeconómicos más desfavorecidos…), permite sin embargo un análisis más rico en cuanto a características de las poblaciones atendidas, accesibilidad y equidad, ayudando a la reorientación de los servicios hacia la perspectiva de dar más a quién más necesita o más puede beneficiarse.

Desde hace ya algunas décadas, también se han ido incorporado y desarrollando indicadores de calidad asistencial como son las encuestas de satisfacción o resultados clínicos. Por ejemplo, % de infección de heridas quirúrgicas, reingresos, mortalidad, o los más clásicos en relación a la práctica enfermera de incidencia de úlceras por presión e incidencia de caídas. Resulta una obviedad, y aun así creo que conviene recordar, que solo podemos obtener datos de los datos que registramos, y hoy añadiría, de los datos que registramos informáticamente.

La evolución de la historia clínica electrónica, en la que podemos recoger todo tipo de diagnósticos, intervenciones, dispositivos y heridas, y valoración de las diferentes dimensiones física, emocional y social con fechas de aparición, evolución, curación… permite a su vez la explotación de estas circunstancias, pudiendo reorientar las estrategias y los planes hacia áreas concretas que resultan más efectivas en la generación de salud. Por mencionar algunos ejemplos, es posible analizar el tiempo de curación de los diferentes tipos de heridas, el % de lactancia materna exclusiva hasta los 6 meses, o el % de personas que no cuentan con una persona cuidadora aunque la necesiten, y dirigir acciones de mejora a la información nutricional de familias, formación a los profesionales, o activación de los agentes sociales de la comunidad. Una mirada de futuro cercano, además nos hace vislumbrar que la medición de aportación enfermera a la evaluación del grado de consecución de los objetivos esperados del paciente (NOC) y la participación enfermera en la codificación CIE con síntomas o situaciones de salud (Z91.5 Falta de cumplimiento del paciente al tratamiento, Z60 Problemas relacionados con entorno social…), será clave en la reorientación de las políticas y estrategias sanitarias hacia el cuidado.

Pensar, trabajar y destinar recursos y esfuerzos al área de explotación y análisis de información es una clave fundamental para sostener, adecuar y mejorar los servicios sanitarios y el cuidado. Si bien, esta área, cobra su mayor sentido y utilidad cuando los análisis son compartidos con todos los agentes que deben movilizarse para el cambio.

SECTOR DE
FARMACIA

Coordina: **Comité Tecnológico de Farmacia de la SEIS**

Inforfarma: próxima jornada dirigida a la Farmacia en el Congreso de Inforsalud 2021

Angela Smits Cuberes. Luz Fidalgo Garcia, Ana Teresa Lopez Navarro, Alberto Gómez Lafón

EN EL MOMENTO ACTUAL, Y DE FORMA CONCRETA EN ESTOS ÚLTIMOS MESES CON LA EMERGENCIA SANITARIA MUNDIAL DESENCADENADA POR LA PANDEMIA DEL COVID-19, EL CAMPO DE LA INFORMÁTICA DE LA SALUD SUPONE UNA HERRAMIENTA IMPRESCINDIBLE PARA PERMITIR ADAPTAR LA ATENCIÓN FARMACÉUTICA DE LOS PACIENTES TANTO A NIVEL HOSPITALARIO COMO EN LA ATENCIÓN PRIMARIA, MANTENIENDO SIEMPRE LAS GARANTÍAS DE CALIDAD Y SEGURIDAD EN EL CUIDADO DEL PACIENTE Y MAXIMIZANDO LOS RESULTADOS EN SALUD.



Imagen de Jukka Niittymaa en Pixabay

Bajo esta premisa, el Comité Tecnológico de Farmacia de la Sociedad Española de Informática de la Salud ha organizado INFORFARMA, un espacio propio en el próximo Congreso de INFORSALUD, en el que los expertos de nuestro país en informática de la salud aplicada al ámbito farmacéutico se reunirán para compartir proyectos, estrategias implementadas para hacer posible la atención farmacéutica y soluciones encontradas ante la crisis de la COVID-19.

Para ello, se ha organizado una mesa de comunicaciones en la que se expondrá una selección de las 10 comunicaciones más interesantes recibidas relacionadas con la farmacia y la tecnología; también incluirá una mesa de debate y una mesa monográfica centradas de forma exclusiva en la aportación farmacéutica a las tecnologías de información y comunicación (TICs), que tendrán lugar el 23 de junio, en el seno del Congreso de Inforsalud.

La mesa monográfica, bajo el título "Adaptaciones tecnológicas en farmacia a raíz del COVID19",

> ***La asistencia a INFORFARMA ofrece una oportunidad única para conocer, contrastar y debatir nuevos proyecto en el ámbito de las TICs farmacéuticas, con un elenco de los mejores profesionales que reflejarán las posibilidades de la Informática de la Salud en la atención farmacéutica"***

será moderada por la Directora General de Cartera Común de Servicios del Sistema Nacional de Salud y Farmacia (DGCCSF), Doña Patricia Lacruz Gimeno, y consistirá en un entorno de puesta en común y discusión respecto a los cambios tecnológicos en farmacia desarrollados debido a la pandemia. Los invitados a esta mesa incluirán a representantes de todas las áreas de farmacia: Doña Mireia Massot, farmacéutica de Atención Primaria en el Institut Català de la Salut, que expondrá las adaptaciones llevadas a cabo en centros sociosanitarios como consecuencia de la pandemia por la COVID-19. En representación de las Consejerías de Sanidad de las Comunidades Autónomas participará Don Felipe Santana, responsable del Servicio de Informática del Área de Salud de Gran Canaria, que nos presentará un sistema de seguridad para la dispensación de la medicación en las oficinas de farmacia, basada en el sistema "One Time Password"; y con Cristina Agudo, jefa del Servicio de Prestaciones Farmacéuticas del Servicio Navarro de Salud. Por parte de la Farmacia Comunitaria participará Don Cecilio Venegas, presidente del Colegio Oficial de Farmacéuticos de Badajoz y miembro de la Real Academia Nacional de Farmacia del Instituto de España, que presentará el desarrollo tecnológico de aplicaciones de *Big Data*. Se contará a su vez con Don Luis Margusino, facultativo especialista adjunto del Servicio de Farmacia Hospitalaria del Hospital de A Coruña, que compartirá el proyecto desarrollado de atención farmacéutica no presencial al paciente externo, a través de la telefarmacia.

La mesa de debate, titulada "Avances en los sistemas de información de farmacia", será moderada por Doña Nieves Martín Sobrino, Directora Técnica de Asistencia Farmacéutica de la Gerencia de Salud de Castilla y León; y tendrá como objetivo analizar los nuevos desarrollos, bases de datos y sistemas de información del ámbito farmacéutico. Los ponentes invitados a esta mesa pertenecen también a diversos entornos: Doña Maria Dolores Fraga, Subdirectora de la DGCCSF, compartirá el proyecto Valtermed desarrollado en el Ministerio de Sanidad. José Manuel Simarro, jefe de la División de Sistemas de Información de la Agencia Española de Medicamentos y Productos Sanitarios (AEMPS), informará de los avances en el proyecto BIFAP, la base de datos informatizada de registros médicos de Atención Primaria para la realización de estudios farmacoepidemiológicos de la AEMPS. La mesa contará además con la presencia de un representante de la Autoridad Independiente de Responsabilidad Fiscal (AIReF), para debatir los posibles puntos débiles encontrados en el último informe *Spending Review* para contener el gasto hospitalario; con Caridad Pontes, gerente del Área del Medicamento del Servei Català de la Salut, que expondrá las ventajas de las acuerdos de riesgo compartido en el sistema de financiación de nuevos medicamentos y con Iñaki Betolaza., director de Farmacia del Departamento de Salud del Gobierno Vasco, que compartirá los avances desarrollados en el País Vasco en los sistemas de prestación farmacéutica. En esta mesa debate también participara la Industria Tecnológica especializada en farmacia.

La asistencia a INFORFARMA ofrece una oportunidad única para conocer, contrastar y debatir nuevos proyecto en el ámbito de las TICs farmacéuticas, con un elenco de los mejores profesionales pertenecientes, entre otros, a los Servicios Centrales de Atención Primaria y de Atención Especializada de las Consejerías de Salud de las Comunidades Autónomas, al Ministerio de Sanidad, al Consejo General de Colegios Farmacéuticos y a la Industria Farmacéutica; que reflejarán el amplio abanico de posibilidades de la Informática de la Salud en la aplicación de la atención farmacéutica.

AGENDA 2021

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

XXVI ENTREGA PREMIOS NACIONALES DE INFORMÁTICA Y SALUD

Fecha: 8 de julio - Madrid

XVIII FORO DE SEGURIDAD Y PROTECCIÓN DE DATOS DE SALUD

Fecha: 19 y 20 mayo - Oviedo

XXIV CONGRESO NACIONAL DE INFORMÁTICA DE LA SALUD "INFORSALUD"

Fecha: 21, 22 y 23 junio - Madrid

XIX REUNIÓN DE SALUD CONECTADA

Fecha: 22 y 23 de septiembre- Gerona

XXVIII JORNADAS NACIONALES DE INNOVACIÓN Y SALUD EN ANDALUCÍA

Fecha: 20, 21 y 22 octubre - Málaga

XI FORO PARA LA GOBERNANZA DE LAS TIC EN SALUD

Fecha: 24 y 25 noviembre - León

VII MASTER EN DIRECCIÓN DE SISTEMAS Y TICS PARA LA SALUD

Fecha: noviembre-octubre 2020-2021



8ª edición

MÁSTER EN DIRECCIÓN DE SISTEMAS Y TIC PARA LA SALUD Y EN DIGITALIZACIÓN SANITARIA

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

DIRIGIDO A:

* Directivos y gestores de las Administraciones autonómicas y estatales en el área de Salud
* Directivos y gestores de organizaciones privadas aseguradoras o proveedoras de servicios de salud
* Responsables de unidades vinculadas con la informática, comunicaciones y sistemas de información (CIOs) de Hospitales y otras organizaciones públicas y privadas proveedoras de servicios sanitarios y sociales
* Profesionales sanitarios que deseen ampliar conocimientos especificos en TIC para la salud
* Gestores de proyectos de TIC para la salud en empresas consultoras
* Directivos y profesionales de empresas tecnológicas proveedoras de herramientas, servicios y soluciones TIC en Salud
* En general profesionales que deseen desarrollar su carrera en la dirección y gestión TIC para la Salud

PROGRAMA

A1: Marco de Referencia y Bases de las TIC en Sanidad
A2: Gestión Directiva de las TIC en Salud
A3: Las TIC en el Sistema Sanitario
A4: Tecnologías y Soluciones TIC en Salud
TFM: Trabajo fin de Master

Comienzo: noviembre 2021

Plazo de Matriculación: Hasta el 15 de octubre de 2021

EQUIPO DOCENTE

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

Duración: 1 año académico (60 ECT´s) y por trabajo fin de master y otras actividades)

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

Becas y Ayudas

Se ofrecen una serie de becas y ayudas económicas para facilitar el acceso a la realización del Máster:

- Becas SEIS, destinadas a los socios de la SEIS (de acuerdo con las normas establecidas por la Sociedad)
- Bonificaciones para alumnos pertenecientes al Sistema Nacional de Salud
- Bonificaciones de la Fundación Tripartita Para la Formación en el Empleo, dirigidas a trabajadores asalariados y otros colectivos que coticen en concepto de formación profesional. Quedan excluidos los trabajadores de la Administración Pública.(http://www.fundaciontripartita.org/Pages/default.aspx)

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

GOBIERNO DE ESPAÑA · MINISTERIO DE SANIDAD · MINISTERIO DE CIENCIA E INNOVACIÓN · Instituto de Salud Carlos III · SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

Para más información e inscripción consultar www.seis.es y a través de masterdstics@seis.es