NÚMERO
149

I+S

ABRIL
2022

REVISTA DE LA SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

ESPECIAL

# PROTECCIÓN DE DATOS Y CIBERSEGURIDAD EN LOS NUEVOS MODELOS ASISTENCIALES

# ENTIDADES ASOCIADAS

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

Abbott

Dedalus

NTT DATA

accenture

DOOLE
Quality Healthcare. Everywhere.

oesia grupo

AGFA HealthCare

EY Building a better working world

PLEXUS TECH

aws

gmv INNOVATING SOLUTIONS

Roche

pahia

Ibermática
EMBRACING THE FUTURE

sham
SEGUROS Y GESTIÓN DE RIESGOS
una sociedad del grupo relyens

BlueStar

IBM

sia
An Indra company

Canon
CANON MEDICAL

InterSystems
Creative data technology

T-Systems

CGM CompuGroup Medical

werfen

COSTAISA

Microsoft

ZEBRA

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

**Directora**
Zaida Sampedro

**Coordinador de Especiales:**
Juan Carlos Oliva

**Comité Editorial**
Luciano Sáez
Jesús Galván
Francisco Martínez del Cerro
Guillermo Vázquez
José Manuel Morales Pastora

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

**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

# AÑO 2022 NÚMERO 149 **SUMARIO**

ENTIDADES
**COLABORADORAS**

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

COLEGIO OFICIAL DE FARMACÉUTICOS DE CÁCERES

COLEGIO OFICIAL DE FARMACÉUTIOS DE BADAJOZ

CONSEJO GENERAL DE COLEGIOS OFICIALES DE FARMACÉUTICOS

EMERGRAF, S.L. CREACIONES GRÁFICAS

HOSPITAL CLINIC. SISTEMAS DE INFORMACIÓN

IDCSALUD

MUTUAL CYCLOPS-CENTRE DOCUMENTACIÓ

OSAKIDETZA - SERVICIO VASCO DE SALUD

**SOCIOS TECNOLÓGICOS PRINCIPALES**

Abbott · Dedalus · Fujitsu · Microsoft

**SOCIOS TECNOLÓGICOS COLABORADORES**

Atos · EY · inetum · Philips · Roche · Siemens Healthineers

# La SEIS ingresa en la Orden Civil de Sanidad

La Sociedad Española de Informática de la Salud lleva trabajando por la innovación del sector Salud desde 1977, basando todas sus acciones en la aplicación de las tecnologías de la información y las comunicaciones como el mejor modo de garantizar una atención sanitaria segura y de calidad, facilitar mejores servicios a los ciudadanos y contribuir a la propia sostenibilidad del sistema sanitario.

Siempre hemos considerado imprescindible una visión holística en el sector, teniendo en cuenta las necesidades y visión de los profesionales, de las organizaciones de salud y de las propias soluciones tecnológicas existentes en cada momento, con el objetivo de mejorar el estado de salud de los ciudadanos y promover una sanidad enfocada en la prevención.

En estos 45 años, a medida que se producían importantes avances tecnológicos que incidían positivamente en nuestro sector, hemos tenido muy en cuenta las opiniones de multitud de organizaciones y asociaciones con las que podíamos encontrar puntos coincidentes, otorgando el peso necesario a aquellas que ostentan responsabilidad institucional, ya que en definitiva son las que tienen la potestad de abordar los proyectos, proveer los recursos necesarios y proceder a su implantación.

La SEIS ha ido adaptando la composición de los miembros de su Junta Directiva, tanto al mapa territorial competencial como a las delegaciones temáticas o de las diferentes profesiones sanitarias. Esa organización, homogénea y convencida del papel que debía desempeñar, mantenida a lo largo de estos años, es la que ha permitido desarrollar nuestra actividad impulsora de la transformación digital del sector.

Una tarea que ha venido desarrollando nuestra sociedad y que consideramos importante es la de poner en contacto a los diferentes profesionales, a las distintas organizaciones sanitarias y empresas tecnológicas, para que pudieran confluir sus visiones de mejorar nuestro sistema de salud. Esto ha sido así por nuestro espíritu corporativo y nuestra creencia de que las TIC rompen todo tipo de barreras, tanto territoriales como de conocimiento e, incluso, políticas.

Durante estos 45 años, hemos entendido que nuestra misión era intentar convertir los frenos y debilidades de nuestro sector en elementos impulsores y en mantener caminos equidistantes entre tantos intereses, muchas veces contrapuestos, no perdiendo esa visión de servicio al ciudadano y a nuestro sistema de salud.

**El Ministerio de Sanidad le concede el ingreso en la Orden Civil de Sanidad, en su categoría de Encomienda a la Sociedad Española de Informática de la Salud.**

Después de tantos años impulsando el papel que esta Sociedad debía desempeñar en un sistema de salud tan disperso, en todos los sentidos, esta distinción que nos hace el Ministerio de Sanidad con el ingreso en la Orden Civil de Sanidad, el día Mundial de la Salud, nos da un impulso renovado para seguir avanzando y nos congratula que se reconozca el papel de los profesionales que integran nuestra Sociedad, sobre todo sanitarios y tecnólogos, que dedican su trabajo a la innovación del sector sanitario.

Es, en definitiva, un reconocimiento a todos los profesionales que han aportado sistemas de información, que han permitido una mejor toma de decisiones y más adecuadas en momentos de incertidumbre. El esfuerzo realizado por los diferentes profesionales relacionados con los sistemas de información del sistema sanitario, ha sido encomiable durante la pandemia y ha puesto en valor esta actividad profesional de largo recorrido.

Es una importante noticia para nuestra Sociedad tras tantos años de trabajo.

# Adoptar un enfoque múltiple para asegurar las prácticas de telemedicina

**José Luis Laguna**
Director Systems Engineering Fortinet España y Portugal

**La telemedicina ha ido adquiriendo cada vez más peso en la asistencia médica española, y la pandemia no ha hecho más que apuntalar esta tendencia. De acuerdo con los datos de la Sociedad Española de Medicina Familiar y Comunitaria (Semfyc), en tiempos de covid-19 un médico de cabecera registra una media de 32 actos médicos a través de la teleasistencia (cinco horas y 20 minutos de su jornada) y atiende una decena de pacientes de forma presencial.**

Recientemente, la Comunidad de Madrid anunciaba que la puesta en marcha de la telemedicina en centros públicos en disciplinas como la dermatología, con el objetivo de agilizar las consultas, reducir las listas de espera y proteger a los pacientes y sanitarios frente a la pandemia.

La necesidad de asegurar la telemedicina es una preocupación constante en la comunidad médica y en las instituciones sanitarias. De hecho, la Asociación Americana de Telemedicina considera que mitigar el riesgo de ciberseguridad es uno de sus nueve "principios políticos" para la atención conectada. El verdadero reto al que se enfrenta el sector sanitario es que hablar de la seguridad en este ámbito es más fácil que aplicarla. Las organizaciones sanitarias deben tomar medidas proactivas para aglutinar la tecnología, el personal y los procesos adecuados para satisfacer esta demanda. En otras palabras, tienen que realizar algunos cambios de comportamiento.

Incluso antes de la pandemia, el sector sanitario ya era objetivo del cibercrimen, si bien es cierto, que en 2020 el sector en su conjunto pasó a un modelo a distancia, incluyendo servicios de teleconsulta y la realización de pruebas diagnósticas de Covid-19 en remoto, mientras que la industria farmacéutica se centraba en el desarrollo y la fabricación de vacunas.

Los cambios en la industria y las políticas gubernamentales más complejas están impulsando las fusiones, adquisiciones y asociaciones entre organizaciones sanitarias. La convergencia resultante de las tecnologías solo complica aún más las infraestructuras de red ya inundadas por el Internet de las Cosas Médicas (MIoT) y la necesidad de apoyar la rápida adopción de la telemedicina. El resultado es un entorno difícil de asegurar, ante el creciente número de usuarios -ya sea personal administrativo, personal médico o pacientes-. que acceden a los recursos de la red, y la proliferación de dispositivos conectados, ya sea dispositivos de usuario final o soluciones médicas conectadas, muchas de los cuales nunca fueron diseñadas teniendo en cuenta la seguridad. En consecuencia, las organizaciones deben abordar un sinfín de problemas posteriores relacionados con la gestión de la infraestructura, la visibilidad, el control y la eficiencia operativa

Para responder a estos nuevos modelos, muchas organizaciones sanitarias renovaron su infraestructura de seguridad. Al mismo tiempo, los ciberdelincuentes aprovecharon la oportu-

nidad para explotar la pandemia. En medio de todo esto, los equipos de seguridad trabajaron incansablemente para garantizar la seguridad, el rendimiento y el cumplimiento. Se produjo un aumento del *ransomware* en la sanidad y las organizaciones de la salud alertaron sobre los riesgos de ciberseguridad en la telemedicina.

En el momento de mayor necesidad y crecimiento, los servicios vitales del sector seguirán enfrentándose a importantes amenazas. Las consultas en remoto a través de vídeo están preparadas para expandirse, al igual que el uso de sensores y equipos de diagnóstico remoto. Al mismo tiempo, la investigación de FortiGuard Labs muestra que los *hackers* seguirán tratando los dispositivos del Internet de las Cosas (IoT) y del Internet de las Cosas Médicas (IoMT) como vectores de ataque.

## ELEGIR LAS TECNOLOGÍAS ADECUADAS PARA ASEGURAR LA TELEMEDICINA

Las organizaciones sanitarias y sus responsables de TI deben trabajar de forma coordinada y conjunta para abordar los riesgos de ciberseguridad al igual que hicieron durante la pandemia. Entre los procesos en los que deben colaborar se encuentran los siguientes: adopción de la tecnología *cloud* y hacer posible el teletrabajo seguro y el despliegue de las plataformas virtuales para pacientes.

Una tecnología que puede ayudar a reducir el riesgo es la SD-WAN. La SD-WAN resuelve varios retos al mismo tiempo, como una rápida implantación, una rápida conectividad a las aplicaciones y recursos en la nube y la gestión unificada para reducir los gastos generales de TI. También permite a las organizaciones añadir más ancho de banda de forma económica, a la vez que proporcionan a los usuarios un acceso directo y de alta calidad a los recursos basados en Internet.

En el sector salud, la SD-WAN segura garantiza conexiones de gran ancho de banda que permiten el paso de información de vídeo y diagnóstico en tiempo real entre los pacientes y la organización de atención sanitaria. También facilita la conexión de ubicaciones remotas a las redes, ofreciendo menor latencia, mejor rendimiento y una conectividad más fiable. Esta tecnología ayuda a proteger los datos y las transacciones entre las organizaciones sanitarias, permitiendo el cumplimiento de la Ley de Disponibilidad y Portabilidad del Seguro Médico (HIPAA).

> ***La ciberhigiene debe basarse en tareas de seguridad básicas, como la actualización de dispositivos, la identificación de comportamientos sospechosos y la práctica de una buena ciberhigiene"***

La SD-WAN proporciona todas estas eficiencias de seguridad, disponibilidad y cumplimiento sin romper los bancos de datos de los proveedores de salud, una de las principales preocupaciones de sus juntas directivas.

Las soluciones SD-WAN son una inestimable ayuda para impulsar las capacidades de las organizaciones sanitarias transformando la WAN corporativa y aprovechando la conectividad *multi-cloud* para ofrecer un rendimiento de aplicaciones de alta velocidad en el perímetro de la WAN o delegación, incluyendo sitios como clínicas, hospitales satélites, laboratorios, centros de atención urgente, centros de emergencia independientes y centros de atención de larga duración.

Por otro lado, es importante asegurarse de que todos los dispositivos *enpoint* tengan instalada una protección de seguridad avanzada, como soluciones antiexplotación y EDR (*Endpoint Detection Response*). Las soluciones antiexploit y EDR, que permiten identificar, detectar y prevenir amenazas avanzadas (APT) con mayor facilidad, son excelentes herramientas para descubrir el *malware* en un dispositivo *enpoint* antes de que se extienda al resto de la red y, a continuación, compartir esa información con el resto de los dispositivos.

El sistema de protección, detección, investigación y respuesta de los *endpoints* basado en el comportamiento no sólo puede bloquear un porcentaje mucho mayor de ataques (con precisión) tanto antes como después de la ejecución, sino que también sigue evaluando y, lo que es más importante, clasificando el comportamiento sospechoso.

## CIBERHIGIENE PARA PROTEGER LA TELEMEDICINA

La seguridad de la telemedicina debe empezar por las personas: enseñar una buena ciberhigiene y reforzar esas lecciones con una tecnología que capacite a los usuarios debe ser parte de la solución. Esto incluye garantizar que todos los empleados de las organizaciones sanitarias reciban la formación necesaria para poder actuar con rapidez ante un ciberataque.

La higiene en ciberseguridad es un proceso de aprendizaje continuo. Los empleados deben aprender a detectar e informar sobre actividades *online* sospechosas y aplicar medidas de ciberhigiene. Ahora más que nunca, también deben aprender a proteger sus dispositivos personales y sus redes domésticas.

La cibersalud debe tratarse de forma parecida a la salud física. Los CISO deben asegurarse de que los usuarios -especialmente los trabajadores remotos- sepan cómo mantener la distancia en el mundo *online*, permaneciendo atentos a las solicitudes sospechosas e implementando herramientas y protocolos de seguridad básicos. Ya sea mediante talleres presenciales o cursos online, el aprendizaje continuo construye una defensa de base en la zona más vulnerable.

## SENTAR LAS BASES PARA SUPERAR AMENAZAS COMPLEJAS

La ciberhigiene debe basarse en tareas de seguridad básicas, como la actualización de dispositivos, la identificación de comportamientos sospechosos y la práctica de una buena ciberhigiene. Después de crear un sólido programa de educación y concienciación, los CISO deben invertir en las tecnologías y soluciones que refuerzan estas mejores prácticas, como la SD-WAN, el software *antimalware* y el cifrado. Lograr una visibilidad clara y un control granular en todo el panorama de amenazas permite a los CISO proteger los datos sensibles de la telemedicina.

La complejidad es el enemigo de la seguridad. Empezar por lo básico, comenzando por la ciber higiene, es la mejor respuesta a los problemas digitales cada vez más complicados y altamente dinámicos a los que se enfrenta el sector sanitario hoy en día.

# ¿Cómo mejorar el nivel de resiliencia para afrontar un *ransomware*?

**Andrés Martín Roldán**
Preventa y Responsable de Servicios de Detección y Respuesta en Fujitsu

**Los últimos ataques en el entorno sanitario, y su gravedad, han incrementado el grado de concienciación y su preocupación por la mejora del nivel de resiliencia.**

Los ataques de *ransomware* se han incrementado significativamente en el último año, llegándose a pagar más de $590 millones en 2021, según indica la agencia FinCEN (*Financial Crimes Enforcement Network*, oficina del Departamento del Tesoro de Estados Unidos). A pesar de las afirmaciones de los grupos de *ransomware* de que no buscan dañar a las personas, la realidad es que los ataques contra los Servicios de Salud y atención médica se han incrementado en 2021:

- En 2021 el FBI (*Federal Bureau of Investigation)* identificó 16 ataques del ransomware Conti en Centros Médicos de USA.
- Health Services Executive HSE IT – Ireland (May 2021).
- Waikato District Health Board - New Zealand (May 2021).
- Macquarie Health Corporation, Australia (Oct 2021).
- Newfoundland Healthcare System – Canada (Nov 2021).

Ante estos datos y el previsible incremento de ataques de 2022, conviene analizar con profundidad las principales causas que facilitan un ataque de *ransomware* en el sector de Sanidad, donde conviven el mundo de los datos en un entorno complejo que combina IT y OT:

**Falta de visibilidad** de los activos sanitarios: desconocimiento de lo que hay en nuestra red (IT/OT) y su criticidad, inventario inexistente o desactualizado, etc.

**Debilidades en la segregación** de los entornos: escasa segregación interna, falta de control en movimientos laterales, fácil acceso a la información, etc.

**Carencias en el gobierno** de la seguridad: IT vs OT, personal no concienciado adecuadamente, falta de medidas claras para implementar un control, falsa sensación de seguridad, auditorías sin resultados y medidas claras, procedimientos no adecuados o incompletos, etc.


> ***Para solucionar estas debilidades que facilitan los ataques de ransomware, se deben tomar medidas abarcando los pilares de Gobierno, Prevención, Detección / Respuesta y Recuperación***

**Debilidades en los sistemas de protección y detección:** Directorio Activo sin protección, ausencia de soluciones PAM (Gestión de Usuarios Privilegiados), mal funcionamiento en detección y alerta temprana, carencias en la gestión de eventos y alertas, etc.

**Vulnerabilidades desconocidas o no corregidas** en los activos: desconocimiento de la criticidad de las vulnerabilidades que tenemos, carencia de planes de mitigación / resolución, etc.

Para solucionar estas debilidades que facilitan los ataques de *ransomware*, se deben tomar medidas abarcando los pilares de Gobierno, Prevención, Detección / Respuesta y Recuperación, teniendo claro cuál es nuestro estado actual frente a un ataque (*Ransomware Readiness Assessment*):

## MEDIDAS RELATIVAS AL GOBIERNO

- Conoce tus debilidades. "Solo los aficionados atacan a las máquinas; los profesionales se dirigen a las PERSONAS" – Bruce Shneier (criptógrafo).
- Eres tan vulnerable como el eslabón más débil de la cadena (personas, terceros, cadena de suministro, etc.).
- El Esquema Nacional de Seguridad permite la adopción de un catálogo de controles clave así como el establecimiento de un Sistema de Mejora Continua.
- CCN proporciona diferentes herramientas para mejorar el nivel de protección ante un *ransomware*.

## MEDIDAS RELATIVAS A LA PREVENCIÓN

- Mantén actualizados todos los dispositivos. Los entornos *legacy* son un eslabón débil y es necesario Visibilidad y Protección.
- Foco en la segmentación de entornos críticos y capacidad de contención automatizada.
- Protección de entornos de *back up* y Directorio Activo.
- Control de identidad y accesos en entornos con dispositivos compartidos. Control de usuarios con permisos privilegiados.

## MEDIDAS RELATIVAS A LA DETECCIÓN Y RESPUESTA

- Integración entre las distintas herramientas de detección. Casos de uso concretos que detecten: robo de credenciales, escalado de privile-

gios, movimientos laterales y exfiltración de información.

- Simulación de ejercicios de ataque de forma periódica y en entornos realistas (evaluación de controles de seguridad, herramientas de protección y servicios de detección y respuesta).
- Planes actualizados de respuesta y recuperación a nivel de toda la organización.

## MEDIDAS RELATIVAS A LA RECUPERACIÓN

- Actualizaciones y pruebas periódicas del Plan de Recuperación (DRP).
- Realizar pruebas periódicas de restauración de *back up*, segregadas según la criticidad de los sistemas.

Fujitsu cuenta con elevada experiencia en implantación de medidas para disminuir el riesgo de ataques *ransomware* en el entorno sanitario, destacando:

- Implantación de tecnología de Breach & Attack Simulation (BAS) para la reducción de superficie de exposición.
- Implantación de tecnología de Control de Acceso NAC, tanto en entorno IT como en entorno OT-Hospitalario.
- Implantación de tecnología de Virtual Patching para entornos de misión crítica en Hospitales.
- Implantación de tecnología de Identificación y Autenticación Segura en entornos OT hospitalarios.
- Implantación de tecnología de Gestión de Usuarios Privilegiados (PAM) en Servicio de Salud Pública.
- Implantación SIEM, monitorización de eventos y gestión de incidentes de Seguridad.
- Consultoría y asesoramiento para cumplimiento y certificación del Esquema Nacional de Seguridad.
- Operación, Administración y Soporte de la Infraestructura de Seguridad en Servicio Sanitario Público.

A continuación, se muestra un caso de uso reciente implantado en *ib-salut*:

# Ciberseguridad, protección de datos y privacidad

**Guillermo Pirez**
Gigamon

**La protección de datos y la seguridad están a la orden del día, concretamente las cuestiones relacionadas con la protección de datos de carácter personal. Son frecuentes los sucesos y noticias referentes a personas y organizaciones que han sido víctimas de la ciberdelincuencia a través de hechos tales como el hackeo de cuentas de correo electrónico, aplicaciones, plataformas de comunicación y en redes sociales, acceso a usuarios y contraseñas de seguridad, acceso no autorizado a sistemas, redes y bases de datos, sustracción de información confidencial (datos, documentos, imágenes,...), suplantación de identidades, espionaje, delitos económicos, etc.**

Todo ello pone de manifiesto la importancia que tiene para las personas y las organizaciones (empresas) el diseño, la implementación y la integración suficiente y adecuada de sistemas, herramientas y procesos de seguridad de la información, que garanticen unos adecuados niveles de prevención, protección y gestión de contingencias, especialmente en todo lo referente a los datos de carácter personal asociados a sus trabajadores, clientes, proveedores y otras partes interesadas.

Por esto, una solución bastante completa e interesante para ayudar a lidiar con el día a día de esta protección de la red en los entornos actuales son los Network Hackett Brokers.

La tecnología de los Network Packet Brokers (NPB) nace en su origen en el año 2004 para solventar la problemática de la inserción de sondas de seguridad y monitorización en las redes de comunicaciones.

En una arquitectura tradicional de red, con una capa de cómputo habitualmente virtualizada, conectada a una red de conmutación de acceso (Leaf) que a su vez se interconecta con otra de Core (Spine) para posteriormente conectarse a los Firewalls y Routers de salida a internet, con conexiones a otras sedes remotas y/o a la cloud. Esta red acostumbra a ser operada por el departamento de redes y sistemas (NetOps) cuya prioridad es la velocidad y estabilidad de la red.

El reto se presenta cuando el departamento de monitorización y seguridad (SecOps) adquiere sus soluciones de Seguridad (Firewall, IDS, IPS, SIEM, NAC, Forensico, DDoS, NDR...) y de monitorización (NPM, APM...) y tiene que insertar esta sonda en la red para poder recibir el trafico, bien en línea o bien fuera de banda (copias de trafico). En este caso la arquitectura de red se complica enormemente y empiezan a surgir fricciones entre los departamentos que hacen que los proyectos de despliegues de sondas se eternicen.

Los NPBs solventan esta problemática al separar la red de comunicaciones de las herramientas de seguridad y monitorización mediante las 3 funciones que realizan:

## 1. CAPTURA DE TRÁFICO

Independientemente de que hablemos de redes locales, remotas, físicas (fibra, cobre) o virtuales (VMWare, Openstack, AWS, Azure, Kubernetes...) la solución de Gigamon es capaz de realizar una copia exacta y fidedigna del tráfico de la red.

## 2. INGENIERÍA DE TRÁFICO

Una vez disponemos de las copias del trafico necesarias, toda esa información es procesada por los NPB para poder filtrarlo y enviar a cada sonda únicamente el trafico que ha de re-

cibir, racionalizando el coste del despliegue de la propia sonda al no enviarle anchos de banda innecesarios. Igualmente podemos realizar manipulaciones de trafico para aumentar la eficiencia de estas sondas.

## 3. ENTREGA A HERRAMIENTAS

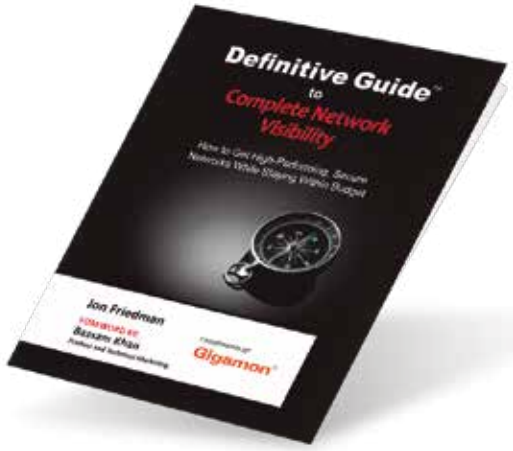
Entrega del tráfico filtrado y manipulado adecuadamente a las sondas de seguridad y monitorización

## ¿QUÉ BENEFICIOS APORTA UN NETWORK PACKET BROKER?:

· Mejora en la operación de la red: una vez depongamos de la red de captura e ingeniería de trafico en la red, desplegar nuevas sondas de seguridad resulta una tarea sencilla, ya que es posible enviarle a cada herramienta el tráfico que requiera y en el formato mas adecuado, sin siquiera disponer de ventanas de mantenimiento

- Reducción de costes: gracias a las capacidades de filtrado de trafico L2-3-4-7 permitimos enviar a cada sonda el trafico que ha de recibir.
- Habilitación de herramientas: al disponer de la solución de NPB en la red podemos centralizar el uso de las herramientas en una/pocas sedes centrales.

### QUÉ ES NETWORK PACKET BROKER?




*https://www.gigamon.com/resources/resource-library/book/definitive-guide-to-next-generation-network-packet-brokers.html*

- Visibilidad y Seguridad en la Cloud Publica, Privada e Hibrida.
- Cumplimiento de normativa: gracias a las técnicas de enmascarado de información podemos ofuscar información confidencial financiera, de salud…

# Identidad digital en el entorno sanitario: privacidad y protección de datos

**Carlos Pastor Matut**
Director de Estrategia Blockchain Inetum

**La Identidad Digital es una realidad cada vez más prevalente en todos los ámbitos. Todos conocemos la dificultad de saber quién tiene nuestros datos, para qué están siendo usados, qué personas tienen acceso a los mismos, etc., por no mencionar los casos de robo de identidad o la dificultad para recordar nuestros usuarios y *passwords* en decenas de sitios web. La identidad digital tiene, por otra parte, una especial significación en el entorno sanitario.**


La Identidad Digital Autogestionada (Self-Sovereig Identity, SSI) responde a la necesidad de poner los datos bajo el control del usuario, normalmente usando un *Wallet* o cartera digital desde su móvil.

De esta manera, el usuario tendrá acceso a una copia de sus datos en formato digital estandarizado y será capaz compartir o dar acceso a los mismos de forma fácil y segura. De la misma manera podrá solicitar la suspensión del uso de sus datos con la idéntica facilidad, simplemente pulsando un botón de su *Wallet*.

En nuestro entorno, esta solución es fácilmente aplicable en áreas tan significativa como la tarjeta sanitaria electrónica, utilizable tanto de forma *online* como presencial; la gestión de su historia clínica, tanto para obtener una copia como para dar acceso a la misma cuando sea necesario; el consentimiento informado, incluyendo no sólo la firma del mismo, sino también el registro de lo firmado; o la receta electrónica integrada en el *Wallet* de identidad y de uso sencillo y seguro para evitar fraudes.

Las soluciones SSI, como el proyecto Dalion, cubren toda la "vida digital" del usuario, de esta manera el usuario podría usar la misma *Wallet* para sus gestiones sanitarias, gestiones bancarias, contratación de electricidad, compras electrónicas, etc., facilitando la adopción de esta herramienta como solución de uso común, tanto dentro como fuera del sector sanitario, fomentando así su adopción por los usuarios.

Las soluciones mencionadas en este breve artículo se alinean con las iniciativas de *Wallet de Identidad Europeo* y con la revisión de la normativa eIDAS de gestión de identidad, en las que España está jugando un papel de liderazgo, especialmente a través del proyecto EBSI, que trata de aprovechar las características de inmutabilidad y seguridad de los registros distribuidos (DLT) y en particular *blockchain* en la gestión de la identidad digital, siempre con la normativa de Protección de Datos europeas, RGPD, como referencia y guía.

# Reflexiones sobre el estado del arte de la seguridad de la información en el entorno sanitario

**Jesús Sánchez**
CEO de AUDEA Logicalis

**La seguridad de la información sanitaria continúa siendo un reto para la salud pública como pudimos observar en el XIX Foro de Seguridad y Protección de Datos de Salud «Protección de datos en los nuevos modelos de atención social y sanitaria». La prestación de la atención sanitaria depende cada vez más de los sistemas de información, entre otros factores, debido a la acelerada implementación de tecnologías para dar respuesta a la crisis sanitaria de estos dos últimos años, la evolución de la telemedicina y los propios avances tecnológicos en el sector.**

En consecuencia, las interrupciones de estos sistemas provocan cada vez más problemáticas en la atención clínica, pudiendo perjudicar a los pacientes. Estos ceses de actividad pueden darse generalmente por ataques externos o por un uso inadecuado de la información sanitaria protegida.

Como expusimos en este foro, para minimizar estos riesgos, los agentes involucrados en la atención médica deben mantener una sólida postura en relación a la seguridad de la información, para ello, deben contar con planes de contingencia comprobados, además de implementar y demostrar las mejores prácticas a través de esquemas de certificación como el Esquema Nacional de Seguridad (ENS) para las entidades públicas u otras reconocidas internacionalmente (ISO/IEC 27001, ISO/IEC27701…. etc.), sin olvidar el Reglamento General de Protección de Datos (RGPD).

El valor de la información y la importancia de esta es un elemento vital de los sistemas de información de las instituciones sanitarias, por ello, estas deben ser los principales actores en examinar sus entornos y cumplir con las medidas de seguridad adecuadas. Además, estas deben asegurar también el cumplimiento de los requisitos en materia de privacidad y seguridad de sus proveedores de servicios de atención médica.

Algunas de las razones principales por las que el sector aún no cuenta con un nivel adecuado respecto al cumplimiento de determinados estándares de seguridad, siguen siendo la falta de financiación para la seguridad de las tecnologías de información, la insuficiente inversión en recursos humanos y tecnología, así como la carencia de concienciación y formación del personal sanitario en esta área.

Este último, es un factor esencial para minimizar los riesgos, en este sentido, las instituciones deben contar con proveedores especializados que aporten conocimientos específicos en el ámbito de la seguridad de la información en el sector salud, con el objetivo de promover una cultura de prevención y detección temprana de posibles incidentes de seguridad.

Todos estos factores hacen fundamental conocer y gestionar los riesgos de seguridad de la información para prevenir incidentes, o al menos, para reducir el impacto en los pacientes en caso de que ocurran, sobre todo, teniendo en cuenta el valor subyacente de los datos en este sector en comparación con los datos en otros sectores, realizarlo correctamente será el elemento clave para mantener el servicio sanitario de forma óptima.

# Gestión de accesos de usuarios a los recursos de la sanidad

**Pablo Chapinal**
Microsoft

**En el modelo tradicional en que las arquitecturas de seguridad han ido evolucionando, todo estaba dentro del perímetro de la red y la seguridad de la red era todo lo que necesitábamos en ese momento. Pero luego, Internet comenzó a permitirnos transformar realmente la forma en que hacíamos las cosas. Ahora, nuestra población de usuarios abarca a todos los empleados, socios y proveedores, y todos disponen de sus propios dispositivos. Y todos accediendo a la información, infraestructura y redes de nuestras organizaciones.**

Hemos conectado dispositivos desplegados en nuestros hospitales, centros de salud, y oficinas. Incluso, compartimos usuarios, dispositivos, aplicaciones y datos con nuestros socios y proveedores. Nuestra huella corporativa y cómo la protegemos se ve muy diferente de lo que era hace unos años con perímetros duales que protegen nuestros activos en diferentes circunstancias.

Actualmente, las organizaciones se enfrentan a muchos desafíos relacionados con la identidad y el acceso en su organización. Principalmente debido a lo siguiente:

- Notable incremento de aplicaciones, dispositivos y usuarios dentro y fuera de la red corporativa. A medida que las barreras organizacionales se desdibujan entre quién está en su red y fuera de ella, las organizaciones luchan por administrar identidades no solo para sus empleados, sino también para socios externos, proveedores y distribuidores, e incluso para consumidores finales y clientes o ciudadanos.
- Los ataques de identidad siguen aumentando -un 300% el año pasado.
- Regulaciones en evolución que debe cumplir para proteger su privacidad y la privacidad y seguridad de sus clientes (por ejemplo, GDPR).


- Demandas de mayor productividad y modernización de TI, habilitadas por la identidad (por ejemplo, transformación digital).

Adicionalmente, tenemos la urgencia provocada por los altos riesgos de ataques cibernéticos ocasionados por el ataque de Rusia a Ucrania, donde una correcta y segura gestión de accesos se hace imprescindible, y así lo indica el ENS y el CCN Cert.

A menudo, la parte más difícil es equilibrar múltiples prioridades, con frecuencia competitivas, de reducir costes y aumentar la eficiencia, la seguridad y la experiencia del usuario.

Antes de sumergirnos en las nuevas características, cabe destacar las tendencias tecnológicas actuales y el papel de la identidad en la transformación digital.

1. El perímetro de la red está desapareciendo
2. Los recursos se están moviendo a la nube
3. Una empresa promedio está viendo un incremento de dispositivos y aplicaciones con un promedio de 181 aplicaciones, utilizadas por las empresas.
4. Las personas tienen múltiples identidades y se conectan desde cualquier lugar, usando múltiples dispositivos.

## LA IDENTIDAD ES UN PLANO DE CONTROL PARA LA TRANSFORMACIÓN DIGITAL

En este mundo, su sistema de identidad en la nube es su plano de control que puede conectar todo, darle visibilidad a su patrimonio digital al completo, garantizar que solo las personas adecuadas tengan el acceso correcto a los recursos correctos y mantener a los malos jugadores fuera.

Azure Active Directory de Microsoft es una plataforma de identidad universal que ayuda a administrar y proteger a todos sus usuarios y el acceso a todas sus aplicaciones. Está liderando la transformación digital para ayudar a sus empresas a prepararse para las oportunidades en la era de la nube y reinventar la forma en que trabajamos.

Microsoft es uno de los mayores proveedores de identidad. La escala de nuestra solución es enorme:

Azure AD es un servicio de identidad verdaderamente global que funciona a hiperescala.

- Más de 100 mil organizaciones confían en Azure AD.
- Administramos más de 254 millones de usuarios activos mensuales, con un promedio de 30 mil millones de solicitudes de autenticación diarias.

Microsoft ha sido un contribuyente clave a los estándares de identidad durante más de 20 años. Trabajamos en estrecha colaboración con alianzas de la industria y expertos en seguridad de todo el mundo para desarrollar prácticas seguras para la identidad.

Creamos Azure AD sobre estándares abiertos para una mayor interoperabilidad y seguridad.

Microsoft Azure Active Directory proporciona una plataforma con todas las funciones con capacidades para que pueda administrar y proteger las identidades de sus organizaciones.

Con la identidad como plano de control y Azure AD, desbloquea una seguridad de clase mundial.

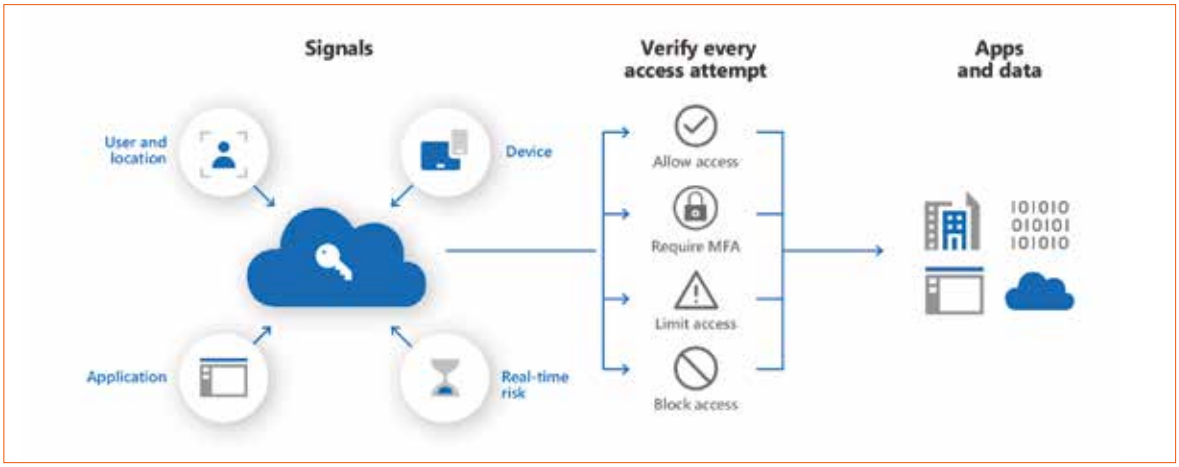
Azure AD puede ayudar a:

Conectar a su fuerza de trabajo a cualquier aplicación con inicio de sesión único sin problemas y acceso seguro desde cualquier ubicación. Es posible aumentar la productividad y reducir los costes con procesos de identidad automatizados, como el ciclo de vida del usuario, agregando nuevos derechos de acceso cuando un empleado se une o cambia de equipo, y revocándolos cuando la persona se va. El portal de autoservicio permite ahorrar tiempo y dinero en el restablecimiento de contraseñas y la configuración de la autenticación multifactor para sus usuarios.

Proteger y controlar el acceso: es crítico proteger las credenciales de usuario mediante un enfoque de confianza cero. Zero Trust es un modelo de seguridad en el que la organización siempre verifica primero antes de confiar en un usuario o dispositivo. Requiere visibilidad de los usuarios y dispositivos, un motor de políticas y administración de acceso. La autenticación segura (MFA) y las directivas de acceso condicional inteligente en Azure AD, combinadas con la administración y seguridad de endpoints en M365 E3/E5, pueden proporcionar todo lo necesario para implementar un enfoque de confianza cero. (más sobre Zero Trust aquí: https://cloudblogs.microsoft.com/microsoftsecure/2018/06/14/building-zero-trust-networks-with-microsoft-365/). Recomendamos comenzar con una línea de base de autenticación fuerte de dos factores y acceso condicional adaptativo basado en el riesgo.

Interactuar con clientes y socios para hacer crecer el negocio, utilizando herramientas centradas en el usuario y colaboración moderna. Para ello, es necesario mover las identidades de los clientes y socios a la nube para proporcionar mejores experiencias y mayor seguridad. Invitar a los socios a colaborar y administrar su acceso es sencillo, al igual que personalizar los viajes de los usuarios para el registro y el inicio de sesión en sus aplicaciones y servicios desde una web o un dispositivo móvil con nuestra solución B2C.

Acelerar la adopción de las aplicaciones: a medida que las organizaciones trasladan sus sistemas de identidad a la nube, son necesarias aplicaciones y desarrollos para integrarse con ese sistema de identidad. Con Azure AD como plataforma, los desarrolladores pueden y deben integrar y crear aplicaciones conectadas a la identidad en el ecosistema de identidad de Azure AD y Microsoft. Esto permitirá que las aplicaciones que cree se adopten más ampliamente en la organización o, si es un ISV, en la empresa.



# La guerra cibernética en el sector sanitario

**Amaya Bretón**
OESIA

**En un mundo cada vez más tecnológico, los ataques contra la seguridad de la información, los datos personales y la privacidad tienen como caldo de cultivo la utilización de Internet. Si bien hoy en día conocemos las diferentes afecciones que puede tener el concepto "guerra", ya sea civil, comercial, atómica, nuclear, biológica, etc, nos encontramos ante un nuevo escenario bélico, el ciberespacio, en el que los objetivos de ataque son los sistemas informáticos que soportan organizaciones, edificios o infraestructuras con el objetivo de robar información, paralizar o destruir cualquier servicio o actividad proporcionado por los mismos mediante diferentes técnicas de ingeniería social, especialmente mediante el uso de *ransomware*, aprovechando las vulnerabilidades o deficiencias en sus sistemas. Hablamos de una guerra cibernética.**

En el contexto actual, un ataque cibernético o tecnológico puede originarse en cualquier momento. Un ejemplo de ello son los ciberataques que se están produciendo a raíz del conflicto entre Rusia y Ucrania. El hecho de que los sistemas de información de una organización estén conectados a la red multiplica exponencialmente la probabilidad de que se materialicen las amenazas contra los mismos, en forma de fuga de información, denegación del servicio o paralización de la actividad. Uno de los sectores que por su especial naturaleza e importancia en la sociedad puede ser objeto de un ataque tecnológico a gran escala es el sector sanitario. De hecho, a raíz de la pandemia motivada por el Covid-19, los ciberataques a hospitales, centros médicos y laboratorios de investigación han aumentado de forma exponencial y la tendencia (preocupante) sigue creciendo.

¿Cómo impacta un ciberataque a una entidad u organismo sanitario? o, en otras palabras, ¿Qué pasa si se produce un ataque contra los sistemas de información de un hospital, clínica, farmacia o laboratorio de investigación biomédica que paralice el servicio, extorsione, robe o destruya la información contenida en sus sistemas de información? ¿Cuántas personas pueden verse potencialmente afectadas por ese ataque y qué consecuencias tiene para la vida de las mismas? Si lo trasladamos a un escenario de conflicto armado como el actual, la respuesta es bastante clara: devastadora.

En el ámbito sanitario hay dos máximas que sobresalen respecto a todas las demás, la privacidad y la confidencialidad de los datos de los pacientes. En un ciberataque las máximas son el daño y perjuicio a la víctima, que pueden ir además acompañados de la consecución de un beneficio económico por parte del atacante. La privacidad es el ámbito de la vida privada que debe protegerse frente a cualquier intromisión, es uno de los principios esenciales sobre los que versa la Declaración Universal de Derechos Humanos de 1948 y un derecho fundamental reconocido por la Constitución Española (artículo 18). A su vez, la protección de las personas físicas en relación con el tratamiento de sus datos personales es un derecho fundamental recogido en la Carta de los Derechos Fundamentales de la Unión Europea y protegido como tal en nuestra Constitución (artículo 18.4). Pero, además, si hablamos de pacien-


tes, nos referimos a datos de salud o relacionados con la misma, esto implica que estamos ante información especialmente sensible o de categoría especial, tal como lo define el artículo 9 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (RGPD), ypor tanto, objeto de máxima protección.

Volviendo a los objetivos de un ciberataque, el daño o perjuicio a un organismo sanitario mediante la destrucción de sus sistemas informáticos o la toma de control de los servidores y dispositivos empleados para paralizar o inactivar sus servicios (atención médica, urgencias, operaciones) en un escenario de conflicto bélico, es evidente. El robo o secuestro de la información almacenada en sus sistemas de información con la finalidad de extorsionar o pedir un rescate económico es el otro objetivo fundamental de un ciberataque. Y cuanto más sensible o confidencial sea la información atacada, mayor será el importe económico solicitado por los ciberdelincuentes para recuperarla.

Ante una situación como esta, en aras de proteger la seguridad de los sistemas, la información, los datos personales y la privacidad, es imprescindible disponer de una estrategia de ciberseguridad basada en la implantación de un Centro de Operaciones de Seguridad (SOC) que permita reforzar y mejorar la capacidad de detección, análisis, prevención, monitorización y vigilancia de amenazas en las actividades diarias y servicios proporcionados por una organización, así como la respuesta a incidentes de seguridad y la elaboración de planes de contingencia frente a posibles ciberataques. Esta estrategia de ciberseguridad debe fundamentarse en 5 aspectos esenciales:

- **Identificación de los objetivos y contexto de la organización:** establecer una comprensión organizativa de la gestión de los riesgos de ciberseguridad en relación con los sistemas, activos, recursos y capacidades de la misma.
- **Medidas de protección:** desarrollo e implementación de las medidas de seguridad apropiadas para garantizar la seguridad de la organización, ya sea información, tecnología, infraestructuras o personas y minimizar cualquier efecto resultante de un incidente de ciberseguridad.
- **Detección de amenazas:** vigilancia digital y monitorización continua para identificar, a tiempo, cualquier actividad inusual o anomalía que pueda convertirse en una potencial amenaza para la organización.
- C**apacidad de respuesta:** aplicación de las medidas pertinentes en relación con un incidente de ciberseguridad detectado y capacitar a la organización para adaptarse a su impacto.
- **Recuperación del servicio o actividad:** elaboración de un plan estratégico para restaurar cualquier servicio o actividad que haya sido dañado como consecuencia de un incidente de ciberseguridad.

***La guerra cibernética ya es una realidad, no es ciencia ficción.***

# La OT Médica, en el centro de las vulnerabilidades en las redes hospitalarias

**Javier Alonso**
Cyber Sales Manager SHAM

**Actualmente la OT médica se puede considerar como el eslabón débil de las redes sanitarias respecto a la ciberseguridad. Es imprescindible una gestión adecuada para detectar y mitigar los riesgos derivados de sus vulnerabilidades.**

Durante el pasado Foro de Ciberseguridad y Datos personales organizado por SEIS en Madrid, unos de los temas que se trataron en diferentes sesiones fue la problemática respecto a la ciberseguridad asociada a los equipos médicos en los centros sanitarios.

La gestión de los dispositivos médicos tiene unas características específicas diferenciadas de la gestión de los entornos TIC debido a sus requisitos respecto a la seguridad del paciente (disponibilidad y seguridad en la operación) y a los periodos de reposición y actualización de los equipos.

Los equipos y sistemas involucrados en las operaciones TIC (sistemas de información, conectividad y redes, bases de datos) son sistemas donde es habitual disponer de actualizaciones que, además de mejorar funcionalidades, resuelven problemas de seguridad detectados. Estas actualizaciones se pueden realizar por el equipo técnico del hospital, contando incluso con herramientas automatizadas para su gestión. Y aún con estas actualizaciones constantes, tenemos ventanas de oportunidad para la explotación de vulnerabilidades hasta que son conocidas y corregidas (vulnerabilidades Zero Day).

La existencia de estos fallos en los sistemas de información y las redes parece algo difícil de evitar, ya que el rápido desarrollo de aplicaciones, interconectividad y protocolos y servicios hace imposible la verificación de todos los posibles fallos a detectar. La solución pasaría por realizar análisis del código y certificaciones rigurosas, actividades que se realizan tan solo en aplicaciones con altos requisitos de seguridad.

Esta problemática de los equipos TIC se acentúa en los equipos médicos. En general, son equipos con un periodo de utilización muy alto, sobre todo si lo comparamos con los 'tiempos TI', pero estos equipos incorporan software embebido con la misma problemática que los sistemas TI: vulnerabilidades que los exponen a un ciberataque. Y estas vulnerabilidades están expuestas a ser explotadas desde el momento en el que se conectan a las redes del hospital.

Sin embargo, debido a criterios de seguridad del paciente, estos equipos están sometidos a verificaciones y homologaciones que hacen que las actualizaciones de software tengan unos plazos de despliegue no asumibles en un mundo conectado. Incluso tenemos equipos con S.O obsoletos que ya no tienen posibilidad de actualización. Por otro lado, en muchas ocasiones la OT médica presenta problemas para ser detectada e inventariada, por lo que el equipo de ciberseguridad no tiene visibilidad sobre


estas vulnerabilidades para tomar medidas preventivas que mitiguen la explotación de las vulnerabilidades.

Esta falta de visibilidad se debe los problemas que enfrentan los centros sanitarios para mantener un inventario actualizado: los inventarios tradicionales del centro sanitario no pueden mantenerse actualizados con todos los equipos conectados y las soluciones TIC de inventario más extendidas no pueden detectar los protocolos específicos de los equipos médicos. Y esto es también un reflejo de la separación de responsabilidades en la gestión de los equipos médicos en los centros sanitarios.

Habitualmente la gestión de los equipos médicos en los hospitales recae en el ámbito de responsabilidad de los departamentos de electromedicina. Aquí se planifican las necesidades, adquisición y mantenimiento de la equipación médica. Hasta el momento, los requisitos de ciberseguridad no han sido criterios tenidos en cuenta en esta gestión de compras y mantenimiento, pero está situación está empezando a cambiar. La ciberseguridad se está convirtiendo en una preocupación para este sector profesional ya que afecta de forma muy seria a la disponibilidad de los equipos y a la seguridad del paciente. Como ha sucedido en otros sectores industriales, es imprescindible una estrecha colaboración entre los responsables de ciberseguridad y de electromedicina para determinar las necesidades en esta materia que se deben incorporar tanto en la compra como en el mantenimiento y operación de los equipos.

La solución definitiva a este problema no está cerca en este momento. Las certificaciones de seguridad en el entorno europeo que marcarían unos niveles mínimos de seguridad y gestión desde el propio diseño de los equipos médicos aún no están desarrolladas y posiblemente se retrasen unos años, por lo que, si el sector no demanda más seguridad en los equipos a los fabricantes, esta seguridad desde el diseño tardará en llegar.

ENISA; en su documento publicado en febrero de 2020 '*Directrices sobre contratación para la ciberseguridad en los hospitales*', da algunas recomendaciones interesantes en esta línea. Además de recomendaciones sobre análisis de riesgo, seguridad de red, pruebas y auditoría habitualmente recogidas en los sistemas de gestión en la ciberseguridad en redes TIC, podemos destacar las siguientes en línea con lo expuesto:

- Involucración del departamento de informática en las diferentes etapas de la contratación
- Identificación y gestión de las vulnerabilidades de los equipos médicos
- Gestión de las actualizaciones de hardware y software
- Exigir certificados de ciberseguridad a los proveedores
- Realización de un inventario de activos.

Como ejemplo ilustrativo de las vulnerabilidades detectadas en los equipos médicos, podemos hablar de la vulnerabilidad ICSMA-20-343-01, con un score de riesgo CVSS v3 9,8 sobre 10. Dicha vulnerabilidad afecta a más de 100 modelos de equipos de imagen médica y permite conectarse a ellos a través de protocolos FTP/Telnet/REXEC. Una vez conectados, es posible extraer información, enviar actualizaciones o escribir archivos en el equipo. Este acceso está protegido por un password y usuario que están grabados en el código, por lo que no permiten actualización y dichas credenciales están disponibles en internet. Por lo tanto, una vez ganado el acceso al equipo, además de afectar a su operación e información (datos personales) puede utilizarse como punto de inicio de un ataque a mayor escala.

Y mientras tanto ¿qué puede hacer un hospital para proteger sus equipos y, en definitiva, la seguridad de sus pacientes? Para identificar los riesgos, anticipar medidas preventivas y conseguir una rápida respuesta en los inicios de un ciberataque, es imprescindible implementar tecnologías de ciberseguridad adaptadas a las redes hospitalarias. Sham, como gestor de riesgos del sector sanitario, cuenta con una solución específica para gestionar la seguridad de las redes sanitarias, prestando especial atención a los dispositivos médicos. Se trata de la solución CyberMDX. Como principales funcionalidades podemos destacar:

1. **INVENTARIO:** Identifica, clasifica y aporta información de cualquier dispositivo conectado a la red del hospital. Además de los equipos TI y OT de infraestructuras, es capaz de identificar cualquier dispositivo médico por su BBDD específicamente diseñada para sanidad.
2. **GESTION DE RIESGO.** Valora el riesgo de los dispositivos incorporando criterios de seguridad del paciente, análisis de vulnerabilidades y evaluación de conformidad (contraseñas, versión SO, etc.). Además, es capaz de proponer medidas para gestionar el riesgo y aplicarlas mediante integraciones con otras soluciones de seguridad.
3. **DETECCIÓN, PREVENCION Y MITIGACIÓN:** Monitorizando el tráfico de la red, detecta ataques a la red o comportamientos anómalos en un hospital. Esto permite una reacción inmediata ante los ataques en una fase temprana, evitando incidentes que pudieran afectar gravemente al servicio del centro hospitalario.
4. **COORDINACION DE EQUIPOS**: CyberMDX cuenta con funcionalidades expresamente diseñadas para los equipos de electromedicina, apoyándoles en las tareas de mantenimiento y optimización del uso de los equipos. De esta forma, pretende ser un punto de conexión entre ambos perfiles de responsabilidad facilitando la tarea conjunta tan necesaria para el óptimo funcionamiento del hospital.

*Más información: www.sham.es – LinkedIn: Sham España – Twitter: @Sham_Espana*
*Más información: www.relyens.eu – LinkedIn : Relyens – Twitter : @Relyens – Youtube : Relyens*

# Los marcos de control integrado como palanca para la gestión eficiente de los programas de cumplimiento y riesgo

**Luis Alonso Albir**
Responsable de la práctica de GRC Tools & Processes Integration en SIA, an Indra company

En el ámbito de la gestión de los riesgos tecnológicos, las Administraciones Públicas competentes en materia de sanidad se enfrentan al reto de tener que dar cumplimiento de múltiples regulaciones aplicables, tales como:

- En materia de privacidad, el Reglamento General de Protección de Datos y Ley Orgánica 3/2018.
- En materia de ciberseguridad, el Esquema Nacional de Seguridad.
- En el ámbito de la protección de infraestructuras críticas (para aquellos servicios de salud que hayan sido designados operador crítico y gestionen alguna infraestructura crítica) y/o de prestación de servicios esenciales, la ley 8/2011 y su regulación de desarrollo o el Real Decreto-Ley 12/2018 y regulación de desarrollo (seguridad de las redes y sistemas de información).

Más allá de estos requisitos normativos, los servicios de salud autonómicos también están abordando procesos de alineamiento respecto a buenas prácticas y estándares internacionales, tales como ISO/IEC 27001 (sistema de gestión en seguridad de la información), ISO/IEC 27701 (sistema de gestión en privacidad), ISO 22301 (sistema de gestión de continuidad de negocio), o el NIST Cybersecurity Framework, entre otros.

Todos estos lineamientos con los requisitos regulatorios como con buenas prácticas deben ser realizados en un contexto de políticas y planes de contención del gasto en las Administraciones Públicas, que requieren de la búsqueda y aplicación de nuevas fórmulas de eficiencia en su gestión, sin menoscabo de la eficacia y efectividad.

La adopción de marcos de control integrado (*Integrated Risk Management* o IRM, por sus siglas en inglés) aparece como una solución adecuada a este contexto de incremento de la complejidad y búsqueda de la eficiencia. Su adopción persigue orquestar todos los esfuerzos que se realizan en este sentido y materializar sinergias a la hora de afrontar los retos habituales de una organización en el momento de implantar y operar marcos de control interno:

- Funciones descentralizadas.
- Independencia orgánica y funcional (estructura de silos).
- Nomenclaturas y taxonomías particulares.
- Excesivos costes tecnológicos y humanos.
- Bajo nivel de documentación en los procesos.
- Déficit de comunicación entre unidades organizativas.
- Elevado grado de manualidad en los procedimientos.
- Heterogeneidad en los sistemas, programas y estructuras de datos.
- Ausencia de una visión holística y transversal.
- Esfuerzo creciente en la adaptación a nuevas regulaciones y normativas.

Uno de los habilitadores clave a la hora de implementar estos marcos de control integrados son las herramientas de GRC (*Governance, Risk & Compliance*), que permiten gestionar las múltiples dimensiones del riesgo y el cumplimiento de manera centralizada, aportando múltiples capacidades de manera nativa:

- Gestión unificada de elementos comunes (maestros) tales como procesos, políticas, controles, riesgos, amenazas, roles, flujos, etc.
- Gestión unificada de los catálogos de controles, lo que permite racionalizar los esfuerzos de

gestión de todo el ciclo de vida de los mismos (implantación, operación, supervisión y mejora continua).

- Automatización de los procesos y *workflows* de control.
- Gestión documental de las trazas y registros de auditoría, facilitando el principio de *accountability*, esencial a la hora de abordar cualquier aproximación en materia de *compliance*.
- centralizado de KPIs, KRIs, etc.

La adopción de este tipo de herramientas permite aligerar la carga de trabajo de los equipos en las organizaciones, sobre todo, aquellas de menor valor añadido. De este modo, pueden centrar sus esfuerzos, no sólo en aquellas tareas de mayor valor, sino también en incrementar la madurez de dichos procesos de gestión. Adicionalmente, estas herramientas facilitan la experiencia de usuario de todos los participantes en estos procesos; algo que incrementa los niveles de su implicación efectiva, permitiendo la creación de una cultura de gestión del riesgo.

Por último, es importante destacar que esta adopción no ofrece beneficios únicamente desde el punto de vista de la gestión de los riesgos tecnológicos, sino que sus capacidades se pueden poner al servicio de otras muchas necesidades similares de este tipo de organizaciones (modelos de prevención de delitos, modelos de seguridad del paciente, control interno en la información financiera, etc.).

Son muchas las promesas que ofrece la adopción de marcos de control integrado apoyados en herramientas GRC, pero, por último, hay una serie de aspectos clave a la hora de implantar exitosamente este tipo de soluciones:

- Disponer de herramientas maduras que ofrezcan de manera nativa muchas de las capacidades necesarias para poder dar soporte transversal al mayor número de necesidades dentro de la organización.
- Contar con un *partner* especialista que, no sólo aporte conocimiento en la parametrización técnica de la herramienta, sino también sobre los procesos de gestión y los marcos de control a implantar sobre la herramienta.
- Planificar adecuadamente el *roadmap* de adopción de este tipo de planteamientos, que permita, por una parte, reducir los riesgos de implantación y, por otra, maximizar las potenciales sinergias.
- Prestar atención a la gestión del cambio necesaria que deberán realizar todos los participantes en el modelo de control interno de la organización.

En definitiva, los marcos de control integrado se presentan como una solución adecuada para atajar la complejidad y búsqueda de la eficiencia en la gestión de riesgos tecnológicos y de otra índole, y dan respuesta a algunos de los desafíos que el cumplimiento legal y regulatorio impone a las organizaciones y entidades públicas.

# Protección de datos y privacidad, dos conceptos estrechamente ligados al ámbito de la ciberseguridad

**José de la Cruz**
Technical Director - Iberia en Trend Micro

**2021 ha supuesto un punto de inflexión, pues tras el Covid se ha acelerado la transformación digital y la adaptación a modelos de trabajo híbridos en las organizaciones, aunque es probable que surjan nuevos puntos débiles.**

En 2022, las amenazas emergentes continuarán poniendo a prueba la resistencia y resiliencia de las cadenas de suministro en todo el mundo. Los modelos de cuádruple extorsión, que han ganado popularidad entre los ciberdelincuentes, provocarán interrupciones operativas con un impacto de gran alcance no solo en las propias víctimas, sino también en sus clientes y socios. Además, la adopción la nube pública obligará a apuntalar las defensas en múltiples frentes, y vectores.

Descubrimiento de nuevas vulnerabilidades, ransomware moderno y otras amenazas serán protagonistas. Por otro lado, hay que destacar que cada vez más organismos se esfuerzan por mejorar la visibilidad para ser más eficientes para responder a incidentes, aquí un vector especialmente expuesto es el mundo OT, los dispositivos IoT y el equipamiento hospitalario.

> ***Los atacantes diversifican en los métodos de ataque que emplean, ya sea en el ámbito, las técnicas, las herramientas, o los métodos de extorsión. Y según se van haciendo fuertes, el coste de responder a dicho incidente crece exponencialmente"***

La adopción de IoT abre un nuevo vector de ataque y la información asociada a este entorno se convertirá en un punto candente para el ciberdelincuente, lo que incitará a las empresas a tener en cuenta las brechas de seguridad que podrían conducir a la filtración o manipulación de datos en estos entornos.

Mención especial requiere la protección de la cadena de suministro. A medida que las empresas se centran en hacer que sus cadenas de suministro sean más sólidas a través de la diversificación y la regionalización, continuarán con la adopción de principios de Zero Trust para mantener sus entornos más seguros.

¿Y cómo consiguen los ciberdelincuentes sus objetivos?, esencialmente diversificando.

Los atacantes diversifican en los métodos de ataque que emplean, ya sea en el ámbito, las técnicas, las herramientas, o los métodos de extorsión. Y según se van haciendo fuertes, el coste de responder a dicho incidente crece exponencialmente.

Por tanto, ante la diversificación, nuestra respuesta deberá estar alineada y se debe analizar la foto completa. Así recurrimos al modelo Zero-trust, que establece que las organizaciones deben asumir que en algún momento van a sufrir un ataque con éxito. Así, la respuesta deber permitir analizar todos los vectores ex-


puestos de la organización (correo, servidores, endpoints, redes, etc.) y que lo haga contextualizando tanto los eventos de seguridad registrados como la telemetría.

Tecnologías como XDR amplían las capacidades de los tradicionales EDR implementando correlación sobre la información (detecciones y telemetría) recibida desde diversos vectores de la organización con el objetivo de generar alertas de calidad que adviertan de manera clara, concisa y temprana sobre un incidente de seguridad.

Una vez detectado el incidente, esta tecnología permitirá al investigador efectuar un análisis en profundidad y tomar acciones correctivas y de respuesta para contener y mitigar el ataque.

Nuestras recomendaciones de seguridad se pueden resumir en los siguientes puntos básicos: asegurar los conceptos básicos de seguridad; mantener estrictas políticas de gestión de parches; comprender y aplicar el modelo de responsabilidad compartida en entornos de cloud híbrida y cifrar periódicamente los datos críticos; aplicar modelos Zero Trust para mantener las aplicaciones y los entornos seguros y mejorar la postura de seguridad; reforzar la seguridad de los entornos productivos, ya sean servidores o cargas en nube; priorizar la visibilidad y apostar por una seguridad sólida con soluciones avanzadas, automatizadas y flexibles que detecten de manera eficiente los ataques en todos los vectores.

***"XDR ayuda a las organizaciones a proporcionar una alerta temprana que les permita reaccionar a tiempo y reducir el impacto económico y reputacional que puede representar un ciberataque"***

## CONCLUSIÓN

Los ataques modernos son cada vez más complejos y distribuidos, trabajando de manera silenciosa hasta que es demasiado tarde.

XDR ayuda a las organizaciones a proporcionar una alerta temprana que les permita reaccionar a tiempo y reducir el impacto económico y reputacional que puede representar un ciberataque. Ofrecer una solución de primer nivel en investigación y respuesta ante incidentes, ayudando a optimizar los equipos de respuesta con correlación e investigación exhaustivas gracias también a la inteligencia de amenazas globales de Trend Micro, es nuestro cometido.

# Plan de sensibilización basado en campañas de *phishing* en el Servicio de Salud de las Illes Balears (Ib-Salut)

**Aurora Ripoll**
Ingeniero Superior de Tecnologías de la Información en el Servicio de Salud de las Illes Balears

PALABRAS CLAVE
**Concienciación, sensibilización, phishing, correo electrónico, campañas**

## INTRODUCCIÓN

El *phishing* es una técnica de ciberataque por medio de correo electrónico en la que los ciberdelincuentes, suplantando la identidad de una persona u organización, tratan de obtener información personal o confidencial de los usuarios. Este ataque es comúnmente utilizado para comprometer directamente a las organizaciones, por lo que la sensibilización de sus trabajadores en esta materia es uno de los aspectos clave para reducir el riesgo de exposición a este tipo de ataques y minimizar cualquier impacto relacionado.

El Servicio de Salud de las Illes Balears (de aquí en adelante, "IB-Salut") invierte grandes esfuerzos en formar y concienciar a sus trabajadores en materia de ciberseguridad, prestando especial atención a la actuación que estos deben realizar ante la recepción de posibles correos de *phishing*. Uno de los métodos utilizados por el IB-Salut para formar y concienciar a este respecto, es el lanzamiento de campañas internas de *phishing*, las cuales se basan en el envío controlado de correos electrónicos a sus profesionales simulando ser ataques reales de este tipo.

## OBLIGACIONES LEGALES

Al hablar de la importancia que tiene la concienciación y sensibilización en materia de seguridad de la información, sin duda cabe 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 5 y las medidas referentes a Concienciación [mp.per.3] y Protección del correo electrónico (*e-mail*) [mp.s.1] las cuales son aplicables a todos los sistemas de información:

**Artículo 5. La seguridad como un proceso integral.**

[...]

2. Se prestará la máxima atención a la concienciación de las personas que intervienen en el proceso y a sus responsables jerárquicos, para que, ni la ignorancia, ni la falta de organización y coordinación, ni instrucciones inadecuadas, sean fuentes de riesgo para la seguridad.

Medidas de protección referentes a la Concienciación [mp.per.3].

Se realizarán las acciones necesarias para concienciar regularmente al personal acerca de su papel y responsabilidad para que la seguridad del sistema alcance los niveles exigidos.

En particular, se recordará regularmente:

a) La normativa de seguridad relativa al buen uso de los sistemas.

b) La identificación de incidentes, actividades o comportamientos sospechosos que deban ser reportados para su tratamiento por personal especializado.

c) El procedimiento de reporte de incidentes de seguridad, sean reales o falsas alarmas.

***Medidas de protección referentes a la Protección del correo electrónico (e-mail) [mp.s.1]***

El correo electrónico se protegerá frente a las amenazas que le son propias, actuando del siguiente modo:

[...]

d) Se establecerán normas de uso del correo electrónico por parte del personal determinado. Estas normas de uso contendrán:

1.º Limitaciones al uso como soporte de comunicaciones privadas.

2.º Actividades de concienciación y formación relativas al uso del correo electrónico.

## PLAN DE SENSIBILIZACIÓN BASADO EN CAMPAÑAS DE PHISHING

El IB-Salut incluye en su plan anual de formación y sensibilización la realización de campañas internas de *phishing*. Estas permiten medir el grado de concienciación, en materia de seguridad de la información, de sus trabajadores, evaluar el nivel de riesgo frente a este tipo de ataques, analizar la efectividad de las campañas de concienciación realizadas en años anteriores e identificar en que grupos de usuario es necesario incidir en términos de formación.

Las citadas campañas, consisten en el envío controlado de correos electrónicos, que simulan ser casos reales de *phishing*, a todos los usuarios de sus nueve gerencias territoriales. Estas campañas son gestionadas mediante una herramienta especializada del mismo fabricante del antivirus de la organización.

Cada Gerencia se ve sometida trimestralmente a las citadas campañas (4 veces al año), las cuales tienen una duración de una semana por cada Gerencia y se realizan en el transcurso de 4 semanas, realizándose así de manera paralela entre dos o tres Gerencias.

En cada campaña cada Gerencia recibe 6 posibles casos de *phishing* (un total de 24 al año), los cuales son repartidos en 6 grupos distintos del total de los usuarios de cada gerencia (evitando así la sospecha de la simulación por parte de los usuarios y la sobrecarga en el tráfico).

Para el diseño y elaboración de los casos de *phishing*, el IB-Salut ha definido 6 temáticas diferentes y, en base a las mismas, los ha personalizado en función de la realidad de cada gerencia y en materias del sector de la salud. Las principales temáticas utilizadas para elaborar los casos de uso y llamar la atención de las víctimas, son las siguientes:

- **Promociones especiales:** invitaciones al uso de servicios y/o productos que habitualmente son de pago. Por ejemplo: un año gratis de plataformas multimedia, día gratuito en aparcamientos de la zona, regalo de *smartphones* de alta gama, etc.
- **Curiosidades:** información relacionada con aspectos privados y/o confidenciales de otras personas u organizaciones. Por ejemplo: listados de nóminas de otros trabajadores, *ranking* de hospitales del país que han realizado una mejor gestión sanitaria durante la pandemia, etc.
- **Información de salud:** información relacionada con el estado de salud de pacientes. Por ejemplo: acceso a la historia clínica de un paciente que padece un diagnóstico poco habitual.
- **Soporte técnico:** comunicaciones sobre el mal funcionamiento de recursos tecnológicos. Por ejemplo: fallo en la recepción del correo electrónico, avisos de caducidad de contraseñas, etc.
- **Corporativo:** información sobre la organización. Por ejemplo: regalo de días de vacaciones, cambios de citas para la revisión de salud laboral, invitación a eventos internos, etc.
- **Tendencias:** temas que tratan información de actualidad. Por ejemplo: nuevas medidas relacionadas con el Covid-19, acciones solidarias para el volcán de La Palma, etc.

Asimismo, los citados casos de *phishing* serán a su vez de dos posibles tipologías:

- Aquellos en los que su contenido incluye un enlace a un sitio web, supuestamente fraudulento. Los sitios web a los que redirigen los citados enlaces, son también personalizados de tal manera que parecen casos reales. En la mayoría de los casos, se solicita la introducción de información personal y/o confidencial (usuario, contraseña, número de cuenta, etc.)
- Y aquellos en los que se adjunta un archivo, supuestamente malicioso. Del mismo modo que en el caso de los enlaces, los archivos ad-

> ***El IB-Salut incluye en su plan anual de formación la realización de campañas internas de phishing que permiten medir el grado de concienciación, en materia de seguridad de la información, de sus trabajadores, evaluar el riesgo frente a este tipo de ataques e identificar en que grupos de usuarios es necesario incidir en términos de formación"***

juntos también son personalizadas para que parezcan tratarse de un caso real.

Una vez finaliza la campaña, los usuarios reciben de manera automática un mensaje de finalización en su correo electrónico, dónde el Servicio de Seguridad de la Información del IB-Salut, les informa acerca de su resultado en la misma, les recuerda los principales aspectos a tener en consideración en el caso de recibir un posible correo de *phishing* y facilita un enlace a un curso de formación recomendado (el cual varía en función de la temática y caso de *phishing* concreto).

A su vez, tras finalizar las pruebas, el Servicio de Seguridad de la Información del IB-Salut, procede a la recolección de la siguiente información sobre los resultados de la misma:

- Porcentaje de usuarios que han abierto los correos de *phishing*.
- Porcentaje de usuarios que han accedido al enlace, supuestamente fraudulento.
- Porcentaje de usuarios que han accedido al enlace y que, adicionalmente, han introducido sus credenciales.
- Porcentaje de usuarios que han descargado el archivo adjunto, supuestamente malicioso

Una vez obtenida esta información se procede a su explotación y correlación junto con otra información de carácter organizativo, la cual permite al IB-Salut conocer:

- El grado de concienciación de la organización y de cada gerencia.
- Las categorías de profesionales menos concienciadas.
- Las temáticas de correos de *phishing* de mayor riesgo para la organización

Puesto que el principal objetivo de esta actividad no es otro que el de concienciar y sensibilizar a los trabajadores de la organización, se procede a compartir con cada Gerencia los resultados de la campaña, a través de un comunicado oficial dirigido a todos sus usuarios. Aunque para el IB-Salut es un principio evidente, se considera importante aclarar que esta información es puramente estadística y se proporciona anonimizada en su totalidad.

## CAMPAÑAS DE CORREOS DE PHISHING A DIRECTIVOS

El IB-Salut también incluye en su Plan de Formación y Concienciación la realización de campañas de *phishing* al personal directivo. Aunque la metodología es prácticamente la misma que la de las campañas dirigidas a todos los usuarios, cabe destacar algunas pequeñas diferencias:

- Destinatarios de las pruebas: las víctimas de estas campañas son los miembros formales de los Comités de Seguridad de la Información de cada Gerencia.
- Periodicidad de las pruebas: las campañas se realizan con carácter semestral (2 veces al año).
- Casos de *phishing*: los casos de correo utilizados para las pruebas se personalizan en su totalidad en función de la categoría de cada directivo y se elaboran tantos casos como el número máximo de miembros de los Comité de Seguridad de la Información.
- Presentación de los resultados: los resultados de la campaña se comparten directamente con el responsable de Seguridad de la Información de cada Gerencia y se presentan formalmente en los respectivos comités.

## REFERENCIAS

[1] Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

# XIX FORO de Seguridad y Protección de Datos de Salud

*"Protección de Datos en los nuevos modelos de atención social y sanitaria"*

**LA XIX EDICIÓN DEL FORO DE SEGURIDAD Y PROTECCIÓN DE DATOS DE SALUD DE LA SEIS SE CELEBRÓ EL 16 Y 17 DE FEBRERO DEL 2022 EN MADRID. EL ENCUENTRO GIRÓ EN TORNO A LOS NUEVOS MODELOS DE ATENCIÓN SOCIAL Y SANITARIA, LA NECESIDAD DE GARANTIZAR LA PRIVACIDAD Y LA SEGURIDAD DE LA INFORMACIÓN EN LOS NUEVOS TRATAMIENTOS Y LA SECURIZACIÓN DE LOS DISPOSITIVOS MÉDICOS.**

## INAUGURACIÓN OFICIAL


Durante su intervención, Luciano Sáez agradeció la rápida respuesta del Servicio Madrileño de Salud por el cambio de sede del Foro y la presencia de la directora de la Agencia Española de Protección de Datos, así como de los responsables de Protección de Datos de las comunidades autónomas. Sáez destacó que "el reto durante la pandemia ha sido garantizar la calidad en la asistencia sanitaria, así como la elaboración de informes que han ayudado a la gestión y la necesidad de compartir los datos de forma segura". También resaltó que la finalidad del Foro era la "concienciación a directivos y responsables de la importancia de la protección de datos y seguridad de la información".

A continuación, tomó la palabra María Luz de los Martires Almingol, directora general de Sistemas de Información y Equipamientos Sanitarios del Servicio Madrileño de Salud, que agradeció el compromiso de la directora de la Agencia Española de Protección de Datos, así como de la SEIS y de todos los profesionales del sector sanitario. Sobre el impacto de la pandemia destacó que "ha supuesto un cambio de paradigma en Atención Primaria y Especializada. Se debe ofrecer el servicio donde esté el paciente (telea-sistencia, vídeo consulta, etc.), lo que supondrá una alta inversión en herramientas tecnológicas para conseguirlo de forma segura y eficaz. Estas nuevas capacidades abren el campo de exposición, por lo que se han aumentado los ataques recibidos en el sector de sanidad".

Posteriormente tomó la palabra Mar España Martí, directora de la Agencia Española de Pro-

tección de Datos quien destacó que "la salud y la protección de datos solo se valoran cuando se pierden. Por este motivo se debe poner el foco en la protección de la privacidad por defecto y desde el inicio de cualquier sistema de información. La persona es el centro del sistema sanitario y los datos de salud deben ser el corazón y el motor de toda la investigación sanitaria, que debe realizarse con base en los principios de transparencia e información de los interesados".

**PRIMERA SESIÓN: AUTORIDADES DE PROTECCIÓN DE DATOS**

La moderadora, **María Luz de los Mártires Almingol,** directora general de Sistemas de Información y Equipamientos Sanitarios del Servicio Madrileño de Salud presentó a los ponentes.

Durante su intervención, **Jesús Rubí Navarrete,** adjunto a la Dirección de la Agencia Española de Protección de Datos, trató dos temas. Sobre el primero: la monitorización de los ensayos clínicos; señaló que tuvieron que "coordinarse la Agencia Española de Protección de Datos y la Agencia Española del Medicamento, diseñando documentos y protocolos de seguridad, que en un principio solo debían ser para el tiempo que durara la pandemia. La polémica surgió con los accesos remotos a los monitores, pero se llegó a la conclusión que la cesión de los datos por parte del promotor debía realizarse mediante un acuerdo, pero no con la posición jurídica de encargado de tratamiento. También se acordó que se podría llevar a cabo esta monitorización de las investigaciones más allá de la pandemia. Las autoridades resolvieron que las garantías que se habían llevado a cabo durante la pandemia eran suficientes para prolongar la monitorización".

Sobre el segundo tema: la Comisión de salud digital, puntualizó que "esta iniciativa debe permitir un análisis masivo de todas las finalidades establecidas en el RGPD y está incluido en el espacio europeo de protección de datos. Se insistirá en que primero debe hacerse una Evaluación de Impacto, que incluya la participación de los delegados de Protección de Datos de las comunidades autónomas, para que se expongan y evalúen correctamente todos los aspectos que puede conllevar".

A continuación, tomó la palabra **María Àngels Barbará i Fondevila**, directora de la Autoridad Catalana de Protección de Datos quien destacó que "debido a la pandemia, se ha tenido que trabajar en diferentes actuaciones para garantizar la protección de datos. En todos los casos, los principios de limitación de la finalidad y proporcionalidad permiten conseguir los objetivos perseguidos y al mismo tiempo garantizar la privacidad de los datos de las personas. El intercambio de información sensible ha puesto de manifiesto que el RGPD permite realizarlos cuando es una necesidad vital. Se ha podido observar la interrelación entre el sector social y el sanitario, que permite mejorar las condiciones de las personas necesitadas. El intercambio de información está permitido en determinados casos, siempre que se tenga en cuenta el principio de minimización. Las personas deben saber cuándo, quién y por

qué tratan sus datos. La pandemia ha acelerado la digitalización de la sociedad".

Posteriormente, **Margarita Uría Etxebarría,** directora de la Agencia Vasca de Protección de Datos señaló que "el intercambio de información entre la atención social y la atención sanitaria ha sido muy relevante durante la pandemia, con la complejidad sobre las competencias y sobre los datos tratados. Ha sido un reto tecnológico, pero se ha respondido. Durante la pandemia se ha creado un convenio para el uso compartido de la historia cínica en determinados casos. El marco normativo, en algunos casos no ha sido suficiente y desde las CC AA se ha tenido que aprobar alguna legislación específica. En este aspecto, la Autoridad Vasca ha propuesto una Ley de Protección de Datos específica para el País Vasco".

Por último, tomó la palabra **Jesús Jiménez López,** director del Consejo de Transparencia y Protección de Datos de Andalucía. "La pandemia ha analizado el intercambio de información de atención social y sanitaria y ha detectado una asimetría. La tecnología está mucho más avanzada en la atención sanitaria. El tratamiento masivo de los datos debe ser conocido por la ciudadanía. Este tratamiento masivo de datos produce un resultado que el médico debe ser capaz de explicar al paciente. En el trámite para legislar en materia de protección de datos no existe ningún procedimiento a seguir como sí existe en otras materias", destacó.

## CONFERENCIA INAUGURAL: CIBERSEGURIDAD

**Carlos Córdoba**, jefe de Centros de Operaciones de Ciberseguridad del Centro Criptológico Nacional, pronunció la conferencia inaugural. Durante su intervención destacó "la necesidad que tienen los organismos públicos y en especial los servicios de salud de contar con servicios de SOC, los cuales, como norma general, se deberán contratar, ya que el personal de la organización no puede asumir la carga de trabajo que se genera y es un mundo muy complejo. Desde el CCN se asesora a las organizaciones para la implantación de un SOC, implantando las medidas de seguridad adecuadas a cada organización.

La tecnología y los procesos nos proporcionan las alertas que se deben revisar para evitar los ataques. Un ejemplo son las sondas de Detección del Sistema Alerta Temprana (SAT). Para interpretar y solucionar estas alertas es necesaria la intervención de las personas. En el sector de la salud se ha desarrollado la sonda de control industrial (SAT- ICS), ya que hay muchas cosas conectadas a Internet, como pueden ser los equipos médicos, equipos IoT, etc.".

Carlos Córdoba también explicó el proceso de creación de la Red Nacional de SOC (RNS), que se está liderando desde el CCN y cuyo objetivo principal es estandarizar para que todas las organizaciones tengan un nivel mínimo de seguridad. Esta estandarización se basa en 9 puntos:

- Uso de LUCIA federado para el intercambio automático y fluido de ciberincidentes. Eliminar

el correo electrónico y adherirse a la Plataforma Nacional.

- Compartir reglas para la Vigilancia y Detección, tanto perimetral como interna.
- Despliegue de EDR o XDR en toda la organización, según catálogo CCN – STIC 105, complementado con µClaudia.
- Capacidad de recolección y correlación de los logs necesarios para la detección, según catálogo CCN-STIC 105.
- Impulso al cumplimiento del ENS en las organizaciones atendidas. Uso de INES / AMPARO para conseguir la certificación.
- Realización de auditorías continuas para valorar el estado de seguridad de las organizaciones atendidas.
- Detección del perímetro y la red interna basadas en anomalías. Disponer de equipos de investigación ante ataques complejos.
- Intercambio de ciberinteligencia con la Plataforma Nacional.
- Colaboración e intercambio de mejores prácticas, investigaciones en curso y otras actividades de Vigilancia Digital.

## SEGUNDA SESIÓN: SOLUCIONES PARA LA CIBERSEGURIDAD EN ENTORNOS SANITARIOS

La segunda sesión estuvo moderada por **Francisco García Lombardía**, director técnico de la Consejería de Sanidad de la Comunidad de Madrid.

En primer lugar, intervino **Toni Martínez**, Systems Engineer de Fortinet Iberia con el lema: "Sanidad segura: Zero Trust Access para entorno sanitario", quien expuso el concepto Security Fabric: productos que puedan interactuar entre ellos y no de forma individual para cubrir la mayor exposición de ataque, de forma sencilla, intentando automatizar al máximo el día a día en un entorno tan distribuido como el sanitario donde se hace necesaria la optimización de recursos.

**Amit Har-Esh**, sales director de South EMEA de la empresa Medigate, trasladó la propuesta de la compañía para ayudar a los hospitales en España a través de la tecnología, la cual dota de capacidades de visibilidad de todos los dispositivos de forma pasiva conectados a la red, evaluación Riesgo de cada dispositivo e identificación del uso de los dispositivos médicos. Asimismo, resaltó que estas capacidades se proporcionan sin necesidad de instalar nada en los dispositivos.

**Alberto Sempere Blanco**, global director For CyberSecurity Products de Telefónica Cybersecurity & Cloud Tech, destacó la necesidad de contextualizar la situación de cada organismo con base en su madurez lo cual "permitirá la definición de los proyectos a corto, medio y largo plazo". En lo referente al cómo abordar los retos, recordó la importancia de las cuatro fases: evaluación, planificación, implantación y gestión. Por último, resaltó la necesidad de que los servicios de salud cuenten con SOC adaptados a sus necesidades.

**José de la Cruz**, director técnico de Trend Micro intervino con el tema "Conectando los puntos" y expuso que los ataques se están realizando a cualquier nivel. "Para minimizar riesgos, se usa

la tecnología Zero Trust, aunque no es segura al 100%. Se asume el riesgo de que nos atacarán seguro, pero debemos estar lo mejor preparado posible, es decir, no solo cuando suceda. En este sentido, la regla de las 3 C's puede ayudar a estar mejor preparado:

Coste = Cómo (medios invertidos para proteger) x Cuándo (tiempo que se tarda en mitigar el riesgo)

El tiempo es oro, cuanto más tiempo se tarde en responder, mayor coste tendrá el ataque. Los virus utilizan múltiples vectores de ataque. Ante un ataque, necesitamos el contexto y reaccionar lo más rápidamente posible. La tecnología EDR utiliza la telemetría, que sirve para detectar eventos, mientras que la tecnología XDR utiliza la tecnología EDR para encontrar el origen, es decir, XDR lo une todo. La solución propuesta es Vision One", señaló de la Cruz.

A continuación, Andrés Martín Roldán, Presales and Managed Detection & Response Services de Fujitsu intervino con el lema "¿Cómo mejorar el nivel de resiliencia del sector para afrontar un *ramsomware*?". Sobre este apartado explicó que "los últimos ataques en el entorno sanitario y su gravedad han incrementado el grado de concienciación y su preocupación por la mejora del nivel de resiliencia; el análisis de situación frente al *ransomware*. Las causas de los ataques de *ransomware* básicamente son cinco: falta de visibilidad de los activos, mala segregación de entornos, debilidades de los sistemas de protección y detección, carencias de gobierno, vulnerabilidades y amenazas. La adopción de medidas debe basarse en los cuatro pilares: gobierno, prevención, detección / respuesta, recuperación)". Y remarcó: "nunca pagar".

Roldán señaló que tienen experiencia en la implantación de tecnología Breach & Attack Simulation (BAS); implantación de tecnología Virtual Parching; implantación de tecnología Gestión Usuarios Privilegiados (PAM); consultoría y asesoramiento de certificación ENS; implantación de tecnología Control Acceso NAC; implantación de tecnología de identificación y autenticación segura en entornos OT; implantación SIEM; operación, administración y soporte de la infraestructura de seguridad. Sobre el caso concreto de la implantación de tecnología BAS en el IB-Salut, matizó que "el reconocimiento e impacto de nuevas amenazas se analiza de forma automatizada; te da una foto en cada momento, no en un momento concreto".

Finalmente, Daniel Urbina, de Iberia Public Sector Solutions Architect Manager de AWS, participó con el lema "No soy inseguro, doctor... ¿O sí?". Indicó que "se crean aplicaciones que procesan datos y estos datos deben estar seguros. La oferta de AWS son controles que cumplen con diferentes medidas de seguridad, incluidas las del ENS para el almacenamiento en la nube, con un modelo de responsabilidad compartida, aportando herramientas para todo el ciclo de vida del dato, con todos los elementos que hay que securizar, herramientas de gestión y herramientas de respuesta y recuperación". En este sentido, presentó el caso del uso de las medidas que lleva el acceso a la historia clínica para garantizar la seguridad del acceso. "Es donde aparece el dilema: Innovar o estar seguro; pues las dos cosas". También destacó las soluciones de seguridad, identidad y cumplimiento para el sector sanitario: Amazon GuardDuty (monitorización útil para la toma de decisiones); Amazon Inspector (se aplican políticas sobre diferentes capas de trabajo para "obligar" a cumplir con la seguridad); Amazon Macie (vigila la información privada); Amazon Detective (ayuda a investigar elemento de seguridad hasta encontrar origen del ataque); AWS Audit Manager (crea informes de forma automática, por tanto, máxima disponibilidad).

Por último, el moderador, Francisco García Lombardía, director técnico de la Consejería de Sanidad de la Comunidad de Madrid lanzó las siguientes reflexiones: Es muy importante el tema de la reputación; Los dispositivos OT son muy vulnerables y este problema es común a todos; Las herramientas son muy valiosas, pero se desconoce la capacidad y el valor real de las mismas. Hay que poner sentido común cuando se utilizan; Con cualquier metodología es muy importante saber cómo actuar en cada momento, hay tantas cosas que hacer, que frecuentemente provoca una desorganización que es aprovechada por el atacante; Debe haber equilibrio entre los cuatro pilares: gobierno, prevención, detección/Respuesta, recuperación; Nos pueden atacar por el eslabón más pequeño; El temor a la nube hay que superarlo.

## TERCERA SESIÓN: TRATAMIENTO DE LA INFORMACIÓN PARA UNA ATENCIÓN INTEGRAL DE LAS PERSONAS

La tercera sesión estuvo moderadora por Blanca Peraferrer Vayreda, jefa de Área de Inspección de la Autoridad Catalana de Protección de datos, que sustituyó a Santiago Farré Tous, quien indicó que "el intercambio de información entre atención social y sanitaria durante la pandemia ha sido muy relevante, y sobre todo a partir de la ley 2/2021 de medidas urgentes para hacer frente a la situación".

Sara Hernández Corbacho, responsable d'Organització de la Oficina del Delegat de Protecció de Dades de Salut explicó que "la atención sanitaria y la atención social están fragmentados, por ello, se promovió la historia clínica compartida, que se basa en el principio de interoperabilidad. Los servicios sociales disponen de varios sistemas de información, pero no disponen de historia social compartida, por lo que se promovió un piloto para trabajar en el intercambio de información, desde el punto de vista legal y funcional. Se promovió mediante un convenio con las siguientes condiciones: El acceso a este intercambio de información, solo podrán realizarlo los profesionales implicados en el proceso, con el deber de secreto de confidencialidad; Las entidades deberán garantizar las medidas de seguridad adecuadas y el ejercicio de derechos de los interesados; Está basado en el principio de minimización; Diccionario semántico para tener un vocabulario común; No existe una historia común compartida, sino que se consulta cada vez que es necesario mediante webs. Este intercambio de información tiene como finalidad la atención integral de las personas".

A continuación, intervino Joaquín Cañada González, delegado de Protección de Datos de la Generalitat Valenciana. "En la Generalitat valenciana la legislación está muy dispersa. La relación actual es más de colaboración. Expongo dos casos: el primero, un sistema fragmentado. Los servicios sociales para la dependencia utilizan un formulario que es ingestionable en un plazo razonable. Se propuso priorizar por enfermedades. Se estudió y se descartó solicitar el consentimiento, al considerarse que el interés público esencial era una base de legitimación adecuada. Se tuvo que comprobar si en el formulario figuraba alguna casilla que indicase el derecho de oposición, lo cual ocurría. Se realizaron algunas propuestas adicionales de mejora; el segundo, un sistema integrado. Su origen fueron unos pliegos de un sistema informático que pretendía integrar sistemas mediante la legislación vigente. Se planteó que hubiera un régimen de corresponsabilidad, ya que aportan garantías adicionales y facilita a los usuarios no tener que ir de un sitio a otro. Para finalizar, se indicó que la coherencia en el desarrollo legislativo aporta seguridad".

Por su parte, José María Molina, jefe del Servicio de Informática de los Servicios Sociales de Castilla y León explicó su experiencia en el intercambio de datos entre servicios sociales y salud. Bajo su criterio, los servicios sociales deben tener la máxima cooperación, pero la mínima dependencia con los servicios de salud. "En Castilla y León se integraron todos los servicios sociales de base en

un único sistema unificado (SAUS). Que los profesionales de salud y servicios sociales solo accedan con informes en papel, en ambos sentidos, se considera precario, ya que la legislación permite el intercambio de información, pero parece que no hay voluntad de cambio. Esta falta de acceso a los datos perjudica a los pacientes (personas) al estar solo coordinado con informes o por teléfono (dietas, tratamiento farmacológico, atención en domicilio, derivaciones a centros sociales, etc.). Esta es la realidad. Se realizó el proyecto Argos que aportó mucho conocimiento en nomenclatura en salud, llegando a la conclusión de que se tenía que hacer también para servicios sociales. Se considera que lo ideal es el intercambio y la interoperabilidad, ya que la tecnología existe y la legislación también. Es bastante sencillo, pero parece que no hay voluntad política para ponerlo en marcha. Lo importante tendría que ser facilitar la vida al ciudadano, como se ha hecho en otras administraciones como en Empleo o Hacienda".

Por último, **Marcos Sánchez Martínez**, Manager en Ciberseguridad y Protección de Datos de EY explicó que "el contexto de la ciberseguridad es el aumento de los ataques al sector de salud. Los retos que se afrontan en el intercambio de información se basan en cuatro pilares: gestión de las identidades de los profesionales para garantizar la privacidad de los datos; correcta configuración de los dispositivos y de las comunicaciones; categorizar, clasificar y almacenar la información; y garantizar la cadena de suministro. Estos retos se pueden convertir en oportunidades. Actualmente, hay muchas copias no controladas. La privacidad desde el diseño y por defecto, nos permite configurar que esto no pueda suceder, excepto ante los casos que sea estrictamente necesario. Debería aplicarse el lema de la gestión de identidades: *Just in time* (tener acceso a la información en el momento que sea necesario y evitar así las copias)".

## CUARTA SESIÓN: CIBERSEGURIDAD EN EL INTERNET DE LOS DISPOSITIVOS MÉDICOS

El moderador, **José Luís Falcón**, director del Área de Protección de Datos del Consejo de Transparencia y Protección de Datos de Andalucía realizó la reflexión: "los dispositivos médicos facilitan tratamientos y la investigación, pero a la vez introducen riesgos que hay que minimizar".

Luis Santiago Sánchez Fernández, jefe de Sección de Sistemas para Sevilla del Servicio Andaluz de Salud, destacó que "la cantidad de recursos y sistemas que se tienen es insostenible. Indica que muchos fabricantes no están concienciados con la seguridad y que sus dispositivos van a funcionar en un entorno que debe cumplir con la legislación vigente.

A continuación, **Jorge Pardo Casal,** delegado de Protección de Datos del Servicio Gallego de Salud, indicó que "la evaluación de riesgos cobra mucha importancia y es muy compleja. Los riesgos tienen que ser aceptados y sobre todo aceptables. Muchos dispositivos acaban su vida porque el ordenador asociado no puede ser actualizado. La Inteligencia Artificial puede ser

peligrosa, ya que puede predecir dolencias sin saber si será real ni por qué".

Seguidamente, Teresa Ramos, head of Personalised Healthcare de Roche Farma S.A., demostró la importancia de los datos para tomar decisiones clínicas y del propio paciente. "La importancia está en salvar la barrera que impida la compartición de los datos, la integridad y la disponibilidad. La medicina personalizada es imposible sin tener datos. Son productores e integradores de datos. Están explorando cómo la Inteligencia Artificial puede ayudar a predecir la enfermedad que el paciente padecerá. También son consumidores de datos, por lo que apoyan la cultura de la compartición de los datos ya que los datos son la fuente de conocimiento y ayudan a crear nuevas terapias. Se tiene conciencia en proteger los datos de salud, pero no en proteger otros campos, como las redes sociales".

Carlos Abad, head of Phygital Security de SIA, expuso la problemática que afecta a los dispositivos médicos: "Los dispositivos *IoT* en salud suponen un porcentaje bajo en referencia a otros entornos como los *smartphones*, de los que se pueden beneficiar. Lo primero que identifican es quién es el propietario del equipo, qué normativas deben aplicarse y la complejidad del propio dispositivo. En este complejo entorno se dispone de herramientas para una gestión eficiente. La terna importante es el fabricante y el propietario del activo, así como el especialista de ciberseguridad. Los riesgos a mitigar son la confidencialidad, la integridad, la disponibilidad y que el dispositivo se pueda utilizar para otras cosas".

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

El moderador, Pedro Alberto González, responsable del Registro y Auditoría de Ficheros de la Agencia Vasca de Protección de Datos, indicó que los casos expuestos se centrarían en los principios de licitud, lealtad y transparencia y de la minimización de datos.

Cristina Gómez Piqueras, coordinadora de Instrucción de la Subdirección General de Inspección de Datos de la Agencia Española de Protección de Datos, expuso los casos sobre licitud, lealtad y transparencia de toma de temperatura de un centro comercial por parte de los vigilantes de seguridad; el de la decisión de quién es el responsable de tratamiento en una clínica privada; y del uso de pruebas realizadas de forma privada para un uso posterior con otra finalidad. En cuanto al principio de minimización; expuso el de solicitud de datos como el diagnóstico y tratamiento en un justificante médico.

A continuación, Blanca Álvarez Yaque, jefa del Gabinete de Investigación y Correctivo del Consejo de Transparencia y Protección de Datos de Andalucía comentó los casos sobre licitud, lealtad y transparencia del pasaporte covid; el de transferencias de datos entre organismos públicos; así como el de transferencia de datos entre trabajadora social y médico de cabecera para un trámite social del paciente. En cuanto al principio

de minimización, expuso el del informe médico para una ortopedia, el de la solicitud de informe sobre el uso de un dispositivo electrónico para realizar un examen y el de la exención de llevar mascarilla para entrar en un centro de salud.

Por su parte, **Blanca Peraferrer Vayreda,** jefa de Área de Inspección de la Autoridad Catalana de Protección de Datos mostró los casos sobre licitud, lealtad y transparencia del cambio de circuito de recogida de la medicación de un paciente; el de la declaración responsable de unos padres de un colegio; y el del acceso a los datos de Atención Primaria de todos los pacientes de una clínica privada. En cuanto al principio de minimización, expuso el del listado de turnos de un hospital.

Para finalizar, **Juana Vegas Fernández,** letrada instructora de la Asesoría Jurídica de la Agencia Vasca de Protección de Datos, expuso los casos sobre licitud, lealtad y transparencia del homenaje de un ayuntamiento a los fallecidos por covid de una residencia. En cuanto al principio de minimización, mostró el del informe de alta de un accidente doméstico, el del justificante de ingreso del suegro, el de la denuncia por *mobbing* de un técnico a su jefe y el de la cancelación de un episodio de la historia clínica.

## SEXTA SESIÓN: SOLUCIONES DE SEGURIDAD ANTE EL TRATAMIENTO DE DATOS DE SALUD

Intervino como moderador **Juan Antonio Gómez** Palomeque, director de Tecnologías de la Información y de la Comunicación del Servicio Andaluz de Salud.

**Alex López de Atxer**, Regional Sales Manager IBERIA de Gigamon, intervino con el tema "Captura de tráfico para análisis en sondas de IoHT". Sobre este aspecto destacó que "lo importante es conseguir los datos para que se analicen. La solución es desacoplar las aplicaciones de la red para capturar los datos. Filtran esos datos y los envían donde corresponde, copiando el tráfico con TAPS. Esta tecnología está homologada en la guía CCN 607".

**Javier Aguado Benito,** ingeniero de Preventa del Grupo Oesía, habló sobre la "Importancia de la monitorización del *IOT* en Sanidad". En este sentido, señaló que "es importante monitorizar los activos ya que pueden costar vidas y la información que almacenan es muy sensible. Se pueden utilizar conocimientos de *IT* y *OT* para aplicarlos a los dispositivos médicos. Debido a la multitud de dispositivos (estáticos y móviles que van con el paciente) se necesitan unos requisitos de monitorización que tienen como objeto detectar y prevenir amenazas. Las fases para obtener monitorización eficiente son: Diseño de la arquitectura; Visibilidad en tiempo real de los dispositivos; y Búsqueda, detección y Análisis. Todo esto necesita un SOC para que sea útil y que no se quede ahí, sino que gestione los datos que se obtienen".

**Carlos Pastor Matut**, responsable de estrategia *blockchain* de Inetum presentó su intervención: "Identidad autogestionada en entornos sanitarios" a través de la cual explicó la dificultad de "borrar los datos porque no sabemos quién los

tiene y para qué los usa. La identidad autogestionada es aquella en la que el propio usuario gestiona sus datos. La aplicación en entornos sanitarios típicos es la tarjeta sanitaria, la historia clínica, el consentimiento informado y la receta electrónica. Para ello se utiliza un *wallet* o cartera de identidad digital para almacenarla y poder compartirla con quien queramos. También se puede hacer gestión de contraseñas en la propia aplicación del móvil. Por tanto, se tiene una única identidad para todo y la podemos facilitar con un clic en el móvil. Para dejar de compartirla; es igual de fácil. Se usa la tecnología *blockchain*. El usuario es el que controla sus datos, pero cuando se escribe algo, no se puede modificar, aunque seas administrador. Todo queda en el móvil, quién lo ha solicitado, a quién lo ha dado y cómo puedo cancelarlo. El proyecto en España se llama Dalion y España es referencia a nivel mundial. Se está colaborando para realizarlo a nivel europeo".

A continuación, Javier Alonso, Cyber Sales Manager de Sham (Grupo Relyens) definió el tema "Vulnerabilidades de dispositivos médicos y estrategias para su control". Explicó que "la red hospitalaria es un sistema complejo, por la obsolescencia de los sistemas que gestionan dispositivos, falta de visibilidad…". También destacó ejemplos de vulnerabilidades en dispositivos de imagen mediante tres protocolos que se conectan con contraseñas públicas de Internet. En esta línea presentó "la solución CyberMDX con la que la prevención es relativamente fácil, mediante la recopilación de información, entender qué debe securizarse y cómo, por último, hay que actualizar la seguridad del dispositivo. El riesgo ciber dentro del hospital es único".

Para finalizar, Pablo Chapinal, de Microsoft participó con el tema "La nube como habilitador de la Seguridad". Explicó que el "modelo tradicional en una red cerrada se ha convertido en la dispersión de equipos. Pasan más cosas fuera de la red que dentro, por tanto, el nuevo perímetro es la identidad del usuario. Esto requiere nuevos principios como: verificar explícitamente que cualquier cosa (usuario, servicio…) es quien dice ser; el uso de los servicios sin tenerlos asignados, sino solo cuando se necesiten; y asumir que se tendrá una brecha en cualquier momento. La solución que proponen en Microsoft es Zero Trust que tiene seis pilares: identidad, dispositivos, apps, Infraestructura, red y datos. La arquitectura son recursos, por un lado, y gestión, identidades y los dispositivos, por otro.

Microsoft propone Azure AD mediante un conector que tenga la información necesaria de los directorios que estén *on premise*. También plantea evitar las contraseñas e impulsar la identificación biométrica. Primero mediante el análisis de la identidad (NCA) y después con el análisis del dispositivo de formas dinámicas (EDR). Un ataque suele entrar por correo (enlace o fichero), que hace un *exploit* para controlar la identidad y la organización con posterioridad. Microsoft 365 Defender es una plataforma única que simplifica mucho la resolución del ataque.

## SÉPTIMA SESIÓN: PROTECCIÓN DE DATOS Y SEGURIDAD DE LA INFORMACIÓN EN LA TELE-ASISTENCIA

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

Manuel Jimber del Río, responsable de la Unidad de Seguridad TIC del Servicio Andaluz de Salud expuso que por parte del responsable de Seguridad, los riesgos pueden verse desde las siguientes perspectivas: "Ciberseguridad (análisis de riesgos, que se pueden incrementar por la difuminación del perímetro y los accesos remotos, incluidos ahora los de los pacientes) y de Vulneración de derechos de los pacientes (evaluaciones de impacto que nos indican cómo actuar, no solo en la privacidad, sino directamente en su salud). Hay dos factores que en teleasistencia complican un poco más. En primer lugar, es posible realizar procesos sin utilizar la infraestructura sanitaria. Esto puede crear desigualdades, ya que puede que estos procesos existan en unos hospitales o centros de salud y en otros no. En segundo lugar, esto genera también equipos TIC desconocidos y no sabemos ni cómo funcionan y las medidas de seguridad de-

penden de ellos. Tienen su propio DPD, su propio responsable TIC…".

José Ignacio Sánchez Brezmes, delegado de Protección de Datos de la Consejería de Sanidad y de la Gerencia Regional de Salud de Castilla y León indicó que "ser delegado de Protección de Datos no es una posición cómoda, ya que el sector sanitario está caracterizado por la urgencia, lo cual dificulta el análisis. Durante la pandemia se ha trabajado en tres proyectos: Telepresencia (que permite la asistencia de diferentes profesionales a la vez, unos *in situ* y otros en remoto); Video consulta (permite la asistencia sanitaria no presencial); y Video consulta grupal (uso de videoconferencia con diferentes personas, como la preparación al parto…). La base de legitimación es lo más difícil de conseguir y se debe estudiar cada caso. El análisis de riesgos evidenció un alto grado de riesgos, pero se constató que el responsable los había previsto y tenía un nivel de madurez ENS de L3, en los tres proyectos. Se tuvo que elaborar un plan de acción para conjugarlo todo. La conclusión es que es posible realizar una gestión de riesgos proactiva junto con los profesionales".

Juan Ignacio Coll Clavero, director general de Transformación Digital, Innovación y Derechos de los usuarios del Servicio Aragonés de Salud matizó que "la pandemia ha dado un empujón a la telemedicina por la necesidad de proteger a los pacientes. Se colapsó el canal habitual del teléfono y se tuvieron que buscar nuevos canales de comunicación. El uso masivo de las diferentes tecnologías de monitorización, mensajería, etc. crea un problema de seguridad de todas ellas".

Jesús Sánchez de Coo de Áudea Seguridad de la Información destacó que el mero hecho de que se permita establecer y verificar controles como ISO27001 o ENS es muy importante. "Que las empresas tengan que certificar sus sistemas hace que la seguridad cada vez sea más importante. El paradigma de diseño y por defecto ha cambiado de ser *stopper* por parte de la seguridad a ser un colaborador más. La falta de presupuesto suele ser el mayor problema para la empresa pública; pero para el sector privado es la falta de talentos. La formación y concienciación es muy necesaria ya que el factor humano es el eslabón más débil", puntualizó.

## ACTO DE CLAUSURA

La clausura fue presidida por Juan Fernando Muñoz Montalvo, secretario general de Salud Digital, Información e Innovación en el Sistema Nacional de Salud del Ministerio de Sanidad. Contó con las intervenciones de Juan Díaz García, coordinador del Comité Técnico de Seguridad de la Información en Salud de la SEIS y coordinador del Programa de la XIX edición del


Foro de Seguridad y Protección de Datos de Salud y por Miguel Ángel Benito Tovar, coordinador general del Foro.

Miguel Ángel Benito agradeció la presencia de todos los participantes, ponentes y empresas colaboradoras y detalló las conclusiones del Foro:

El covid ha supuesto un reto en todos los sentidos que hay que aprovechar.

- Es imposible proteger lo que no se sabe que se tiene o sobre lo que no se tiene control.
- No se debe crecer en seguridad ni privacidad basándose en el miedo. Se debe aprender de los incidentes propios y de los demás.
- Es especialmente importante tener en cuenta las obligaciones de transparencia y confianza en el uso de los sistemas de información que tienen las Administraciones Públicas, lo cual impacta directamente en su reputación.
- Para hacer frente a todos los retos se debe disponer de gobernanza y estrategia basada en los riesgos, siendo imprescindible trabajar de forma conjunta.

En segundo lugar, tomó la palabra Juan Díaz, quien agradeció la presencia de los asistentes, proveedores, ponentes, autoridades y miembros del Comité y resumió las conclusiones derivadas del Foro:

- Es necesario contar con guías específicas por parte del Centro Criptológico Nacional para la securización de los dispositivos médicos.
- Destaca la importancia de los dos factores de autentificación como método de protección de acceso a los sistemas de información.
- Existen problemas de financiación para llevar a cabo los proyectos de seguridad.
- Es importante delimitar la compartición sociosanitaria solo a la información necesaria, aplicando de este modo el principio de minimización.

Para finalizar el acto de clausura tomó la palabra Juan Fernando Muñoz quien destacó:

- El covid es y ha sido la amarga oportunidad, pero que hay que poner el foco en la oportunidad.
- El trabajo conjunto y la confianza que se ha generado en la Atención Primaria se ha plasmado en la vacunación, pero se ha forjado durante muchos años.
- Los dispositivos médicos suponen un reto porque están ampliamente difundidos y generan una información muy interesante por su utilidad. Dejarán de ser útiles si se pierde la confianza generada.
- Hay que ser conscientes del equilibrio entre el valor y el riesgo que suponen la utilización de los dispositivos médicos.
- El cambio del modelo sanitario que aproveche toda la tecnología no será posible si no se conserva la confianza.

# Entrega de los XXVII Premios Nacionales de Informática y Salud 2021

## EL 9 DE MARZO TUVO LUGAR LA ENTREGA DE LOS XXVII PREMIOS NACIONALES DE INFORMÁTICA Y SALUD EN EL HOTEL MELIÁ CASTILLA

### ACTO DE INAUGURACIÓN

El evento estuvo presentado por Zaida Sampedro Préstamo, coordinadora de los premios y contó con la presencia de Vicenç Martínez Ibáñez, director general de Ordenación Profesional de la Secretaría de Estado de Sanidad; Javier Olave Lusarreta, vicepresidente de la Asociación de la Prensa; Esperanza Nicolás y Patricio Jiménez, codirectores de Acta Sanitaria; y Esther Macías Casado, coordinadora editorial de ComputerWorld.

Durante su intervención, Sampedro destacó que "tras un 2021 que ha continuado marcado por la situación derivada de la covid-19, en el que las restricciones han ido disminuyendo y nos han permitido reunirnos de nuevo, seguimos manteniendo un formato 'híbrido' al que ya todos nos hemos acostumbrado. Unos estamos físicamente aquí y otros nos acompañan de forma virtual. Es el momento del reconocimiento a la labor realizada por organizaciones y profesionales en pro de la Informática en el sector de la salud, en el contexto de transformación digital en el que estamos inmersos.

Ha sido un año en el que hemos sido testigos del incremento del uso de herramientas video colaborativas, gracias a las que se está haciendo realidad la transformación en la atención sanitaria. La ciberseguridad y los aspectos relativos a la privacidad de los datos también han tenido un papel destacado en este nuevo contexto, en el cual el dato y su gestión están siendo protagonistas. Todo ello aderezado con la oportunidad para la digitalización del sector gracias a los fondos de recuperación Next Generation.

Y como broche de oro, el 2 de diciembre de 2021, el Consejo Interterritorial del Sistema Nacional de Salud (CISNS) aprobó la Estrategia de Salud Digital. Tras un año de impulso a la digitalización del sistema sanitario y la sanidad española, se dio luz verde a un plan para el desarrollo de la transformación tecnológica del sector; un docu-


mento altamente demandado por los profesionales de la salud".

A continuación, tomó la palabra Luciano Sáez Ayerra, presidente de la Sociedad Española de Informática de la Salud quien agradeció la presidencia y participación de Vicens Martínez Ibáñez, director general de Ordenación Profesional del Ministerio de Sanidad. "En nombre de la SEIS le doy gracias por la presidencia de este acto. El papel del Ministerio de Sanidad es vital para la innovación de nuestro sector. Confío que el próximo año podamos retomar nuestro acto tradicional en la facultad. Nos encontramos inmersos en la transformación digital de la sociedad en su conjunto y el sector de la salud necesita adecuar sus servicios, sus recursos y sus organizaciones a esta nueva época digital.

Las TIC son el instrumento que permite esta renovación del sistema de salud y son la plataforma para aplicar medidas que, garantizando la sostenibilidad del sistema, mejoran a su vez el acceso, la equidad, la seguridad, la continuidad y la calidad de los servicios sanitarios y sociosanitarios.

Estos premios se enmarcan en nuestras líneas fundamentales, como una sociedad científica abierta a todos los profesionales, a todas las instituciones y entidades que se identifiquen con nuestra misión: promover la investigación, el

desarrollo, la innovación, la implantación y buen uso de las TIC en el ámbito de la salud, siempre en beneficio de la sociedad y con pleno respeto a los derechos de las personas; en particular a su intimidad y privacidad. La SEIS integra a todos aquellos profesionales y entidades tanto públicas como privadas que encuentran en las TIC un medio para el avance en el conocimiento científico y para la mejora de la salud de los ciudadanos, ya que nuestro interés es impulsar la innovación de nuestro sector, avanzar en lo que hoy denominamos la salud digital y para ello es necesario contar con el esfuerzo de todos los profesionales y de todas las organizaciones que participan de nuestro escenario", señaló.

Posteriormente, tomó la palabra Vicenç Martínez Ibáñez, director general de Ordenación Profesional de la Secretaría de Estado de Sanidad, quién destacó que "los sistemas de información son un pilar básico. Estos premios reconocen el esfuerzo tecnológico y ponen en valor el uso de las tecnologías para la mejora en la asistencia al ciudadano".

Tras las intervenciones se procedió a la lectura del Acta del Jurado:

**Premio a la entidad pública o privada que destacó en proyectos de Transformación Digital en el ámbito sanitario:** se entregó al **Hospital Universitario 12 de Octubre**, por su decidida apuesta por la incorporación de nuevas tecnologías de la información y comunicación TIC a la práctica clínica diaria.

A lo largo de su proceso de transformación en un hospital digital, el 12 de Octubre ha colaborado en el diseño e implantación de soluciones con el objetivo de facilitar y agilizar el trabajo asistencial y ganar en seguridad para el paciente, incorporando soluciones de movilidad. Además, el Hospital, desde hace tiempo, viene trabajando intensamente en proyectos de análisis de datos y modelos predictivos, especialmente en la pandemia. Así mismo, es una referencia de innovación en materia de información sanitaria y su aplicación en proyectos nacionales e internacionales. Este conocimiento se aplicó en la pandemia de covid-19 para hacer ágil y eficiente la obtención de datos en un escenario crítico. Recogió el Premio Carmen Martínez de Pancorbo González, directora gerente.

**Mención Honorífica al Premio a la Entidad Pública o Privada que destacó en proyectos de Transformación Digital en el ámbito sanitario:** recayó en la **Clínica Universidad de Navarra**, por su continua mejora de la calidad asistencial que tiene su base en la innovación y en el desarrollo de sus sistemas de información clínicos. Recogió el Premio Josep María Gost Prat, director de Proyectos de la Clínica Universitaria de Navarra, que lidera proyectos de innovación y mejora continua en el Departamento de Sistemas.

**Premio a la Organización que realizó un mayor esfuerzo tecnológico para desarrollar soluciones en el sector sanitario** se entregó a **Dedalus Iberia**, por ser un gran proveedor de soluciones de salud digital y poseer una fuerte posición en España, donde sus soluciones gestionan más de 17 millones de historias de salud digital y dan cobertura a más de 30 millones de ciudadanos. Así mismo ofrece al ecosistema sanitario soluciones que permiten acelerar la transformación digital del sector y ha elegido a España como hub global de I+D en salud digital, para desarrollar soluciones que respondan a las necesidades del sistema sanitario nacional y global en materia de plataforma de datos, patología digital, gestión de crónicos, IA para

la mejora de procesos quirúrgicos, apoyo a la decisión clínica, medicina personalizada, etc. Recogió el Premio **Marisa de Felipe,** directora general de Dedalus Iberia.

**Mención Honorífica al Premio a la Organización que realizó un mayor esfuerzo tecnológico para desarrollar soluciones en el sector sanitario:** fue para la **Sociedad Española de Farmacia Clínica, Familiar y Comunitaria**, por el desarrollo de SEFAC eXPERT®, un software para la gestión en farmacia comunitaria de los servicios profesionales farmacéuticos asistenciales, y realizar un correcto seguimiento del paciente y alcanzar los resultados esperados del tratamiento en salud, que tiene además el objetivo de facilitar el uso de protocolos consensuados con otras sociedades científicas. Recogió el Premio **Vicente J. Baixauli Fernández,** presidente de la Sociedad Española de Farmacia Clínica, Familiar y Comunitaria.

**Premio al Profesional que, por su trayectoria y dedicación, colaboró especialmente en promover la Transformación Digital en el entorno sanitario:** se entregó a **Alberto Gómez Lafón,** por haber dedicado su carrera profesional hasta su jubilación a las TIC y mayoritariamente a los sistemas de información farmacéuticos, siendo un referente en esta materia. Alberto Gómez Lafón es licenciado en Farmacia por la Universidad Complutense de Madrid, farmacéutico inspector del INSALUD, especialista en Farmacia Hospitalaria y Master en Dirección de Sistemas y Tecnologías de la Información y de las Comunicaciones por el INAP.

A lo largo de su dilatada carrera profesional ocupó entre 1980 y 2017 puestos TIC de alta responsabili-

dad tanto funcionales como tecnológicos pertenecientes al organigrama del Ministerio de Sanidad, entre otros: en el INSALUD como integrante del CINIME; en la Dirección General de Farmacia, como jefe del Servicio de Bases de Datos de Medicamentos; en la Subdirección General de Sistemas y Tecnologías de la Información, fue jefe del Área de Proyectos; en la Agencia Española de Medicamentos y Productos Sanitarios, fue jefe de la División de Sistemas de Información y secretario general y en la Dirección General de Cartera Básica de Servicios y Farmacia, vocal asesor TIC, desde los cuales participó en la implantación de las TIC en Sanidad y especialmente en todas las etapas relativas al ciclo de vida del medicamento, investigación clínica, registro y autorización, prestación farmacéutica, estudios de post comercialización, farmacovigilancia, etc. Además, Alberto Gómez participó en proyectos internacionales TIC/Salud tanto en Europa, como en Iberoamérica a través de la OPS, y ha sido miembro de la Junta Directiva de la SEIS durante 30 años, en calidad de vocal de Farmacia, Tesorero y en tres ocasiones secretario general. Ha sido un prolífico escritor de artículos técnicos, y participante como ponente o profesor en numerosos congresos, seminarios, masters, etc.

**Premio al CIO del sector Salud que destacó por sus logros en la implantación de proyectos de Transformación Digital** se entregó a **Juan Antonio Gómez Palomeque,** por su aportación a la Transformación Digital del Sistema Sanitario Público de Andalucía. Además de su larga experiencia en la gestión TIC en Hospitales públicos, ha destacado en la última etapa como CIO del SAS por su notable éxito en la consolidación del modelo de gestión TIC integrado en todo el Sistema Sanitario Público de Andalucía, con una gestión del cambio impecable y una involucración, compromiso y complicidad alta por parte de la comunidad de profesionales de la informática sanitaria de Andalucía.

**El Premio al Directivo que destacó por su apuesta por la implantación de las TIC en el sector Salud** recayó en **Juli Fuster Culebras,** por su compromiso e impulso a la implantación y la gobernanza de las TIC en el sector de Salud durante más de 30 años como personal directivo del Sistema Nacional de Salud. Juli Fuster, médico de Familia y máster en Economía de la Salud y Gestión Sanitaria, se ha dedicado a la gestión sanitaria desde el año 1994, tanto en atención primaria como hospitalaria y desde hace siete años es director general del Servei de Salut de les Illes Balears, siendo esta su segunda etapa en el cargo que ya ocupó entre los años 2001 y 2003. Comprometido desde el primer momento con la utilización de las aplicaciones informáticas en el desarrollo de los sistemas de información sanitaria, Son Llàtzer fue en el año 2002 el primer hospital sin papeles de España y actuó como palanca


para el impulso de la informatización en atención primaria en ese mismo año. Es impulsor de múltiples proyectos que tienen que ver con la interoperabilidad, la ayuda a la toma de decisiones clínicas y las exploraciones en red, entre otros.


**Premio al Esfuerzo institucional o personal en investigación o innovación en proyectos para la utilización de las TIC en Salud o en la internacionalización de la actividad Informática de la Salud desarrollada en España** fue para **Joaquín Dopazo Blázquez,** por haber sido pionero en el desarrollo de soluciones TIC en el campo emergente de la genómica, por sus publicaciones de soluciones TIC para la detección de biomarcadores diagnósticos o la búsqueda de variantes genómicas de enfermedad, que han sido la base para el desarrollo de otras aplicaciones usadas en la actualidad y con gran repercusión internacional. Joaquín Dopazo es director del Área de Bioinformática de la Fundación Progreso y Salud, investigador del Instituto de Biomedicina de Sevilla, jefe de grupo del Instituto nacional de Bioinformática (ELIXIR-ES) y del CIBERER (CIBER de Enfermedades raras).


**Premio al Proyecto realizado con la aplicación de las TIC en el sector Salud o en el ámbito socio-sanitario que destacó por la aportación de valor a los ciudadanos** se entregó a la **Gerencia Regional de Servicios Sociales de la Junta de Castilla y León,** por el impulso en el área TIC que está dando a sus proyectos tanto regionales como de ámbito europeo y transfronterizo, cubriendo áreas de población en Castilla y León tan importantes como la llamada "España Vaciada". Esta población diana tan afectada está pudiendo ser atendida en igualdad de condiciones que la población urbana.


**Premio a la Mejor iniciativa en materia de Ciberseguridad, privacidad y protección de datos en el ámbito sanitario** se entregó al **Centro Criptológico Nacional,** por su apoyo al sector sanitario ante el continuo aumento del número de ciberincidentes a hospitales públicos y privados. Dicho apoyo se brindó tanto en la respuesta ante incidentes de seguridad, como de forma continuada en labores de asesoramiento y desarrollo de soluciones y herramientas que han venido a mejorar las capacidades de respuestas de las organizaciones sanitarias públicas. Recogió el Premio Luis Jiménez, subdirector general del Centro Criptológico Nacional.

**Premio a la Aportación más relevante presentada en las actividades de la SEIS durante los últimos 12 meses** fue para el **Departamento de Salud del Gobierno Vasco.** Las aportaciones de Osakidetza realizadas a los distintos eventos y publicaciones de la SEIS durante el año 2021 tuvieron una clara orientación al paciente y a su cuidado, ayudando a hacer realidad la permanente afirmación de que el ciudadano es el centro del sistema sanitario. En este sentido destacamos: el Proyecto Otago, implantación de un sistema centralizado para la gestión de críticos en Osakidetza; Sistemas de información y comunicación en salud, en tiempos de crisis; Gestión de Cuidados basada en datos; Tecnología a pie de cama y El uso humano de las TIC en el entorno sociosanitario. Recogió el Premio Benjamín Juez Fernández, subdirector de Informática y Sistemas de Información del Departamento de Salud del Gobierno Vasco, Osakidetza.

**PREMIO ESPECIAL** a la **Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud del Ministerio de Sanidad,** por haber elaborado la "Estrategia de Salud Digital del Sistema Nacional de Salud", que ha sido aprobada en el Consejo Interterritorial de Salud. Es un documento marco, sin precedentes, que facilitará la inversión y el desarrollo de proyectos armónicos con una Transformación Digital de todo el sector salud de nuestro Estado. La Secretaría General de Salud Digital, Información e Innovación para el SNS se creó en agosto de 2020 como órgano directivo del Ministerio de Sanidad responsable de los proyectos de modernización, innovación, mejora y transformación del Sistema Nacional de Salud (SNS) a la luz de los nuevos retos derivados de la pandemia por covid-19, en particular los relacionados con la salud digital y los sistemas de información. A la Secretaría General le corresponde asimismo la realización de actividades tendentes a la traslación de la innovación y avances de la investigación al Sistema Nacional de Salud, en colaboración con el Ministerio de Ciencia e Innovación y las comunidades autónomas. Desde su creación, la Secretaría General ha trabajado intensamente con las comunidades autónomas en la elaboración


de la Estrategia de Salud Digital del Sistema Nacional de Salud, que el Consejo Interterritorial aprobó el 2 de diciembre. Recogió el Premio Mercedes Alfaro Latorre, subdirectora general de Información de la Secretaría General de Salud Digital, Información e Innovación del SNS del Ministerio de Sanidad.

## FOTO DE FAMILIA DE TODOS LOS PREMIADOS

## IMÁGENES PARA EL RECUERDO


PREMIOS NACIONALES

# LA SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD (SEIS) HA RECIBIDO, A PROPUESTA DEL MINISTERIO DE SANIDAD, LA ENCOMIENDA DE LA ORDEN CIVIL DE SANIDAD

## EL ACTO DE ENTREGA SE CELEBRÓ EL DÍA 7 DE ABRIL


La Orden Civil de Sanidad es la máxima condecoración civil española que se concede como honor, distinción y reconocimiento público, para premiar méritos, conductas, actividades o servicios relevantes o excepcionales, en el ámbito de la sanidad.

Durante el acto celebrado en el Ministerio de Sanidad el 7 de abril, con motivo del Día Mundial de la Salud, se entregaron 34 condecoraciones de la Orden del Mérito Civil del Ministerio de Sanidad: 3 Encomiendas con Placa, 7 Encomiendas, 21 Cruces sencillas y 3 grandes Cruces.

Una de las Encomiendas fue otorgada a la Sociedad Española Informática de la Salud (SEIS), profesionales que han permitido aportar sistemas de información que posibilitaron tomar las decisiones más adecuadas en momentos de incertidumbre gracias a las TIC. La distinción fue recibida por Luciano Sáez Ayerra, presidente de la SEIS.

El presidente estuvo acompañado por **Jesús Galván** y **José Luis Monteagudo**, vicepresidente y vicepresidente de Investigación, Innovación y Formación de la SEIS, respectivamente.

Tanto el día en que se conoció la noticia de la concesión a la SEIS esta condecoración, como el día en que se celebró el acto de entrega de la Encomienda, se vivieron momentos de gran emoción. La distinción supone un reconocimiento a la labor de muchos años y, en particular, al enorme esfuerzo realizado durante la pandemia, en la que se ha puesto en valor esta actividad profesional. Es, sin duda, una muy buena noticia y un orgullo haber obtenido una distinción pública de este nivel.

**SEGURIDAD** Y PROTECCIÓN DE DATOS

Coordina: **Juan Díaz**

# Código de Conducta de Farmaindustria para la investigación

**La Agencia Española de Protección de Datos (AEPD) ha aprobado el 'Código de Conducta regulador del tratamiento de datos personales en el ámbito de los ensayos clínicos y otras investigaciones clínicas y de la farmacovigilancia' promovido por Farmaindustria, que se convierte en el primer código de conducta sectorial aprobado desde la entrada en vigor del Reglamento General de Protección de Datos (RGPD).**

Este código regula cómo deben aplicar la normativa de protección de datos los promotores de estudios clínicos con medicamentos y las Organizaciones de investigación por contrato (CRO) que decidan adherirse al mismo. Su ámbito de aplicación es nacional, si bien aspira a ser un referente a nivel europeo al ser el primer código en este ámbito que ha sido aprobado en Europa.

El RGPD establece que las asociaciones y organismos representativos de categorías de responsables o encargados del tratamiento pueden elaborar códigos de conducta para facilitar su aplicación efectiva. Estos códigos constituyen un elemento de autorregulación voluntario que responde a las necesidades específicas del sector de actividad que regulan, aportan garantías para los derechos y libertades de las personas, y representan un valor añadido a la normativa aplicable, debiendo ser aprobados por la autoridad de control.

El ámbito objetivo de aplicación del código lo constituyen las actividades de tratamiento de datos personales en el marco de las investigaciones clínicas en general, y los ensayos clínicos en particular, así como las vinculadas al cumplimiento de las obligaciones impuestas por la normativa vigente en materia de farmacovigilancia para la detección y prevención de efectos adversos de los medicamentos ya comercializados. En el caso de los ensayos clínicos, establece protocolos que facilitan la aplicación del RGPD y ofrece seguridad a las entidades que se adhieran. Se regulan entre otras cuestiones: la aplicación de los principios de protección de datos, la evaluación de impacto, la codificación de datos, la responsabilidad de los distintos intervinientes en un ensayo, las bases legitimadoras de los tratamientos, el régimen de las transferencias internacionales de datos, las obligaciones derivadas de las brechas de seguridad y el ejercicio de derechos.

En materia de farmacovigilancia, el código distingue el tratamiento de los datos personales identificativos y codificados, estableciendo protocolos para la recogida de información sobre posibles reacciones adversas en función de quien realice la notificación y los distintos canales de notificación, incluidas las redes sociales.

Asimismo, el código establece un procedimiento de mediación, voluntario y gratuito, que permite dar una respuesta ágil a las posibles reclamaciones que planteasen los interesados frente a las entidades adheridas.

El RGPD establece que todos los códigos de conducta deben designar un organismo de supervisión que actúe con plena independencia tanto del promotor del código como de las entidades adheridas, y que debe ser acreditado por la autoridad de control. En este caso, la AEPD ha acreditado como organismo para la supervisión y control del código al Órgano de Gobierno del Código de Conducta (OGCC). El OGCC, de carácter interno, actuará con plena independencia en el ejercicio de sus funciones.

La directora de la Agencia Española de Protección de Datos, Mar España, ha destacado la importancia de la aprobación de este código de conducta como "una muestra de los instrumentos que ofrece la normativa de protección de datos para favorecer la investigación en el ámbito de la salud, garantizando el derecho a la protección de los datos de los participantes".

El código recoge una nueva figura que se podría considerar contradictoria el "tercero de confianza" en sus funciones y una habilitación para los tratamientos de datos basados en una obligación legal, que contrasta con otras habilitaciones recogidas en el Dictamen 3/2019 sobre las preguntas y respuestas acerca de la relación entre el Reglamento sobre ensayos clínicos (REC) y el Reglamento general de protección de datos (RGPD) [artículo 70, apartado 1, letra b)] , del Comité Europeo de Protección de Datos.

FORO DE
**INTEROPERABILIDAD**

Coordina: **Adolfo Muñoz Carrero**

# Estructuras de referencia clínicas definidas en UNE-EN ISO 13606:2020 – parte 3 (IV) – Estructuras compuestas

Se finaliza en esta entrega el repaso que se está haciendo a las estructuras propuestas en la parte 3 de la norma para armonizar el intercambio de información clínica por medio de los conceptos definidos en la Norma UNE-EN ISO 13940. En las anteriores entregas vimos las estructuras simples y los clústeres, que están disponibles para usarlas en la creación de estructuras compuestas, que se describen en esta entrega.

### Historia de salud personal

La historia de salud personal es un tipo de historia de salud en la que la información sobre un sujeto de la asistencia es recogida, documentada y gestionada por el propio sujeto de la asistencia. En esta estructura se propone el siguiente contenido (entre paréntesis figura la estructura simple o de clúster en que se basa dicho contenido):

- Antecedentes familiares (recursos FHIR)
- Hábitos de vida que influyen en la salud personal (condición de salud)
- Alergias e intolerancias (condición de salud)
- Condiciones/problemas de salud actuales y pasados (condición de salud)
- Servicios asistenciales recibidos actualmente o en el pasado (elementos de actividad sanitaria/plan asistencial/asunto del proceso clínico)
- Lista de medicamentos actualmente consumidos (tratamiento farmacológico)
- Condiciones objetivo (condición de salud).

### Historia de salud profesional

La historia de salud profesional es tipo clásico de historia de salud y es la herramienta clave en la atención sanitaria. La estructura propuesta puede complementarse con las partes relevantes de la historia cuando se considere necesario:

- Antecedentes familiares (recursos FHIR/condición de salud/elementos de actividad sanitaria)
- Condiciones/problemas de salud actuales y pasados (condición de salud)
- Actividades sanitarias pasadas y actuales realizadas/planificadas (elementos de actividad sanitaria/plan asistencial/asunto del proceso clínico)
- Condiciones de riesgo, incluidas las relacionadas con estilo de vida (condición de salud)
- Condiciones objetivo (condición de salud)
- Condiciones pronóstico (estado de salud)
- Valoraciones de las necesidades sanitarias (valoración de necesidades sanitarias)
- Lista de medicamentos - prescritos (tratamiento farmacológico).

### Planificación de exploraciones sanitarias basada en el conocimiento

Esta estructura ayuda a documentar la motivación, basada en el conocimiento, para planificar exploraciones sanitarias:

- Condición de salud motivadora – por ejemplo, un síntoma (condición de salud)
- Condición considerada - a partir de criterios basados en el conocimiento (condición de salud)
- Elementos de actividad de exploraciones sanitarias – eficacia basada en el conocimiento para la identificación de problemas de salud (elemento de actividad sanitaria)
- Condición resultante – resultados probables basados en el conocimiento de los indicadores de salud (condición de salud)

### Planificación de tratamientos sanitarios basada en el conocimiento

Esta estructura ayuda a aplicar un enfoque sistemático, basado en el conocimiento, para la planificación de tratamientos sanitarios:

- Condición de salud motivadora – problema de salud identificado (condición de salud)
- Condición objetivo – posible resultado basado en el conocimiento (condición de salud)
- Elementos de actividad de tratamiento – eficacia basada en el conocimiento para influir en el estado de salud (elemento de actividad sanitaria)
- Condición resultante – resultados probables basados en el conocimiento de los indicadores de salud (condición de salud).

FORO DE
**SALUD CONECTADA**

Coordina: **Óscar Moreno**

# Los parches electrónicos para la piel podrían restaurar la sensación perdida y detectar enfermedades (I)

**INVESTIGADORES EN EUROPA ESTÁN TRABAJANDO EN PARCHES DE MEMBRANA ELÁSTICA QUE IMITAN EL ASPECTO Y EL TACTO DE LA PIEL Y PUEDEN RECOPILAR INFORMACIÓN RELACIONADA CON EL USUARIO.**

La piel electrónica (e-skin) se clasifica como un 'wearable' electrónico, es decir, un dispositivo inteligente que se lleva sobre la superficie de la piel o cerca de ella para extraer y analizar información relacionada con el usuario. El dispositivo portátil electrónico más conocido es un registro de actividad, que generalmente detecta el movimiento o las vibraciones para dar información sobre la actividad del usuario. Los dispositivos portátiles más avanzados recopilan datos sobre la frecuencia cardíaca y la presión arterial de una persona.

Los desarrolladores de e-skins, sin embargo, están poniendo sus miras más allá. Su objetivo es producir membranas elásticas, robustas y flexibles que incorporen sensores avanzados y tengan la capacidad de auto repararse. Las implicaciones potenciales para la medicina y la robótica son inmensas.

Ya están en circulación membranas similares a la piel que se adhieren a la superficie del cuerpo y detectan presión, tensión, deslizamiento, fuerza y temperatura. Se están creando otras para reconocer los cambios bioquímicos que señalan enfermedades. Varios proyectos están trabajando en pieles que envolverán robots o prótesis humanas, dando a estas máquinas e instrumentos la capacidad de manipular objetos y percibir su entorno con un alto grado de sensibilidad táctil. Y el ideal, por supuesto, es desarrollar una piel electrónica que pueda conectarse con el sistema nervioso central del usuario (alguien que está paralizado, por ejemplo), restaurando así la sensación que se ha perdido debido a una enfermedad o trauma.

Se hará un acercamiento a una primera iniciativa en este ámbito, el proyecto llamado PepZoSkin. Los investigadores de la Universidad de Tel Aviv, en Israel, van camino de convertir este sueño anteriormente mencionado en realidad. Dentro de una década, creen que los parches de piel artificial estarán lo suficientemente avanzados como para alertar a los usuarios sobre los peligros que no pueden percibir de forma natural.

El equipo de Tel Aviv está desarrollando una máscara que extraerá y analizará información de salud sin necesidad de una fuente de energía externa. La membrana se autoalimentará gracias a un fenómeno conocido como piezoelectricidad. Esto se refiere a una carga eléctrica que se acumula en ciertos materiales (incluidos los huesos, el ADN y ciertas proteínas) en respuesta a la tensión mecánica aplicada.

Para una persona con parálisis, por ejemplo, una bebida caliente que se le derramara encima crearía una deformación de la e-skin que sería leída por la piel como una presión mecánica y esto, a su vez, se traduciría en una señal eléctrica. Esta señal podría activar una luz de advertencia o un sonido. A medida que avancen en esta misión, se obtendrá la capa delgada (piel electrónica) para hablar con el sistema nervioso, reemplazando la sensación de sensibilidad que falta.

El desafío en este momento es encontrar materiales piezoeléctricos que no sean tóxicos para el cuerpo, ya que, los materiales piezoeléctricos que se usan hoy en día contienen plomo. Actualmente las líneas de investigación van dirigidas a mo-

léculas biológicas o a moléculas artificiales que imitan a las que se encuentran en el cuerpo.

El profesor Ehud Gazit, que dirige el proyecto, explicó la importancia de encontrar materiales piezoeléctricos que puedan convertirse en productos seguros. "Nuestro trabajo actual sobre los materiales de péptidos piezoeléctricos dará como resultado, muy pronto, productos sin plomo que funcionan tan bien como los productos tóxicos con plomo que están disponibles actualmente, excepto, por supuesto, que nuestros nuevos materiales serán mucho mejores porque serán seguros de usar en contacto con el cuerpo humano, e incluso como implantes.'

El equipo del Prof. Gazit espera llevar su trabajo al siguiente nivel para este año. Para entonces, esperan haber elegido su molécula orgánica y optimizarla para la actividad piezoeléctrica. A continuación, planean convertirlo en nanodispositivos funcionales. Creen que, con el tiempo, se utilizarán ampliamente en aplicaciones biológicas y médicas, sirviendo como recolectores de energía y biosensores, transmitiendo información vital directamente desde el tejido humano y devolviendo una respuesta hacia el usuario o a un tercero.

**Más información:**

• Comisión Europea – Horizon Magazine - https://ec.europa.eu/research-and-innovation/en/horizon-magazine

• Proyecto PepZoSkin: Biocompatible Self-powered Electronic Skin - https://cordis.europa.eu/project/id/875586

AGENDA **2022**

**XII REUNIÓN DEL FORO DE INTEROPERABILIDAD EN SALUD**

27 y 28 abril · Murcia

**XII FORO PARA LA GOBERNANZA DE LAS TIC EN SALUD**

8 y 9 junio · Alicante

**XXIX JORNADAS NACIONALES DE INNOVACIÓN Y SALUD EN ANDALUCÍA**

Fecha: 5, 6 y 7 octubre · Málaga

**XX REUNIÓN DE SALUD CONECTADA**

16 y 17 noviembre · Vitoria

**VIII MÁSTER EN DIRECCIÓN DE SISTEMAS Y TICS PARA LA SALUD:**

noviembre/octubre 2021-2022

FORO DE
**GOBERNANZA**

Coordina: **Martín Begoña**

# Uso de la IA en las enfermedades más recurrentes

**Pilar Ruiz Ayuso**
Head of Innovation Director en I3B (Instituto Ibermática de Innovación)

En el artículo anterior, se explicó cómo la IA, juega un papel importante en la monitorización y seguimiento preventivo de los pacientes que padecen EPOC (Enfermedad Pulmonar Obstructiva Crónica), presentándose ciertos retos tecnológicos importantes, que habrá que tener en cuenta, y serían los siguientes:

- Riesgos en los sensores de respiración, para contar con un sistema preciso con el que evaluar la frecuencia respiratoria del paciente de forma automatizada y precisa es una tarea complicada, ya que a día de hoy no hay una forma de extracción fidedigna de dicho indicador, por lo que habrá que explorar diferentes vías para recoger dicho dato, o bien mediante sensores electrofisiológicos que detecten la actividad diafragmática o explorando su detección, aprovechando los sensores de actividad del paciente.
- Riesgos relacionados con la detección adecuada de posibles brotes que aúne una alta sensibilidad y una buena especificidad que permita que el sistema monitorice automáticamente el gran volumen de datos proveniente de los sensores priorizando la información a monitorizar por el medico

## Síndrome Metabólico en cifras

Dentro de las enfermedades de mayor incidencia en la sociedad, se encuentra el síndrome metabólico, que engloba entre otras patologías, diabetes mellitus de tipo 2 (T2D), y las enfermedades cardiovasculares (ECV), provocados principalmente por el consumo de tabaco, la inactividad física y una dieta desequilibrada. Según la OMS, constituyen la principal causa de defunción en todo el mundo.

El estudio y descubrimiento de nuevos factores fisiopatológicos ligados al desarrollo de estos padecimientos, ha generado la relación innegable entre el grupo de afecciones que describen el síndrome metabólico (hipertensión arterial, los niveles de glucosa, los elevados niveles de triglicéridos en sangre, el exceso de grasa alrededor de la cintura, y un largo etc.) con enfermedades de alta incidencia como son las T2D y ECV.

## ¿En qué consiste el Síndrome Metabólico y de qué medios se disponen para su detección?

El síndrome metabólico es un grupo de afecciones que se presentan al mismo tiempo y aumentan el riesgo de desarrollar una enfermedad cardíaca, accidente cerebrovascular y diabetes tipo 2.

El estilo de vida actual, el estrés, el aumento de la esperanza de vida, y el déficit de actividad física, se suman a este listado de factores de riesgo que no hacen más que complicar la situación.

Por consiguiente, el impacto que conlleva en la salud y en la economía, derivado de las consecuencias asociadas al síndrome metabólico, es muy elevado, siendo una de las más demoledoras el deterioro cognitivo.

A nivel mundial, más de 46 millones de personas en el mundo sufren deterioro cognitivo en forma de demencia, y las previsiones publicadas en el Informe Mundial sobre el Alzheimer ( Alzheimeŕ s Disease International, ADI, 2018) apuntan a un aumento de la cifra hasta los 152 millones en 2050.

A esta situación, que tiene una previsión realmente alarmante, se suma que los tratamientos actuales para este conjunto de patologías son realmente costosos para los sistemas de salud. Por tanto, nos conduce hacia una clara necesidad de mitigar y gestionar estos efectos mediante la prevención y el control de estas enfermedades, el cual dará lugar a una disminución de la dependencia de los enfermos y por lo tanto del impacto socioeconómico que esto supone.

Si nos centramos en la enfermedad TD2, podemos decir que, hasta la fecha, se desconoce la causa fisiopatológica por la que ocurre, la problemática de los

profesionales de la salud radica, en que el diagnóstico se hace de acuerdo con la característica principal de la enfermedad, el aumento de la glucosa en sangre. Se utiliza un algoritmo de decisión de descarte, donde quedan excluidas otro tipo de diabetes, autoinmunidad, embarazo, o daño pancreático. Este diagnóstico lo que puede conllevar, es a una falta de comprensión mecanicista de la enfermedad, derivándose en un posible diagnóstico incorrecto y tardío, o dificultades para encontrar la correcta respuesta a tratamientos

A pesar de que, en la última década, ha habido una proliferación de los estudios asociados al genoma completo, donde se han detectado múltiples interacciones genéticas que aumentan el riesgo a padecer diabetes TD2, los estudios no son concluyentes, pero sí demuestran que hay subtipos de ADN que se hayan asociados con el riesgo de padecer diabetes en estudios genéticos a gran escala.

## Aplicando la Inteligencia Artificial en casos de uso reales

Teniendo en cuenta todo lo expuesto, y considerando la alta morbilidad y mortalidad asociadas con las complicaciones de la T2D, existe una gran necesidad de detectar los factores de riesgo genéticos para las complicaciones de la T2D, así como comprender la fisiopatología del trastorno e identificar objetivos moleculares y vías que podrían conducir a una mejor terapia en el futuro.

La aplicación de métodos de aprendizaje automático y minería de datos en la investigación de T2D, permite aprovechar el análisis de grandes volúmenes de datos disponibles relacionados con los pacientes (diagnósticos, exámenes, muestras, biomédicos, etc.), para extraer conocimiento, y realizar tratamientos predictivos más personalizados, que disminuyan la probabilidad de desarrollar complicaciones futuras mejorando la calidad de vida, ya que hasta la fecha, los pacientes diagnosticados con este tipo de enfermedad, son tratados con el mismo protocolo único, que no se adapta ni a la fisiología de cada persona, y que en muchas ocasiones reciben tratamientos inadecuados.

Estos sistemas de detección de forma preventiva del diagnóstico y complicaciones derivadas de la T2D, deberán estar basados en:

- Desarrollo de un sistema predictivo, que sea capaz de analizar cuantitativamente el riesgo de padecer T2D tras un análisis genético y epigenético. Se investigarán nuevos protocolos y formulaciones algorítmicas que permitan crear sistemas predictivos en torno a las complicaciones derivadas de la diabetes, evitando o retrasando la aparición de problemas asociados a dicha enfermedad y síndrome metabólico, ejerciendo un incremento directo en la calidad de vida de los pacientes.
- Desarrollo de un sistema de diagnóstico, que, mediante el análisis con IA de neuroimágenes, sea capaz de objetivar el análisis de riesgo cuantitativo de sufrir deterioro cognitivo. En los últimos años se han desarrollado diferentes técnicas para procesado automático de estas imágenes, pero la realidad es que en la práctica clínica actual apenas se utilizan, lo que hace que mucha información (no visible con el ojo humano) con gran potencial no esté siendo analizada para caracterizar al paciente y ayudar en la toma de decisiones.
- Desarrollo de un sistema prescriptivo, capaz de sugerir acciones correctoras, con especial incidencia desde la alimentación, para mejorar la esperanza de vida con alta calidad en las personas en riesgo. Basado en analítica de datos, ofrecerá soporte y conocimiento asociados a la personalización de la alimentación y los hábitos saludables buscando objetivos terapéuticos.

## Retos tecnológicos para el desarrollo de soluciones aplicados al Síndrome Metabólico

Para asumir los retos tecnológicos a los que nos enfrentamos en el desarrollo de un sistema que permita detectar el diagnóstico y complicaciones del T2D de forma automatizada, hay que tener en cuenta el volumen y diversidad de la información, así como el coste de capturar dicha información de los pacientes por el número de pruebas clínicas que esto implica. Sin embargo, los avances potenciales compensarán en el largo tiempo los costes.

En conclusión, hacer una apuesta por la Medicina Personalizada, es todo un acierto. Ya son muchos los países punteros como Reino Unido o Francia, que están empezando a implantar este tipo de plataformas en sus sistemas de salud, atendiendo así a las necesidades de dar una atención individualizada a cada uno de los pacientes en los que se tiene en cuenta no solo su tratamiento, sino también otros aspectos realmente importantes como los hábitos de vida saludables, alimentación, etc de cara a ofrecerles el tratamiento más idóneo.

SECTOR DE
**ENFERMERÍA**

Coordina: **Inmaculada Moro**

# La digitalización y su repercusión en salud

**Inmaculada Moro Casuso**

**El pasado mes de marzo, tuvo lugar el congreso inforsalud, con el lema: "compartiendo Datos, Información y conocimiento en Salud", y tuvimos la oportunidad de organizar la l mesa de enfermería que en esta ocasión titulamos "la digitalización y su repercusión en salud".**

El objetivo de esta mesa, que celebramos cada año, es dar a conocer proyectos de digitalización desarrollados en el ámbito de los cuidados o proyectos liderados o co liderados por enfermería desde una perspectiva multidisciplinar.

Este año hemos contado con ponentes que expusieron proyectos muy interesantes, que me ha parecido muy interesante compartir en este artículo.

- Dolores Roldan Valcarcel, enfermera gestora de casos en aceites crónicos, del Hospital Clínico Unversitario Virgen de la Arrixaca, nos habló de la importancia de la gestión de la información para la atención que las enfermera gestoras casos realiza en la atención a los pacientes crónicos y pluripatologicos, disponer de toda información del paciente, es fundamental para atención integral a estos pacientes, y poder tomar las decisiones mas adecuadas en cada momento.
- Nuria de Argila, supervisora de formacion del Hospital de día de Geriatría y procesos enfermeros del hospital Central Cruz Roja San Jose y Santa Adela de Madrid presento" los telecuidados como un modelo síncrono entre atención hospitalaria y Sociosanitaria: ciencia o ficción". Un proyecto de tele cuidados, entre el hospital y las 15 residencias de las que son referencias, con importantes resultados para las y los pacientes atendidos, tanto por el grado de resolución de las consultas, como por la disminución del número de traslados de pacientes desde la residencia para su resolución. Un modelo basado en el uso inteligente de las TIC y los recursos tecnológicos.
- Abraham Delgado Diego, enfermero, técnico asesor de la Subdirección de Cuidados del Servicio Cántabro de Salud, expuso el proyecto TI-CHRON, un proyecto de investigación europeo, para el desarrollo de plataformas tecnológicas innovadoras para el abordaje de la cronicidad infantil, centrado en patologías como el asma, la diabetes y la obesidad. El objetivo es mejorar el seguimiento y tratamiento de la enfermedad, asi como el empoderamiento de los pacientes jóvenes, utilizando para ello tecnologías como la gamificacion,el e-learnig, en plataformas interactivas para dispositivos móviles.
- Sendoa Ballesteros, adjunto de enfermería del hospital e Santamarina, y profesor asociado de la Universidad del Pais Vasco(UPV), nos habló de la "APP para el apoyo a la toma de decisiones clínicas en emergencias pediátricas" un proyecto multidisciplinar realizado en colaboración entre Osakidetza y la UPV, para la creación de una APP de apoyo a la toma de decisiones para profesionales ante las urgencias de pediatría, un ámbito que siendo poco frecuente tiene mucho impacto en la población que atiende, y en los profesionales por lo que la creación de esta herramientas de ayuda que ya se esta utilizando ha sido muy bien recibidas por los profesionales.

Han sido cuatro ejemplos diferentes, en los que el liderazgo y la participación de profesionales de enfermería ha sido fundamental, para la mejora de la atención de los pacientes de manera directa, como para la coordinación de los servicios, o la creación de herramientas que mejoren la atención sanitaria, asi como el trabajo de los profesionales.

Seguiremos en las próximas ediciones mostrando nuevos proyectos que pongan en valor la digitalización de los cuidados y su repercusión en la salud de la población.

# INFORMÁTICA MÉDICA

Coordina: **Gregorio Gómez**

## Ya está operativo el Centro de Coordinación para el Análisis en Red de Datos de la Vida Real de la Unión Europea impulsado por la Agencia Europea de Medicamentos (EMA)l

La EMA ha establecido un centro de coordinación para proporcionar evidencia sobre el uso, la seguridad y la eficacia de los medicamentos para uso humano, incluidas las vacunas, a partir de bases de datos de atención médica del mundo real en toda la Unión Europea (UE). El proyecto, que se denomina Red de análisis de datos e interrogación del mundo real (DARWIN EU®), lleva gestándose desde 2020 y ha arrancado en febrero como proyecto piloto con el objetivo de estar plenamente operativo en 2024.

DARWIN EU proporcionará evidencia válida y fiable con datos del mundo real de toda Europa sobre enfermedades, poblaciones y uso y rendimiento de los medicamentos, lo que permitirá que la EMA y las autoridades nacionales de la red europea de medicamentos utilicen estos datos siempre que sea necesario durante el ciclo de vida de un medicamento.

DARWIN EU pretende dar soporte a futuras decisiones regulatorias a través de:

- Establecer y ampliar un catálogo de fuentes de datos de observación para su uso en la regulación de medicamentos;
- Proporcionar una fuente de datos del mundo real validados y de alta calidad sobre los usos, la seguridad y la eficacia de los medicamentos;
- Abordar preguntas específicas mediante la realización de estudios no intervencionistas de alta calidad, incluido el desarrollo de protocolos científicos, interrogando fuentes de datos relevantes e interpretando y reportando los resultados del estudio.

La gama de bases de datos sanitarias aprobadas que permiten el acceso a datos distribuidos a través de DARWIN EU evolucionará y se ampliará con el tiempo.

*https://www.ema.europa.eu/en/about-us/how-we-work/big-data/data-analysis-real-world-interrogation-network-darwin-eu*

*https://www.diariomedico.com/farmacia/industria/empresas/la-ema-pone-en-marcha-su-centro-de-datos-de-vida-real-en-salud.html*

## Completada la secuenciación del genoma humano, incluyendo regiones importantes del ADN que aún permanecían inaccesibles

Aunque han pasado 21 años desde que se publicó la primera secuenciación completa del genoma humano, existían algunas regiones del genoma de referencia humano que se consideraban difíciles y que han permanecido sin resolver durante todo este tiempo. Esto obligaba a realizar suposiciones sobre esas zonas oscuras que han contribuido a asociaciones erróneas con consecuencias clínicas en algunos casos. Las nuevas tecnologías de secuenciación de "lectura larga", mucho más potente y fiables, han permitido descifrar todas esas zonas, configurando el genoma completo que ahora supone una nueva referencia (T2T-CHM13) que mejora universalmente los análisis genómicos para todas las poblaciones al corregir los principales defectos estructurales y agregar secuencias que estaban ausentes en el patrón que se utilizaba hasta ahora (GRCh38).

Los autores de la publicación en la revista science abogan por una transición rápida al genoma T2T-CHM13 como referencia, aunque entienden que la transición de las bases de datos institucionales, las canalizaciones y el conocimiento clínico de GRCh38 a T2T-CHM13 requerirá un esfuerzo bioinformático y clínico sustancial y por ello proporcionan diversos recursos para avanzar en este objetivo.

*https://www.science.org/doi/10.1126/science.abl3533*

SECTOR DE
**FARMACIA**

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

# Incorporación de alertas de desabastecimiento en receta y su priorización en el sistema de prescripción

**Mª Angeles Giménez Febrer[1], Mónica Izuel Rami[2], Diana Vanesa Bellorín Álvarez[3], Ricardo Gonzalvo Gracia[4], Rocío Arroyo Madueño[5]**

*1. Técnica titulada superior en tecnologías de la información. Responsable técnica del proyecto de Receta Electrónica. Servicio Aragonés de Salud.*
*2. FEA Farmacia hospitalaria. Responsable funcional del proyecto de Receta Electrónica. Servicio Aragonés de Salud.*
*3. Solutions Team Leader. NTT Data .*
*4. Solutions Analyst. NTT Data.*
*5. Solutions Assistant. NTT Data.*

**Los problemas de suministro de medicamentos están adquiriendo especial relevancia en los últimos años. Para facilitar su gestión, la Agencia del Medicamento (AEMPS) ha implementado la difusión de esta información de forma que sea interpretable informáticamente y poder mostrar esta información a los profesionales sanitarios. Sin embargo, con la incorporación de las alertas por Problema de Suministro ya serían cuatro los tipos de alertas diferentes que se pueden mostrar al profesional en cada línea de prescripción en el sistema de prescripción electrónica lo que hace aconsejable su priorización.**

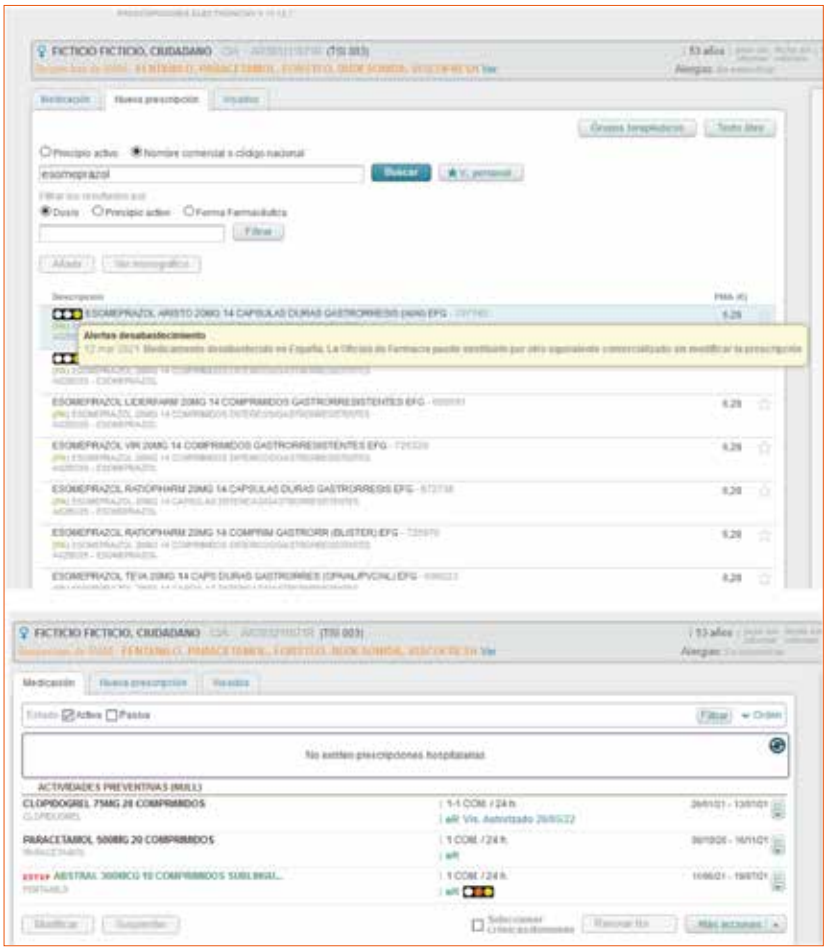
Por ello, se constituyó un grupo a nivel autonómico para la gestión de Problemas de Suministro en el que estuvieron representados Unidad Autonómica de Uso Racional de Medicamento, Servicio de Farmacias hospitalarios y de Atención Primaria, Ordenación farmacéutica, los Colegios Oficiales Farmacéuticos y el Centro de Gestión Integrada de Proyectos Corporativos para establecer el funcionamiento y gestión de las alertas por problemas de suministro.

A nivel técnico se desarrolló una lectura autónoma de los Problemas de Suministro publicada por la AEMPS y se incorporó a la base de datos la información recuperada de estos problemas tal como la publica la AEMPS. Se desarrolló en la aplicación de prescripción, un sistema de priorización de las distintas alertas que afectan a una línea de prescripción activa del paciente.

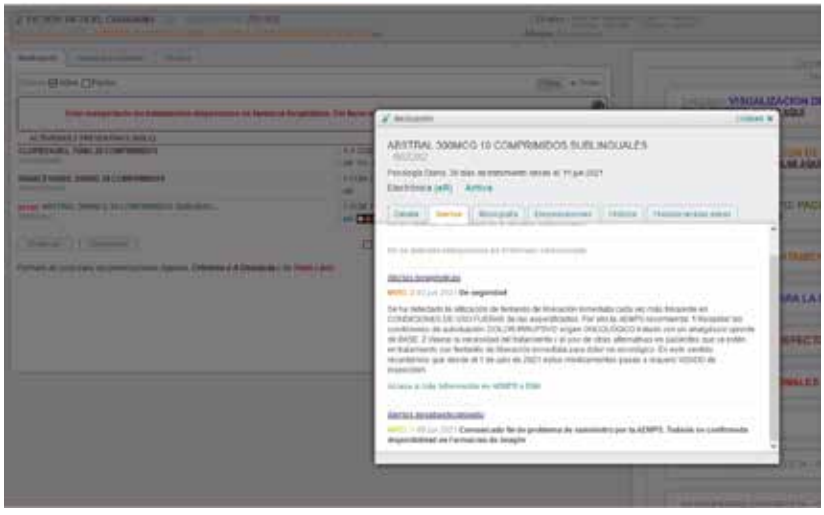
El nuevo sistema de gestión de Alertas sobre la prescripción activa se puso en marcha en octubre de 2020. Desde entonces, hasta enero 2022 se han incorporado 1.730 códigos nacionales distintos asociados a Problemas de suministro. Este sistema funciona de la siguiente manera:

- De forma diaria, se actualiza cada problema con la información proporcionada por la AEMPS (Código Nacional, tipo de problema, fecha inicio, fecha fin estimada, observaciones).
- Además, de forma semanal, el grupo autonómico revisa las alertas generadas/modificadas esa semana e incorpora información adicional al prescriptor sobre cómo actuar. Por ejemplo: si el producto con Problemas de Suministro puede ser sustituido por la oficina de farmacia directamente o debe modificarse la prescripción y, en ese caso, las alternativas disponibles.
- Por último, mensualmente, los miembros del Colegio Oficial de Farmacéuticos del grupo evalúan aquellos Problemas de Suministro con fecha informada de finalización según la AEMPS y confirman su disponibilidad en las Oficinas de Farmacia. Una vez confirmada se muestra esta información durante 4 semanas y posteriormente el Problemas de Suministro se inactiva.

Para favorecer la priorización de las alertas existentes sobre un medicamento en el sistema de pres-



*En la imagen superior se ve un fármaco con un problema de suministro en el que el grupo de trabajo informa sobre al profesional que ese código está desabastecido, pero se puede sustituir en Oficina de Farmacia. Debajo, ejemplo de un fármaco ya prescrito a un paciente en el que aparece el semáforo con dos luces activadas que indican que hay alertas asociadas:*



cripción electrónica, los Problemas de Suministro se han incorporado con el resto de alertas disponibles (interacciones, problemas de seguridad y duplicidades) en un icono tipo semáforo junto a cada línea de prescripción. En función de la gravedad de los problemas detectados se encienden las distintas luces del semáforo (roja, naranja o amarilla).

Como conclusión, consideramos que la incorporación de la información de problemas de suministro en los sistemas de prescripción acerca esta información al profesional en el momento en el que es necesaria (momento de prescripción o consulta del tratamiento del paciente) tratando de facilitar la gestión la toma decisiones y disminuir el riesgo de problemas relacionados con el medicamento.

*Si se solicita más información en el icono específico, se informa de que existen dos alertas: una de seguridad y otra de desabastecimiento. En esta última se comunica el fin de la alerta de desabastecimiento según la AEMPS pero aún no se ha confirmado su disponibilidad en las Oficinas de Farmacia de Aragón:*

# XII Reunión del Foro de Interoperabilidad en Salud

Siguenos en twitter:
@SEISeSalud

**Organiza**

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

**Con la colaboración de**

Región de Murcia

## MURCIA 27 y 28 de abril de 2022

**HOSPITAL UNIVERSITARIO REINA SOFIA**
Salón de Actos Av. Intendente Jorge Palacios, 1
30003 - Murcia

SOCIO TECNOLÓGICO PRINCIPAL

Abbott · Dedalus · FUJITSU · Microsoft

SOCIO TECNOLÓGICO COLABORADOR

Atos · EY Building a better working world · inetum. · PHILIPS · Roche · SIEMENS Healthineers