NÚMERO
139

I+S

ABRIL
2020



REVISTA DE LA SOCIEDAD ESPAÑOLA DE INFORMÁTICA Y SALUD

ESPECIAL

CIBERSEGURIDAD, **CLAVE PARA LA TRANSFORMACIÓN TECNOLÓGICA EN SALUD**



¡GRACIAS, SALVADOR!

FALLECE SALVADOR ARRIBAS VALIENTE, DIRECTOR DE I+S Y VICEPRESIDENTE DE COMUNICACIÓN DE LA SEIS

ENTIDADES ASOCIADAS

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD





























































SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

Director
Salvador Arribas Valiente
Directora de especiales
Zaida Sampedro
Comité Editorial
Luciano Sáez
Jesús Galván
Alberto Gómez Lafón
Francisco Martínez del Cerro
Guillermo Vázquez
Julio Moreno
Comité de Redacción
José Luis Monteagudo
Juan Fernando Muñoz
José Quintela
José Sacristán
Carlos García Codina
Mercedes Alfaro
José Manuel Pastora
Angel Blanco Rubio
Gregorio Gómez
Martín Begoña Oleaga
Juan Díaz
Lola Ruiz
Luz Fidalgo
Juan Ignacio Coll
Inmaculada Moro
Javier López Cavero
Fco. Javier Francisco Verdu
Carlos Gallego Pérez
Carlos Gallego Pérez
Adolfo Muñoz Carrero
Carlos Parra Calderón
Elvira Alonso Suero
Miguel Chavarría
Santiago Thovar
Miguel Angel Benito Tovar
Fernando Martín Sánchez
Inmaculada C. Castejón Zamudio
Colaborador Técnico
Diego Sáez

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

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

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

AÑO 2020 NÚMERO 139 **SUMARIO**

5 **EDITORIAL**

6 **IN MEMORIAN**
6 Julio Moreno González
7 Salvador Arribas Valiente

8 **ESPECIAL** CIBERSEGURIDAD, CLAVE PARA LA TRANSFORMACIÓN TECNOLÓGICA EN SALUD
8 Ciberseguridad, Elemento Clave para la Transformación Tecnológica en Salud
10 Aportaciones del CCN a la Mesa de Ciberseguridad como Elemento Clave para la Transformación Tecnológica de la Salud Informática
13 Ciberseguridad y su Importancia en el Sector Salud. La Experiencia de Madrid Digital
16 Seguridad de los Sistemas de Información en el Servicio Madrileño de Salud (SERMAS)
19 Informe XIV Reunión del CTSIS
22 Adecuación al RGPD y a la LOPDGDD en las Gerencias Asistenciales del Servicio de Salud de las Illes Balears
26 Retos para Implantación de los Servicios de Ciberseguridad
28 SOC del Servicio de Salud de las Illes Balears
32 Ciberseguridad: Clave en el Sector Sanitario
34 La nube, la Oportunidad de Reinventar la Seguridad para el Escenario de Amenazas Actual
36 En Ciberseguridad, mejor Prevenir que Curar
38 Asegurar Internet Industrial de las Cosas (IIoT): Cómo Abordar los Riesgos de IIoT en la Atención Sanitaria

43 **ACTIVIDADES DE LA SEIS**
43 XVII Foro de Seguridad y Protección de Datos de Salud
54 X Reunión del Foro de Interoperabilidad en Salud
56 XXVII Jornadas Nacionales de Innovación y Salud en Andalucía

58 **FOROS Y SECTORES**
58 Foro de Interoperabilidad
60 Foro de Gobernanza
62 Foro de Salud Conectada
64 Foro de Seguridad y Protección de Datos en Salud
66 Sector de Farmacia
66 Sector de Enfermería
69 Sector de Informática Médica

71 **AGENDA 2020**

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

ENTIDADES
COLABORADORAS

SOCIEDAD ESPAÑOLA DE
INFORMÁTICA DE LA SALUD

COLEGIO OFICIAL DE FARMACÉUTICOS DE CÁCERES

COLEGIO OFICIAL DE FARMACÉUTICOS DE BADAJOZ

CONSEJO GENERAL DE COLEGIOS OFICIALES DE FARMACÉUTICOS

EMERGRAF, S.L. CREACIONES GRÁFICAS

HOSPITAL CLINIC. SISTEMAS DE INFORMACIÓN

I.C.P. INGENIEROS S.A.

IDCSALUD

MUTUA UNIVERSAL

MUTUAL CYCLOPS-CENTRE DOCUMENTACIÓ

OSAKIDETZA - SERVICIO VASCO DE SALUD

SOCIO TECNOLÓGICO PRINCIPAL

DXC.technology

Microsoft

SOCIO TECNOLÓGICO COLABORADOR

EY Building a better working world

FUJITSU

HUAWEI

Ibermática

INFORMÁTICA El Corte Inglés

PHILIPS

SIEMENS Healthineers

¡GRACIAS, **SALVADOR!**

Desde nuestra consternación, escribimos estas líneas. La revista está de luto... Nos ha dejado, víctima de esta pandemia, su director, Salvador Arribas, que fue el fundador de la publicación *Informática y Salud I+S* en 1991.

Este es el número 139, que dedicamos a su labor durante 29 años y que es el último realizado bajo su dirección.

Mantener viva la revista de una sociedad científica es una labor de empeño e ilusión, siempre de alguien que cree en lo que hace y la función que esta desempeña en nuestra Sociedad. Han sido muchos los avatares por los que ha pasado a lo largo de estos años, pero ha conseguido mantenerla y convertirla en una prueba documental única. El devenir de la informática de la salud en España a lo largo de todos estos años está contenido en los 139 números publicados. Pueden ver en nuestra web todas las revistas que se consiguieron recuperar en formato digital, para aquellos que deseen o sientan la curiosidad de hacer algún estudio retrospectivo.

Todos los que alguna vez se han responsabilizado de materializar una publicación saben el trabajo que supone, máxime cuando existe el compromiso de unos plazos determinados y es necesario cubrir los contenidos planificados dependiendo de muchos autores y con la calidad precisa. Sin olvidarnos de su financiación o de los reportajes fotográficos necesarios para ilustrar convenientemente cada tema.

Mantener esta revista ha sido una acción prioritaria de la SEIS desde su creación y siempre contando con el impulso y el trabajo de Salvador. Es nuestro empeño y deseo como Sociedad Científica seguir con la edición de esta publicación, como legado de un profesional que dio lo mejor de sí mismo para que pudiéramos



contar habitualmente con este medio de comunicación.

Pero Salvador Arribas no solo dirigió la Revista. Fue creador de nuestra Sociedad, pionero en la utilización de la informática en la Medicina y un actor vital en su desarrollo. Siempre hemos podido contar con su conocimiento y su especial "hacer" en todas las decisiones que teníamos que ir adoptando para dar mayor impulso a la utilización de la informática en nuestro sector. Desde su papel como vocal de la Junta Directiva, como secretario general, como vicepresidente y, finalmente, como vicepresidente de Comunicación y Proyección Social, todos los socios de la SEIS hemos podido contar con él. Por todo esto y mucho más, siempre estará presente en todas nuestras actividades.

Sirva este último número bajo su dirección como homenaje y recuerdo permanente a su labor...

GRACIAS, SALVADOR,
por tu amistad y tu trabajo.

JULIO MORENO GONZÁLEZ

UN PIONERO DE LA INFORMÁTICA SANITARIA EN ESPAÑA

FALLECIÓ EN MÉRIDA EL PASADO 28 DE MARZO



El pasado 28 de marzo falleció en Mérida Julio Moreno González, coordinador de la Comisión Delegada, responsable del Observatorio de Calidad de la SEIS y miembro histórico de su Junta Directiva.

Socio fundador de la SEIS, ha sido coordinador general de las Jornadas Nacionales de Informática Sanitaria en Andalucía entre 2010 y 2013.

Julio Moreno era licenciado en Física y experto en Informática. Se incorporó al Hospital Universitario Virgen Macarena en 1976, iniciando el recorrido de este hospital en el dominio de la Informática Médica.

Posteriormente, se licenció en Medicina y Cirugía. Fue profesor asociado de Medicina Preventiva y Salud Pública y de Ciencias Socio-sanitarias, en la Facultad de Medicina de la Universidad de Sevilla, impartiendo clases además en la Facultad de Farmacia.

"Destacó por su apoyo a la Sanidad Pública y mantuvo una importante actividad de cooperación internacional en distintos países en desarrollo"

Desarrolló una intensa actividad de colaboración con el Colegio de Médicos de Sevilla, siendo pionero en la formación de médicos en habilidades informáticas a principios de los años 80. Fue miembro fundador de la Sociedad Médica de Escritores y Artistas "Nicolás Monardes", bajo el apoyo de dicho Colegio de Médicos, de la cual fue presidente durante más de diez años y que hoy continúa su andadura. También estuvo muy vinculado a la extinta Fundación colegial. Ha sido, además, autor de numerosas publicaciones.

Destacó por su apoyo a la Sanidad Pública y mantuvo una importante actividad de cooperación internacional en distintos países en desarrollo.

Fue una persona entrañable, trascendiendo con creces lo profesional. Nos queda su recuerdo, representó la cara más amable de la SEIS. Su trabajo fue impecable en el ámbito de las relaciones institucionales y nos deja su legado como referente de la SEIS, con la que nunca dejó de comprometerse, desde su versatilidad, cordialidad, amabilidad, cortesía, ironía, elocuencia y compromiso con la Sanidad Pública.

Descansa en Paz, Julio.

SALVADOR ARRIBAS VALIENTE

VICEPRESIDENTE DE PROYECCIÓN SOCIAL Y COMUNICACIÓN DE LA SEIS Y DIRECTOR DE LA REVISTA I+S

FALLECIÓ EN MADRID EL PASADO 14 DE MARZO

Salvador Arribas era Doctor en Medicina por la Universidad Complutense de Madrid y licenciado en Informática por la Universidad Politécnica de Madrid, Título Oficial de Gerente de Hospitales y Médico por oposición del Ayuntamiento de Madrid.

En su larga trayectoria profesional, además de médico asistencial en diferentes instituciones sanitarias, fue jefe de Bioestadística del Hospital La Paz hasta su jubilación y profesor de Bioestadística en la Escuela Universitaria de Enfermería de La Paz.

Incorporó la asignatura de Informática Medica en la Facultad de Informática de la UPM, de la que fue profesor durante muchos años, así como profesor de Inteligencia Artificial en dicha Facultad de Informática. En 1974, creó el Servicio de Informática de la entonces Ciudad Sanitaria La Paz y fue pionero en el desarrollo de soluciones informáticas aplicadas a la medicina, participando en numerosos grupos de trabajo e instituciones.

Entre sus muchas realizaciones, organizó cursos y seminarios de informática médica y ya en 1977 creó conjuntamente con otros jefes de Servicio de Informática de grandes hospitales la Sociedad Española de Informática Médica (SEIM). Fue miembro su Junta Directiva y apoyó la conversión de esta Sociedad en Sociedad Española de Informática de la Salud en 1990. En esta nueva época de la Sociedad, ha estado presente en su Junta Directiva desde su creación ocupando los puestos de secretario general, vicepresidente y en la actualidad era vicepresidente de Comunicación y Proyección Social.

En 1991 creó la Revista *Informática y Salud I+S*, de la que fue su director hasta la actualidad, con la edición de 139 números. Los contenidos publicados en la Revista muestran la historia de la Informática de la Salud en España en los últimos 30 años.



Además de su actividad en la SEIS, Salvador Arribas fue, durante los últimos doce años, secretario general de la Fundación Bamberg, donde mantuvo una labor muy destacada en el desarrollo de sus actividades, dirigidas a la mejora de la gestión de la asistencia sanitaria, así como en la realización de propuestas de políticas sanitarias, orientadas al perfeccionamiento de nuestro Sistema Sanitario.

Salvador ha sido un referente y un miembro muy destacado de la Sanidad Española, creía en la función que desempeñaba en nuestro Sistema de Salud, para la que ha dedicado su vida hasta el final.

Siempre permanecerá en nuestro recuerdo. Descanse en Paz.

Ciberseguridad, Elemento Clave para la Transformación Tecnológica en Salud

La Agencia Española de Protección de Datos (AEPD) es la autoridad de control independiente que vela por el cumplimiento de la legislación en materia de protección de datos. En desarrollo del artículo 51 del RGPD, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales (en adelante, la LOPDGDD) establece que "la Agencia Española de Protección de Datos es una autoridad administrativa independiente de ámbito estatal, de las previstas en la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP), con personalidad jurídica y plena capacidad pública y privada, que actúa con plena independencia de los poderes públicos en el ejercicio de sus funciones".

Por otra parte, en virtud de la previsión contenida en el artículo 57 de la LOPDGDD, existen las autoridades de control autonómicas que ejercen sus funciones en relación con su respectivo sector público y que son la Agencia Vasca de Protección de Datos, la Autoridad Catalana de Protección de Datos, y el Consejo de Transparencia y Protección de Datos de Andalucía.

La AEPD participa de forma activa en el Comité Europeo de Protección de Datos (EDPB), antes Grupo de Trabajo del artículo 29, en el desarrollo de criterios y dictámenes que son asumidos por todas las autoridades europeas.

El derecho a la protección de datos personales es un derecho fundamental y, como tal, regulado por una ley orgánica. Este derecho es un conjunto de principios y garantías que pretenden evitar injerencias arbitrarias en la vida privada y familiar de cualquier persona protegiendo su domicilio, su correspondencia, su honra y su reputación. El RGPD y la LO 3/2018 (LOPDGDD) proporcionan un conjunto de principios entre los que se incluye el principio de seguridad: licitud, lealtad, transparencia, finalidad, proporcionalidad, calidad y exactitud, limitación, y seguridad. Por tanto, debemos de entender que la seguridad, por sí misma, no garantiza el derecho a la protección de datos sino que se suma al resto de principios que hacen posible la misma. Sin embargo, sin la adecuada gestión de la seguridad de los datos personales, no será posible garantizar la protección de los datos personales.

GESTIÓN DE LA SEGURIDAD

La necesidad de la gestión de la seguridad de la información se plantea a medida que se empiezan a construir lo que aún denominamos nuevas tecnologías, por desgracia, inicialmente no disponíamos de mecanismos de gestión de seguridad o de una norma como el ENS, lo que hacía que el trabajo de los responsables de seguridad se desarrollara en un escenario complejo en el que no existía una "cultura de la seguridad" en las organizaciones.

Afortunadamente, la gestión de la seguridad de la información nos permite hoy en día, llevar a cabo un trabajo conjunto por personal cada vez más especializado en materia de seguridad de la información. En este sentido, debemos de tener en cuenta que a medida que los ataques a una organización evolucionan, requiere que la formación y capacidad de los Responsables de Seguridad o del personal implicado en la seguridad de las organizaciones evolucione de forma inmediata, es decir, es necesario un esfuerzo permanente de las organizaciones y una inversión permanente tanto humana como material. En definitiva, la economía digital exige a los responsables de la información un esfuerzo e inversión permanentes para enfrentarse a los, cada vez más complejos, retos de la ciberseguridad. Esfuerzo e inversión que son o deberían formar parte de la estructura de las organizaciones.

DERECHOS Y LIBERTADES: SANIDAD

Como se ha señalado, las normas de protección de datos se orientan hacia un conjunto de principios

entre los que se encuentra el principio de seguridad, intentan garantizar los derechos de las personas en el contexto de cualquier tratamiento de datos y de acuerdo a la sensibilidad de los mismos. La digitalización del sector sanitario ofrece nuevas oportunidades a los investigadores, oportunidades que no se encuentran exentas, al mismo tiempo, de nuevos riesgos y donde las autoridades de control intentan proporcionar criterios y recursos que hagan posible el avance digital y la salvaguarda de los derechos de los ciudadanos.

El derecho de acceso a los servicios sanitarios forma parte de nuestro estado de derecho y, como tal, debe ser protegido. El derecho fundamental a la protección de datos personales tiene por objetivo clave hacer posible el desarrollo de la economía digital sin perjuicio para los derechos y libertades de las personas y aquí es donde la seguridad de la información o la ciberseguridad se convierte en un valor clave para garantizar el funcionamiento del sistema de salud, y en particular para garantizar la confidencialidad, la integridad y la disponibilidad de la información.

Si entendemos que el paciente es el centro del sistema sanitario debemos de entender que es precisamente el paciente lo que protege la ciberseguridad. Un error de la integridad de la información podría poner en riesgo la vida de una persona, por tanto, la calidad del servicio sanitario se asienta, entre otros pilares, en el pilar de la ciberseguridad.

El nuevo contexto normativo en materia de protección de datos personales exige a los responsables una actitud proactiva trabajando de forma prospectiva a fin de identificar posibles riesgos, conocidos o no conocidos, tanto para la seguridad de la información como para el propio interesado cuyos datos fueran objeto de tratamiento, pero también exige a los responsables y encargados de los tratamientos la adecuada gestión de brechas como medida de reacción frente a los incidentes de ciberseguridad o lo que podríamos denominar "lecciones aprendidas". Por tanto, la ciberseguridad debe de entenderse como un valor que se orienta en ambas direcciones (prospectiva y reactiva) y que, en definitiva, no es otra cosa que un trabajo de mejora continua que debe ser realizado por profesionales cada vez más especializados.

Para proteger la salud del paciente, la calidad del sistema sanitario es fundamental, en este sentido, la especialización del profesional de la seguridad redundará en dicha calidad. Frente al trabajo del profesional de la protección de datos o DPD, el Responsable de Seguridad debe orientar sus esfuerzos hacia el mundo tecnológico mientras que el DPD debe de orientar sus esfuerzos hacia la protección de los derechos y libertades del paciente, lo que en ambos casos redundará en la calidad del sistema a la vez que implicará una mejora en la práctica del concepto del paciente como centro del sistema de salud. La separación de funciones de ambos profesionales y el hecho de que formen parte de las estructuras de las organizaciones, funcional y orgánicamente, son un factor clave para la calidad de los servicios sanitarios. No se trata únicamente de salvar vidas o mejorar la salud de los pacientes, también es necesario garantizar la dignidad del paciente y aquí es donde la protección de sus datos es un beneficio integral para el concepto de paciente como centro del sistema de salud.

CONCLUSIÓN

La ciberseguridad implica un esfuerzo común al que únicamente puede llegarse mediante la concienciación de todos los implicados, entre quienes hay que incluir la alta dirección de las organizaciones y los propios pacientes, en el conjunto de colectivos implicados tampoco tenemos que olvidar a todos los que se ven directa o indirectamente implicados en la investigación sanitaria como es el caso de los propios comités éticos en los que el DPD y el Responsable de Seguridad pueden ayudar a garantizar los derechos de los interesados.

No será posible disponer de un servicio de salud de calidad si no se destinan los recursos adecuados para la protección de la información y, por tanto, para la protección adecuada del paciente, recursos que deben de realizar un trabajo permanente ya que las amenazas a las que se encuentran expuestas las organizaciones sanitarias tienen también carácter permanente y evolucionan a medida que evoluciona la tecnología y el escenario en el que tienen lugar los tratamientos de los datos de salud de los ciudadanos.

Aportaciones del CCN a la Mesa de Ciberseguridad como Elemento Clave para la Transformación Tecnológica de la Salud Informática

EL SECTOR DE LA SALUD PRESTA UN SERVICIO ESENCIAL, ESTRATÉGICO Y PRIORITARIO. POR ESTE MOTIVO, RESULTA IMPRESCINDIBLE GARANTIZAR LA SEGURIDAD DE LOS SISTEMAS QUE EMPLEA, LOS DATOS QUE MANEJA, SUS COMUNICACIONES Y SUS SERVICIOS ELECTRÓNICOS. LA CIBERSEGURIDAD DEBE CONSIDERARSE UN SERVICIO MÁS DEL SECTOR SANITARIO, PUES CONSTITUYE EL ELEMENTO CLAVE PARA LA TRANSFORMACIÓN TECNOLÓGICA DE LA SALUD.

1. SOBRE CCN-CERT, CERT GUBERNAMENTAL NACIONAL

El CCN-CERT es la Capacidad de Respuesta a incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN, adscrito al Centro Nacional de Inteligencia, CNI. Este servicio se creó en el año 2006 como CERT Gubernamental Nacional español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del CNI, el RD 421/2004 de regulación del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015 de 23 de octubre.

Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas, incluyendo la coordinación a nivel público estatal de las distintas Capacidades de Respuesta a Incidentes o Centros de Operaciones de Ciberseguridad existentes.

Todo ello, con el fin último de conseguir un ciberespacio más seguro y confiable, preservando la información clasificada (tal y como recoge el art. 4. F de la Ley 11/2002) y la información sensible, defendiendo el Patrimonio Tecnológico español, formando al personal experto, aplicando políticas y procedimientos de seguridad y empleando y desarrollando las tecnologías más adecuadas a este fin.

De acuerdo a esta normativa y la Ley 40/2015 de Régimen Jurídico del Sector Público es competencia del CCN-CERT la gestión de ciberincidentes que afecten a cualquier organismo o empresa pública. En el caso de operadores críticos del sector público, la gestión de ciberincidentes se realizará por el CCN-CERT en coordinación con el CNPIC.

2. CIBERSEGURIDAD COMO ELEMENTO CLAVE PARA LA TRANSFORMACIÓN TECNOLÓGICA DE LA SALUD

El Esquema Nacional de Seguridad, aprobado por el RD 3 /2010 de 8 de enero y modificado por el RD 951/2015 de 23 de octubre, establece que se debe proteger la información manejada por los sistemas en sus cinco (5) dimensiones:

- [C] CONFIDENCIALIDAD: propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. Ello evita que determinada información sea accesible por personas no autorizadas. Esta dimensión es un



complemento importante a la protección de datos y a la privacidad.

- [I] INTEGRIDAD: propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. En el caso del sector salud, información no íntegra puede afectar de manera directa a la vida del paciente.
- [D] DISPONIBILIDAD: propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. La falta de esta dimensión en la información o en los sistemas afectaría de manera grave a los servicios asistenciales o a las historias clínicas.
- [A] AUTENTICIDAD: propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Una deficiencia en esta dimensión puede ocasionar accesos no autorizados a información de los pacientes.
- [T] TRAZABILIDAD: propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. Es decir, permite que se puedan registrar y trazar las acciones sobre información clínica.

Para el sector sanitario, la protección de todas las dimensiones descritas resulta más crítica que para otros sectores. Además, este sector debe cumplir también con lo establecido en otras legislaciones como la Ley 8/2011 de 28 de abril, por la que se establecen medidas para protección de las infraestructuras críticas y el RD 721/2011, de 20 de mayo, sobre infraestructuras críticas, pues el sector de la Sanidad es un sector estratégico; la Directiva NIS y su RDL 12/2018 de transposición de ésta al ordenamiento jurídico español, que lo considera un servicio esencial; el Reglamento General de Protección de Datos y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, que lo define y amplía por tratar quizás la información más crítica de los ciudadanos: sus datos de salud.

El cumplimiento de toda esta legislación es una tarea irrenunciable en el sector sanitario. No obstante, de la experiencia de los Informes Nacionales del Estado de Seguridad (INES), que se elaboran anualmente, se concluye que el nivel de cumplimiento del sector respecto a la adecuación al Esquema Nacional de Seguridad es BAJO. Por ello, con carácter urgente, se han de implementar los siguientes principios dentro del sector:

- NECESIDAD DE REDUCIR LA SUPERFICIE DE EXPOSICIÓN. AUDITORÍA CONTINUA. El perímetro de protección de las redes es cada vez más difuso, principalmente como consecuencia del teletrabajo de los facultativos y el uso de servicios en la nube.

  Por ello, se debe establecer una política de realización de auditorías que permita una evaluación continua de la superficie de exposición a la ciberamenaza, que no estén guiadas solo por el cumplimiento normativo, sino que también por una vocación real de reducir las vulnerabilidades técnicas y de implementación que existen en nuestras redes y que nos hacen ser objetivos blandos muy fáciles de atacar.

- NECESIDAD DE VIGILANCIA CONTINUA. Los hospitales y centros asistenciales desempeñan una labor crítica: la atención a los ciudadanos.

  Por ello, es necesaria la implementación de centros de operaciones de ciberseguridad que permitan concentrar el conocimiento y que presten un servicio horizontal dentro de un servicio de salud autonómico. Esta iniciativa está siendo impulsada por el CCN bajo el nombre de SOC VIRTUAL.

- NECESIDAD DE CERTIFICACIÓN DE PRODUCTOS. Quizás el sector salud sea el sector que más dispositivos biomédicos tenga desplegados en la población y el que más sistemas industriales –aparatos de pruebas médicas y análisis clínicos– tenga en sus redes corporativas; dispositivos cuyos requisitos de ciberseguridad son escasos o nulos

  La Unión Europea ha identificado este aspecto y está forzando el establecimiento de un modelo de certificación para este equipamiento que ya incorpore medidas de ciberseguridad.

- NECESIDAD DE INTERCAMBIO. Aunque en todas las regulaciones que aplican al sector Salud se establece la obligación de notificar los ciberincidentes de los que un organismo sea víctima, este aspecto todavía no está maduro, y como resultado se notifica tarde y mal. Por ello, es urgente que se implanten modelos de intercambio de información que permitan una automatización en el intercambio de los incidentes y un trabajo conjunto en su resolución.

Lamentablemente, los incidentes de *ransomware* (código dañino que cifra los ordenadores y servidores conectados a una red corporativa) sufridos durante finales de 2019 y principios de 2020 han evidenciado que a día de hoy ataques de poca complejidad pueden lograr que nuestras redes queden completamente inoperativas.

Estos ataques pueden conseguir que un hospital funcione en un modo muy degradado durante al menos 20 días si la infección se ha extendido. Pronto nos enfrentaremos a ataques que se centrarán en el robo de historias clínicas y datos personales de nuestros pacientes, con el daño a la confianza en el servicio que ello conlleva.

Además, el Centro Criptológico Nacional, durante el apoyo de estos incidentes, ha detectado que la acción de NOTIFICAR no es suficiente pues, al existir interconexiones entre todos los hospitales para el intercambio ágil de las pruebas necesarias y las historias clínicas, estas infecciones se pueden extender.

Por ello, es necesaria la existencia de un organismo independiente que acompañe a la víctima en la resolución del incidente y certifique que el sistema se encuentra aceptablemente limpio antes de su reconexión al sistema de salud. Esta es una tarea pendiente de definir en las próximas normas que se publiquen.

Si impulsamos acciones en todos estos campos, la seguridad real de nuestros servicios de salud mejorará drásticamente. El Centro Criptológico Nacional tiene la vocación de ayudar a elevar los niveles de seguridad de todo nuestro Sector Sanitario. Por ello como titular se propone que:

"La ciberseguridad se debe considerar un servicio más del sector sanitario"

Así, trataremos a la ciberseguridad como un elemento clave para la Transformación Digital y Tecnológica de nuestros servicios de salud y evitaremos que posibles ataques limiten la operatividad de estos.

Además, como se ha explicado anteriormente, puede ser un servicio horizontal a muchos hospitales y centros asistenciales para que con personal propio y/o subcontratado se concentre el conocimiento y se pueda proteger adecuadamente este servicio tan crítico para la ciudadanía. Por tanto, la implementación del modelo de Centro de Operaciones de Ciberseguridad (VIRTUAL SOC) resulta absolutamente imprescindible.

Ciberseguridad y su Importancia en el Sector Salud
La Experiencia de Madrid Digital



Esther Muñoz Fuentes
Directora de Ciberseguridad. Madrid Digital

CUANDO A PRINCIPIOS DE MARZO DE ESTE AÑO 2020, SE NOS PLANTEÓ LA POSIBILIDAD DE PARTICIPAR EN ESTE ESPECIAL DE CIBERSEGURIDAD DE LA REVISTA SEIS, CONTANDO LA EXPERIENCIA, RETOS Y PROYECTOS EN MATERIA DE CIBERSEGURIDAD QUE MADRID DIGITAL DESARROLLA Y HA PUESTO EN MARCHA EN LOS ÚLTIMOS AÑOS EN EL ECOSISTEMA DE SALUD, SOCIO-SANITARIO, DE LA COMUNIDAD DE MADRID, PRÁCTICAMENTE NINGUNO DE LOS QUE TRABAJAMOS EN ESTE ÁMBITO, PODÍAMOS LLEGAR A VISLUMBRAR LA QUE SE AVECINABA, Y DE QUÉ MANERA IBA A AFECTAR A NUESTRO TRABAJO. ESTAMOS HABLANDO DE LA CRISIS DEL COVID-19.

También en nuestro caso esta crisis ha supuesto que lo urgente y lo importante se hayan unido en una "mezcla explosiva" bastante complicada de gestionar, ya que era urgente proporcionar medios de teletrabajo de forma masiva para el personal sanitario, al mismo tiempo que se conectaba a la red sanitaria a IFEMA, a los hoteles medicalizados y hospitales de campaña; todo ello de un día para otro, asegurando lo más importante: la disponibilidad 24x7 de la red de datos y de los pcs, tabletas del personal sanitario, desde los que se consulta la historia clínica y demás sistemas sanitarios de los pacientes.

Teniendo este objetivo de disponibilidad tan claro, y conociendo que el riesgo más crítico que teníamos que gestionar era y es que un hospital pudiera sufrir un ataque, entrara ransomware y todos los puestos de un hospital se cifraran, los esfuerzos se centralizaron en su consecución, aumentado la protección de los puestos y redes, considerando que, al mismo tiempo aumentaban de forma exponencial las amenazas externas que iban surgiendo y propagándose desde Internet, a la vez que se disparaba el riesgo que suponía el aumento de la exposición de nuestras redes y sistemas ante el auge del teletrabajo. Todo ello, nos ha obligado y obliga a aumentar, dedicar y diversificar recursos y esfuerzos a recopilar, estudiar e investigar lo que estaba sucediendo, reforzando nuestras capacidades de vigilancia, detección, análisis e intercambio de información de seguridad referente a nuevos tipos de ataques, *malware*, incidentes de seguridad, con otras organizaciones, y especialmente con el centro de referencia en gestión de incidentes de seguridad, CCN-CERT.

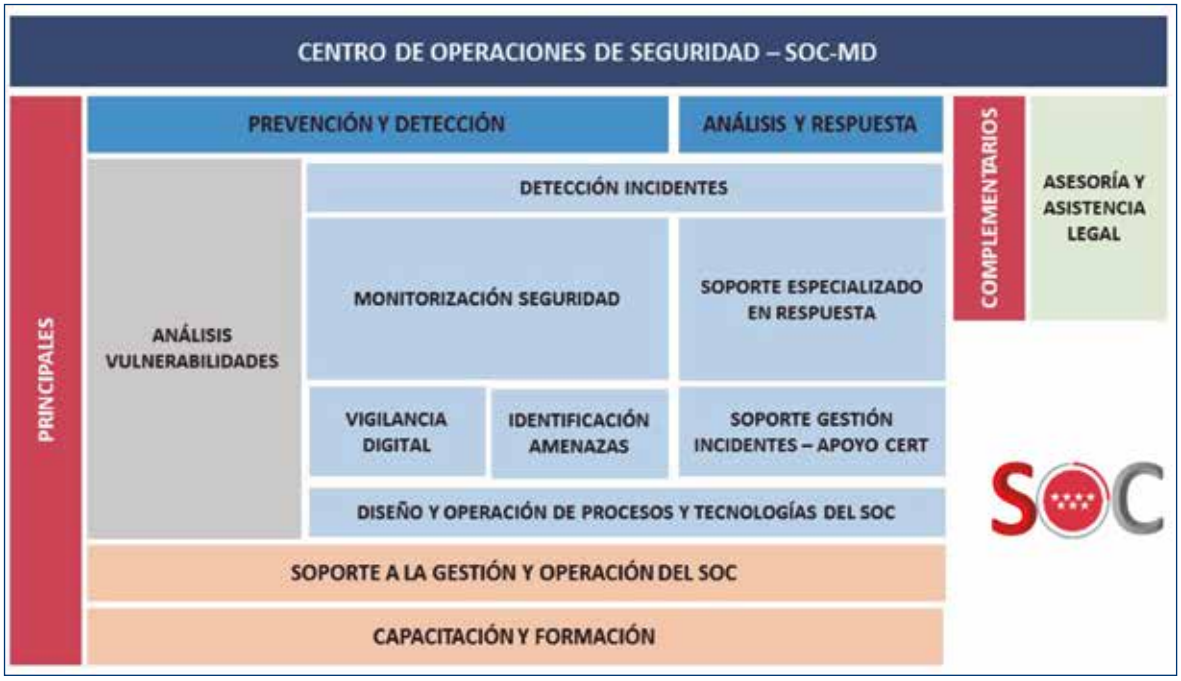
Como ejemplo del aumento exponencial de amenazas que estamos sufriendo durante esta crisis COVID-19, a principios de abril el CCN-CERT anunció que se habían detectado más de 24.000 dominios web relacionados con el Covid-19, de los cuales 16.000 se crearon en el mes de marzo, muchos de ellos sospechosos de ser usados para fraudes, suplantaciones de identidad y envío de correos de *phishing*. Además, el número de *hashes*, firmas de *malware* nuevas superaba ya las 500 conocidas, y se anunciaba que el número de incidentes relacionado con *phishing* en

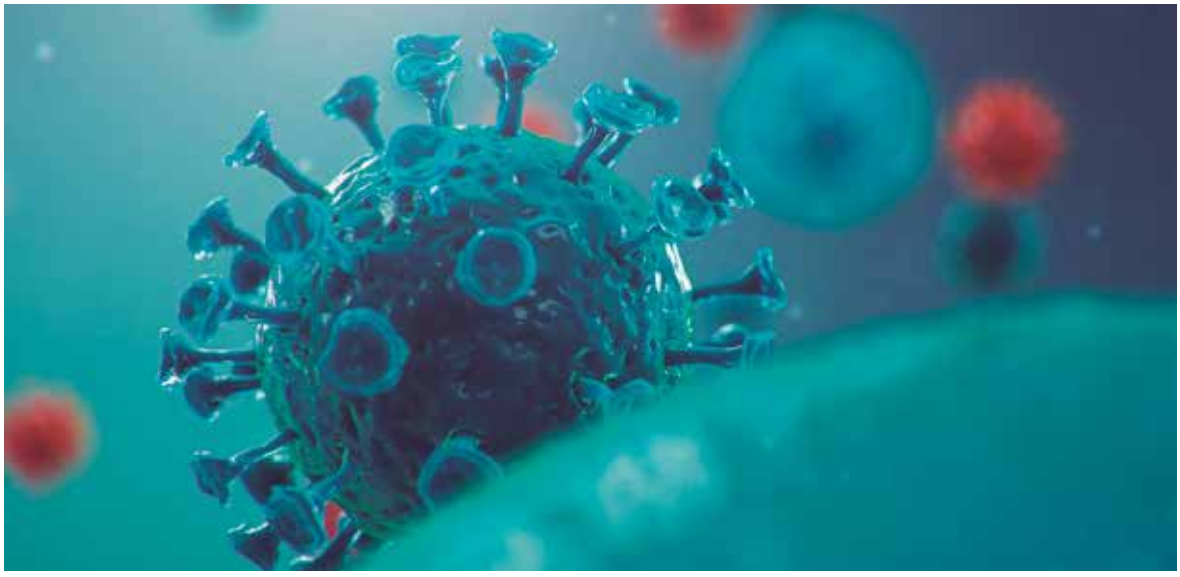
organismos públicos había aumentado un 70%. Ante esta situación el CCN-CERT ha redoblado su comunicación y coordinación con todas las comunidades autónomas, dejando claro que la prioridad es la protección de todo nuestro sistema sanitario. También Europol y ENISA (Agencia de Ciberseguridad de la Unión Europea) han aumentado sus esfuerzos en comunicación y difusión de estado de ciberseguridad, divulgando boletines de seguridad y realizando informes periódicos y extraordinarios de análisis de amenazas, e incidentes de seguridad registrados.

Entendiendo la complejidad y gravedad de la situación, es momento de poner en contexto como nos ha afectado todo esto, considerando el ámbito de actuación y competencias de Madrid Digital en todo lo relativo a la gestión TIC del ámbito sanitario.

Madrid Digital, gestiona la red de datos multiservicio, el servicio de correo electrónico @salud.madrid.org, y los puestos de trabajo, pcs y portátiles de toda la sanidad pública madrileña. Estamos hablando de más de 55.000 pcs y de unos 10.000 portátiles y tabletas conectados en red. Madrid Digital también provisiona, opera y mantiene todos los servicios de voz, fija y móvil para todos los hospitales y centros sanitarios, hospitales tan grandes algunos de ellos como el Hospital de La Paz, el Gregorio Marañón, el 12 de Octubre, el Ramón y Cajal etc., hospitales con miles de profesionales y equipos en red. Esta red de datos multiservicio que une todos estos centros está conectada a Internet.

Pues bien, ha llegado el momento de contar cual es nuestra experiencia en ciberseguridad en el entorno sanitario, y cuales han sido los principales proyectos que hemos desarrollado, los cuales han sido claves para poder encarar mejor esta situación de crisis. Podemos destacar dos: el despliegue de soluciones de EDR (*Endpoint Detection Response*) en puestos de trabajo, con capacidades de análisis de comportamiento, actualización continua de amenazas desde Internet y capacidades de bloqueo y contención de todo el parque de pcs desde consola centralizada ante una infección, todo ello complementado con una monitorización 24x7 del estado de la protección por parte de un equipo de analistas especializados en este tipo de soluciones; y por otra parte, la puesta en marcha del Centro de Operaciones de Seguridad, SOCMD como le hemos llamado. El objetivo de este SOCMD es centralizar las capacidades actuales y futuras en materia de ciberseguridad de Madrid Digital, desarrollando las funciones de prevención, detección temprana de amenazas e incidentes,





análisis de vulnerabilidades, monitorización de eventos e información de seguridad, análisis y resolución de incidentes de seguridad; todo ello de forma centralizada y con procesos y procedimientos operativos de seguridad consistentes, que nos han permitido obtener informes efectivos sobre el estado global de la ciberseguridad y de los riesgos identificados. El SOCMD también cuenta con servicios de asesoría legal y capacitación y formación especializada.

Con el SOCMD estamos alineados con la estrategia de Ciberseguridad 2019 del Gobierno de España, en particular con las líneas de acción I: *"reforzar las capacidades ante las amenazas provenientes del ciberespacio"* y línea de acción II: "*garantizar la seguridad y resiliencia de los activos estratégicos de España*".

Esas dos líneas de acción de la estrategia de Ciberseguridad de 2019 están siendo premonitorias y particularmente importantes en estos tiempos, ya que si hay un activo estratégico en España en estos momentos, es la Sanidad, la cual cada día que pasa es más dependiente de las TIC, y estas últimas, en un mundo cada vez más interconectado, abierto, con más servicios y dispositivos accesibles desde Internet, dependen de una práctica de ciberseguridad más desarrollada que permita generar confianza en la utilización de la tecnología.

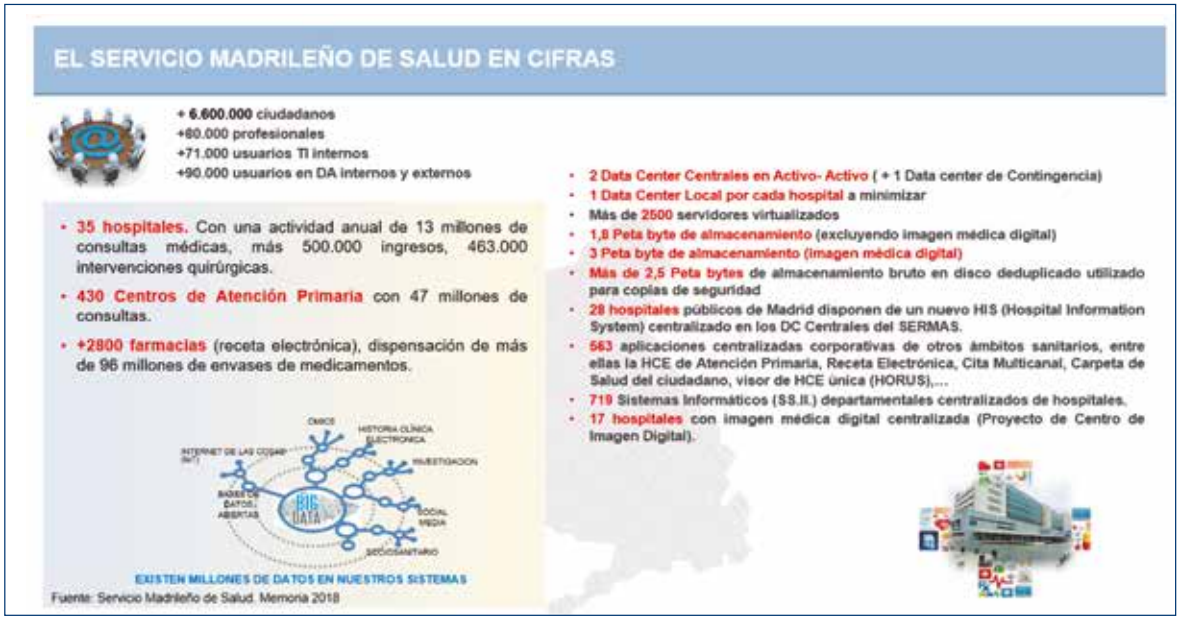
Por último, entre los retos de futuro para la ciberseguridad dentro del entorno sanitario para Madrid Digital, no debemos obviar las recomendaciones que ha realizado ENISA en su informe de febrero de 2020 denominado: "*Procurement Guidelines for Cibersecurity in Hospitals*", "Buenas prácticas en ciberseguridad para la adquisición en hospitales" en donde se indica lo siguiente: *... El hospital puede considerarse una colección de activos (infraestructura, software, sistemas, dispositivos, etc.), y la ciberseguridad debe abordarse explícitamente en todos sus diferentes componentes. En general, el objetivo de este estudio es proporcionar a los profesionales de la salud en los hospitales, pautas sobre cómo mejorar su proceso de adquisición para cumplir con los objetivos de ciberseguridad. Estas pautas cubren múltiples temas y van desde buenas prácticas organizativas para las propias organizaciones de atención médica, hasta qué información solicitar a los proveedores como "evidencia" de ciberseguridad al adquirir sistemas y servicios*. Esta es la clave: si no hay, no se exige ciberseguridad desde la adquisición, desde la compra de *hardware*, *software*, no hay ciberseguridad. Lo que no se tiene en cuenta y no se diseña "aguas arribas" es imposible implementarlo cuando está en producción y lo está usando un profesional sanitario. En estos tiempos, la ciberseguridad desde el diseño no es una recomendación es una necesidad.

Seguridad de los Sistemas de Información en el Servicio Madrileño de Salud (SERMAS)



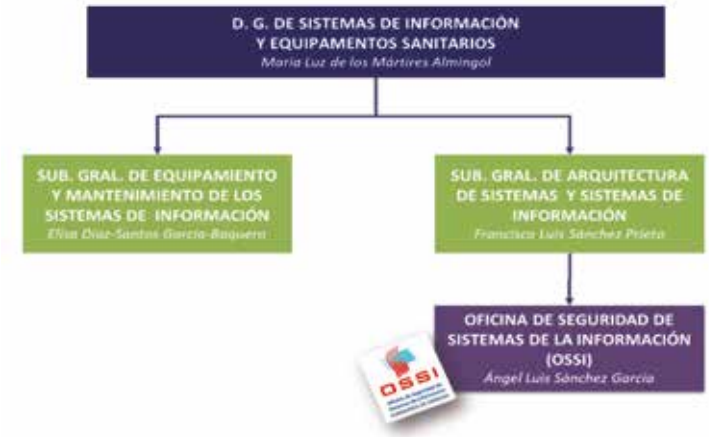
Ángel Luis Sánchez García
Jefe de Servicio de Seguridad de Sistemas de Información (CISO)
Responsable de la Oficina de Seguridad de Sistemas de Información (OSSI)
Dirección General de Sistemas de Información y Equipamientos Sanitarios (DGSIES)
Servicio Madrileño de Salud (SERMAS). Consejería de Sanidad - Comunidad de Madrid

HOY, LA SEGURIDAD DE LA INFORMACIÓN Y LA PROTECCIÓN DE LOS DATOS PERSONALES SON CUESTIONES IMPORTANTES A CONSIDERAR POR TODAS LAS ORGANIZACIONES DE CUALQUIER SECTOR. ADEMÁS, EL HECHO DE QUE LOS DATOS PERSONALES RELATIVOS A LA SALUD SEAN CONSIDERADOS COMO DATOS SENSIBLES Y ESPECIALMENTE PROTEGIDOS, Y TRAS LA PUBLICACIÓN DEL RGPD COMO UNA CATEGORÍA ESPECIAL DE DATOS PERSONALES, LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN SANITARIOS SE HA CONSIDERADO UN OBJETIVO PRIORITARIO DEL SERVICIO MADRILEÑO DE SALUD (SERMAS).



Para poder afrontar con garantías la seguridad de dichos Sistemas, debemos tener en cuenta que el SERMAS:

1) Es uno de los organismos públicos más importantes y grandes del país y, una de las empresas españolas con mayor de número de trabajadores de España y, posiblemente, la mayor de la Comunidad de Madrid. Muchos de ellos son personal sanitario, altamente cualificado.
2) Dispone de *Petabytes* de datos de los ciudadanos, usuarios del Sistema Sanitario Público de la Comunidad de Madrid, principalmente datos personales y de salud.
3) Pone a disposición de sus profesionales y los



ciudadanos más de 1200 Sistemas de Información Sanitarios, desde sus *Data Center* Centrales. Sistemas que requieren un alto nivel de integración e interoperabilidad.

4) Además de tener como actividad principal la asistencia sanitaria, tiene otras actividades importantes como la investigación y la formación que realizan parte de sus profesionales.

Por todo ello, la Consejería Sanidad de la Comunidad de Madrid (CSCM), consciente de los retos de seguridad a los que se enfrentaba, decidió poner en marcha ya en 2006, la Oficina de Seguridad de los Sistemas de Información (OSSI) con el objetivo principal de prevenir, detectar y dar respuesta a todas las amenazas e incidentes. También realiza asesoramientos integrales a los centros dependientes de la Consejería sobre políticas, normativas y medidas de seguridad.

Hoy, con más de 13 años de experiencia, la OSSI, dependiente del CISO de la CSCM, dispone de un equipo multidisciplinar compuesto por una serie de consultores con perfil técnico, legal y mixto, especializados en los diversos ámbitos de la seguridad de la información. El objetivo de la OSSI es disponer de una visión de la seguridad de 360º para prestar un servicio integral a todos los Centros Sanitarios y Direcciones Generales de la CSCM.

Para ello, en la OSSI se han establecido las siguientes líneas de servicio, orientadas a garantizar la seguridad de la información y protección de datos personales a distintos niveles, atendiendo las necesidades de los centros del SERMAS: asesoramiento legal, asesoramiento y auditoría de controles de seguridad, monitorización y correlación de eventos, análisis de *software* y *hardware*, comunicación y formación.

El modelo de gestión de la seguridad del SERMAS ha ido evolucionando en el tiempo, adaptándose a las nuevas normativas, los nuevos escenarios de la Ciberdelincuencia en los ámbitos sanitarios y las nuevas líneas estratégicas de la Consejería. El éxito de la labor del SERMAS y de la OSSI queda reflejado en los múltiples reconocimientos externos recibidos en los últimos años.

ACTUACIONES DE LA OSSI ANTE LA CRISIS DEL COVID-19

Dentro de las actuaciones de la OSSI para gestionar la situación excepcional del COVID-19, resaltan algunas actividades específicas para el fortalecimiento de la seguridad y la mitigación de posibles riesgos, así como facilitar la labor asistencial de nuestros profesionales sanitarios y la relación con los pacientes y sus familiares, cumpliendo con la normativa vigente en protección de datos.

Se ha trabajado en la habilitación y securización del acceso remoto para que los profesionales puedan teletrabajar, de manera que el servicio se vea afectado de la menor manera posible.

Se han emitido correos de comunicación e informes de recomendaciones y buenas prácticas para que los profesionales den asistencia de manera adecuada y se han resuelto una gran cantidad de dudas remitidas al buzón de la Oficina de Seguridad en relación a situaciones puntuales y específicas de profesionales sanitarios.

A raíz de la crisis, se han propuesto diversas aplicaciones en relación a recibir instrucciones y recomendaciones sobre el COVID-19, ya sea para autodiagnóstico, servicio asistencial remoto o información a familiares, de modo que no tengan que acudir a un centro sanitario, con objeto de minimizar la posibilidad de contagio.

Dada la urgencia de la puesta en producción de estas aplicaciones, desde la OSSI se ha intensificado el servicio de auditoría tanto de la parte legal y normativa, elaborando y adecuando contratos, convenios, políticas de seguridad y acuerdos de colaboración con diferentes entidades. En la parte técnica, se han realizado test de intrusión a las plataformas para evaluar y emitir consideraciones, tanto en sus versiones web como móviles, de modo que esta puesta en producción se realizase en plazos y forma, minimizando el nivel de ries-



gos que tenían atribuido en su presentación. Con motivo del incremento de infectados por el virus en la Comunidad de Madrid, se ha habilitado en tiempo récord, un hospital en el recinto de IFEMA, así como múltiples hoteles medicalizados. En este aspecto, con objeto de que el servicio prestado en estos Centros fuese como si de otro hospital de la Comunidad se tratara, ha sido necesario el análisis y emisión de directrices para que las comunicaciones y el acceso a las aplicaciones corporativas fueran seguras. Además, a los nuevos Centros se les habilitó del mismo sistema de monitorización que ya disponen el resto de hospitales de gestión directa, permitiendo que el SOC 24x7 del SERMAS fuera capaz de detectar posibles incidentes de seguridad.

En esta línea, desde la DGSIES, se ha intentado intensificar la monitorización de los Data Center centrales mediante el despliegue de nuevas sondas que monitorizan el tráfico de los mismos.

Por otro lado, la OSSI ha trabajado, en perfecta coordinación con Madrid Digital, en el desarrollo de un nuevo protocolo de actuación frente a una alerta de seguridad, en aras de mejorar los tiempos de respuesta y la eficacia ante posibles incidentes.

NUEVAS LÍNEAS ESTRATÉGICAS PARA LA MEJORA DE LA SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN DE LA CSCM

El mundo de la seguridad de los Sistemas de Información se encuentra en un entorno VUCA (volátil, incierto, complejo y ambiguo según sus siglas en inglés). Esto obliga al CISO de la Consejería a plantear a la Dirección nuevas estrategias para su mejora. De esta manera, la DGSIES ha establecido una serie de líneas estratégicas a medio plazo que permitirán minimizar los riesgos a los que están expuestos los Sistemas de Información de la CSCM:

- La certificación en el Esquema Nacional de Seguridad (ENS) de los hospitales del SERMAS, así como de sus *Data Center* Centrales. Es importante señalar que la CSCM cuenta actualmente con los dos únicos hospitales públicos certificados en el ENS.
- Creación de un nuevo rol de seguridad: Delegados del CISO en cada uno de los hospitales del SERMAS. La finalidad es establecer una conexión directa con el CISO de la CSCM y minimizar el tiempo de respuesta ante cualquier situación que pueda surgir en cuanto a seguridad.
- Actualización de la Política de Seguridad de la CSCM, con la finalidad de poseer un paraguas que determine las directrices centralizadas de seguridad a todos los Centros Sanitarios y departamentos de la Consejería.
- Potenciación del Comité de Seguridad de la CSCM, fortaleciendo la coordinación en seguridad de la Consejería.

Informe XIV Reunión del CTSIS

LUGAR: HOSPITAL CLÍNICO DE SANTIAGO DE COMPOSTELA
FECHA: DEL 4 Y 5 DE FEBRERO DE 2020

LOS SISTEMAS PÚBLICOS DE SALUD TIENEN ANTE SÍ EL FORMIDABLE RETO DE RESPONDER A CUANTO PLANTEAN LA CIBERSEGURIDAD, LA PROTECCIÓN DE DATOS PERSONALES Y EL GOBIERNO DE LA INFORMACIÓN EN UNOS TIEMPOS MARCADOS POR UNA TODAVÍA INCOMPLETA TRANSFORMACIÓN DIGITAL Y LAS DIFICULTADES PRESUPUESTARIAS. LA COLABORACIÓN ENTRE LAS ENTIDADES QUE COMPARTEN LOS MISMOS RIESGOS Y CON AQUELLAS OTRAS QUE PUDIERAN APORTAR SOLUCIONES ES TANTO UNA NECESIDAD COMO UN DEBER.

Para que esa colaboración sea efectiva es necesario disponer de la oportunidad de intercambiar experiencias y soluciones. En este sentido, el Comité Técnico de Seguridad de la Información Sanitaria (CTSIS) de la SEIS viene siendo, desde hace ya siete años, el único foro que reúne a los responsables de esas materias en los servicios públicos de salud y donde pueden tratar abiertamente todos esos asuntos.

La comunicación entre los miembros del CTSIS es permanente e inmediata, sea por teléfono, correo o mensajería electrónica. Además, el grupo dispone de una plataforma colaborativa, celebra videoconferencias cuando la ocasión lo demanda y se reúne presencialmente dos veces al año coincidiendo con la celebración del Foro de Seguridad y Protección de Datos de Salud y el Foro para la Gobernanza de las TIC en salud, ambos organizados por la SEIS.

La última reunión del CTSIS tuvo lugar los días 4 y 5 de febrero en el salón de actos 2 del Hospital Clínico de Santiago. La convocatoria anticipaba los siguientes asuntos:

- Marco autonómico para estudios de investigación (incluidos ensayos clínicos). Galicia.
- *Cyber Europe 2020: Health Sector.* Departamento de Seguridad Nacional.
- Proyecto de implantación de un centro de operaciones de seguridad (SOC) con Gloria. Baleares.
- Cumplimiento del deber de información en los hospitales.
- Procedimientos para informar sobre pacientes ingresados.
- Contratos de ensayos clínicos y presiones de los laboratorios.
- Convenio de colaboración entre la SEIS y el Ministerio de Sanidad
- Colaboración con la AEPD y estado de las iniciativas de la AEPD relativas al sector salud
- Consentimiento e investigación con datos pseudonimizados
- La situación actual de los Delegados de Protección de Datos de los Servicios Públicos de Salud.
- La organización de las funciones de ciberseguridad y seguridad de la información en cada CCAA.
- Las funciones de control del cumplimiento normativo y auditoría interna.
- La realización de los análisis de riesgos y las evaluaciones de impacto en la protección de datos.
- La gestión de los tratamientos de información (inventario de tratamientos y el registro de actividades de tratamiento)
- La atribución de responsabilidades sobre cada tratamiento.
- La formación especializada para DPDs y RSE
- La exigencia de certificaciones de cumplimiento del ENS y otras en las contrataciones del sector

Los tres primeros puntos fueron objeto de sendas

presentaciones que ocuparon prácticamente todo el tiempo disponible sirviendo de hilo conductor para comentar buena parte de los demás asuntos. Otros, como la puesta al día de los datos sobre la organización de la seguridad y la protección de datos en los distintos servicios públicos de salud se trataron de manera informal a lo largo de esas jornadas.

MARCO REGULADOR DEL ACCESO A DATOS DE SALUD CON FINES DE INVESTIGACIÓN EN GALICIA

En esta primera presentación Jorge Prado expuso el marco general para el control de la actividad investigadora en el sistema público de salud de Galicia. Esta iniciativa tiene como uno de sus principales exponentes el reconocimiento de una serie de obligaciones para el personal asistencial en funciones de investigador principal. Este reconocimiento se explicita asignándole el papel de encargado de los tratamientos que emprenda con finalidad investigadora, al tiempo que el órgano autonómico mantiene la responsabilidad última sobre dichos tratamientos y sobre los datos de salud en general. El ejercicio de esta responsabilidad sobre la actividad investigadora la ejerce el órgano autonómico fijando las condiciones para esos tratamientos, estableciendo un circuito de autorización y manteniendo un registro centralizado de los mismos. Entre las condiciones para llevar acabo esos tratamientos están todas las que exige la normativa legal aplicable, además de otras de carácter interno que resultan del ejercicio de la capacidad autoorganizativa de la Administración. Así, el consentimiento y el informe de un comité de ética de la investigación generalmente serán condiciones necesarias, aunque no suficientes.

Una segunda característica importante de este marco regulador es que los consentimientos informados de los pacientes se recaban en soporte electrónico y se mantienen igualmente en un registro centralizado. Galicia dispone de normativa autonómica que reconoce la validez de determinados sistemas de firma múltiple que combinan una firma manuscrita sobre soporte electrónico con firmas y sellos realizados con certificados electrónicos. El resultado ofrece mayor usabilidad y garantías a los pacientes al tiempo que descarga de tareas administrativas a los investigadores.

Otro aspecto destacable se refiere a las evaluaciones de impacto en la protección de datos. Antes de iniciar la mayor parte de esos tratamientos resulta preceptiva la realización de dichas evaluaciones para determinar la viabilidad y, en caso favorable, las medidas de control que será necesario aplicar. En esta tesitura los investigadores pueden tomar como punto de partida alguna de las evaluaciones tipo preparadas por el órgano autonómico y recurrir a sus servicios.

Por último, otra ventaja para los investigadores tiene que ver con el proceso de pseudonimización de los datos. El órgano autonómico ofrece este servicio especializado a los investigadores, con lo que se consigue la separación técnica y funcional entre los investigadores y quienes realizan la disociación, tal como exige la LOPDGDD.

CYBER EUROPE 2020: HEALTH SECTOR. DEPARTAMENTO DE SEGURIDAD NACIONAL

En la segunda presentación Andrés Ruiz comenzó dibujando el panorama de la ciberseguridad en España poniendo el foco en los prestadores de servicios esenciales de carácter asistencial y del sector sanitario. A continuación pasó a informar sobre los ejercicios de ciberseguridad que promueve el organismo europeo encargado de la seguridad de la información y de las redes de comunicación (ENISA) a escala europea y en particular del ejercicio *Cyber Europe 2020*. En este caso se pondrán a prueba las capacidades de respuesta europeas, nacionales y locales ante ciberincidentes que afecten a proveedores de servicios del sector sanitario. El ejercicio está diseñado y dirigido por ENISA, cuenta con la participación del Departamento de Seguridad Nacional (DSN) y de las entidades del sector público que intervienen en este tipo de incidentes, como son los CERT y CSIRT regionales. La participación es voluntaria y desde el Desde el DSN animan a que lo hagan las entidades del sistema nacional de salud.

PROYECTO DE IMPLANTACIÓN DE UN CENTRO DE OPERACIONES DE SEGURIDAD (SOC) CON GLORIA. BALEARES

La tercera presentación tuvo un carácter marcadamente técnico. Miguel Ángel Benito expuso las principales características, aciertos y errores del



proyecto de dotación de un centro de operaciones de seguridad (SOC) para el ibSalut. Un aspecto destacado de este proyecto ha sido el despliegue de la herramienta Gloria, del CCN, como herramienta para la correlación de eventos (SIEM), en lugar del producto comercial que venían utilizando hasta ese momento.

La contratación de este tipo de servicios no es tarea fácil. En esta ocasión se ha añadido una cláusula en la que las rebajas con respecto al importe de licitación deberán hacerse aumentando las prestaciones (bolsa de horas). [NOTA: no todos los interventores aceptan este criterio]

Conocer de primera mano la situación y puntos de vista de otras comunidades autónomas resultó tan provechoso como de costumbre, incluso cuando ese conocimiento no resuelva directamente los problemas de cada una. Precisamente buscando una mayor eficacia, desde la coordinación del CTSIS se propuso adoptar una nueva dinámica consistente en elegir algunos problemas suficientemente maduros como para que el CTSIS pueda proponer alguna actuación concreta que facilite su solución. Estas propuestas pueden tener forma de recomendaciones dirigidas directamente a la SEIS, o a través de ella a otras asociaciones de profesionales, a las autoridades de control (agencias de protección de datos, CNPIC…) o a las distintas autoridades sanitarias. Para cada asunto se nombrará un ponente, que se encargará de buscar refuerzos dentro del grupo para redactar la ponencia, que se discutirá y someterá a votación, preferentemente por medios telemáticos. Desde la coordinación del grupo se dará curso a las ponencias aprobadas.

Los primeros problemas a ser tratados de esta manera serán los siguientes:

1. Necesidad de regular la historia clínica electrónica. La normativa vigente no contempla este tipo de soportes ni el uso de la tecnología.
2. Actualizar la recopilación de modelos organizativos adoptados en las comunidades autónomas en respuesta a las exigencias normativas en materias de seguridad y protección de datos.
3. Compartir el conocimiento sobre los proyectos que se presentan a las instituciones sanitarias en los que, de manera más o menos encubierta, las entidades proponentes pretenden conseguir el acceso a datos asistenciales para finalidades propias. Estos proyectos generalmente son inaceptables para cualquier entidad del sistema nacional de salud en los términos en que se proponen.

El desarrollo y la discusión de estos asuntos por parte del grupo continúa por vías telemáticas.

Adecuación al RGPD y a la LOPDGDD en las Gerencias Asistenciales del Servicio de Salud de las Illes Balears

Miguel Ángel Benito Tovar1; Jesús Úbeda Colom2; Aurora Ripoll Clar3
1. Jefe de Servicio de Protección de Datos en el Servicio de Salud de las Illes Balears
2.Técnico de Gestión de Tecnologías de la Información en el Servicio de Salud de las Illes Balears
3. Senior Security Consultant en EY

PALABRAS CLAVE
Análisis GAP, inventario de actividades de tratamiento, entrevistas, plan de acción, grado de cumplimiento, interesados.

INTRODUCCIÓN

Uno de los principales objetivos del Servicio de Seguridad de la Información de la Subdirección de Tecnología de Información del Servicio de Salud de las Illes Balears, en lo sucesivo Ib-Salut es velar, por el cumplimiento de la normativa vigente de protección de datos. Por ello ha sido el área encargada de liderar y coordinar la adecuación de los órganos del IB-Salut a las exigencias establecidas por el RGPD[1] y la LOPDGDD[2].

ALCANCE Y DESCRIPCIÓN DEL PROYECTO

La adecuación al RGPD y a la LOPDGDD en el Ib-Salut es un proyecto que empezó en el año 2017 en las ocho Gerencias asistenciales que lo componen y se ha estructurado en dos grandes fases diferenciadas, cada una de ellas basada a su vez en la metodología de mejora continua establecida por el *Círculo de Deming* o ciclo PDCA.

Fase I o fase de "adecuación organizativa"

En esta primera fase de adecuación se han englobado el conjunto de actividades necesarias para la consecución de aquellas medidas organizativas precisas para dar cumplimiento a las exigencias formales del RGPD y la LOPDGDD. Para ello, desde el Servicio de Seguridad de la información ha realizado:

1. *El análisis de la normativa* de aplicación y extracción de los requisitos exigidos para su cumplimiento.
2. *La identificación de los servicios y/o áreas* de las Gerencias asistenciales involucradas en el tratamiento de datos personales.
3. La realización de las *entrevistas*, o sesiones, de entendimiento sobre el tratamiento de datos realizado, con los interlocutores de las áreas o servicio identificados.
4. El análisis de la información y elaboración del *inventario de tratamientos*.
5. La comparación entre el estado actual de cumplimiento de cada Gerencia y los requisitos necesarios para cumplir con las exigencias del RGPD y LOPDGDD *(análisis GAP de cumplimiento)*. Este análisis diferencial se ha basado en la evaluación de doce grandes dominios:

- Principios básicos de tratamiento: evaluación, por tratamiento de datos, del respeto a los prin-

Tarea	Dominio	Responsable	Prioridad	Esfuerzo	Fecha límite
Implantar los clausulados estandarizados de solicitud de consentimiento	Consentimiento	Gerencia		2 jornadas	abr-20
Implantar los clausulados informativos de tratamiento de datos	Derechos de los interesados	Gerencia/OS		5 jornadas	abr-20
Cumplir con el Protocolo de Gestión de Incidencias de Seguridad	Notificación de incidencias de privacidad	Gerencia		2 jornadas	abr-20
Revisión y aprobación del registro de actividades de tratamiento	Registro de actividades de tratamiento	Gerencia		2 jornadas	abr-20
Publicación del registro de actividades de tratamiento en la sede electrónica de Gerencia	Registro de actividades de tratamiento	Gerencia		1 jornada	abr-20
Añadir al DPO en el inicio y workflow de nuevos proyectos/servicios	Responsabilidad del responsable de tratamiento	Gerencia		1 jornada	abr-20
Cumplir con el Protocolo de Transferencias Internacionales de Datos	Transferencias internacionales de datos	Gerencia		2 jornadas	may-20
Establecer mecanismos ágiles para el correcto cumplimiento del Protocolo de Gestión de Derechos	Derechos de los interesados	Gerencia/OS		5 jornadas	may-20
Cumplir con la Política de Conservación de Datos	Principios básicos del tratamiento de datos	Gerencia		10 jornadas	may-20
Implantar los modelos de cláusulas, contratos de Encargado de tratamiento, pliegos y convenios estandarizados	Responsabilidad del responsable de tratamiento	Gerencia/OS		1 jornada	may-20
Designar un responsable para cada uno de los tratamiento identificados en el registro de actividades de tratamiento	Registro de actividades de tratamiento	Gerencia		2 jornadas	may-20

Figura 1: Ejemplo no real de plan de acción derivado de la fase I de adecuación

cipios básicos establecidos por el RGPD y la LOPDGDD.

- Licitud de tratamiento: evaluación del tratamiento lícito de datos personales por actividad identificada.
- Consentimiento: en los supuestos en los que el tratamiento se base en el consentimiento del interesado, evaluación del cumplimiento de los requisitos establecidos por el RGPD y la LOPDGDD para dicha circunstancia legitimadora.
- Derechos de los interesados: evaluación del cumplimiento del deber informar al interesado de forma clara, concisa, transparente e inteligible y valoración de la existencia de un procedimiento completo que posibilite al responsable la debida gestión de las solicitudes de los interesados en relación con el ejercicio de sus derechos.
- Responsabilidad del responsable de tratamiento: análisis del estado de adecuación del responsable del tratamiento a los requisitos establecidos en los artículos 24, 25 y 28 del RGPD (revisión recurrente de las medidas técnicas y organizativas, adhesión a códigos de conducta, valoración inicial de riesgos, privacidad desde el diseño y por defecto, etc.).
- Registro de actividades de tratamiento: evaluación del estado del registro de actividades de tratamiento del responsable (existencia y contenido mínimo del mismo).
- Seguridad del tratamiento de datos personales: análisis del estado de las medidas de seguridad, técnicas y organizativas, aplicadas por el responsable de tratamiento (haciendo convergencia entre las referenciadas en el artículo 32 del RGPD y las definidas en el Anexo II del Esquema Nacional de Seguridad).
- Notificación de incidencias de privacidad: valoración de la existencia de procedimientos escritos para la gestión de violaciones de seguridad que constituyan un riesgo para la privacidad de los interesados de conformidad con los requisitos de forma y plazos establecidos en el RGPD,
- Evaluaciones de Impacto en la Privacidad: revisión de la existencia de protocolos que permitan identificar la necesidad de realizar evaluaciones de impacto en la privacidad ("EIPD") y de mecanismos, procedimientos o herramientas que permitan realizar dichas evaluaciones en el caso de que sea necesario.
- Consulta previa: evaluación de la existencia de un procedimiento interno de consulta previa a la AEPD en aquellos casos que la EIPD muestre que el tratamiento a efectuar conllevaría un alto riesgo para los derechos y libertades del interesado.
- Delegado de protección de datos: evaluar la designación de un DPD dentro del Ibsalut y su posición dentro de la organización de tal manera que se garantice la independencia en el ejercicio de sus funciones.
- Transferencias internacionales de datos: evaluar, por tratamiento de datos personales en el que se

> ***Toda la información derivada del análisis realizado en esta primera fase ha quedado definida en un Marco de Control único, que permite tener una visión global y centralizada del estado de cumplimiento del RGPD y la LOPDGDD del responsable de tratamiento.***

realicen transferencias internacionales de datos, si se han tenido en cuenta las consideraciones establecidas por el RGPD.

6. En función del análisis realizados, identificación de aquellos aspectos que requerirán de iniciativas de adaptación y propuesta de un plan de acción para conseguir un grado de cumplimiento objetivo a medio y largo plazo (figura 1).

Toda la información derivada del análisis realizado en esta primera fase ha quedado definida en un Marco de Control único, que permite tener una visión global y centralizada del estado de cumplimiento del RGPD y la LOPDGDD del responsable de tratamiento.

El desarrollo con éxito de esta primera ha sido garantizado gracias a la colaboración directa de los Responsables de Seguridad y al apoyo y soporte recibido por parte de los Comités de Seguridad de la Información de cada una de las gerencias asistenciales.

Fase II o fase de "adecuación operativa"

Esta segunda fase de adecuación comprende el conjunto de aquellas actividades operativas y de tratamiento del riesgo, exigidas por el RGPD y la LOPDGDD, de entre las cuales cabe destacar:

1. Realización de las evaluaciones de impacto en la privacidad en nuevos tratamientos de datos personales.
2. Realización recurrente de los Análisis de Riesgos sobre los tratamientos de datos.

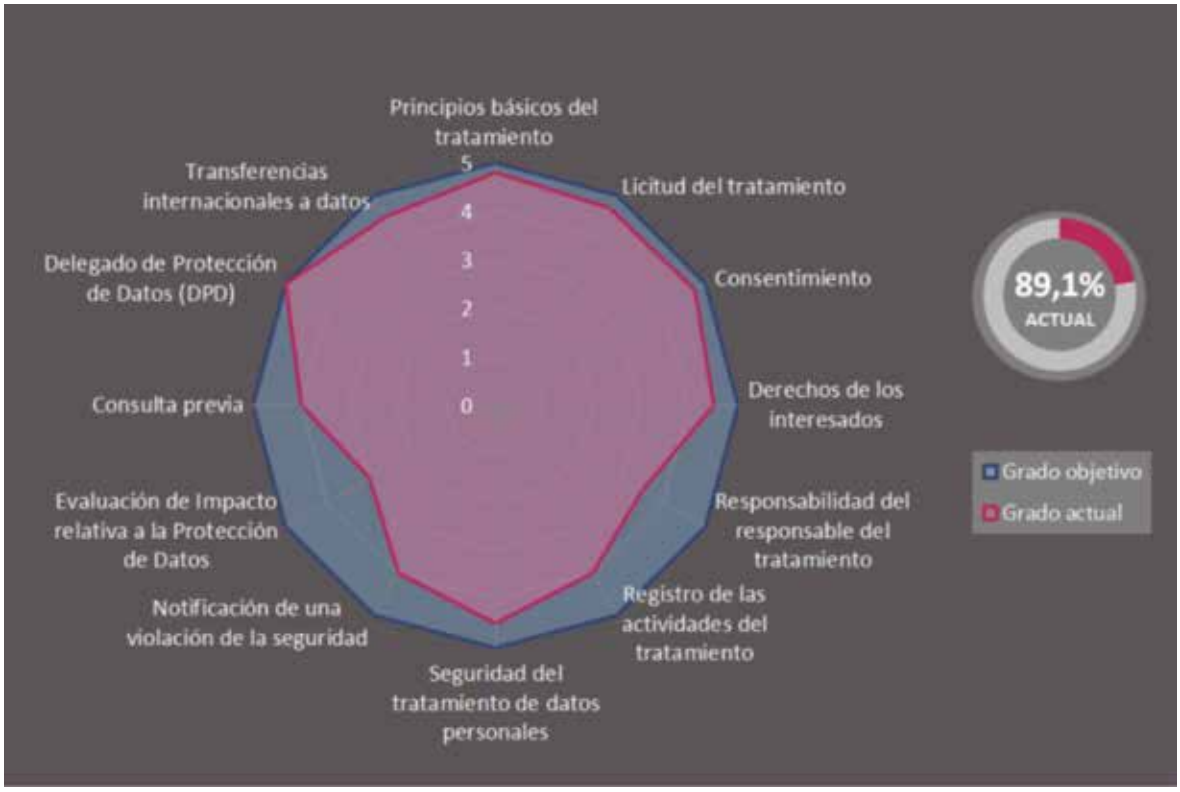


Figura 2: Estado de cumplimiento actual (89,1% frente estado de cumplimiento objetivo (100%)

3. Revisión del estado de implantación de las actividades identificadas en la fase I.

RESULTADOS

Actualmente, la fase I de adecuación al RGPD y la LOPDGDD se encuentra en periodo de cierre, y como resultado de la misma:

- Se han llevado a cabo un total de 166 entrevistas entre todas las gerencias asistenciales de Ib-Salut en las cuales se han entrevistado a más de 200 personas.
- Se han registrado un total de ocho inventarios de actividades de tratamiento, uno por gerencia asistencial o responsable de tratamiento.
- Se han realizado ocho análisis diferenciales de adecuación, uno por gerencia asistencial o responsable de tratamiento.
- Se han elaborado ocho los planes de acción adaptados al grado de cumplimiento de cada gerencia asistencial o responsable de tratamiento.

Las actividades propuestas en cada plan de acción han quedado diferencias por grado de cumplimiento objetivo

Entre las medidas a corto plazo detectadas, /cabe destacar:

- Implantación de clausulados estandarizados de solicitud de consentimiento.
- Publicación del registro de actividades de tratamiento en la sede electrónica en aquellas gerencias que no lo tuvieran.
- Implantar los modelos de cláusulas, contratos de Encargado de tratamiento, pliegos y convenios estandarizados.
- Añadir al DPD en el inicio y *workflow* de nuevos proyectos/servicios.
- Establecer mecanismos ágiles para el correcto cumplimiento del Protocolo de Gestión de Derechos.
- Para permitir la gestión centralizada de las operaciones de tratamiento realizadas por cada una de las gerencias asistenciales, se volcado toda la información derivada del proyecto de adecuación a la herramienta ASSI-RGPD [3]
- Se ha elaborado un marco normativo consolidado en materia de privacidad y protección de datos, que incluye procedimientos tales como: procedimiento de gestión de derechos de los interesados, procedimiento de gestión de incidencias de privacidad, protocolo de transferencias internacionales de datos, protocolo de privacidad desde el diseño y por defecto, etc.
- Se han presentado los principales hallazgos en los respectivos Comités de Seguridad de las Gerencias Territoriales

PRÓXIMOS PASOS

A partir del desarrollo de la fase I, la cual nos ha permitido conocer la situación inicial de cada una de las gerencias asistenciales e implementar algunas de las medidas necesarias para el cumplimiento de la normativa vigente, el desarrollo de la fase II servirá como herramienta para acompañar a las gerencias asistenciales en la implementación de la totalidad de iniciativas de mejora identificadas en la fase I.

REFERENCIAS

[1] REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). https://www.boe.es/doue/2016/119/L00001-00088.pdf

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

[3] ASSI-RGPD (Auditoría de Seguridad de los Sistemas de Información – Reglamento General de Protección de Datos) es una aplicación desarrollada por el Ministerio de Trabajo, Migraciones y Seguridad Social que permite a la organización mantener un registro de actividades de tratamiento de datos personales así como facilitar el cumplimiento de las obligaciones del RGPD y la LOPDGDD, incluyendo, parcialmente, la realización de análisis de riesgos y evaluaciones de impacto de las operaciones de tratamiento en la protección de datos personales. https://administracionelectronica.gob.es/ctt/assir-gpd#.XmtMWMTOHb0.

Retos para Implantación de los Servicios de Ciberseguridad

Manuel Jimber del Río
Responsable Unidad Seguridad TIC
Servicio Andaluz de Salud

LA UNIDAD DE SEGURIDAD TIC DEL SERVICIO ANDALUZ DE SALUD (USTIC) NACE COMO CONSECUENCIA DE LA MATERIALIZACIÓN DEL DECRETO 1/2011 DE POLÍTICA DE SEGURIDAD DE LA JUNTA DE ANDALUCÍA Y EL DECRETO 70-2017, QUE MODIFICA ESTA POLÍTICA ESTABLECIENDO LA ORGANIZACIÓN DE LA SEGURIDAD TIC PARA TODAS NUESTRAS CONSEJERÍAS Y EQUIPARANDO, EN LO QUE SE REFIERE A SEGURIDAD DE LA INFORMACIÓN, AL SERVICIO ANDALUZ DE SALUD Y AL INSTITUTO ANDALUZ DE EMPLEO A UNA CONSEJERÍA MÁS. COMENZAMOS A TRABAJAR EN JULIO DE 2019, ASÍ QUE, COMO UNIDAD, PODEMOS DECIR QUE ESTAMOS TODAVÍA EN CONSTRUCCIÓN.

Sin embargo, a pesar de contar una vida muy corta, sí que nos ponemos a trabajar rápidamente en la puesta en marcha de los procesos necesarios para emprender el camino hacia una prestación de los servicios sanitarios seguros.

Se establecen unos mínimos recursos distribuidos por las 8 provincias andaluzas, responsables de seguridad provinciales, que actúan como asesores tanto en materia de privacidad como de cumplimiento legal respecto del Esquema Nacional de Seguridad (ENS) en su ámbito territorial.

Se inicia un proyecto para la implantación de ISO 27001 como metodología de trabajo de la USTIC y otro para llevar a cabo el análisis de situación de nuestros sistemas de información respecto del cumplimiento del ENS, con el objetivo de comenzar cuanto antes los proyectos necesarios para la certificación de estos.

De forma paralela, comenzamos a trabajar en los procesos de identificación y gestión de incidentes con la intención de poner en marcha un Centro de Operaciones de Ciberseguridad al igual que ya han hecho otras comunidades, o que están ya en ello.

Ya disponemos de los resultados de estos primeros análisis y estamos en disposición de conocer cuál será el camino que tendremos que recorrer, tanto humano como económico que tendremos que desplegar y de cuáles son los restos a los que tendremos que enfrentarnos.

Algunos más o menos ya conocidos de antemano. Cuestiones como la concienciación en materia de ciberseguridad de más de 100.000 profesionales, la gestión de incidentes de una organización con 90.000 puestos de trabajo o los aspectos de continuidad de negocio, actualización y parcheado de miles de servidores.... Pero otros, aunque también probablemente intuidos, presentan a nuestro entender mayores dificultados para su abordaje.

La generación de una conciencia en la organización sobre los riesgos a los que está expuesta.

Esta falta de esta conciencia dificulta enormemente el compromiso de la alta dirección con la seguridad de la información, y, por tanto, dificultaría a su vez, la elaboración de las políticas y normas imprescindibles para que las prácticas seguras establecidas se cumplan y se lleven a cabo. Pretendemos abordar este reto adoptando un enfoque desde la seguridad del paciente.

El verano de 2019 el Servicio Andaluz de Salud publicó su estrategia para la seguridad del paciente, en la que además de las líneas estratégicas tradicionales desde una perspectiva clínica, se ha incluido como novedad una línea estratégica de seguridad del paciente en relación con las tecnologías de la información sanitarias. Desde esta línea de trabajo

se incluye la visión del daño a la salud del paciente que podría ocasionar un mal diseño, mala implantación o mal funcionamiento de las tecnologías de la información sanitaria. Esta visión nace desde la consideración de que las Tecnologías de la Información Sanitarias tienen capacidad para ocasionar un daño al paciente en su salud. Un abordaje de la ciberseguridad desde esta perspectiva, alineados con la estrategia de seguridad del paciente del SSPA, nos ayudará a provocar el cambio en la visión de la ciberseguridad como un aspecto puramente tecnológico, hacia una visión en la que el paciente es el objetivo a proteger. Incorporar la perspectiva de la Seguridad del paciente a la seguridad de la información será clave en este sentido.

Tenemos claro que la ciberseguridad puede afectar a la prestación de los servicios sanitarios, pero también que está directamente relacionada con el paciente, razón de ser de los sistemas sanitarios. No se trata sólo de cómo se ve afectada la disponibilidad de los servicios sanitarios que prestamos, es que hay servicios, que, si caen, y en las circunstancias adecuadas, pueden conllevar complicaciones de salud para los pacientes. Por ejemplo, una caída en los servicios de emergencias puede suponer retrasos en el envío de las ambulancias a una emergencia, donde el tiempo puede ser un factor vital. O un retraso en la entrega de unos resultados analíticos o un informe radiológico en un servicio de urgencias, que puede suponer que un profesional sanitario tenga que tomar decisiones vitales sin contar con la información necesaria para ello.

Por otro lado, un ataque que afectara a la integridad de la información podría ser aún peor. Podría significar que un médico está tomando decisiones respecto de técnicas o tratamientos con información parcial o incluso falsa. Esta información podría tanto curar "milagrosamente a un paciente" como hacer que le aparezca una enfermedad que en realidad no padece,llevando a un paciente a un quirófano para ser operado de una enfermedad que no padece en realidad. Por no hablar de cambios en la dosis de medicamentos, que los harían, o bien inútiles, o por el contrario provocar una sobredosis, que, dependiendo del medicamento y del paciente y su patología, podría llevarle a la muerte. Podríamos poner algunos ejemplos reales de este tipo.

Otro reto será la implantación de las metodologías de mejora continua y el cumplimiento legal. Debido a nuestro tamaño el esfuerzo para la certificación de los sistemas de información al ENS va a ser enorme. La Junta de Andalucía puso como objetivo en 2019 que todas las consejerías contaran con las estructuras organizativas para la seguridad de la información decretadas, las políticas y como último hito, la certificación de todos los sistemas de información de categorías BÁSICA, MEDIA Y ALTA, certificados en el ENS para junio de 2020. Es evidente que no vamos a conseguir estos hitos en las fechas planificadas. Sin embargo, si que disponemos ya de la hoja de ruta para alcanzarlos.

Será también un gran reto hacer de la ciberseguridad una cosa todos. Se adquieren y contratan productos y servicios que incluyen tecnologías de la información y que necesitan de las infraestructuras de comunicaciones, sin embargo, en los procesos de planificación, adquisición y gestión o mantenimiento no se tienen en cuenta los aspectos tecnológicos y de seguridad. En ocasiones no hay participación de los equipos TIC, y menos aún de los equipos de seguridad de la información, de manera que no se incluyen condiciones técnicas y de seguridad en los contratos. Será necesaria la implicación de los órganos decisores en las compras en el conocimiento de los riesgos de seguridad y de los profesionales TIC en los procesos de adquisición. En febrero de 2020 ENISA ha publicado *"Procurement Guidelines for Cybersecurity in Hospitals. Good practices for the security of Healthcare services. February 2020"*, estableciendo buenas prácticas en los procesos de adquisición de productos y servicios tecnológicos más seguros.

Por otro lado, y en relación con lo anterior, será fundamental la colaboración de los profesionales de ingeniería y electromedicina. Disponemos de decenas de miles de dispositivos electromédicos conectados a nuestras redes que no disponen de medidas de seguridad, no pueden ser parcheados ni actualizados, cuentan con sistemas operativos fuera de soporte, y que por tanto constituyen agujeros de seguridad difíciles de abordar. Los riesgos de seguridad deben ser también conocidos por estos colectivos profesionales, que tienen las competencias sobre este tipo de dispositivos. No olvidemos que, una vez más, un fallo en estos, afectará a la seguridad del paciente, un aspecto fundamental del trabajo de estos colectivos profesionales.

SOC del Servicio de Salud de las Illes Balears

Miguel Ángel Benito Tovar
Jefe de Servicio de Protección de Datos del Servicio de Salud de las Illes Balears

PALABRAS CLAVES
CiberSeguridad, SOC, Esquema Nacional de Seguridad, seguridad de la información, amenazas, incidentes

ANTECEDENTES

Ante el continuo aumento de amenazas, ataques e incidentes en materia de seguridad de la información y protección de datos en el sector de la salud, así como ante las obligaciones legales existentes relativas a la necesidad de disponer se servicios monitorización continua y la obligación de la comunicación de los incidentes de seguridad, se hace necesario que las organismos públicos, y especialmente en aquellos que tratan datos especialmente protegidos como son las organizaciones sanitarias, cuenten con sistemas de identificación, detección y respuesta ante potenciales incidentes.

Es por lo anterior, que el Servicio de Salud de las Illes Balears, en lo sucesivo Ib-Salut, en su compromiso continuo de garantizar la seguridad y confidencialidad de los datos de sus pacientes, durante los últimos cuatro años ha llevado a cabo distintas iniciativas encaminadas a dotar al organismo de nuevas infraestructuras y capacidades que permitan dar respuesta a los retos que se le presentan cada día en materia de ciberseguridad.

Entre las principales iniciativas llevadas a cabo en materia de ciberseguridad desde el 2016 por el Ib-Salut es necesario destacar las relativas a:

- La creación de un nuevo servicio de Ciberseguridad dentro del área de Seguridad de la In-

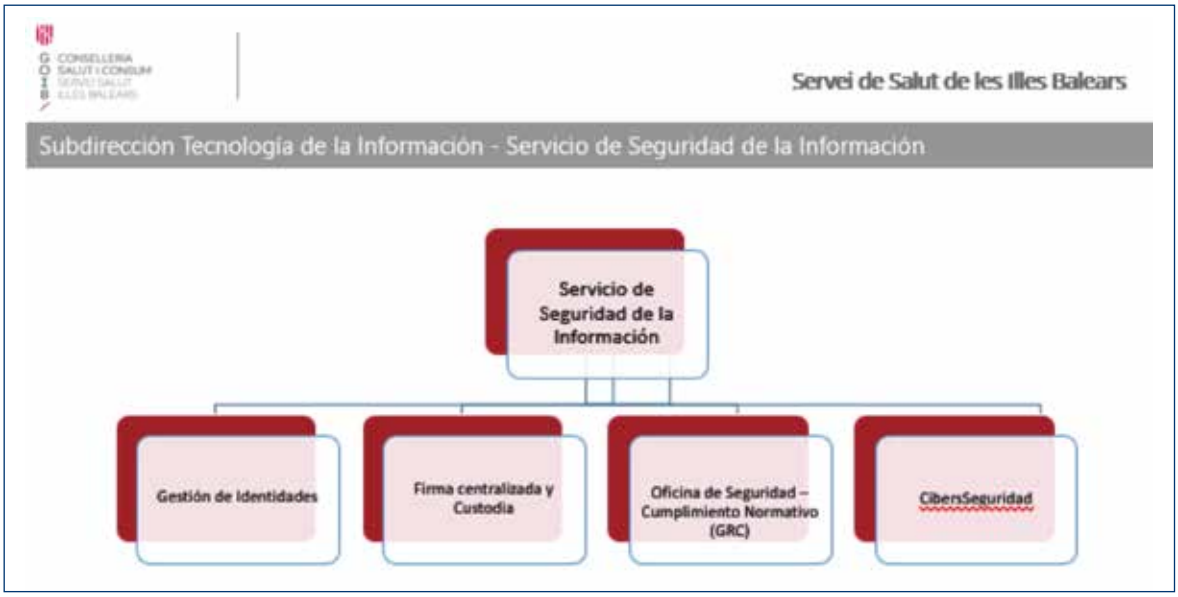


Figura 1. Estructura servicio de seguridad de la información

formación dependiente de la Subdirección de Tecnología de la Información, en adelante STI, el cual ha venido a cumplimentar a los servicios ya existentes de Gestión de Identidades, Gobierno Riesgo y Cumplimiento así como el de Firma y Custodia Electrónica

- La ampliación del equipo de trabajo del área de Seguridad de la Información
- La instalación de nuevos *firewalls* en todos los centros y homogenización del nivel de *logs* de los mismos
- El despliegue de nuevas soluciones de protección de equipos y servidores
- La realización de auditorías continuadas de identificación de sistemas y vulnerabilidades
- La implantación de un SIEM en el cual se integraron los principales sistemas de actividad asistencial, los sistemas de seguridad perimetral así como los sistemas de protección de puestos de trabajo y servidores (figura 1).

Fruto de todas las iniciativas anteriormente mencionadas, el pasado mes de julio el Ib-Salut puso en marcha la primera piedra de su SOC (*Security Operations Center*) corporativo, en lo sucesivo SOC v1, el cual viene a cumplir con los objetivos de la Subdirección de Tecnología de la Información de:

- Incrementar la capacidad de vigilancia y detección de amenazas en las actividades diarias de los sistemas de información y comunicaciones de todos los centros del Ib-Salut
- Dotar al Organismo de sondas y herramientas centralizadas para la gestión de eventos y logs de seguridad
- Analizar los ataques o posibles amenazas a los que se enfrenta a diario el Organismo
- Mejorar la capacidad de respuesta ante cualquier incidente
- Disponer de mecanismos y procedimientos para la respuesta coordinada ante incidentes
- Cumplir con la legislación vigente y especialmente con el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad, el Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información así como la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales,

DESPLIEGUE DE LA INFRAESTRUCTURA DEL SOC

Para poner en marcha el SOC v1, el Ib-Salut ha contado con los servicios de la empresa S2 Grupo la cual ha sido la encargada en una primera fase de la instalación, parametrización y puesta en marcha de la solución GLORIA, el despliegue de 3 sondas HIDS y NIDS en los centros del Ib-Salut que cuentan con salida propia a Internet y la instalación de una sonda para la red de imagen médica en el hospital de referencia de las Illes Balears. Igualmente, dentro de la fase de la puesta en marcha, se ha llevado a cabo la integración de distintos orígenes de datos entre los que cabría destacar por supuesto los eventos de los sistemas de antivirus y *firewalls*.

Tal como se indicó anteriormente, el Ib-Salut para el despliegue de su SOC ha optado por desplegar la solución GLORIA la cual se trata de la plataforma para la gestión de incidentes y amenazas de ciberseguridad a través de técnicas de correlación compleja de eventos que el Centro Criptológico Nacional pone a disposición de todas las Administraciones Públicas dentro de de las suite de soluciones disponibles del CCN-CERT (Centro Criptológico Nacional *Computer Emergency Response Team*). Atendiendo a lo indicado en el portal del CCN-CERT, las principales funcionalidades de las solución GLORIA son:

- Monitorización de entornos tecnológicos (IT/OT) y recolección de eventos de seguridad
- Inteligencia mediante técnicas de correlación compleja de eventos que sirve de base para el desarrollo y parametrización de los mismos.
- Gestión del servicio a través de una consola única de gestión de alertas e incidentes que recoge todas las incidencias o alertas automáticas generadas por el sistema de correlación.
- Automatización, orquestación y reducción de tiempos de respuesta

Asimismo, es necesario destacar que en esta primera fase también se ha llevado a cabo la integración del despliegue de la solución GLORIA del

IB-Salut con la plataforma de gestión de incidentes LUCIA del CCN-CERT.

PUESTA EN MARCHA DEL SERVICIO DE PREVENCIÓN, RESPUESTA Y ALERTA TEMPRANA

Una vez superada la etapa de implantación y puesta en marcha de toda la infraestructura, el pasado mes de enero empezaron los servicios de operación de seguridad del SOC los cuales son prestados desde las instalaciones de S2 Grupo, bajo la monitorización del personal del servicio de seguridad del Ib-Salut, y los cuales consisten en la prestación de:

- Servicios de detección y respuesta:
  - Monitorización de eventos de seguridad mediante la plataforma GLORIA.
  - Correlación y análisis de eventos
  - Notificación de alertas
  - Coordinación de respuesta a incidentes
- Servicios de prevención de alerta temprana
  - Alerta temprana

PROCEDIMIENTOS DE GESTIÓN Y RESPUESTA ANTE INCIDENTES

Uno de los aspectos más importante a tener en cuenta para el correcto funcionamiento y eficiencia del SOC es el relativo al procedimiento de gestión y respuesta ante incidentes.

Para ello, el Ib-Salut ha puesto en marcha un circuito de atención y respuestas ante incidentes en el cual se han identificado 5 fases y en el que participan equipos multidisciplinares tanto externos como propios del Ib-Salut.

A modo ilustrativo, a través del siguiente gráfico se identifican las etapas y equipos involucrados en el procedimiento de gestión y respuesta ante incidentes (figura 2).

INDICADORES

Aunque el servicio de prevención, respuesta y alerta temprana comenzará a rodar el pasado mes de enero y aún sea pronto para dar indicadores contrastados, si se considera interesante dar una muestra cuantitativa de los primeros datos obtenidos en dos meses de funcionamiento del SOC v1.

Entre los datos que se consideran más relevantes caben destacar:

- Se han definido, calibrado y puesto en marcha más de 35 casos de uso/riesgo.
- En los dos meses de funcionamiento del servicio se han gestionado más de 105 millones de eventos con picos de más de 5.000 EPS (eventos por segundo.



Figura 2. Procedimientos de gestión y respuesta ante incidentes



Figura 3. Hoja de ruta del SOC corporativo

- Durante los meses de enero y febrero de 2020 se han generado y gestionado un total de 12.395 alertas de seguridad. De las cuales 28 se han considerado como posibles incidentes de seguridad y que por consiguiente se han escalado desde el SOC al IB-Salut para su investigación. Sobre este punto es necesario destacar la importancia de tener una correcta correlación e inteligencia de alertas en aras de filtrar falsos positivos que puedan llegar a saturar a los equipos de trabajo.

PRÓXIMOS PASOS

La mejora continua debe ser una máxima en la prestación de cualquier servicio de ciberseguridad y especialmente en los servicios de monitorización y alerta temprana. Es por ello que el Ib-Salut ha definido una hoja de ruta de mejoras divididas en acciones a corto, medio y largo plazo.

Dentro de las acciones a corto y medio plazo, las cuales se han iniciado desde febrero 2020 hasta julio del 2021 se enmarcan las actividades de:

- Formación casos de usos a CESIC (Centro de Explotación de Sistemas de Información Corporativo)
- Integración de eventos de seguridad incluidos actualmente en la solución *Logstash*
- Integración de GLORIA con las soluciones de correo
- Integración de GLORIA con la solución tenable.SC
- Mejora continua del servicio
- Aprender y medir

De las actividades mencionadas anteriormente, sin lugar a duda la actividad más importante es la correspondiente a aprender y medir la eficacia y eficiencia del SOC v1 pues a partir de esta actividad se sentarán las bases de lo que será el futuro SOC v2 y en el que sin duda tendrán cabida, entre otras, las iniciativas enumeradas a continuación:

- Ampliación horas de dedicación de SOC
- Despliegue de la solución CARMEN
- Despliegue de nuevas sondas IT/OT/DICOM
- Integración de nuevas fuentes

REFERENCIAS

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

[2] Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-1330

[3] Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información. https://www.boe.es/buscar/doc.php?id=BOE-A-2018-12257

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

[5] Solución GLORIA CCN-CERT. https://www.ccn-cert.cni.es/soluciones-seguridad/gloria.html

[6] Solución LUCIA CCN-CERT. https://www.ccn-cert.cni.es/gestion-de-incidentes/lucia.html

Ciberseguridad: Clave en el Sector Sanitario



Álvaro Fraile Hernández
Director del CoE (Centre of Excellence) de Ciberseguridad de Ibermática

ITS SECURITY, COMPAÑÍA ESPECIALIZADA EN CIBERSEGURIDAD PERTENECIENTE AL GRUPO IBERMÁTICA, DA LAS CLAVES PARA ELABORAR UNA ESTRATEGIA SÓLIDA DE CIBERSEGURIDAD, ESPECIALMENTE EN EL SECTOR SANITARIO.

La digitalización de la economía ha provocado que el riesgo cibernético se haya convertido en la principal preocupación de las empresas a nivel global. En España también, incluso desbancando por primera vez a la pérdida de beneficios como mayor inquietud histórica de las organizaciones. Así lo confirman estudios de entidades de la talla de Gartner, PwC o Allianz, entre otras.

Hoy ya no es realista preguntarse si nuestra compañía sufrirá o no un incidente de ciberseguridad. La pregunta es cuándo y cómo ocurrirá. La contundencia con que cualquier compañía enfrente este tipo de incidentes dependerá totalmente de hasta qué punto haya implantado las medidas de seguridad apropiadas.

Esta estrategia de ciberseguridad es especialmente sensible cuando hablamos de ciberataques dirigidos al sector salud, en el que se vulneran directamente los derechos de las personas enfermas.

VISIÓN DE LA CIBERSEGURIDAD 360º

Nuestra visión de la ciberseguridad está basada en un amplio *know-how* tecnológico y metodológico que tiene como base el conocimiento del negocio y de los procesos de nuestros clientes. Esto nos permite posicionar en el mercado servicios, productos y soluciones de ciberseguridad de gran especialización y orientados a sectores de actividad específicos.

Teniendo como objetivo la protección de la información y sistemas frente a ciberataques y amenazas, garantizando la continuidad de los procesos de la organización y asegurando el cumplimiento legal y normativo, nuestra oferta incluye servicios de ciberseguridad gestionada (SOC), ciberseguridad ofensiva para mejorar la ciber resiliencia, análisis forense y respuesta ante incidentes, así como formación y concienciación a usuarios, otro aspecto clave sin duda. Todo ello sin olvidar capacidades en torno a la evaluación del riesgo y cumplimento regulatorio y normativo alrededor de GDPR, ISO 27001, ENS, PCI DSS, LEY PIC y otros muchos. Esta visión 360º de la ciberseguridad es clave para garantizar una estrategia de defensa completa, que adaptamos a las características y necesidades de cada sector.

CIBERSEGURIDAD EN EL SECTOR SALUD

Los desafíos y retos de ciberseguridad a los que se enfrenta el sector salud son de enorme calado, dadas las implicaciones que un ciberataque podría tener en el paciente. ITS Security by Ibermática centra su oferta principal para el sector salud en torno a estos pilares: servicios de ciberseguridad gestionada (SOC), ciberinteligencia aplicada al sector sanitario, monitorización 24x7 y securización de dispositivos médicos IoT.

Dado que los cibercriminales están aprovechando la situación actual provocada por la epidemia del COVID-19 para lanzar ataques cuyo principal objetivo es el sanitario, se hace imprescindible contar

con el apoyo de servicios expertos de SOC, encargados de realizar un seguimiento y análisis de la actividad en redes, servidores, puntos finales, bases de datos, aplicaciones, sitios web y otros sistemas, buscando anomalías que puedan indicar un incidente o compromiso de seguridad.

Nuestro servicio de monitorización y alerta temprana para el sector salud consiste en una ciber-vigilancia que nos permite detectar amenazas dirigidas contra las entidades sanitarias, facilitando una respuesta ágil ante cualquier actividad sospechosa y la aplicación de medidas de contención y erradicación. Nuestro equipo de ciberinteligencia, UNIT71, recolecta los principales indicadores maliciosos de ciberamenazas (IOCs) para detectar infecciones antes de que se produzcan.

ROBOTS Y DISPOSITIVOS MÉDICOS: OBJETIVO DE CIBERATAQUES

Cada vez son más los robots que sustituyen a los humanos en sus puestos de trabajo. En el ámbito de la medicina, es muy frecuente acceder a diagnósticos médicos vía videoconferencia o encontrarnos a cirujanos asistidos por robots. La aplicación de estas tecnologías en el sector salud es una realidad que está ganando cada vez más terreno.

De la misma forma, la probabilidad de que estos robots puedan ser ciberatacados crece exponencialmente día a día.

Todo aparato conectado a una red, ya sea un PC, un electrodoméstico, un avión, un coche, o un robot médico, es susceptible de ser 'hackeado'. En el caso del sector sanitario, una vulnerabilidad en un dispositivo médico podría modificar la dosis a administrar a un paciente, poniendo en peligro su vida.

Los dispositivos de uso médico no son dispositivos de control tradicionales, como puede ser la máquina-herramienta, al no disponer de los PLC ni RTU habituales. Su tipología implica que no se puedan aplicar medidas de seguridad generales para todos ellos, sobre todo en lo referente a actualizaciones y parcheos, o ejecución de copias de seguridad, por ejemplo.

¿Cómo podemos protegerlos? El sector médico no puede ser tratado como un sistema de TI tradicional, ni tampoco responde al esquema de ciberseguridad de los entornos industriales OT. Sus peculiaridades hacen que se aproxime más a sistemas del Internet de las Cosas (IoT). Estos entornos deben incorporar soluciones de seguridad propias de los dispositivos de IoT. En ITS Security by Ibermática contamos con experiencia y soluciones específicas para garantizar la ciberseguridad en estos entornos, a través de:

- Monitorización del tráfico de red, así como de uso del dispositivos, a través de soluciones de monitorización, alerta y respuesta ante amenazas, como nuestra solución Nuklea360.
- Gestión de accesos. La gran parte de los robots médicos disponen de pantallas táctiles para su control por parte del equipo médico. Hay que evitar por tanto cualquier posible error humano y que alguien del equipo médico que manipula dicho robot pueda acceder y modificar por error su configuración, separándolos claramente. Otras opciones son incorporar factores de seguridad adicional como el uso de tarjetas RFID por parte del equipo médico para poder desbloquear el dispositivo.
- Realización de auditorías técnicas del robot y de sus aplicativos de control mediante técnicas ofensivas, que permitan identificar posibles vulnerabilidades y puntos débiles del sistema, apoyadas por la realización de un análisis de vulnerabilidades específico.
- Segmentación de la red IT/OT, así como protección de la red perimetral del entorno IoT, para evitar que las amenazas puedan propagarse por la red y afectar al dispositivo.
- Protección de las comunicaciones no seguras mediante el uso de elementos de cifrado específicos.
- Uso de protocolos de nueva generación, como ZigBee o los protocolos basados en el estándar IEC 802.15.4, que permiten aplicar diferentes niveles de seguridad a los mensajes enviados.

Ante un panorama cada vez más desafiante en términos de ciberseguridad, la mejor forma de ser resilientes ante ataques cibernéticos es generar nuestra propia Estrategia de Ciberseguridad, que nos permita el manejo eficiente y eficaz de los recursos tecnológicos para la prevención, identificación, respuesta y recuperación ante ciberataques que busquen poner en riesgo la operación de los procesos críticos del negocio.

La nube, la Oportunidad de Reinventar la Seguridad para el Escenario de Amenazas Actual

Fernando Rubio*
Cybersecurity Digital Advisor en Microsoft

EMPECEMOS HABLANDO DE LA SITUACIÓN ACTUAL Y DE LOS RETOS A LOS QUE NOS ENFRENTAMOS. EL CRECIMIENTO DEL MUNDO DIGITAL ESTÁ AUMENTANDO DE FORMA EXPONENCIAL EL RIESGO DE CIBERATAQUES. HEMOS ASISTIDO EN LOS ÚLTIMOS AÑOS A UNA EXPLOSIÓN Y DISPERSIÓN DE LOS DATOS EN TODOS LOS ÁMBITOS Y EN CONCRETO A LA TRANSFORMACIÓN DIGITAL DEL SECTOR DE LA SALUD, INCLUYENDO LA TELEMEDICINA, EL TELETRABAJO, LOS DISPOSITIVOS MÉDICOS CONECTADOS Y EL USO DE IA PARA EL DIAGNÓSTICO, POR NOMBRAR ALGUNAS DE LAS TENDENCIAS MÁS RELEVANTES. PRÁCTICAMENTE TODO PUEDE SER ATACADO.

El impacto de estos ataques es variado. Por una parte, existe el riesgo de una brecha de datos, afectando a la confianza de los pacientes, a la reputación de marca, a las responsabilidades legales y financieras, etc. Por otro lado, se hace muy real el riesgo a la continuidad del negocio, donde vemos que el *ransomware* sigue haciendo estragos. Además, y de manera especial para el entorno sanitario, el riesgo de pérdida de integridad en los sistemas médicos como, por ejemplo, sistemas de farmacia o radioterapia puede tener consecuencias directas en la salud de los pacientes.

Como resultado de los múltiples incidentes en los que nuestros equipos de respuesta se ven involucrados, somos conscientes que sigue existiendo una media de 78 días entre el compromiso y la detección, siendo las causas principales para ello, primero, que las herramientas y set de datos en silo tienen carencias de visibilidad, y segundo, la falta de profesionales de seguridad que puedan, de manera efectiva, integrar y correlacionar las alertas de las distintas herramientas.

Además, los atacantes están variando sus tácticas, y si con incidentes como el de WannaCry del año 2017 el factor más relevante era asegurarnos de que los equipos se encontraban bien parcheados, ahora se usan principalmente técnicas de robo de credenciales, ante lo cual la nueva realidad es que parchear sigue siendo necesario, pero no suficiente. La mayor parte de los ataques se basan en la falta de higiene en la operación de los sistemas, por ejemplo, el uso de cuentas privilegiadas en sistemas expuestos como equipos cliente y la obsolescencia que impide tener herramientas adecuadas de protección, detección y respuesta frente a las nuevas amenazas.

Por último, es preocupante el desarrollo de la industria del cibercrimen, donde los diferentes actores maliciosos se están especializando y generando un mercado de actividades ilícitas en el cual los datos y los accesos se venden al mejor postor, amparados por las diferentes legislaciones existentes y la falta de cooperación internacional efectiva en algunos casos.

Ante esta situación Microsoft considera que está en la posición de mejorar de manera relevante la situación mediante una serie de acciones que está llevando a cabo en diferentes ámbitos.



Empezando por nuestra fuerte apuesta por la nube, la cual proporciona estructura, agilidad y escala a la seguridad. Es importante que la adopción de la nube sea mediante una aproximación a la seguridad nativa, simple e integrada con un foco en eliminar la complejidad. Hemos de evitar trasladar los problemas que heredamos a las nuevas plataformas. La visión de Microsoft es la de generar una plataforma segura sobre la que construir aplicaciones con las máximas garantías, tanto de protección como de cumplimiento normativo.

Además, creemos firmemente en la inteligencia artificial y la automatización como medida clave para empoderar a los defensores, librándoles de las tareas repetitivas y dotándoles de cuatro capacidades estratégicas: en primer lugar, simplificando la gestión de identidades y accesos para crear un nuevo perímetro de seguridad basado en la identidad en lugar del existente de red que cada vez es más difuso por las tendencias previamente nombradas, en segundo lugar, dando capacidades de protección contra amenazas, orientadas a romper la economía de los atacantes, continuando con medidas destinadas a la protección de la información allí donde se encuentre, y, por último, mediante una gestión integral de la seguridad que incluya visibilidad unificada de clientes, aplicaciones, identidades y servicios, control en tiempo real de los mismos y simplificando el cumplimiento normativo.

Es destacable, en este último aspecto, el reciente trabajo conjunto de Microsoft con el Centro Criptológico Nacional en la creación de las guías CCN-STIC de configuración segura para Office 365 y Azure, siguiendo el Esquema Nacional de Seguridad (ENS), para el cual ambos servicios están certificados desde 2016 en su nivel alto, de tal modo que podamos construir aplicaciones que alberguen datos médicos con todas las garantías y de manera sencilla y predecible. Estas guías ya están disponibles en el portal del CCN-CERT.

---

* *Fernando Rubio es Arquitecto digital de Ciberseguridad en Microsoft, donde trabaja con múltiples organizaciones, mejorando su posición de seguridad y diseñando arquitecturas resilientes. Anteriormente, ha liderado la respuesta a incidentes de seguridad y asegurado redes basadas en sistemas Microsoft. Fernando es un habitual presentador del sector de la seguridad, habiendo estado involucrado, entre otras, en las jornadas STIC del CCN-CERT, Rooted o Inforsalud.*

En Ciberseguridad, mejor Prevenir que Curar



Gloria Tamayo
Más información en: https://www.cytomic.ai/es/

LOS HOSPITALES, COMO LA MAYORÍA DE LAS ORGANIZACIONES MODERNAS, DEPENDEN CADA VEZ MÁS DE SISTEMAS DE INFORMACIÓN PARA LLEVAR A CABO SU ACTIVIDAD. HABLAMOS DE ORGANIZACIONES COMPLEJAS QUE, POR SU PROPIA NATURALEZA, PUEDEN LLEGAR A TENER UNA ACTIVIDAD CONSTANTE 24X7X365. SIN OLVIDAR QUE LA MAYORÍA DE LOS EQUIPOS Y MEDIOS DE DIAGNÓSTICOS ACTUALES TIENEN UN ALTO COMPONENTE INFORMATIZADO, CREANDO UNA RED DE DISPOSITIVOS QUE, EN OCASIONES, NECESITAN ESTAR CONECTADOS CON SISTEMAS EXTERNOS CONFORMANDO UN ENTORNO CRÍTICO Y COMPLEJO DE CONTROLAR.

Un sector hiperconectado, inmerso en un proceso de adopción tecnológica y de transformación digital constante, y que pierde cada año un promedio de 6,5 millones de dólares por brechas de seguridad, más del 60 por ciento más que todos los demás sectores, según un informe del Ponemon Institute.

Esto se puede explicar por dos razones: primero, los hospitales contienen gran cantidad de datos personales, que pueden venderse en el mercado negro, donde un historial médico puede ser varias veces más valioso que una tarjeta de crédito. Sin olvidar que en algunos países incluso se puede comerciar con esta información de forma legal, y hay empresas muy interesadas en hacerse con ella, desde centros de investigación a compañías aseguradoras. Segundo, en muchos casos son datos todos ellos con un calor increíblemente alto que están rodeados de la última tecnología pero protegidos con un sistema de seguridad informática anticuados. Esta situación les expone a un riesgo aumentado debido a la mayor cantidad de vulnerabilidades que existen en estos sistemas.

Paradójicamente, se prevé que los dispositivos IoT dedicados al cuidado de la salud crecerán de 95 millones en 2015 a 646 millones en 2020. El Internet *of Things* en los hospitales permite operaciones más eficientes, pacientes más satisfechos e instalaciones sanitarias más seguras. Es este mismo adelanto el que genera un serio problema de seguridad para la industria sanitaria: por un lado, centros mejor gestionados donde la tecnología elimina barreras entre el personal hospitalario y los pacientes mientras consigue un importante ahorro de costes; a la vez que deja entrever el riesgo de *hackeo*. No podemos vivir de espaldas al avance técnico, pero hay que ser conscientes de que es imposible proteger al 100 % un dispositivo que se conecta a Internet.

Dispositivos conectados que están físicamente dentro de la red de equipos médicos informatizados en los 13. 444 centros que conforman la red de sanidad española, entre hospitales y centros de atención primaria; pero también aquellos que en estos días nuestros cerca de 646.000 profesionales del sector han trasladado a sus casas para continuar con su actividad laboral. Porque el COVID-19 ha cambiado casi todos los aspectos de nuestra vida cotidiana, incluyendo nuestros hábitos laborales. Nuevas costumbres, que sin lugar a dudas, debemos contemplar en esta revolución digital de todos los sectores, incluido el sanitario. Derivado de las prácticas de teletrabajo y de las conexiones que se abren para facilitar la comuni-

cación entre empresa y empleados, los sistemas de las organizaciones en general

están poniendo a prueba la capacidad técnica de nuestro tejido empresarial. Uno de los sectores más críticos por todos los motivos es, precisamente, el sanitario. Incluso también ahora por el reto que supone soportar un mayor número de sesiones remotas y de ampliar sus conexiones a otras organizaciones para mantenerse informados y alerta. Microsoft, por ejemplo, ha registrado un aumento en la demanda de llamadas y reuniones del 775%, desde que comenzaron las primeras medidas de aislamiento. Y añadir dependencia tecnológica a una sociedad ya hiperconectada, abre nuevas oportunidades para los criminales que quieran explotar esta crisis. Eso implica que los cibercriminales ya están aumentando sus esfuerzos para sacar partido de los cambios en el modelo laboral y social, por ejemplo el aumento del recurso al teletrabajo.

Sin embargo, las transformaciones que representa la pandemia pueden enfocarse como una oportunidad para construir una infraestructura digital más segura, que acompañe al sector de la sanidad en este proceso de adopción de nuevas tecnologías. La ciberseguridad debe ser tomada muy en serio y abordada con conciencia y visión estratégica. Así, los hospitales tienen necesidad de adoptar medidas serias y estructurales para proteger su parque informatizado libre de ataques, puesto que una caída o no disponibilidad de las tecnologías y los equipamientos puede resultar en una amenaza grave para la continuidad operativa de la organización, además de en la atención oportuna y de calidad a los pacientes. Muchas de las vulnerabilidades pueden controlarse contando con un buen análisis de situación y un planteamiento estratégico para enfrentar y gestionar el reto de la seguridad informática en nuestros hospitales.

La falta de recursos humanos especializados, la falta de recursos financieros o la falta de tiempo para una implementación de soluciones de seguridad como las que estas infraestructuras requieren pueden ser barreras o dificultades para enfrentar el problema. Es por ello que una de las opciones más recurridas en la actualidad pasa por la implementación de soluciones en la nube, que permite reducir los costes y obtener un mayor retorno de la inversión.

Una protección avanzada de nuestros terminales de trabajo y personales es fundamental para hacer frente tanto a las amenazas externas como internas que ponen en peligro a día de hoy nuestra sanidad. Sabemos que la inexistencia de perímetros bien definidos debido a la proliferación de dispositivos móviles, uso de aplicaciones en *cloud* o dispositivos IoT, entre otros, añade un reto más a la hora de gestionar la ciberseguridad de las redes sanitarias. Somos conscientes de que la falta de recursos –tanto en número como en especialización-, la obsolescencia tecnológica y la existencia de sistemas heterogéneos no son problemas menores. Por todo ello, creemos que la tecnología sin servicios integrados y con demasiados requerimientos de compatibilidad implican, por un lado, proyectos inmanejables ; y por otro proporcionan un valor muy limitado. Cytomic se ha creado con la ambición de poner al servicio de las organizaciones con retos de ciberseguridad complejos, una tecnología que con servicios "de serie" y compatibilidad extendida simplifique el panorama actual. Hablamos de prevención, de incrementar la visibilidad, de monitorizar continuamente lo que pueda parecer extraño, de no dejar en manos del administrador decisiones complejas (la inteligencia de amenazas, el *machine learning*, la analítica de datos a escala deben automatizar los procesos) para que en definitiva impidamos que las amenazas lleguen a los dispositivos de los usuarios. Los servicios avanzados de ciberseguridad *Zero Trust Application Service* y *Threat Hunting* son los encargados tanto de determinar de forma automática y en tiempo real la naturaleza de los procesos en cada uno de los puestos de trabajo para autorizar su ejecución o por el contrario proceder a su bloqueo, así como de buscar proactivamente indicios sospechosos que puedan transformarse en un riesgo real en nuestros parques.

Desafortunadamente, como sociedad, muchas veces reaccionamos tarde a los eventos y nos falta continuidad y visión, donde la ciberseguridad sea parte de la agenda de la Transformación Digital de los hospitales. Las organizaciones tienen todavía un arduo trabajo por delante, pero desde Cytomic seguiremos trabajando de la mano como *partner* tecnológico, para que puedan monitorizar en tiempo real su red y reduzcan el tiempo de respuesta a incidentes, ayudando a reducir los costos totales y a salvaguardar su reputación.

Asegurar Internet Industrial de las Cosas (IIoT): Cómo Abordar los Riesgos de IIoT en la Atención Sanitaria



Raúl Guillén
Director de Alianzas Estratégicas - Trend Micro

LA BÚSQUEDA CONSTANTE PARA PROLONGAR Y PRESERVAR LA VIDA HUMANA HA IMPULSADO CONTINUAMENTE A LAS TECNOLOGÍAS A DESARROLLAR INNOVACIONES REVOLUCIONARIAS EN LA PRESTACIÓN DE SERVICIOS DE SALUD Y TRATAMIENTOS DE VANGUARDIA. COMO EN MUCHOS OTROS SECTORES Y EMPRESAS, IIOT HA TRANSFORMADO RÁPIDAMENTE LA RED Y LA INFRAESTRUCTURA DE DATOS EN LA SALUD Y LA MEDICINA. CON EL IIOT, LOS DATOS Y LA INFORMACIÓN MÉDICA SE HAN VUELTO MÁS ACCESIBLES Y PORTABLES, LO QUE HACE QUE LA MONITORIZACIÓN REMOTA DE LOS PACIENTES SEA PERFECTA Y QUE SE ACTUALICEN LAS TENDENCIAS DE LOS TRATAMIENTOS CRÍTICOS.

Sin embargo, la rápida adopción de IIoT no está exenta de riesgos. Las partes interesadas en la asistencia sanitaria deben comprender primero los peligros que conlleva sobre el terreno cuando se aplica de forma aleatoria. En el caso de los servicios públicos, las amenazas relacionadas con IIoT podrían causar problemas en cascada a una comunidad más amplia, la sanidad es un servicio primordial básico, uno de resiliencia como sociedad ante una situación de emergencia.

En la asistencia sanitaria, estas consecuencias podrían ser más limitadas, pero muy peligrosas para la vida, la gestión y remediación de vulnerabilidades se hace cada vez mas crítico.

IIOT EN EL ÁMBITO DE LA SALUD

En el sector de la atención sanitaria, IIoT ha marcado el comienzo de una nueva era de posibilidades ampliadas en la que, cuando se conectan a Internet, los equipos médicos ordinarios ahora pueden recopilar y compartir datos importantes, lo que permite a los proveedores de atención médica y a los doctores comprender mejor y tener una visión adicional de los síntomas y las tendencias de los tratamientos. Además, el IIoT ha reducido drásticamente la carga de trabajo de los profesionales sanitarios, permitiéndoles disponer de más tiempo y energía para atender mejor las necesidades de los pacientes.

Los siguientes sistemas y dispositivos son componentes comunes de un hospital o centro de salud conectado.

SISTEMA DE INFORMACIÓN HOSPITALARIA (HIS)

La atención al paciente es una tarea complicada que involucra no solo los aspectos médicos, sino también los administrativos, financieros y, en algunos casos, legales, donde la información de cada uno de ellos se integra en una única plataforma, el Sistema de Información Hospitalaria o HIS.

Un paciente suele ser atendido por un equipo de profesionales de la salud que incluye médicos y enfermeras. La atención especializada



que brindan está respaldada por una amplia base de información, que incluye la historia clínica de los pacientes, a la que deben tener acceso cuando lo necesiten. El acceso fácil e inmediato a esta información, por parte de las personas apropiadas, garantiza que el paciente reciba el tratamiento y la atención adecuados. Además, es vital salvaguardar la integridad de dicha información.

Aparte de las actividades médicas y relacionadas con el hospital (por ejemplo, diagnóstico, admisión/alta, etc.), un HIS puede incluir registros legales, administrativos, financieros y otra información necesaria para las operaciones diarias de un hospital.

Riesgos. HIS representa un objetivo deseable para cualquier potencial cibercriminal debido a la información crítica que contiene, como la información personal identificable (PII) de los pacientes, que puede ser utilizada para la extorsión, especialmente cuando la condición médica del paciente requiere confidencialidad. Además, las personas o partes con intenciones maliciosas pueden ir tras la institución médica utilizando la Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPAA, por sus siglas en inglés) por las sanciones por chantaje. Si se compromete, no solo pondría en peligro la privacidad de sus pacientes, sino también su seguridad.

En un hospital conectado, un HIS es susceptible a amenazas que incluyen -pero no se limitan solo a ellas- denegación de servicio distribuida (DDoS), *ransomware* y ataques de *phishing*. Otros dispositivos conectados a las redes de los hospitales podrían servir como punto de entrada para los agentes maliciosos, que podrían realizar movimientos laterales para obtener acceso a información más crítica. Una vez que se accede a un HIS, los actores maliciosos pueden manipular datos, robar información o interrumpir las operaciones diarias del hospital.

Recomendaciones. La seguridad de un HIS depende en gran medida de la seguridad de la red. La segmentación de la red podría ayudar a prevenir o reducir el impacto de un compromiso. Esto implica dividir una red en subredes que podrían reducir el riesgo de movimiento lateral. El software de cifrado también podría ser útil para mitigar las consecuencias del robo y la pérdida de datos, por supuesto también debemos asegurar el entorno productivo y proteger el entorno global de servidores y aplicaciones, así como las bases de datos con soluciones de protección del



runtime con soluciones de *antimalware* avanzado, bastionado y parcheo virtual.

DISPOSITIVOS MÉDICOS

Existen innumerables dispositivos médicos que cumplen funciones altamente especializadas y críticas dentro de las instalaciones de atención médica, utilizados principalmente para monitorizar las señales vitales del paciente o administrar medicamentos, como bombas de infusión, máquinas de anestesia, de diálisis y ventiladores respiratorios. Las versiones modernas de estos dispositivos pueden conectarse de forma inalámbrica a una red, lo que permite que estos dispositivos se controlen de forma remota y transfieran la información recopilada, como la cantidad de medicamento que un paciente ha llevado a un HIS.

Riesgos. Al igual que con cualquier equipo o dispositivo, las vulnerabilidades previamente desconocidas son peligros prevalentes que amenazan constantemente a las máquinas conectadas. El robo de información de los pacientes, así como los ataques a estos dispositivos médicos podrían conducir a lecturas inexactas, lo que puede perjudicar a los pacientes que están bajo atención. Un ejemplo de ello fue una vulnerabilidad reciente que los investigadores han descubierto

en una marca de equipos de anestesia, que podría permitir a un atacante modificar a distancia los parámetros del aparato, es decir, cambiar la composición de los gases aspirados, poniendo en riesgo a los pacientes. Los dispositivos conectados también pueden ser víctimas de ataques DDoS, *malware* y otros ataques a la red.

Además, existe la posibilidad, aunque remota, de que los *hacktivistas* utilicen historias médicas robadas de ciertos individuos para dirigirse a un grupo étnico o político específico y llamar la atención sobre su causa.

Recomendaciones. Los fabricantes, distribuidores e instalaciones de atención médica comparten la responsabilidad de garantizar que estos dispositivos médicos sigan siendo seguros para su uso. Las partes interesadas deben tener cuidado con las vulnerabilidades y las divulgaciones de *exploits*, de modo que puedan ser ágiles en la mitigación de posibles amenazas. También pueden consultar a organismos gubernamentales, como la Administración de Alimentos y Medicamentos de Estados Unidos (FDA) o el Departamento de Seguridad Nacional (DHS) para obtener orientación sobre cómo abordar las amenazas descubiertas. La FDA, por ejemplo, continúa desarrollando un plan de acción para la seguridad de los dispositivos médicos, para ayudar a mitigar los riesgos causados por los descuidos en la seguridad de los dispositivos y reunir a las partes interesadas para abordar estos descuidos y realizar retiradas del mercado en caso de que se descubran vulnerabilidades. Los centros de salud también pueden utilizar el parcheo virtual, que ayudaría en gran medida a gestionar las vulnerabilidades, reduciendo la ventana de exposición de sus sistemas y equipamiento. Recordemos que no solo debemos tener visibilidad de las vulnerabilidades, debemos ir un paso mas allá y remediarlas.

SOFTWARE PARA SISTEMAS DE SALUD

Las instituciones médicas necesitan software para ayudar a controlar diferentes sistemas que utilizan para ejecutar y transferir información dentro de sus instalaciones. La interfaz de estos sistemas puede contener los controles para funciones críticas o información crítica como la Información de Identificación Personal (PII) de los pacientes.

Riesgos. La mera exposición de la interfaz de estos sistemas es un riesgo alarmante. Estos sistemas expuestos se pueden encontrar utilizando el motor de búsqueda industrial Shodan. Una investigación de Trend Micro en la que se analizaba el tema de los hospitales conectados reveló que entre los sistemas expuestos había software para la gestión de farmacias, la programación de pacientes y el mantenimiento de registros. La investigación mostró un pequeño número de sistemas médicos expuestos, aunque este reducido número contenía registros médicos, historial e información financiera. Los posibles atacantes también pueden infectar el dispositivo expuesto con *ransomware* o emitir comandos incorrectos. Un atacante también podría tener la vista puesta en otros dispositivos de la red, utilizando el software comprometido simplemente como punto de entrada.

Recomendaciones. Las instituciones médicas deben asegurarse de que sus dispositivos, equipos y sistemas de software no se vean expuestos inadvertidamente *online*. Esto puede evitarse mediante la configuración cuidadosa de estos instrumentos y sistemas, especialmente los que contienen PII tanto de los pacientes como del personal del hospital, clave en este aspecto la seguridad domestica, proteger las comunicaciones y la privacidad del usuario.

SISTEMAS HEREDADOS

Muchas instituciones médicas siguen utilizando sistemas heredados a pesar de la integración de un número cada vez mayor de dispositivos de IoT en sus instalaciones. Esto se debe a que la sustitución de los sistemas heredados se traduciría en un amplio período de inactividad, que las instalaciones sanitarias podrían no estar en condiciones de costear. Sin embargo, esto conlleva ciertos riesgos y consecuencias que estas instituciones deben tener en cuenta.

Riesgos. Los sistemas heredados podrían estar mal equipados para proporcionar las ciberdefensas que los dispositivos de IoT necesitan para funcionar de forma segura. Además, existe la posibilidad de que los fabricantes hayan dejado de desarrollar parches y actualizaciones, pasando en su lugar a iteraciones más nuevas de un sistema similar. Esto hace que el sistema heredado sea

vulnerable a nuevas amenazas y tenga medidas de seguridad inadecuadas que podrían convertirlo en el punto de entrada perfecto para comprometer otros dispositivos y robar más información.

Recomendaciones. Si las instituciones médicas no prevén la posibilidad de sustituir sus sistemas heredados en un futuro próximo, deberían optar por reforzar sus defensas mediante una arquitectura de seguridad aplicable. El uso de soluciones como el parcheo virtual podría mitigar algunas de las vulnerabilidades a las que se enfrentan los sistemas heredados no parcheados.

OTRAS APLICACIONES IOT

Aparte de las consideraciones y aplicaciones del IoT mencionadas anteriormente, otras aplicaciones presentes en instalaciones médicas conectadas simplemente proporcionan una mayor comodidad a su personal. La tecnología RFID, un componente del IoT, puede utilizarse, por ejemplo, para ayudar al personal del hospital a localizar e identificar rápidamente el equipo que necesitarían para tratar a un paciente. Aunque tales aplicaciones no tienen un valor médico obvio, alivian la carga del personal y les permiten concentrarse en el tratamiento de sus pacientes.

Riesgos. Las aplicaciones de IoT que son aparentemente inocuas por naturaleza podrían pasarse por alto y quedar desprotegidas frente a los actores malintencionados que buscan la oportunidad de meterse en sus defensas. Aunque las consecuencias de un compromiso son menos impactantes que las de un dispositivo médico crítico, un compromiso podría permitir un ataque aún mayor con consecuencias mucho menores de recuperación.

Recomendaciones. Los integradores deben mapear y gestionar sus dispositivos conectados, incluidos los que tienen funciones más simples, ya que podrían utilizarse como puntos de entrada para objetivos más grandes. Los integradores de sistemas también deben considerar dispositivos con características de cercado virtual que desactivarán los dispositivos una vez que estén fuera de su alcance.

CONCLUSIÓN

El IoT en el ámbito de la asistencia sanitaria aún no ha alcanzado su plena madurez y sigue rebosando de posibilidades. El desarrollo de tecnologías como 5G ampliará los límites de lo que IoT puede hacer y, en consecuencia, de lo que IoT puede hacer por la asistencia sanitaria. Solo por poner un ejemplo, recientemente, la primera cirugía remota en 5G se realizó en China, donde un médico operó a un paciente a más de 48 kilómetros de distancia. Es fácil dejarse arrastrar por acontecimientos similares, pero es imperativo desarrollar una estrategia de seguridad paralelamente a estos cambios.

Los *stakeholders* -fabricantes, distribuidores, centros y profesionales sanitarios y usuarios- comparten la responsabilidad de proteger el valor que el IoT aporta a la sanidad mediante la adopción de medidas para garantizar su seguridad. Los fabricantes deben acatar las directrices de instituciones y organizamos competentes, como la FDA o la Agencia Española de Medicamentos y Productos Sanitarios (AEMPS) dependiente del Ministerio de Sanidad, Consumo y Bienestar Social, para producir dispositivos de salud estandarizados y de calidad. La seguridad también debe existir desde la fase de diseño, y no solo como algo secundario, es una prioridad. Mientras tanto, los centros de salud deben planificar una arquitectura de seguridad que se adapte mejor a sus necesidades y a los dispositivos que planean conectar a su red. También pueden aplicar un sistema de protección multicapa que proporcione una mejor visibilidad y protección contra vulnerabilidades conocidas y desconocidas, parcheo virtual a nivel de red de datos y a nivel de activos productivos y servidores.

Por último, los usuarios o pacientes también deben asumir la responsabilidad de sus respectivos dispositivos y ser cautelosos ante los signos de un posible ataque o compromiso de estos dispositivos, extremar la precaución e invertir en formación y concienciación, por supuesto utilizar soluciones de *antimalware* y proteger el acceso de sus conexiones a internet.

Todas estas medidas son necesarias porque una sola amenaza puede echar por tierra las ventajas del IoT e introducir nuevos riesgos para un sector ya de por sí delicado, como lo es el de la sanidad. Al igual que la salud, la seguridad no debe descuidarse hasta que sea demasiado tarde...

XVII FORO DE SEGURIDAD Y PROTECCIÓN DE DATOS DE SALUD

"Impacto de la innovación tecnológica en la información de salud"

LA SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD (SEIS) Y EL SERGAS, CELEBRARON XVII FORO DE SEGURIDAD Y PROTECCIÓN DE DATOS DE SALUD. LA REUNIÓN TUVO LUGAR EN EL AULA MAGNA DEL EDIFICIO DE ROBERTO NOVOA SANTOS DE LA UNIVERSIDAD DE SANTIAGO DE COMPOSTELA, EL PASADO 5 Y 6 DE FEBRERO.

Nota: *Nota: Como siempre, advertimos que a continuación ofrecemos un breve resumen de lo tratado en el acto, ya que la falta de espacio en esta revista no nos permite dar una información más amplia. Todo aquel que esté interesado puede obtener una información completa consultando la web de la SEIS.*

CONFERENCIA DE APERTURA

"Estrategia nacional sobre ciberseguridad"

Fernando Suárez, presidente del Colegio Profesional de Ingeniería de Galicia, después de dar la bienvenida a todos manifestó que, "si bien, la aplicación de las tecnologías en el sector salud producen múltiples beneficios, también aumentan los ciberataques. Tenemos que considerar la ciberseguridad como algo muy importante. Los modelos de privacidad y el tratamiento de los datos personales implican a todos los profesionales. La protección de datos siempre tiene que estar presente. No falta mucho tiempo para que el ordenador más rápido que exista hoy se convierta, en breve en un ábaco."



María del Mar López Gil, jefa del Área de Seguridad y Lucha contra la Desinformación del Departamento de Seguridad Nacional de la Presidencia del Gobierno, quiso destacar la orientación que están manteniendo frente al mundo de la ciberseguridad, como ámbito de especial interés para la seguridad nacional. "Lo primero, lógicamente es mencionar nuestra razón de ser que podemos resumir en: asesorar al Presidente del Gobierno en materia de Seguridad Nacional, Impulsar el desarrollo e integración del Sistema de Seguridad Nacional, mantener y asegurar el centro para el ejercicio de las funciones de seguimiento y gestión de crisis y, por último, gestionar y asegurar las comunicaciones especiales de la Presidencia del Gobierno".

También hizo referencia al hecho de que "en 1996 se presentaron en España las primeras denuncias relativas a delitos que utilizan la informática, creándose así unidades especializadas en Guardia Civil y Policía", y que," las amenazas en el mundo digital adquieren una dimensión global que supera la tecnología". "Hoy, la ciberseguridad nacional consta de 5 objetivos generales: desarrollar el modelo general de gestión de crisis, promover una cultura de Seguridad Nacional,

favorecer el buen uso de los espacios comunes globales, impulsar la dimensión de seguridad en el desarrollo tecnológico y fortalecer la proyección internacional de España. En definitiva, la ciberseguridad está en la agenda de todos los gobiernos", concluyó.

PRIMERA SESIÓN



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

Tuvo como moderador a Benigno Rosón Calvo, subdirector general de Sistemas y Tecnologías de la Información del Servicio Gallego de Salud. Recordemos que Benigno obtuvo el Premio al CIO del sector salud por sus logros en la implantación de proyectos de transformación digital, el de los premios de la SEIS del pasado año.

Tras una breve presentación de la mesa durante la que comento que "tenemos la robótica aquí, ya no solo llegan a hacer un diagnóstico de la mano de un profesional, sino que realizan intervenciones quirúrgicas como un profesional a distancia. Y en lo relativo a los ciberataques, opino que, al menos en España, creo que estamos haciendo las cosas bien."

Los ponentes fueron:

David Núñez, security principal sales consultant de Oracle, fue el primero en intervenir. Lleva 13 años en Oracle, siempre centrado en temas de seguridad, y quiso destacar que "en los medios empezamos a ver cosas que tienen que ver con la ciberseguridad y en las empresas ya tenemos metodologías para saber si estamos o no seguros. Compartiréis conmigo que muchas veces no somos gestores de unos procedimientos para llegar a nuestros objetivos, sino que actuamos como bomberos apagando fuegos. Tenemos que ser eficaces y saber valorar. "Quiero señalar que los ciberataques se encuentran a nivel mundial. Tenemos que pedir apoyo a terceros para que nos ayuden buscando partners en fabricantes que nos cedan su experiencia para que nos podamos proteger. Somos conocidos por nuestra base de datos que probablemente muchos de vosotros tenéis y que usareis aplicaciones que utilizan bases de datos Oracle. Resulta que la información más valiosa de vuestras organizaciones está en sistemas de almacenamiento de datos", concluyó.

Nur Pulard, major account manager de Fortinet, dedicó su ponencia a hablar de la seguridad IOT en el entorno hospitalario y quiso mostrar el listado de todos los hospitales que tenemos en España que en 2019 llegaban a 925. "¿Cuál me puede tocar?, da lo mismo. Siempre que se habla de seguridad hay que hablar de probabilidad. Mejor que hablar de probabilidad hay que hablar de sensatez. Hay que pensar que en el hospital hay muchos dispositivos conectados y que, por supuesto, lo que está conectado puede estar hackeado, por lo que no hay que fiarse", expuso.

También quiso ofrecer cuatro consejos en nombre de Fortinet y que resumió en: identificar activos, clasificarlos y priorizar su valor. Segmentar la red

dinámicamente. Analizar tráfico y buscar amenazas. Y, por último, vigilar el control de acceso. Y finalizó diciendo que "en Fortinet tenemos un compendio de soluciones que trabajan entre sí como es el control de acceso, dispositivos corta fuegos tanto convencionales como industriales, wifi, etc."

José de la Cruz, director técnico de Trendmicro habló sobre "el paciente en riesgo: Profilaxis Ciberseguridad". Empezó exponiendo que "cuando hablamos de protección, para mí el paciente riesgo sería el dato, por lo que me gustaría centrarme en la protección de datos, pero desde la arquitectura que manejamos para manipularlo".

También destacó que para él "algo obligatorio cuando hablamos de ciberseguridad, es la visibilidad, que es clave. Seguro que voy a recibir un ataque, lo más importante no es bloquearlo, porque no siempre lo voy a conseguir, sino saber cuál es su alcance, ver que parte de mi red se ha visto afectada y, por lo tanto, minimizar ese ataque, aislando esas máquinas, las puedo formatear o hacer lo que sea, pero todo ello sólo lo puedo hacer si tengo la visibilidad de lo que está ocurriendo".

Efrain Castaneda, global privacy researcher de Onetrust, habló de "cómo mejorar su plan de respuesta a incidentes". "La gestión de incidentes y brechas en seguridad son la principal causa de fuga de datos personales o de algún otro tipo de violación a la confidencialidad. Todo el mundo sabe que, hasta antes de la aplicación del RGPD, había que notificar este tipo de brechas de seguridad a la AEPD, pero esto se refería solo a operadores de servicios de comunicaciones electrónicas. Pero la obligación de notificar las brechas de seguridad es una parte de un todo que se integra dentro de lo que hasta ahora sería el registro y procedimientos de gestión de incidencias. Hay que ser conscientes de que tenemos que estar preparados. Todos hemos tenido brechas independientemente del tamaño de la organización o del número de empleados o de pacientes en el caso de los hospitales", expuso.

Carlos Andrade, responsable técnico de ciberseguridad de zona sur de IECISA, trató el tema "Desafíos de la Ciberseguridad en la interconexión en entornos complejos". Bajo este título, IECISA nos mostró que "a los ya complejos entornos de comunicaciones inherentes al marco IT; hay que añadir nuevos desafíos asociados a las necesidades de intercomunicación del mundo IOT con las tecnologías y usuarios existentes en IT. La integración de ambos contextos tecnológicos lleva al mundo IOT todas las amenazas de ciberseguridad existentes en IT, así como traslada a IT una nueva superficie crítica de ataque a la que debe hacer frente".

"Los altos niveles de disponibilidad que estos servicios demandan y el elevado grado de conocimiento que se requiere para su gestión, hace que los departamentos de IT en el ámbito sanitario, al no estar dimensionados para esas demandas, necesiten de la colaboración de empresas proveedoras de servicios de ciberseguridad gestionados (MSSP). IECISA, a través de su LiveSOC, puede prestar estos servicios gestionados y colaborar en las fases previas de diseño e implantación de las soluciones de seguridad IT-OT que puedan necesitarse", concluyó.

INAUGURACIÓN OFICIAL

Estuvo presidida por Jesús Vázquez Almuiña, consejero de Sanidad de la Xunta de Galicia. Le acompañaron en la mesa Mar España Martí, directora de la Agencia Española de Protección de Datos; Luciano Sáez Ayerra, presidente de la SEIS; Alberto Fuentes Losada, secretario general de la Consejería, y Eloina Núñez Masid, gerente del área sanitaria de Santiago de Compostela y Barbanza.

Eloína Núñez presentó a todos los componentes de la mesa y agradeció la celebración de este foro en Santiago de Compostela, así como "a la Facultad de Medicina de Santiago por facilitar el aula magna para poder celebrarlo, con un tema que cada día nos preocupa más. Resulta imparable la digitalización de todos nuestros procesos asistenciales que cada día generan una ingente cantidad de datos. La incorporación de las nuevas tecnologías y, sin duda, la inteligencia artificial, suponen un soporte muy importante para todos los profesionales de la salud, tanto en los hospitales como en los centros de salud, para su toma de



decisiones. Estoy segura del éxito de este foro."

Después, cedió la palabra a Luciano Sáez que comenzó diciendo que "celebramos este XVII Foro de Seguridad y Protección de Datos gracias a la colaboración del SERGAS y de la Consejería de sanidad de la XUNTA de Galicia, y continuó afirmando que "como en ocasiones anteriores, hemos contado con la colaboración de la Agencia Española de Protección de Datos, la Agencia Vasca de Protección de Datos, la Autoridad Catalana de Protección de Datos y del Consejo de Transparencia y Protección de datos de Andalucía. Estamos en una comunidad pionera en la consolidación de una historia clínica electrónica única y tanto para la atención primaria como hospitalaria y accesible desde toda la red sanitaria gallega". Para finalizar, expuso que "con este foro queremos concienciar a los directivos sanitarios y a los responsables de la tecnología de que para garantizar una atención sanitaria de calidad es necesario definir políticas adecuadas para la protección de datos personales e implantar en los sistemas de información las medidas de seguridad necesarias que garanticen la seguridad de sus procesos".

Seguidamente, intervino Mar España, quien manifestó que "el RGPD ha actualizado la normativa europea para adaptarla al entorno de una sociedad digital y a la evolución cada vez más intensa del desarrollo tecnológico. Por su parte, la nueva ley ha adaptado el derecho español a las previsiones del reglamento y, en las materias en las que se remite al derecho interno de los Estados miembros, ha incorporado nuevas regulaciones sectoriales. Regulaciones que tienen una especial importancia en el tratamiento de datos de salud al incluir una novedosa normativa de la investigación sanitaria y, en particular, de la investigación biomédica, en las que se ha generalizado el uso innovador de tecnología, cuyo impacto será objeto de análisis en la tercera sesión del foro. Este marco normativo trata de dar respuesta a las necesidades de la investigación sanitaria ofreciendo soluciones más flexibles sobre las bases jurídicas para el tratamiento de datos para estos fines."

SEGUNDA SESIÓN

"Autoridades de protección de datos"

Moderó la mesa Alberto Fuentes Losada, secretario general técnico de la Consejería de Sanidad de la Xunta de Galicia. En primer lugar, habló Margarita Uría, directora de la Agencia Vasca de Protección de Datos, exponiendo que "en el programa de este año se dice que la mejor herramienta para resolver los problemas que puedan presentarse, es esta reunión que la SEIS celebra anualmente. Como autoridad vasca a la que represento hemos sido, en este tiempo de aplicación de un nuevo derecho, especialmente cuidadosos en cumplir lo que nos encomienda el Art.57 del Reglamento General de Protección de Datos que, con carácter general, manda controlar la aplicación del reglamento y ser muy respetuosos en nuestros respectivos ámbitos competenciales de actuación y que nos manda promover la sensibilización de la ciudadanía y su comprensión de los riesgos, normas, garantías y derechos en relación con el tratamiento de los datos per-



sonales. Un ejemplo de ello ha sido citado por la directora de la Agencia Española cuando se ha elaborado con la calidad habitual, la guía a la que ha hecho referencia y que tengo delante para los usuarios de la sanidad y que fue objeto de una publicación en noviembre del pasado año."

Seguidamente, tomó la palabra **Manuel Medina Guerrero,** director del Consejo de Transparencia y Protección de Datos de Andalucía, "hoy me siento en esta mesa como miembro de pleno derecho puesto que efectivamente hemos asumido la competencia en materia de protección de datos hace muy pocos meses. Nuestra experiencia, como pueden imaginarse, es muy reducida y limitada. Sin embargo, esto no quiere decir que antes, cuando operábamos solo y especialmente como autoridad de transparencia no tuviéramos que abordar algún asunto en el que estaba en juego datos personales en materia de salud. Esto puede parecer algo paradójico y automáticamente no se tiene la percepción de que transparencia y protección de datos se encuentren en una tensión dialéctica constante por decirlo así. Entre transparencia y protección de datos también hay puntos de conexión y de contacto y me pregunto cuál es el pilar fundamental del sistema de transparencia de España, siendo el derecho de acceso a la información pública que se considera en unos términos muy generales. Un ciudadano puede pedir cualquier documento o contenido de información que esté en manos de una administración pública. En el derecho fundamental a la protección de datos personales hay un componente esencial en el acceso a la información del titular de los datos".

TERCERA SESIÓN

"Impacto de la Innovación Tecnológica en la Información de Salud"

En esta ocasión, el moderador fue **Pedro Alberto González González**, responsable de registro y auditoría de ficheros de la Agencia Vasca de Protección de Datos.

El primero en hablar fue **Juan Díaz,** coordinador del Comité Técnico de Seguridad de la Información de Salud. "Este comité están representados los responsables de seguridad que nacen en el marco de la LOPD y su reglamento de desarrollo, posteriormente definidos en los perfiles del Esquema Nacional de Seguridad. Integrando miembros del Sistema Nacional de Salud, tanto en la vertiente de seguridad como en la de privacidad mediante sus delegados de Protección de Datos. El Comité nos permite buscar puntos de apoyo y colaboración entre sus miembros y para ello disponemos de una plataforma colaborativa. Se ha revisado la implementación práctica de la cláusula adicional decimoséptima de la LOPD, los planes de Ciber-ejercicios europeos o la implementación de SOC en entornos sanitarios. También se plantean líneas de trabajo futuras de normalización sobre consentimientos clínicos o de investigación, o los criterios en pseudonimización en *BIG-data"*, expuso.

Seguidamente. tomó la palabra **Javier Candau,** jefe del departamento de ciberseguridad de CCN, "el sector salud, de todos los servicios esenciales

que hay, es, sin duda, el más importante porque nos afecta a todos. En 2006 se creó el CCN-CERT, que se encarga de que nuestras administraciones sean más difíciles de atacar, que seamos capaces de detectar el mayor número de ataques posibles, y en caso de que se sufra uno, ayudar a las administraciones a recuperarse, mejorando su resiliencia para ser un objetivo difícil", explicó, y continuó diciendo que "últimamente se están produciendo ataques de *Ramsomware* y específicamente en entornos sanitarios, intentando aprovechar posibles deficiencias como configuraciones por defecto de servicios ofrecidos por proveedores, la falta de certificaciones, escasez de personal especializado, etc. Por ello es muy importante estar prevenido contra los ataques como puede ser el uso de Emotec Stoper, las actualizaciones de las protecciones de equipos finales o la segmentación de la red. Como conclusiones se proponen tres líneas de actuación: reducir superficie de exposición, vigilar y desplegar equipos de respuesta ante incidentes (SOC)".

A continuación, José Luis Rojo Luque, *associate partnes/advisory services EY*, tomó la palabra afirmando que "tenemos la suerte de saber lo que está pasando en el sector, pero no sólo a nivel público sino también en el privado nacional e internacional. Lo que nos estamos encontrando a día de hoy en cuanto a los retos que nos puede deparar la innovación tecnológica, es el cibercrimen, y cuando hablamos de él, intentamos que se entienda que hablamos del crimen organizado. El cibercrimen supone ya la tercera economía ilegal del mundo, por delante del tráfico de drogas y, los que están detrás, disponen de los recursos necesarios para sacarle rédito a estos ataques. También tienen un terreno de juego muy favorable como es internet oscuro y las criptomonedas, que permiten vender nuestra información y ponerla en valor y luego cerrarlo con transacciones económicas".

Posteriormente, habló Juan Carlos Muria-Tarazón, director del sector salud de S2 Grupo que nos dio su opinión sobre los riesgos que corren las infraestructuras sanitarias desde el punto de vista del funcionamiento actual, "este año hemos realizado un informe para la agencia europea de la seguridad, EU-OSHA sobre recomendaciones y buenas prácticas para compras de equipamiento médico y de servicios de todo tipo, por parte de los hospitales y organizaciones de salud en general. Ha sido un informe de ámbito europeo y nos hemos dado cuenta de dos cosas. Primero, que en Europa no están mejor que aquí, lo cual no tiene que servir para conformarnos, sino para apresurarnos y tapar todos los agujeros que ahora estén abiertos y asumir los retos existentes en el sector salud. Y, en segundo lugar, nos ha servido para conocer, de la mano de expertos, las mejores prácticas de cara a prevenir los ciberataques".

Por último, tomó la palabra Alfredo Díaz Fernández, responsable de ciberseguridad y DPO del grupo OESIA. "En el grupo OESIA tenemos diversos proyectos importantes en muchas organizaciones sanitarias, en Castilla La Mancha y Castilla y León, así como en Cantabria. Yo tiendo a ser muy pragmático y como este sector lo conozco, sé los problemas que nos podemos encontrar. Cuando hablamos de innovación tecnológica, me vienen a la cabeza términos como *machine learning, blockchain,* inteligencia artificial, y otros que son los que están más en boca. Desde el grupo OESIA nos hemos encontrado varios problemas principales en las organizaciones sanitarias



a la hora de implementar este tipo de proyectos de nueva generación. Principalmente, creemos que la organización sanitaria no tiene claro lo que desea hacer y hacia donde quiere ir con su innovación tecnológica, y que a veces queremos ir a procesos de este tipo utilizando big data, inteligencia artificial ya que suenan y se venden muy bien, pero que realmente desconocemos".

CUARTA SESIÓN - DEBATE

"Casos prácticos: La experiencia de las autoridades de Protección de Datos"



La sesión estuvo moderada por **José Luis Falcón Pliego,** jefe del gabinete de Publicidad Activa y delegado de Protección de Datos (Consejo de Transparencia y Protección de Datos de Andalucía).

Como suele ser habitual en esta sesión, se presentaron los principales casos que se han atendido en las diferentes agencias de Protección de Datos, durante el pasado año. En primer lugar, **Cristina Gómez,** inspectora/instructora de la Subdirección General de Inspección de Datos, expuso el caso de un hospital psiquiátrico en el que un paciente, después de haber sido tratado y dado de alta, escribió una carta para agradecer la atención recibida. Esa carta se publicó en la web del centro, aunque sin el conocimiento del autor, y, al cabo de dos años, una amiga le cuenta que ha visto su nombre y dos apellidos en la web del hospital, así como el contenido de la carta. Él lo comprueba y llama al centro para preguntar que ha ocurrido cuando él no ha consentido que aparezca en *google* ni la publicación de su carta. Acto seguido, presenta la reclamación y el hospital contesta que varios testigos presenciaron como el paciente accedió a que la carta fuera publicada, pero de palabra, según el hospital y sin consentimiento escrito. La agencia no creyó al hospital ya que, siempre es necesario el consentimiento escrito y el paciente insistía en que el mandó la carta por correo y nadie le pidió autorización. Así pues, se le comunicó al hospital que su actuación no había sido correcta.

A continuación, **Eva García**, inspectora y gestora de transparencia de la Autoridad Catalana de Protección de Datos comentó un caso sobre la legitimidad del tratamiento. Expuso que una persona había formulado una denuncia a la Autoridad Catalana porque en la historia clínica de la que había sido su esposa, existían datos relativos a su persona y que él no había dado su consentimiento. Se quejaba, concretamente, de que en el mencionado documento aparecía una nota de la doctora en la que se podía leer su nombre de pila, sus apellidos, que era paciente del centro de salud mental y que tenía rasgos autistas. El denunciante no entendía porque esta información tenía que figurar en la historia clínica. Preguntando a la doctora porque había introducido esos datos, manifestó que también trataba al denunciante y conocía esa información sin que nadie se lo hubiera dicho.

Seguidamente, **Juana María Vega Fernández,** inspectora y letrada de la Asesoría Jurídica de la Agencia Vasca de Protección de Datos expuso el caso de un señor que había presentado una denuncia porque dentro de los documentos de una interconsulta, en la que no figuraba el motivo, había un exceso de información innecesaria sobre él. El centro reconoció el hecho y aseguró que no volvería a pasar. A pesar de ello, este año llegó

otra denuncia muy similar. Una señora sufre un accidente doméstico, acude al hospital, la tratan y le dan un informe de alta en el que figuran los siguientes antecedentes personales: transexual de varón a mujer, inicio de tratamiento hormonal, mamas operadas, hipotiroidismo, etc. Se preguntó al centro médico el motivo por el cual habían introducido esa información y respondieron que no había violación de secreto porque el informe de alta era para ella y ella ya sabía lo que tenía. La Agencia Vasca respondió diciendo que ellos no hablaban de violación de secreto, sino del principio de minimización. Es decir, para tratarle de una herida en el tobillo, no hacía falta esa información.

QUINTA SESIÓN DEBATE

"Acceso a la información clínica para la docencia y la investigación"



Moderó la mesa **Eva García García,** inspectora y gestora de transparencia de la Autoridad Catalana de Protección de Datos.

El primero en tomar la palabra fue **Julián Álvarez Escudero,** decano de esta facultad y Jefe del Servicio de Anestesiología del Complejo Hospitalario Universitario, comentando que "sobre la ley del 5 de diciembre de 2018 hemos hecho una interpretación restrictiva y sesgada. Hace ya varios años, teníamos en nuestra unidad un paciente de VIH, además con un linfoma, al que habían dado quimioterapia, tenía una insuficiencia respiratoria y estábamos ventilando como podíamos. Intentamos explicar a alumnos de quinto de carrera que era la confidencialidad diciéndoles: si este paciente que es VIH positivo, sale adelante y dentro de tres meses está ligando con una amiga vuestra en una discoteca, tú no le puedes decir nada a tu amiga. Eso es la confidencialidad. Y creo que en la mayor parte de las veces no la utilizamos adecuadamente. No podemos tratar toda la información de la misma manera, como si fuéramos delincuentes, pero debe haber una normativa que proteja al enfermo. Hace falta disponer de grandes bases de datos anónimas para que podamos trabajar. Yo pediría a los jurídicos, a la gente dedicada a la ética y a los informáticos que encontraran un campo confortable donde pudiéramos trabajar, analizar, publicar y enseñar, respetando los derechos de los pacientes con una normativa rígida".

Seguidamente, intervino **Susana María Romero Yuste,** presidenta del Comité de Ética de Investigación con Medicamentos de Galicia, exponiendo que "el papel del comité de ética en investigación respecto a la docencia es en cierto modo tangencial, porque como su nombre indica se encarga del análisis de los proyectos en sus aspectos éticos, metodológicos y legales. El comité ha estado trabajando mano a mano con el secretario general de la Consejería, con el delegado de protección de datos para elaborar una instrucción que se lleva a cabo cumpliendo la normativa legal que nos obliga a preservar la información de los pacientes que intervienen en la investigación, así como su derecho a ser respetados la protección de los datos. Venimos de una época en la que todo valía, y no teníamos conciencia de que el paciente era el dueño de su cuerpo y de sus datos".

En tercer lugar, intervino **Javier Ureña Morales,** jefe del servicio jurídico del Hospital de Inca y miembro del Comité de Ética de Investigación de las Islas Baleares. "Es importante centrarnos en el paciente, ya

que si hablamos de seguridad es debido a que tenemos datos y pacientes, hecho que no hay que olvidar en ningún procedimiento o en ningún proceso que realizamos a nivel profesional. Existen ciertas dificultades en el acceso a la historia clínica, pero está claro que nos abre vías de actuación y la posibilidad de utilizarlo. Nos encontraremos con una serie de requisitos y, el principal, es que vamos a tener que separar los datos de identificación del paciente de los datos asistenciales, y la información debe ser tratada con ciertos niveles de secretismo. Una de las recomendaciones que hace la Agencia Española de Protección de datos es: trata los datos de los pacientes como te gustaría que trataran los tuyos. Creo que está claro que nadie querría que 40 personas entraran en nuestra historia clínica sin ninguna razón que lo justificara", afirmó.

Posteriormente fue el turno de **Mercedes Alfaro Latorre,** subdirectora general de información sanitaria y evaluación, del Ministerio de Sanidad que expuso que "comentaba el Decano que los estudiantes necesitan aprender cuestión es de protección de datos si queremos tener buenos médicos. Ese es uno de los aspectos que debemos tener absolutamente en cuenta a la hora de tratar estos temas, desde mi punto de vista. Respecto a la historia clínica creo que ha pasado de ser una herramienta o un instrumento propia del médico, a serlo de un equipo de profesionales de diferentes perfiles. Después, pasó a ser un documento propiedad del propio paciente que tenía gran control sobre ella. Y finalmente, desde un punto de vista más moderno, la historia clínica se considera como un elemento de relación entre todos ellos donde se van recogiendo las anotaciones sobre la enfermedad, y el proceso diagnóstico y terapéutico para la mejora del paciente. Esto, evidentemente, cambia bastante las reglas del juego, ya que son muchos los que pueden acceder a esa información. Y ahora aquí, en esta mesa, de lo que hablamos es de las personas en formación que pueden acceder a esa información con datos relativos a la enfermedad y al diagnóstico y tratamiento para la mejora del paciente".

SEXTA SESIÓN- DEBATE

"Experiencia de los delegados de protección de datos"



La moderadora en esta ocasión fue **Rosario Heras Carrasco**, responsable de la Unidad de Evaluación y Estudios Tecnológicos, de la Agencia Española de Protección de datos, quien tras una breve introducción dio paso a los ponentes.

El primero en intervenir fue **Jorge Prado Casal,** delegado de protección de datos del Sistema Público de Salud de Galicia, quien aseguró que "en Galicia, hay una ley de Salud que establece que el sistema de información es único para todo el sistema público por lo que el delegado de procesos de datos en justa correspondencia también es único para todo el sistema público de Salud gallego. Debo decir que es importante en los comienzos saber lo que tenemos que hacer con lo poco que dice la ley y que el cambio realizado, por mi parte y por el resto de compañeros con los que tengo contacto habitual, tenemos que agradecérselo a la Agencia Española de Protección de Datos. La realidad es que cuando empiezas a saber lo que se espera de ti, llega una nueva petición, una nueva reclamación que hace que descubras que

realmente es un mundo muy amplio, con todo lo que se nos está pidiendo y tantas expectativas que se han depositado por parte de los que contactan".

Seguidamente, intervino **Juan Miguel García Riego,** delegado de Protección de Datos de la Consejería de Salud de la Junta de Andalucía. "He vivido como una especie de ficción el alumbramiento a la protección de datos como un derecho fundamental. Yo entré en el 98 y mi actividad principal eran los ficheros. Era la gran actividad que tenía. Yo decía que el que no tuviera un fichero inscrito no era nadie. Todo el mundo decía que quería tener un fichero. Todo esto ahora ha cambiado, así como el papel del técnico de procesos de datos", afirmó.

A continuación, tomó la palabra **José Jiménez Perales**, delegado de Protección de datos de Quirón. "Si me permitís un segundo debo decir que Quirón Salud son 50 hospitales, tenemos 15 millones de historias clínicas y somos 40.000 empleados. Estamos en un proceso actual de consolidación para que todo el grupo trabaje como una sola entidad, apoyándonos en las nuevas tecnologías y una cosa que tiene que estar totalmente clara es la protección de datos. Nosotros creamos una estructura en el grupo Quirón Salud y aprovechamos todas las que ya teníamos en la antigua protección de datos. Tenemos los comités de seguridad de los centros, que son multidisciplinares y nos ayudan mucho porque al final, evidentemente, la lucha por la privacidad compete a toda la organización y a todos los estamentos de un hospital. Nosotros situamos al paciente siempre en el centro, esa es nuestra estrategia y, por supuesto en que confíe en que los datos que vamos a tratar estarán siempre seguros con nosotros", expuso.

A continuación, habló **Sergio Manuel Gallego Riestra** delegado de Protección de datos del Servicio de Salud del Principado de Asturias, afirmando que "cuando el Consejero me dijo que tenía que hacerme cargo de este embrollo podría haber dicho que no, pero dije que sí. Mi función como delegado de protección de datos ha sido mantener la figura del delegado como un órgano de apoyo que es el comité de sistemas de información. Mis problemas, fundamentalmente, son de investigación con los trabajos de fin de master. Ya sabemos que el comité ético tiene que analizar la disposición adicional. Debemos llegar a lo que son las denuncias en los accesos indebidos y en las auditorías. Nos encontramos con accesos manifiestamente indebidos constitutivos de violación de la seguridad. Me estoy planteando que cuando haya una auditoría donde se hayan cometido accesos indebidos, no sólo tenemos que decírselo al interesado, sino que además tenemos que personarnos y formular la denuncia en la fiscalía."

El último en intervenir fue **Tomás Pérez Gómez,** jefe del área de Plataformas Tecnológicas de la Dirección General para el avance digital, de la Consejería de Desarrollo Autonómico de la Rioja. "La Rioja cuenta con 345.000 habitantes lo que indica que somos menos que en muchas capitales de provincia. Yo no estoy aquí como delegado de protección de datos sino como presidente de este comité de seguridad. Lo que hemos pasado durante estos años ha sido mucho y me gustaría destacar sobre todo la concienciación, para que la organización lo entienda. Hemos tenido una gran cantidad de consultas, unas razonables y apropiadas y otras no, y hemos orientado a los propios profesionales. Hemos formado a más de 2000 empleando mucho tiempo en discutir y en pelear contra todos los grandes retos que tenemos. Y aquí, en este ámbito, es verdad que es donde hemos tenido más dificultad para conciliar el puesto como responsable de seguridad y como delegado de protección de datos ya que hay que bailar un poco entre los dos. Pero en general, en los proyectos con el resto de la administración no es excesivamente complejo. Resulta más complicado sobre todo por cómo se gestionan los proyectos ya que muchas veces ni la propia organización sabe lo que está haciendo en un servicio concreto" concluyó.

CHARLA MAGISTRAL

El conferenciante **Roberto Baratta,** director de Prevención de Pérdida, Continuidad de Negocio y Seguridad y Delegado de Protección de Datos de ABANCA, fue presentado por **Jorge Prado Casal,** delegado de Protección de Datos del Sistema Público de Salud de Galicia. **Baratta** quiso compartir con los asistentes unas ideas algo diferentes basadas en la experiencia de una entidad financiera donde "además de ocuparnos y preocuparnos de lo que tiene que ver con la protección de datos tam-

bién somos una compañía de seguros, intentando hacer mucho por la salud. Desde el punto de vista de nuestras funciones, de la mía y de la vuestra, la orientación es la misma, generar confianza y nuestros usuarios internos, que acceden a donde tienen que acceder, al proceso de lo que tienen que procesar y a custodiar lo que tienen que custodiar. Nadie quiere que su historia clínica no esté donde debe estar. La gran diferencia entre la transformación digital, la de antes y la de ahora, es que en la de antes una empresa, un hospital, lo que fuera, hablaba con un proveedor y decidía que le convenía. La gran diferencia ahora es que ya no tenemos ese paradigma. Ahora somos nosotros los que tenemos mayor capacidad de concentración. Todos los días nuestros clientes nos rechazan alguna forma de uso. Todo cambia", expuso.

Para finalizar, habló de ciberataques, "es un hecho, que el volumen de ataques, incidentes, brechas y fugas de informaciones se está incrementando. El entorno, año a año, es más complejo incrementando la profesionalización y sofisticación de las ciberamenazas".



CLAUSURA OFICIAL

El acto de clausura estuvo presidido por **Alberto Fuentes Losada,** secretario general técnico de la Conselleria de Sanidade de la Xunta de Galicia, y contó también con la participación de **Miguel Angel Benito Tovar,** coordinador general del XVII Foro de Seguridad y Protección de Datos de Salud, así como **Mercedes Alfaro Latorre**, subdirectora general de Información Sanitaria y Evaluación del Ministerio de Sanidad.

En primer lugar, tomó la palabra **Miguel Ángel Benito Tovar** quien agradeció el acogimiento recibido en Santiago y destacó los "pilares sobre los que debe sustentarse este evento: compartir, tener visibilidad sobre los tratamientos y tecnologías, dar soluciones prácticas al día y a día, y concienciar y sensibilizar, así como crear y proporcionar confianza".

A continuación, tomó la palabra **Mercedes Alfaro,** quien alabó la organización del evento y destacó la importancia de reunir a estos profesionales en torno a una cita institucional y afirmó que "la educación es fundamental para cumplir con las



bases legales en nuestro día a día. Se debe mejorar el acceso a perfiles por parte de la tecnología".

Ya para finalizar, el último en intervenir, **Alberto Fuentes Losada,** concluyó diciendo que "se ha cumplido sobradamente con los objetivos planteados. Las instituciones de protección de datos han demostrado su implicación con el sector de la salud, un sector crítico en esa materia, y eso es fundamental para avanzar en la sanidad digital en la que todos estamos ya trabajando".


X Reunión del Foro de Interoperabilidad en Salud
Síguenos en twitter:
@SEISeSalud
Organiza
SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD
Con la colaboración de
Osakidetza
VITORIA-GASTEIZ
1 y 2 de julio de 2020
Osakidetza
Dirección General, Salón de Actos
Calle Álava 45
01006 Vitoria-Gasteiz
Aforo Presencial - de acuerdo a las normas sanitarias
Aforo Virtual – Ilimitado
SOCIO TECNOLÓGICO PRINCIPAL
SOCIO TECNOLÓGICO COLABORADOR
DXC.technology
Microsoft
EY
FUJITSU
HUAWEI
Ibermática
INFORMÁTICA El Corte Inglés
PHILIPS
SIEMENS Healthineers

X REUNIÓN DEL FORO DE INTEROPERABILIDAD EN SALUD

NTRODUCCIÓN Y OBJETIVOS

El Foro de Interoperabilidad en Salud es el espacio transversal donde debatir los diferentes temas relacionados con la interoperabilidad como herramienta para el desarrollo del Sistema Nacional de Salud. En este sentido, se presentará el resultado de los trabajos que está realizando el Comité Técnico para la Interoperabilidad del Sistema Sanitario y, por otro lado, en el Foro de Interoperabilidad en Salud del 2020 debatiremos cómo la interoperabilidad es la puerta para desarrollar la Inteligencia artificial en una salud de calidad.

Uno de los retos actuales en salud es cómo la IA puede ayudar a realizar una transformación del Sistema Nacional de Salud, pero para poder cambiar y realizar una transformación, es necesario que la inteligencia artificial pueda saltar de la investigación (entrenamiento, etc.) al ámbito real de la práctica clínica y, para eso, uno de los pilares es disponer de información de calidad, información normalizada.

Pero el algoritmo ha de estar integrado, ha de poder formar parte de los diferentes flujos de trabajo y, por lo tanto, ha de poder ser interoperable y también interoperable con otros algoritmos que formen una red de soluciones de Inteligencia artificial. Y aquí la interoperabilidad tiene un papel importante para el desarrollo de la aplicación de la Inteligencia Artificial en Salud.

El Foro de Interoperabilidad en Salud del 2020 debatirá cómo dar respuesta al reto de la incorporación de la inteligencia artificial en el proceso asistencial y cómo la normalización y la interoperabilidad pueden ser una de las herramientas que facilitará el desarrollo de la adopción de la Inteligencia artificial en salud.

CRONOGRAMA

MIÉRCOLES, 1 DE JULIO DE 2020

09:30 - 14:00 **Reunión del Comité de Interoperabilidad del Sistema Sanitario**
Sesión Cerrada

15:30 - 16:00 **Recogida de Documentación**

16:00 - 16:30 **Acto Inaugural**

16:30 - 17:45 **PRIMERA SESIÓN**
Comité Técnico de Interoperabilidad del Sistema Sanitario "Guía de recomendación compra de equipamiento medico, como integrarlo"

17:45 - 18:00 **Pausa**

18:00 - 19:45 **SEGUNDA SESIÓN**
"Avances de la interoperabilidad en el Sistema Nacional de Salud (proyectos de la CCAA)"

21:00 **Cena - Cocktail**

JUEVES, 2 DE JULIO DE 2020

09:00 - 10:30 **TERCERA SESIÓN**
"La calidad de la información, los fundamentos de la IA"

10:30 - 11:00 Pausa Café

11:00 - 12:45 **CUARTA SESIÓN**
"Interoperabilidad la puerta para la Inteligencia Artificial"

12:45 - 14:00 **QUINTA SESIÓN**
"La interoperabilidad como eje para el desarrollo de la estrategia en IA"

14:00 - 14:30 **Clausura**

XXVII JORNADAS NACIONALES DE INNOVACIÓN Y SALUD EN ANDALUCÍA

"Digitalizando en las crisis para saber de salud" (Cómo ir a los SIS deseados con el impacto COVID)

En sintonía con las circunstancias actuales, las XXVII Jornadas de Innovación y Salud que ocurren cada año en Andalucía, se transforman incorporando los siguientes cambios:

La crisis COVID ha creado una gran oportunidad para aprender lecciones acerca de la utilidad, capacidad de evolución, de la infraestructura de información disponible, de carencias organizativas y del riesgo de involución después del momento agudo. El reto actual es identificar en qué y cómo ubicar las próximas acciones prioritarias y asignaciones presupuestarias.

El objetivo principal de estas Jornadas es promover la cooperación necesaria entre todos los actores del sistema sanitario para que los Sistemas de Información y Conocimiento evolucionen hacia lo definido con las próximas infraestructuras y recursos TIC. Ello incluye crisis COVID, otras similares y muchos otros retos.

Los trabajos preparatorios, iniciados en enero 2020, se materializarán en un encuentro en la web entre el 3 y el 4 de junio en el que participarán responsables de los talleres y plenarios, junto con algunos dinamizadores para ir generado contenidos y discusiones en espacios digitales compartidos.

> ***El encuentro presencial tendrá lugar cuando pueda llevarse a cabo con todas las garantías de seguridad para los asistentes.***

El encuentro presencial tendrá lugar cuando pueda llevarse a cabo con todas las garantías de seguridad para los asistentes.

La reflexión colectiva versará en torno a 6 "dimensiones" expresadas en forma de dilemas para visualizar cómo hacer la transición desde la posición actual a la deseada en cada una de ellas. Durante la primera parte del encuentro aplicaremos este método para aprender de la crisis COVID19 y, a continuación, para identificar "cómos" aplicables a todo el Sistema de Información de Salud.

LOS DILEMAS ELEGIDOS SON:

a. Eje personas: 1. "Paciente tutelado vs Enfermo activo" y 2. "Profesional alienado vs alineado."

Esta es la interacción fundamental sobre la que se construyen todos los servicios de salud para resolver los problemas planteados por ciudadanos (1), estén en estado sano o enfermo, pasivo o activo. Son los resultados en salud consecuentes a las tratamientos y cuidados después de esta interacción los que deben determinar las siguientes decisiones. En contexto de pandemia, y más producida por un nuevo germen, esta interacción afecta al comportamiento de cada individuo, de toda la sociedad y sus valores fundamentales, y a todo el conocimiento adquirido hasta ahora, sometiendo a un enorme estrés a todo el Sistema de Servicios de Salud.



Los profesionales (2), vinculados por sus relaciones contractuales, con su progresivo desarrollo de habilidades y conocimiento son componentes intrínsecos de la calidad de los servicios y de la eficiencia global del Sistema.

b. Eje saber: 3. "'Ojo clínico' vs diagnóstico asistido" y 4. "Algoritmos 'Ad hoc' vs 'Ad scientia'"

El diagnóstico (3) adecuado determina la eficacia de las soluciones adoptadas. Puede llevarse a cabo a partir del conocimiento aplicable a una gran variedad de síntomas, signos, mediciones, percepciones, con o sin diferentes ayudas de distintas tecnologías (imagen, bioquímica, genómica, etc.) según las circunstancias.

Toda la información que se genera en cada crisis individual o colectiva de salud se organiza en algoritmos aprendidos y adaptados a cada entorno y tiempo (4) y publicados para integrar las ciencias del curar y cuidar. En escenarios de escasez de evidencia disponible como es este brote epidémico, se hace relevante la diferencia de aproximación al diagnóstico, desde el caso a caso clínico asumiendo riesgos pero ajustando las decisiones, hasta la adherencia a la evidencia disponible por muy escasa que sea y poco evidente que sea, como dogma defensivo.

c. Eje TIC: 5. Información en silos vs recursos conectados y 6. Lenguaje local vs universal.

Las Tecnologías de la información y conocimiento (analógicas y digitales) son la plataforma (5) donde se guarda lo que ocurre, lo que influye en cada crisis, se reutiliza para generar nuevo conocimiento y mejora continua de los procedimientos en curso y se lega para los siguientes. Para que los datos y percepciones en diferentes culturas puedan contribuir a una ciencia universal y ser útiles en la libre circulación de personas, conceptos, datos, algoritmos y resultados, es imprescindible contar con conexiones de distinta índole (codificado, semántico, conceptual, computacional, etc.). La inmensidad y complejidad de los datos que manejamos, así como el conocimiento disponible que crece exponencialmente, requieren de "la solución final computacional", los datos y el conocimiento deben ser "machine readables". Los métodos y las herramientas existen, solo esperan para ser aplicados bajo unas condiciones de mercado sostenible.

FORO DE
INTEROPERABILIDAD

Coordina: **Adolfo Muñoz Carrero**

Centro Nacional de Referencia de SNOMED CT
Servidor de Terminologías de referencia para el SNS

Arturo Romero, Jorge Rangil

EL CENTRO NACIONAL DE REFERENCIA DE SNOMED CT Y EL ÁREA DE SISTEMAS CLÍNICOS DE INFORMACIÓN DEL MINISTERIO DE SANIDAD, PERTENECIENTES A LA SUBDIRECCIÓN GENERAL DE INFORMACIÓN SANITARIA, TIENEN COMO MISIÓN FOMENTAR, PROMOVER Y FACILITAR EL USO DE LA TERMINOLOGÍA SNOMED CT EN EL ÁMBITO NACIONAL, Y ESPECIALMENTE EN EL SNS (SISTEMA NACIONAL DE SALUD).

Para ello desarrollan diferentes estrategias, basadas en productos y servicios, que pueden facilitar la adopción e implementación de sistemas basados en la interoperabilidad, en sus diferentes niveles y en una variedad de dominios y casos de uso.

El Sistema strSNS (Servidor de Terminologías de Referencia para el Sistema Nacional de Salud) es un conjunto de recursos terminológicos y módulos de software que permiten el acceso a los diferentes recursos semánticos (terminologías, valuesets, clasificaciones) utilizados en los proyectos en los que participa y colabora el Ministerio de Sanidad, tales como HCDSNS (Historia Clínica Digital del SNS) y EUPS (*EU Patient Summary*).

El sistema utiliza tecnologías estándar ampliamente difundidas, muy accesibles para implementadores y de uso gratuito: servidor web Apache, base de datos MySQL 7, PHP, HTML5, servicios REST, JSON.

Hasta el momento, el uso principal del strSNS ha sido el mantenimiento de los recursos de SNOMED CT publicados por SNOMED International (IHTSDO) y la gestión continuada de la Extensión Nacional para España.

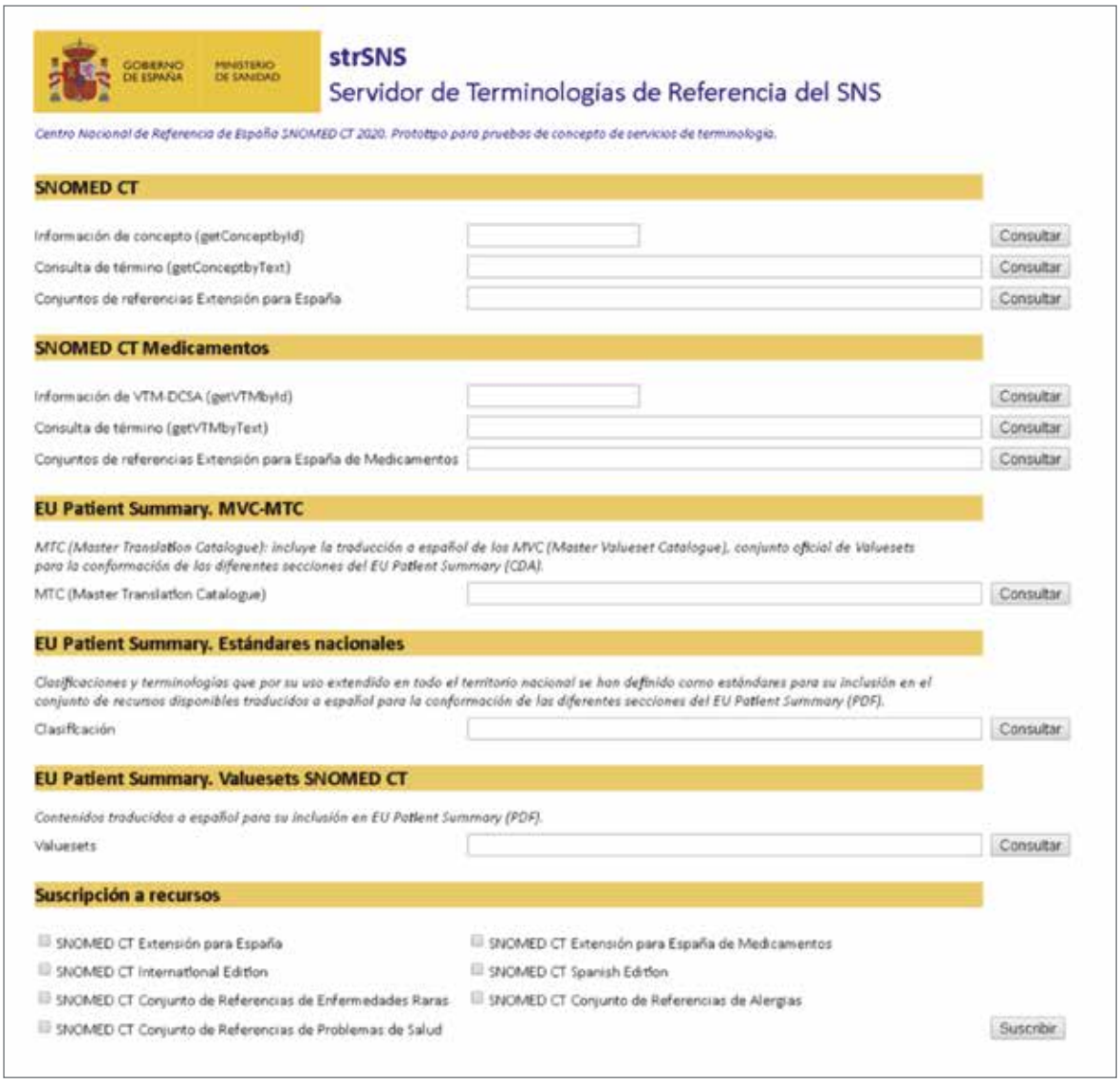
La consulta y descarga de los diferentes contenidos puede realizarse por diferentes vías:

- Aplicación Web strSNS (interfaz de usuario con servicios directos)
- Suscripción a contenidos
- Enlace desde aplicaciones externas: consulta online de información desde otros sistemas, con devolución de resultados en formato JSON o HTML.

Contenidos disponibles

- SNOMED CT: Ediciones Internacionales y Nacionales, conjuntos de referencias, valuesets
- Proyecto EU Patient Summary:
  - MVC-MTC (Catálogos Maestros bilingües)
  - Estándares nacionales con descripciones bilingües (familia CIE, ATC, CIAP2)
  - Valuesets bilingües
- Otros recursos: lexicón, Ontología de Seguridad Clínica de Medicamentos…

Los recursos íntegros del Servidor de Terminologías pueden ser transferidos a otras organiza-



La interfaz Web de los Servicios de Terminología de Referencia del SNS

ciones licenciatarias de SNOMED CT en España. De esta forma, los servicios de asistencia sanitaria, de Salud Pública, de investigación y de formación asociados a dichas organizaciones podrán beneficiarse de unos contenidos muy completos y de unos servicios Web con capacidades de desarrollo, adaptación y configuración muy versátiles, que se actualizan de forma continua y se someten a rigurosos procesos de calidad.



FORO DE
GOBERNANZA

Coordina: **Martín Begoña**

Cómo viajar en la TRANSFORMACIÓN DIGITAL (7)

Pilar Ruiz Ayuso
Consultora en Transformación Digital e Inteligencia Artificial

INTRODUCCIÓN

En el artículo anterior, expliqué la importancia que tiene realizar un diagnóstico de la madurez digital en los sistemas sanitarios, para poder mejorarlos, y así poder realizar una atención sanitaria más innovadora y de calidad, optimizando la relación médico-paciente, y haciendo posible una mayor accesibilidad de los servicios sanitarios.

AUTOMATIZACIÓN DE PROCESOS EN EL SECTOR SALUD

En las instituciones sanitarias, diariamente se atienden a miles de pacientes con circunstancias diversas y particulares, generándose aproximadamente, más de setecientos cincuenta mil billones de bytes diarios de datos clínicos de atención de la salud.

Estos datos clínicos, principalmente son procedentes de sistemas informáticos (pruebas de laboratorio, anotaciones de los facultativos, radiografías, etc.); datos que se generan a través del IoT, como sensores que monitorizan ciertos aspectos del paciente, o incluso de fuentes menos precisas como información más subjetiva, o derivada de terceras personas, procedente de familiares o cuidadores de los pacientes.

Ante tal magnitud de información y casuísticas diferentes, es imprescindible contar con tecnologías de automatización de procesos, *wearebles*, inteligencia artificial, la nube y el *big data,* que saquen el mayor provecho a esos datos, para ayudarnos a tener un mayor entendimiento de lo que está sucediendo en el sector, pudiendo ofrecer una mejor cobertura a los pacientes, tomando cada vez mejores decisiones tanto en la prestación de los servicios como en el diagnostico, en términos de tiempo, atención y calidad.

AUTOMATIZANDO CON RPA, ¿QUÉ ES Y QUÉ NOS APORTA EN EL SECTOR SALUD?

La tecnología RPA es considerado como el primer paso de la automatización digital inteligente de nuestro Modelo de Trabajo ADI, haciendo uso de trabajadores virtuales, donde imitando las acciones humanas y basándose en reglas, permiten focalizar el esfuerzo de las personas en actividades de mayor valor y que requieran creatividad o interpretación personal.

Existen robots RPA atendidos y desatendidos, que su uso irá en función de las tareas que se quieran ejecutar.

Robots atendidos: Permitirá a los empleados optimizar aún más los procesos de *front-office* , ya que el robot trabajará conjuntamente con la interfaz de usuario para ayudarle a completar un proceso de *desktop* de forma automática.

Robots desatendidos: Permitirá ejecutar procesos de *back-office,* manejando grandes volúmenes de información sencilla y compleja a gran velocidad, con reglas previamente definidas, que no requerirán ninguna intervención humana para aplicar todas las decisiones necesarias.

La tecnología RPA, pueden ayudar tanto a proveedores, como los profesionales de la salud en el ahorro de costes, siempre buscando una eficiencia operativa de calidad, aunada con la prestación de servicios de salud centrada en el paciente, más eficientes, seguras y asequibles, consiguiéndolo a través de la escalabilidad, dis-



minución de errores humanos y trabajo 24*7 que proporcionan los robots virtuales.

APLICANDO TÉCNICAS DE AUTOMATIZACIÓN EN CASOS DE USO REALES

Un caso de uso real que estamos realizando en el sector salud, es un clasificador de documentos provenientes de diferentes fuentes (correos, documentación interna, archivos, etc.), de forma que el sistema, con una base histórica ya catalogada, es capaz de generar modelos de clasificación automática, en base a un aprendizaje automático, y de esta forma, clasificar el resto de información existente en el sistema.

Además de clasificar cada documento en base a la información interna que contiene, es capaz de realizar resúmenes sobre los documentos (una especie de "*abstract*" general), de las frases más relevantes dentro del documento, de forma que permite a los usuarios, de un vistazo rápido, ver en líneas generales de qué habla el documento, y si es de interés ahondar más en el mismo

En el entorno de la Sanidad Privada, tenemos una casuística típica en la relación Aseguradora – Prestador de Servicios Sanitarios, concerniente al proceso admisión, autorización y todo lo relacionado con la cobertura de servicios que tiene un paciente contratados con su aseguradora.

A día de hoy existen ejemplos de integración que soportan esta relación Aseguradora – Prestador de Servicios Sanitarios, y permiten una gestión global del proceso de atención. Sin embargo en muchos casos un equipo de profesionales son los encargados de realizar de forma manual la gestión del ciclo de verificación/ autorización de servicios que se tienen cubiertos o no, de cara a validar si se produce un ingreso hospitalario, la prolongación del citado ingreso y/o se admite la realización o no de pruebas adicionales.

En el caso de los Prestadores de Servicios Sanitarios que colaboran con diversas aseguradoras, la cuestión administrativa adquiere una relevancia mayor. Este proceso con una solución RPA, se tendría cubierto, ya que haría toda la gestión administrativa *end to end* interactuando con los sistemas y aplicaciones necesarias para poder saber la cobertura de cada paciente.

CONCLUSIÓN

La automatización de procesos en el sector sanitario, traerá múltiples beneficios en el procesamiento de grandes volúmenes de información de forma ágil, ayudando a la búsqueda del mejor tratamiento para los pacientes, y en un ahorro significativo de costes operativos e ineficiencias, pudiendo derivarse, en la aplicación de tecnologías como AI e IoT, que ayudarán en la prestación de servicios al paciente de mayor calidad y excelencia.

FORO DE
SALUD CONECTADA

Coordina: **Óscar Moreno**

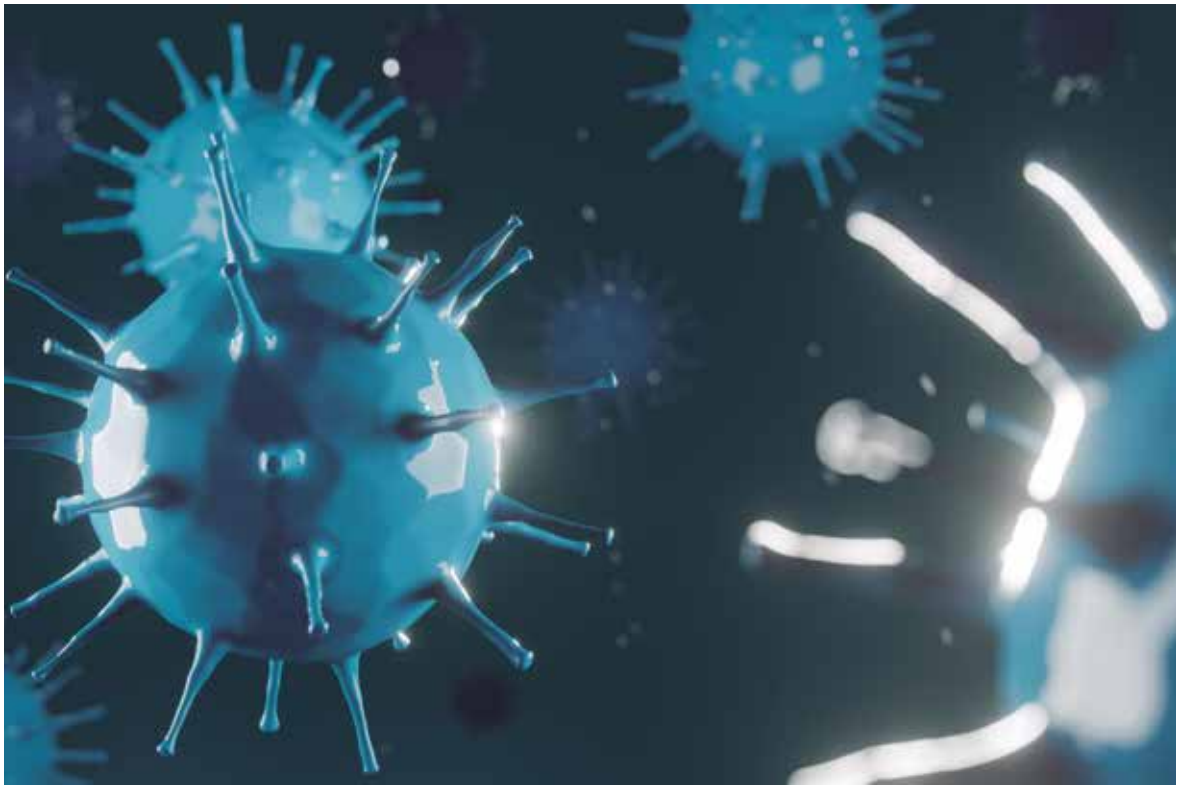
Coronavirus: enfoque de la UE de aplicaciones eficientes de rastreo de contactos para contribuir a la supresión gradual de las medidas de confinamiento

LOS ESTADOS MIEMBROS DE LA UE, CON EL APOYO DE LA COMISIÓN, HAN CREADO UN CONJUNTO DE INSTRUMENTOS PARA EL USO DE APLICACIONES MÓVILES DE RASTREO DE CONTACTOS Y ENVÍO DE ADVERTENCIAS CON EL FIN DE HACER FRENTE A LA PANDEMIA DE CORONAVIRUS. ESTO FORMA PARTE DE UN ENFOQUE COORDINADO COMÚN EN APOYO DE LA SUPRESIÓN GRADUAL DE LAS MEDIDAS DE CONFINAMIENTO, TAL COMO SE ESTABLECE EN UNA RECOMENDACIÓN DE LA COMISIÓN (EU) 2020/518 PRESENTADA EL 8 DE ABRIL DE 2020.

Desde el estallido de la pandemia de coronavirus, los Estados miembros, con el apoyo de la Comisión, han estado evaluando los aspectos de eficacia, seguridad y de la privacidad y protección de datos de las soluciones digitales para hacer frente a la crisis. Si respetan plenamente las normas de la UE y están bien coordinadas, las aplicaciones de rastreo de contactos y envío de advertencias pueden desempeñar un papel fundamental en todas las fases de la gestión de la crisis, especialmente cuando llegue el momento de ir suprimiendo gradualmente las medidas de distanciamiento social. Estas aplicaciones pueden complementar el rastreo manual de contactos existente y contribuir a romper la cadena de transmisión del virus. El conjunto de instrumentos va acompañado de directrices sobre la protección de datos para estas aplicaciones móviles, que se ha publicado el 20 de abril.

Este anuncio es el primero relativo a un conjunto de instrumentos comunes de la UE, creado con carácter de urgencia y en colaboración por la Red de Sanidad Electrónica y con el apoyo de la Comisión Europea. Ofrece una guía práctica para los Estados miembros a la hora de desplegar aplicaciones de rastreo de contacto y envío de advertencias. El conjunto de instrumentos establece los requisitos esenciales de estas aplicaciones:

- Deberán ser plenamente conformes con las normas de protección de datos y de la intimidad de la UE, expuestas en las directrices presentadas recientemente tras la consulta al Comité Europeo de Protección de Datos.
- Deberán desplegarse en estrecha coordinación con las autoridades de salud pública, y ser aprobadas por estas.
- Deberán instalarse de forma voluntaria y desinstalarse tan pronto como dejen de ser necesarias.
- Deberán tener por objeto explotar las últimas soluciones tecnológicas que refuercen la protección de la intimidad. Probablemente se basen en tecnología de proximidad Bluetooth, y no permiten el rastreo de la ubicación de las personas.
- Deberán basarse en datos anonimizados, pudiendo alertar a quienes hayan estado cerca de una persona infectada durante cierto período de tiempo para que se sometan a pruebas o se aíslen, pero sin revelar la identidad de las personas infectadas.



- Deberán ser interoperables en toda la UE para que los ciudadanos estén protegidos incluso cuando crucen las fronteras.
- Deberán basarse en directrices epidemiológicas aceptadas y reflejar las mejores prácticas en materia de ciberseguridad y accesibilidad.
- Deberán ser seguras y eficaces.

Aunque facilitan un rastreo más sencillo, rápido y eficiente que los sistemas tradicionales basados en entrevistas con los pacientes infectados, el rastreo manual seguirá aplicándose a los ciudadanos que puedan ser más vulnerables a la infección pero con menos probabilidades de poseer un teléfono inteligente, tales como las personas de edad avanzada o con discapacidad. En futuras versiones del conjunto de instrumentos podrá formularse un enfoque común sobre otras funcionalidades, por ejemplo, de información y seguimiento de síntomas.

El conjunto de instrumentos forma parte de un proceso en curso en el que los Estados miembros colaboran para planear y perfeccionar en las próximas semanas y meses la utilización de este y otras herramientas prácticas.

Los Estados miembros deberán informar acerca de sus acciones a más tardar el 31 de mayo de 2020 y poner las medidas a disposición de los demás Estados miembros y de la Comisión para su revisión por sus homólogos. La Comisión valorará los progresos realizados y publicará informes periódicos a partir de junio de 2020 y mientras dure la crisis, en los que recomendará la adopción de medidas o la eliminación gradual de las que ya no parezcan necesarias.

MÁS INFORMACIÓN:

- Comisión Europea – Reacción al Coronavirus - https://ec.europa.eu/info/live-work-travel-eu/health/coronavirus-response_en
- Comisión Europea - Coronavirus: An EU approach for efficient contact tracing – https://ec.europa.eu/commission/presscorner/detail/en/ip_20_670
- Recomendación de la Comisión (EU) 2020/518 - https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1587153139410&uri=CELEX:32020H0518

Apps y webs de autoevaluación del Coronavirus

LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD) HA PUBLICADO UN INFORME SOBRE LOS TRATAMIENTOS DE DATOS EN RELACIÓN CON EL COVID-19 Y UN COMUNICADO SOBRE LAS APPS Y WEBS DE AUTOEVALUACIÓN DEL CORONAVIRUS. LA AGENCIA HA CONSTATADO QUE SE ESTÁN LANZANDO INICIATIVAS, TANTO DESDE EL ÁMBITO PÚBLICO COMO DESDE EL PRIVADO, QUE SOLICITAN QUE LOS CIUDADANOS LES FACILITEN INFORMACIÓN PERSONAL, FUNDAMENTALMENTE RELACIONADA CON LA SALUD, AL AMPARO DE LA SITUACIÓN DE EMERGENCIA QUE VIVE NUESTRO PAÍS.

Estas iniciativas tienen un espectro amplio, desde el ámbito local al global, y utilizan apps o páginas web.

Ante esta situación, la Agencia recuerda los criterios que deben aplicarse para que el tratamiento de los datos personales sea lícito.

Los fundamentos que legitiman/hacen posible dichos tratamientos son la necesidad de atender las misiones realizadas en interés público, así como la de garantizar los intereses vitales de los propios afectados o de terceras personas.

Las finalidades para las que pueden tratarse los datos son, únicamente, las relacionadas con el control de la epidemia, entre ellas, las de ofrecer información sobre el uso de las aplicaciones de autoevaluación realizadas por las administraciones públicas o la obtención de estadísticas con datos de geolocalización agregados para ofrecer mapas que informen sobre áreas de mayor o menor riesgo.

> ***Si los ciudadanos utilizan aplicaciones o webs de las que no son titulares las autoridades públicas, sino que son ofrecidos por entidades o personas privadas, no existirá la legitimidad que se ha indicado anteriormente para el tratamiento de los datos***

Los datos que pueden obtenerse y utilizarse han de ser los que las autoridades públicas competentes consideren proporcionados/necesarios para cumplir con dichas finalidades.

Estos datos sólo podrán ser facilitados por quienes sean mayores de 16 años. En el caso de tratar datos de menores de 16 años, se requeriría de la autorización de sus padres o representantes legales.

Únicamente podrán tratar dichos datos las autoridades públicas competentes para actuar conforme a la declaración del estado de alarma, es decir, el Ministerio de Sanidad y las Consejerías de Sanidad de las Comunidades Autónomas, que podrán cederse datos entre ellas, y a los profesionales sanitarios que traten a los pacientes o que intervengan en el control de la epidemia.

Las entidades privadas que colaboren con dichas autoridades sólo podrán utilizar los datos conforme a las instrucciones de estas y, en ningún caso, para fines distintos de los autorizados.



Si los ciudadanos utilizan aplicaciones o webs de las que no son titulares las autoridades públicas, sino que son ofrecidos por entidades o personas privadas, no existirá la legitimidad que se ha indicado anteriormente para el tratamiento de los datos. En este sentido, es importante recomendar a los ciudadanos que sean especialmente cuidadosos a la hora de informarse de quién, para qué y con qué garantías van a tratarse sus datos personales.

En cuanto a la previsión de que todos aquellos ciudadanos que hayan dado positivo en la prueba del COVID-19 puedan ser geolocalizados a través del teléfono móvil que hayan facilitado previamente, de modo que se pueda llevar a cabo un seguimiento de su cuarentena, hay que partir de nuevo de las amplias competencias que en situaciones excepcionales, como sin duda lo es la presente epidemia, tienen las autoridades sanitarias, teniendo en cuenta, además, que una de las medidas excepcionales para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19 es la de limitar la libertad de circulación de las personas. De nuevo, nos encontramos ante una obligación impuesta por las autoridades sanitarias con el fin de evitar la propagación del virus, y que requiere un especial control de las personas que han dado positivo y que han sido obligadas a permanecer en su domicilio en cuarentena, así como también permite conocer las zonas con mayor número de afectados a fin de adoptar las medidas oportunas.

No obstante, el único dato que a los efectos de la geolocalización debería facilitarse a los operadores de telecomunicaciones, en su caso, sería el correspondiente al número de teléfono móvil que se tiene que geolocalizar, salvo que el Ministerio de Sanidad considerara que fuera imprescindible facilitar algún otro dato a los efectos del seguimiento de la enfermedad.

En todo caso, quienes pretendan obtener y tratar los datos de los ciudadanos deberán informarles de forma clara, accesible y fácilmente comprensible de todos los aspectos que se han descrito.

SECTOR
FARMACIA

Coordina: **Alberto Gómez Lafón**

Adherencia al Tratamiento y Aplicaciones Móviles

Almudena Martín Fernández
Subdirección General de Información Sanitaria. Ministerio de Sanidad

INTRODUCCIÓN

Independientemente de la enfermedad o la complejidad de la medicación, la tasa promedio de adherencia a la terapia con medicamentos crónicos es del 50%, aproximadamente (1).

Las intervenciones de adherencia se pueden dividir en: técnicas, conductuales, educativas y multifacéticas o complejas (2). El uso de aplicaciones móviles para mejorar la adherencia terapéutica y el comportamiento del paciente a través de un sistema de recordatorio, es el tipo más común de intervención conductual, dirigiéndose a los pacientes que se olvidan de tomar su medicación.

PILARES FUNDAMENTALES PARA QUE LAS APLICACIONES MÓVILES SEAN ÚTILES PARA LA MEJORA DE LA ADHERENCIA TERAPÉUTICA

Estas aplicaciones se pueden clasificar en tres tipos según sus funcionalidades: recordatorios de medicamentos simples, recordatorios de medicamentos avanzados y aplicaciones de gestión de medicamentos (3).

Para que una aplicación móvil sea útil y segura para el usuario se debe centrar en varios pilares:

1. El usuario o paciente: cada vez más los más pacientes están más formados e informados sobre su enfermedad, lo que facilita su autogestión. Sin embargo, en este punto hay que tener en cuenta la conocida como "brecha digital".
2. Los médicos o profesionales sanitarios: necesitan sentirse seguros de que las aplicaciones hayan demostrado que realmente funcionan, son seguras y útiles para los pacientes.
3. El tipo de aplicación móvil que se utiliza: hay aplicaciones móviles para la adherencia terapéutica que tienen características básicas (alerta para tomar la medicación o seguimiento de las tomas), y otras poseen características más avanzadas como una base de medicamentos, posibilidad de almacenar datos en la nube, puede exportar/sincronizar y enviar datos al médico, e incluso algunas se basan en la gamificación para conseguir los objetivos de adherencia.
4. Diseño de la aplicación: cualquier persona o entidad puede desarrollar una aplicación móvil. El reto para que estas aplicaciones ofrezcan todo su potencial está en cumplir estándares, garantizar la calidad e integridad de los datos e implicar a todas las partes interesadas en el desarrollo
5. Evaluación de las aplicaciones: entre la gran cantidad de aplicaciones disponibles en las plataformas de descarga hay que seleccionar, en la medida de lo posible, aquellas que estén certificadas por algún organismo o hayan sido evaluadas mediante algún método, teniendo en cuenta que no existe una regulación común para este tipo de aplicaciones móviles.
6. Privacidad y protección de datos: las aplicaciones móviles deben cumplir el Reglamento



General de Protección de Datos (4). Es también responsabilidad del usuario descargar sólo aquellas aplicaciones que cumplan con este Reglamento.

CONCLUSIÓN

La utilización de una aplicación móvil para mejorar la adherencia es un enfoque novedoso, que está constantemente accesible, involucra y educa al paciente, y proporciona un depósito de información específica sobre el paciente y la medicación, pero la falta de interoperabilidad con otros sistemas, representa una barrera para su desarrollo. Estas aplicaciones son baratas, escalables, ubicuas y accesibles para cualquier persona con teléfono móvil inteligente. Se necesita más investigación para conocer si las aplicaciones móviles pueden mejorar la adherencia y los resultados terapéuticos.

BIBLIOGRAFÍA

(1) Fundación Farmaindustria. (2016). Encuesta sobre adherencia terapéutica en España. Madrid: Fundación Farmaindustria. Disponible en: http://www.farmaindustria.es/web/documento/encuesta-adherencia-terapeutica-espana/

(2) Patel, S., Jacobus-Kantor, L., Marshall, L., Ritchie, C., Kaplinski, M., Khurana, P.S., y Katz, R.J. (2013). Mobilizing your medications: an automated medication reminder application for mobile phones and hypertension medication adherence in a high-risk urban population. Journal of diabetes science and technology, 7 (3), 630-639. Doi: 10.1177/193229681300700307. Disponible en: hhtp//www.ncbi.nlm.nih.gov/pmc/articles/PMC3869130/pdf/dst-07-0630.pdf

(3) Stawarz, K., Cox, AL. Y Blandford, A. (2014). Doń t forget your pill! Designing effevtive medication reminder apps that support user's daily routines. In: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. (pp. 2269-2278). New York (USA): ACM. Doi: 10.1145/2556288.2557079. Disponible en: http://discovery.ucl.ac.uk/1418104/1/StawarzCoxBlandford2014-reminders-dubmittedManuscript.pdf

(4) Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Disponible en: hhtp//www.ncbi.nlm.nih.gov/pmc/articles/PMC3869130/pdf/dst-07-0630.pdf

SECTOR
ENFERMERÍA

Nursing Now Euskadi
@eusakdiNow

Coordina: **Inmaculada Moro**

2020, el año de las enfermeras y matronas. ¿Que és *Nursing Now*?

NURSING NOW (HTTPS://WWW.NURSINGNOW.ORG/) ES UNA CAMPAÑA GLOBAL DE TRES AÑOS REALIZADA EN COLABORACIÓN ENTRE EL CONSEJO INTERNACIONAL DE ENFERMERAS Y LA ORGANIZACIÓN MUNDIAL DE LA SALUD. SE TRATA DE UN PROGRAMA QUE SURGE EN RESPUESTA A LOS HALLAZGOS IDENTIFICADOS EN EL INFORME "TRIPLE IMPACT" (HTTP://WP.AMEENFERMERIA.COM/WP-CONTENT/UPLOADS/2019/08/TRIPLE-IMPACTO_ESP.PDF).

Este informe concluye que el desarrollo de la enfermería genera un triple impacto en la comunidad: mejora la salud, la igualdad de género y contribuye a la construcción de economías más sólidas. De acuerdo a ello, esta campaña tiene como objetivo mejorar la salud de la población a nivel mundial mediante la potenciación de las competencias y las actividades de la enfermería.

La campaña se centra en cinco áreas centrales:

1. Asegurar que las enfermeras y las matronas tengan una voz más destacada en la formulación de políticas de salud;
2. Fomentar una mayor inversión en la fuerza laboral de enfermería;
3. Abogar por más enfermeras en posiciones de liderazgo;
4. Fomentar la innovación y la investigación que ayuden a determinar dónde las enfermeras pueden tener el mayor impacto
5. Compartir ejemplos de mejores prácticas de enfermería.

Nos enfrentamos a enormes desafíos en la atención sanitaria como consecuencia del envejecimiento de la población, el aumento de enfermedades crónicas, y la sostenibilidad del sistema sanitario. En este contexto, es preciso aprovechar al máximo el potencial del personal de enfermería, las enfermeras y los enfermeros están llamados a adquirir una mayor responsabilidad y protagonismo, siendo una parte fundamental de la solución a los desafíos emergentes.

La enfermería se presenta, como un tractor de cambio para la transformación de las políticas de salud, ofreciéndose para liderar de forma colaborativa programas y proyectos transversales de salud junto con otros agentes, y como nexo de unión con aquellos implicados en el diseño de las políticas de salud.

La campaña *Nursing Now* engloba a profesionales de todos los entornos sanitarios (socio-sanitario, comunitario, hospitalario) y ámbito de actuación (asistencial, gestor, docente e investigador), tanto del sector público como del privado. El cambio debe venir tanto desde las instituciones, como de cada profesional individual.

Se ha convertido en un movimiento social en crecimiento con una red activa de grupos que trabajan para influir en la política global y nacional. A día de hoy, existen 266 grupos de *Nursing Now* activos en 89 países con nuevos grupos que se registran y lanzan cada mes, y a la que se ha sumado).

La campaña se extenderá hasta finales de 2020, año del bicentenario del nacimiento de Florence Nightingale y en que las enfermeras de todo el mundo celebraremos el Año de la Enfermera y la Matrona. España se ha adherido a la campaña con la firma de la Ministra de Sanidad Mª Luisa Carcedo y el Consejo General de Enfermería, así como 18 grupos regionales apoyados por los gobiernos autonómicos de cada CC AA y Ceuta y Melilla, asociaciones profesionales, grupos profesionales y otros agentes de interés, buscamos la movilización goblal... Y tú... ¿te sumas también a *Nursing Now*?

INFORMÁTICA **MÉDICA**

Coordina: **José Sacristán**

Tratar trastornos mentales con nuevas tecnologías, un fenómeno imparable

Woebot es un robot de asistencia psicológica. Ese ser que chatea contigo cuando todo se pone feo, ese que se preocupa a diario por tus emociones es simplemente un programa informático, inteligencia artificial especialmente diseñada para tratamientos psicológicos cotidianos. No hay nadie detrás, más allá de los ingenieros que la crearon. Pero va aprendiendo de sus miles de experiencias con miles de pacientes, y da el pego.

Este tipo de chatbots son solo un ejemplo extremo de cómo la tecnología está incidiendo en el campo de la atención psicológica. Las llamadas ciberterapias son acogidas de buena gana por muchos psicólogos, sobre todo para tratar determinados procesos, pero también causan ciertas inquietudes, en especial en el tratamiento de los datos.



https://retina.elpais.com/retina/2020/04/10/innovacion/1586539741_202944.html



https://www.technologyreview.es/s/11849/nace-la-primera-ia-capaz-de-identificar-las-relaciones-causa-efecto

Nace la primera IA capaz de identificar las relaciones causa-efecto

La técnica, inspirada en la criptografía cuántica, podría revolucionar el diagnóstico médico al aprovechar grandes bases de datos de salud para encontrar vínculos causales. Probada con conjuntos de datos bien estudiados, esta inteligencia artificial ha señalado los mismos vínculos.

Los investigadores del proveedor de atención médica digital con sede en Reino Unido Babylon Health, Anish Dhir y Ciarán Lee han ideado una técnica para encontrar relaciones causales en diferentes conjuntos de datos. Un hallazgo que permitiría crear grandes bases de datos con información médica no usada para detectar causas y efectos, y posiblemente también habilitaría el descubrimiento de nuevos vínculos causales. La aplicación estábasada en un chatbot que solicita al paciente una descripción de sus síntomas antes de ofrecer un diagnóstico tentativo y consejos sobre el tratamiento.

NOTICIAS DEL SECTOR

Coordina: **Diego Sáez**

■ **El Servicio de Salud de Castilla-La Mancha** va a participar en un proyecto para el desarrollo de herramientas que utilizan la inteligencia artificial para el diagnóstico de lesiones en la piel. Utilizando las imágenes de lesiones dermatológicas se aplicará una tecnología de procesamiento, para validar su precisión diagnóstica y fiabilidad, con el objetivo de que sirva de ayuda a los profesionales médicos en el procesamiento de imágenes a distancia. Este proyecto se pone en marcha tras el acuerdo de colaboración firmado entre el SESCAM y Ernest & Young (EY), empresa que desarrolla herramientas informáticas capaces de leer e interpretar las imágenes y generar algoritmos inteligentes de reconocimiento. El SESCAM cuenta con un sistema de Historia Clínica Electrónica implantado en todos los centros asistenciales de la región y más de una década de experiencia de registros unificados, lo que facilita el entorno adecuado para el estudio.

■ **El Servicio de Salud de Castilla-La Mancha (Sescam)** aplicará telemedicina a los pacientes de zonas rurales. El SESCAM está trabajando en un modelo de servicio sanitario que dé respuesta al nuevo perfil de la ciudadanía, introduciendo tecnologías emergentes e innovación en la provisión de servicio desde múltiples canales, presencial y no presidencial, asegurando la calidad y la seguridad y añadiendo valor a la salud y a la experiencia de las personas. Así se ha puesto de manifiesto en la primera reunión mantenida entre representantes del Sescam, de la Comisión Europea y la empresa consultora Everis, una sesión de arranque de este proyecto innovador para mejorar la calidad de atención al paciente, sobre todo en zonas rurales para reducir la necesidad de desplazamientos, teniendo en cuenta el contexto de esta región, con más de dos millones de habitantes, una dispersión territorial de 80.000 kilómetros cuadrados, más de 25.000 profesionales y más de 1.300 Centros de Salud y Consultorios de Atención Primaria.



https://www.latribunadealbacete.es/noticia/ZDD5B6249-0F8C-3F86-7184C38C618CB5CB/202001/El-Sescam-aplicara-telemedicina-en-las-zonas-rurales

■ **El SESCAM publica el anuncio previo del concurso "ISOHCE:** Modelo de Historia Clínica Electrónica estándar, interoperable y multiregional: El anuncio previo se encuentran publicadas en el portal de contratación del Estado."



■ **Cecilio Venegas, presidente del Colegio Oficial de Farmacéuticos de Badajoz,** ingresó el pasado 13 de febrero de 2020 en la Real Academia Nacional de Farmacia del Instituto de España..

AGENDA 2020

SOCIEDAD ESPAÑOLA DE INFORMÁTICA DE LA SALUD

X REUNIÓN DEL FORO DE INTEROPERABILIDAD EN SALUD

Fecha: Pendiente situación sanitaria

(en virtual y presencial limitada)

Lugar: Vitoria

XXVII JORNADAS NACIONALES DE INNOVACIÓN Y SALUD EN ANDALUCÍA

Fecha: 3-20 junio talleres virtuales.

Convocatoria presencial pendiente situación sanitaria

Lugar: Málaga

X FORO PARA LA GOBERNANZA DE LAS TIC EN SALUD

Fecha: 6 y 7 octubre

Lugar: Zaragoza

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

Fecha: Noviembre

Lugar: Escuela Nacional de Sanidad

XVIII REUNIÓN DE SALUD CONECTADA

Fecha: 18 y 19 noviembre

Lugar: Murcia

7ª edición



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

DIPLOMA DE EXPERTO EN GESTIÓN DIRECTIVA DE LAS TIC EN SALUD

DIPLOMA DE EXPERTO TIC EN EL SISTEMA SANITARIO

DIPLOMA DE EXPERTO EN TECNOLOGÍAS Y SOLUCIONES TIC EN SALUD

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

DIRIGIDO A:

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

PROGRAMA

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

Comienzo: noviembre 2020

Plazo de Matriculación: Hasta el 15 de octubre de 2020

EQUIPO DOCENTE

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

Duración: 1 año académico (60 ECT´s) o (15 ECT´s por diploma y por trabajo fin de master y otras actividades)

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

Becas y Ayudas

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

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

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

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

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