it

Retos y soluciones para una Sanidad en cambio

Patrocinadores:

ARMIS

iBERLAYER Cloud Email Security

logitech

MicroStrategy

SOPHOS

STORMSHIELD

Retos y soluciones para una Sanidad en cambio

La pandemia del coronavirus ha puesto en evidencia la necesidad de acelerar la transformación digital de prácticamente todos los sectores. En España, al igual que en el resto del mundo, una de las áreas que más afectada se ha visto por su propia naturaleza ha sido la de la sanidad, que se ha enfrentado a una situación sin precedentes que ha obligado a buscar nuevos modelos de atención basados en la tecnología.

Durante estos últimos años, hemos sido testigos de un momento de gran aceleración en la adopción de nuevas tecnologías en todos los sectores. Uno de los más importantes ha sido el sanitario, donde la pandemia ocasionada por la COVID-19 ha puesto de manifiesto la necesidad acuciante de implantar soluciones tecnológicas que dieran respuesta a los grandes retos del presente y del futuro. En una crisis de salud pública como la que vivimos se ha evidenciado que las organizaciones sanitarias no estaban preparadas para atender de forma personalizada a pacientes que no llegaran a través de las vías habituales.

RETOS Y SOLUCIONES PARA UNA SANIDAD EN CAMBIO

Desde la aparición de los primeros casos en febrero de 2020, son ya 11,3 millones de personas las que se han infectado con la Covid-19, y se contabilizan 101.703 fallecidos, a fecha de marzo de 2022. Con estas cifras, España ocupa la décima posición a nivel mundial en cuanto a número de casos confirmados de coronavirus.

Estas cifras han puesto de manifiesto una serie de nuevos retos que ha tenido que afrontar el sector de manera acuciante. Accenture señala en su informe Rapid Response seis retos principales: incremento de pacientes, sobrecarga de llamadas al servicio, monitorización y reporting, coordinación en la respuesta, peligros en la continuidad de la actividad y eficacia del personal.

Como indican las cifras de infectados, el primer reto al que tuvo que hacer frente el sector sanitario ha sido el del incremento de pacientes, que ha llegado casi a colapsar el sistema en momentos determinados. Es por ello que se necesitaron tomar medidas de urgencia, como la utilización de pabellones multiusos para las campañas de vacunación, plantas enteras de hospitales dedicadas a pacientes con Covid e incluso la construcción de nuevos centros hospitalarios para poder dar servicio a la población infectada. Esta sobrecarga de pacientes también se vio reflejada en las líneas telefónicas, con las centralitas de los centros sanitarios completamente colapsadas por las llamadas de los pacientes en busca de información.

Además, la necesidad de mantener una monitorización constante sobre toda la situación se convirtió en una prioridad, de manera que esa recogida de datos de lo que estaba sucediendo permitiera a las autoridades sanitarias tomar las mejores decisiones en función de cómo iban evolucionando las cifras de la pandemia. Otro de los retos más importantes que está encarando el sector es el de la coordinación en la respuesta, para ofrecer al ciudadano información precisa en cuanto a la situación y a las medidas necesarias que debiera tomar en función de su situación.

En España, al igual que en el resto del mundo, una de las áreas que más afectada se ha visto por su propia naturaleza ha sido la de la sanidad, que se ha enfrentado a una situación sin precedentes que ha obligado a buscar nuevos modelos de atención basados en la tecnología

Esta situación afectó directamente al colectivo de los profesionales de la salud, que al estar en primera línea, sufrieron directamente las consecuencias de la pandemia, llegando a contraer el virus hasta el 20% del colectivo en algunos casos, lo que suponía un problema a la hora de poder dar un servicio ya de por sí colapsado por el gran número de contagios que se estaban dando. Además, en muchas ocasiones este personal no contaba con los recursos necesarios para poder dar un servicio de calidad, ni a nivel de protección, ni a nivel tecnológico, en un sector que en la mayoría de los casos no había dado muchos pasos para afrontar su transformación digital.

LA HORA DE LA TELEMEDICINA

Para afrontar esta situación, en una pandemia cuya base ha sido la distancia social y el confinamiento de las personas infectadas, uno de los primeros campos que tuvo que revolucionar el sector sanitario fue el de la asistencia, apostando por un modelo remoto a través de la telemedicina, algo que hasta la fecha no era nada común. Un estudio de Capterra señala que un 62% de los españoles ha consultado al médico por medio de esta tecnología a raíz de la pandemia, e incluso para el 92% de las personas había sido su primera vez.

La implantación de este nuevo modelo ha sido todo un éxito, como demuestran datos como los de mediQuo, que señalan que las consultas de telemedicina habían aumentado un 153% en España a los pocos meses desde que se decretara el estado de alarma. Claramente se trata de un modelo que ha llegado para quedarse. Incluso la Organización para la Cooperación y el Desarrollo Económicos (OCDE) señalaba en un informe la necesidad de fortalecer los servicios de salud prestados de forma electrónica a través de internet.

El informe "Telemedicine: Emerging Technologies, Regional Readiness & Market Forecasts 2021-2025" de Juniper Research indica que gracias a la telemedicina el sector sanitario podrá ahorrar 21.000 millones de dólares en costes para el año 2025 y señala que para ese año ya se habrán realizado más de 765 millones de teleconsultas a nivel global.

Pero la velocidad a la que se ha impuesto este nuevo modelo hace que tanto profesionales sanitarios como pacientes se enfrenten a una serie de retos que tendrán que ir afrontando poco a poco. Uno de los más importantes es el de la reducción de la brecha digital, algo a lo que ayudaron mucho otros sectores como las compras online o las videollamadas con la familia durante el confinamiento, que pusieron sobre la mesa estas tecnologías para toda la población. Además, los profesionales sanitarios requieren de formación específica en el uso de esta nueva modalidad, de manera que sean capaces de ofrecer la mejor experiencia al paciente, ofreciéndole la mayor cercanía posible. Otro reto es el puramente tecnológico, con la necesidad de equipos

y conexiones de calidad que no entorpezcan la videoconsulta.

LOS DATOS Y SU CONFIDENCIALIDAD

Como en la mayoría de las industrias, la importancia del dato es primordial para ofrecer un servicio de calidad al paciente. En el caso del sector sanitario más si cabe, puesto que se trata de datos inherentes a las personas, con lo que la necesidad de mantener la confidencialidad médico-paciente se vuelve mucho más acuciante si cabe.

Por un lado, el sector utiliza todo el aglomerado de datos abiertos que puede obtener con el fin de optimizar su gestión y la organización de recursos, como indica el estudio "The Open Data Impact Map" de Open Data for Development Network (OD4D). Esto es muy importante en casos como el de la medicina preventiva, ya que permite el desarrollo de modelos predictivos capaces de diseñar patrones de comportamiento, que a través del análisis de los datos facilita una mejor atención del paciente, predecir su evolución e incluso adelantarse a sus necesidades.

El Big Data es un sector que está creciendo exponencialmente en todos los ámbitos, como demuestra el estudio de Technavio "Big Data Market by Type, Deployment, and Geography - Forecast and Analysis 2021-2025" que señala que para 2025 este mercado crecerá hasta los 247.300 millones de dólares con un CAGR del 18%. En concreto aplicado a la salud, el informe Big Data Analytics In Healthcare Market de Allied Market Research indica que su valor alcanzará los 67.820 millones de dólares para 2025.

En los proyectos estratégicos para la recuperación y transformación económica (PERTE), el Gobierno de España ha tenido muy en cuenta al sector sanitario, estableciendo un PERTE para la salud de vanguardia

En el sector sanitario se recaban una gran cantidad de datos que pueden provenir de diferentes fuentes: desde la información proporcionada por la maquinaria médica (pruebas de imagen y de laboratorio), hasta la información aportada por el propio paciente. La recogida, almacenamiento, tratamiento y posterior análisis de esos datos debe seguir un cuidadoso protocolo que permita facilitar la labor de los profesionales de la salud, para que puedan disponer de ellos siempre que los necesiten de una forma rápida y sencilla, pero teniendo en cuenta la importancia máxima de su seguridad, de manera que no haya brechas ni a la hora de almacenarlos ni en el momento de ser transferidos, sea por el medio que sea.

Para ello, la tecnología se pone al servicio del sector, por lo que es tarea de las organizaciones de salud implementar las soluciones adecuadas a la hora de velar por la privacidad de los datos, de contar con los dispositivos adecuados para su recogida y almacenamiento, y de preparar a los profesionales que están en contacto con ese dato, de manera que realicen un tratamiento y mantenimiento correcto.

EL GRAN RETO DE LA SEGURIDAD

Por si era poco la situación de pandemia que se desató a principios de 2020 con la aparición del coronavirus, el sector sanitario ha tenido que enfrentarse en este tiempo a un nuevo reto, el gran aumento de ciberataques que se ha producido con el punto de mira puesto en la industria de la salud. El pasado año, el Instituto Nacional de Ciberseguridad de España (INCIBE) señalaba que más de 500 instituciones sanitarias españolas habían notificado incidentes o reportes de vulnerabilidad, lo que suponía un 48% más con respecto al año anterior.

Uno de los principales riesgos a los que se enfrenta el sector sanitario es el de los ataques de ransomware, a través de los cuales el ciberdelincuente es capaz de cifrar toda la información del sistema para pedir un rescate a cambio de su liberación. Este tipo de ataques se han multiplicado en los últimos años. Según el informe "El estado del ransomware en la sanidad 2021" de Sophos, algo más de un tercio de las organizaciones sanitarias españolas (34%) recibieron algún tipo de ataque de ransomware el año pa-

sado. Para poder recuperar sus datos, el 34% decidió pagar el rescate, ya que no consiguieron hacerlo de otra forma, como demuestra que solo el 44% de las instituciones sanitarias consiguieron restaurar sus datos a través de copias de seguridad. Estos datos ponen de manifiesto el éxito que tiene este tipo de ataques para los ciberdelincuentes, lo que explica este aumento en los últimos años.

Pero el ransomware no es el único peligro que amenaza al sector sanitario. Las fugas de datos también están a la orden del día, como demuestran los datos de Bitglass, que indican que tan solo en Estados Unidos se produjeron 599 fugas de información en esta industria que afectaron en conjunto a más de 26 millones de personas. Sistemas desactualizados, tráfico de correo electrónico no cifrado, el Internet de las Cosas cada vez con mayor penetración en el sector sanitario, son muchos los riesgos que se presentan para un sector que ha tenido que afrontar una transformación digital de la noche a la mañana, para la que en muchas ocasiones se primó la necesidad de activar determinados servicios sin pararse a pensar en las capas de protección que serían necesarias para mantenerlos seguros.

Para ayudar a securizar los nuevos entornos digitales creados tras la pandemia, el Instituto Nacional de Ciberseguridad (INCIBE) ha publicado una serie de pliegos por sectores denominados Sectoriza2 con una serie de consejos y herramientas que ayudarán a las organizaciones a protegerse, incluyendo como no podía ser de otra manera también al sector sanitario.

PERTE PARA LA SALUD DE VANGUARDIA

Entre los proyectos estratégicos para la recuperación y transformación económica (PERTE), el Gobierno de España ha tenido muy en cuenta al sector sanitario, estableciendo un PERTE para la salud de vanguardia a finales del pasado año 2021. Su finalidad es la de apoyar la transformación digital de la industria sanitaria y prevé una inversión entre el sector público y el privado de 1.469 millones de euros en el periodo 2021 y 2023.

Los cuatro grandes objetivos que persigue este plan son posicionar a España como país líder en la innovación y desarrollo de terapias avanzadas, impulsar la puesta en marcha de medicina personalizada de precisión de forma equitativa, desarrollar un Sistema Nacional de

Salud digital y potenciar la atención sanitaria primaria a través de la transformación digital.

Como demuestras estos objetivos, el impulso de la transformación digital del sector es un hecho. Por un lado, el Componente 11 (Modernización de las administraciones públicas) está orientado al establecimiento de diferentes medidas para la modernización de los servicios digitales ofrecidos por el Ministerio de Sanidad en tres áreas principales de actuación: el desarrollo de servicios digitales e inteligentes, la interoperabilidad de la información sanitaria y el impulso a la analítica de datos.

Por otro lado, el Componente 18 hace mención de un Data Lake sanitario, que supone la creación de un repositorio de datos alimentado por los diferentes sistemas de información relevantes en Salud y que permitirá un análisis masivo e inteligente de los mismos, con capacidad de respuesta en tiempo real, orientado a la protección de la salud, la predicción sanitaria, así como para el incremento en la eficiencia del diagnóstico, tratamiento y rehabilitación de enfermedades, en las condiciones adecuadas de ciberseguridad.

Además, el Componente 19 hace mención a la necesidad de que los profesionales sanitarios también adquieran competencias digitales avanzadas dentro de los programas de formación, con menciones específicas a tecnologías disruptivas como la Inteligencia Artificial o la robótica, sin dejar de lado la ciberseguridad. ■

MÁS INFORMACIÓN

- Número acumulado de casos confirmados y muertes del coronavirus en España entre el 15 de febrero de 2020 y el 18 de marzo de 2022 de Statista
- Número de casos confirmados de coronavirus en el mundo a fecha de 18 de marzo de 2022, por país de Statista
- Informe Rapid Response de Accenture
- Diario Médico: profesionales sanitarios infectados por el coronavirus en España
- Capterra: Telemedicina en España: la irrupción tecnológica en la relación paciente-médico
- mediQuo: La razón por la que los médicos se deben adaptar a la nueva normalidad
- OECD Economic Surveys Spain
- Informe "Telemedicine: Emerging Technologies, Regional Readiness & Market Forecasts 2021-2025" De Juniper Research
- Estudio "The Open Data Impact Map" de Open Data for Development Network (OD4D)
- Estudio Technavio "Big Data Market by Type, Deployment, and Geography - Forecast and Analysis 2021-2025"
- Informe Allied Market Research Big Data Analytics In Healthcare Market
- Datos sobre aumento de ciberataques al sector sanitario del Instituto Nacional de Ciberseguridad de España (INCIBE)
- Informe "El estado del ransomware en la sanidad 2021" de Sophos
- Informe Bitglass sobre fugas de datos en el sector sanitario de Estados Unidos
- Sectoriza2 Salud, Instituto Nacional de Ciberseguridad de España (INCIBE)
- PERTE para la salud de vanguardia

SOLUCIONES LOGITECH PARA **ENTORNOS SANITARIOS**

Conéctese a través de vídeo de alta calidad cuando y donde sea más necesario.

Retos y Soluciones para una Sanidad en cambio

En el sector sanitario, la pandemia provocada por la Covid-19 ha puesto de manifiesto la necesidad acuciante de implantar nuevas soluciones tecnológicas que dieran respuesta a los grandes retos a los que se enfrenta el sector. Necesitamos una nueva forma de atención digital, una telemedicina que consiga conectar con los pacientes de forma preventiva y que los datos médicos sensibles y su análisis estén siempre disponibles y se pueda acceder a ellos de manera segura.

La llegada de la pandemia del coronavirus supuso una aceleración para la transformación digital de prácticamente todos los sectores, pero impactó a uno de ellos directamente: la sanidad. El sector sanitario se vio en la necesidad de realizar un cambio en sus procesos y aceleró su digitalización a pasos agigantados, tanto a la hora de hablar de teleasistencia como de los datos que manejan las organizaciones sanitarias, en muchos casos de una sensibilidad extrema. Esta rapidez a la hora de adoptar estos nuevos modelos no siempre se vio acompañada de un cuidado por la seguridad, lo que ha implicado grandes riesgos tanto para las propias instituciones sanitarias, como para el ciudadano. Por ello, el sector se enfrenta a una serie de importantes retos a los que debe dar solución de manera rápida y eficaz. Para hablar sobre cómo ha sido la transformación digital de la sanidad y cuáles son

MESA REDONDA IT: Retos y Soluciones para una Sanidad en cambio

“La visibilidad y el inventario de lo que tengas es la base para empezar a hacer políticas, segmentaciones de las redes, para intentar estar lo más seguro posible”

VESKU TURTIA

los principales retos a los que se enfrenta, hemos contado en esta Mesa Redonda IT con la participación de Vesku Turtia, Regional Director España y Portugal de Armis; David Marco, CEO de Iberlayer; Javier Rodríguez, Senior Key Account Manager de Logitech; Fernando Gutiérrez, Account Executive de MicroStrategy; Álvaro Fernández, Enterprise Account Executive de Sophos y Borja Pérez, Country Manager de Stormshield.

ESTADO ACTUAL DEL SECTOR SANITARIO

La mesa redonda comenzó agradeciendo a los profesionales sanitarios los esfuerzos que han realizado durante la pandemia, y que siguen realizando aún a día de hoy. En cuanto al estado actual del sector, para David Marco ha habido una evolución gigantesca. “Vemos una clara progresión hacia adelante, en cuanto a la integración de tecnologías dentro de la sanidad, ha mejorado en todos los sentidos, en lo personal, en lo tecnológico…”. El portavoz señala que muchos aspectos han mejorado muchísimo, como por ejemplo la teleatención. A pesar de ello, cree que hay un pequeño desfase en cuanto a la responsabilidad que tienen estos profesionales y las capacidades que se les dan.

Javier Rodríguez señala que ha habido un cambio de paradigma que ha sucedido de forma muy acelerada, por lo que han surgido algunas carencias. Por ejemplo, en el área de la videocolaboración. “No se ha hecho teniendo en cuenta la tecnología adecuada de audio y video y al final hay mucho por mejorar en ese ámbito”. Puede haber muchas vías de mejora para reducir colas en la atención primaria, para realizar algunas consultas que no requieran exploración de manera remota o para dar mejor calidad a los pacientes, que tengan que evitar desplazamientos y descongestionar un poco los centros de salud.

Por su parte, Fernando Gutiérrez cree que el estado de la sanidad en general en España en relación al dato ha salido reforzado. “Siempre se ha tenido el dato en cuenta, pero esta situación de necesidad tan brutal ha puesto de manifiesto la necesidad de apoyarse en el dato para tomar

“Si sigo construyendo la casa cogiendo piezas de la parte de abajo para crecer en altura cada vez más, pero usando materiales de abajo, llega un momento en que lo de arriba pesa tanto y lo de abajo es tan débil que no va a aguantar”

DAVID MARCO

decisiones y para la gestión”. En esos momentos que se vivieron y que se siguen viviendo de estrés es donde se ponen a prueba todos los sistemas, las cosas que funcionan bien, las cosas que tienen área de mejora… Se ha visto que esa necesidad de analizar de manera inmediata la disponibilidad de camas, de material o de personal, ha hecho que el dato haya cobrado mayor importancia.

UNA ACELERACIÓN EN SU TRANSFORMACIÓN DIGITAL

Sin duda la pandemia creo una situación sin precedentes ante la que prácticamente nadie estaba preparado. ¿La situación vivida durante estos

“Ha habido un despliegue acelerado y masivo de las plataformas de colaboración, pero hay mucho campo de mejora en dotar de los dispositivos adecuados para que los equipos médicos puedan colaborar a distancia”

JAVIER RODRÍGUEZ

últimos años de pandemia ha supuesto una aceleración en los procesos de transformación digital de la sanidad?

Para Vesku Turtia es un rotundo sí. Durante la pandemia no solo el sector de la salud, sino que todos los sectores han acelerado su transformación digital. “Lo que veo ahora con muchísima alegría es también que en el uso de distintos aparatos médicos en los hospitales tanto del sector privado como del público, están poniendo foco para ver cómo se puede securizar el uso de los sistemas médicos, porque hoy en día los hospitales, tanto del sector público como del privado, están bastante digitalizados”. Como vivimos en un mundo que no es perfecto, los ataques de ransomware pueden afectar a los sistemas de IT de un centro hospitalario, pero también ese mismo malware puede entrar en equipos médicos e incluso poner en peligro a los pacientes. “Vamos bien, pero todavía queda mucho que hacer”.

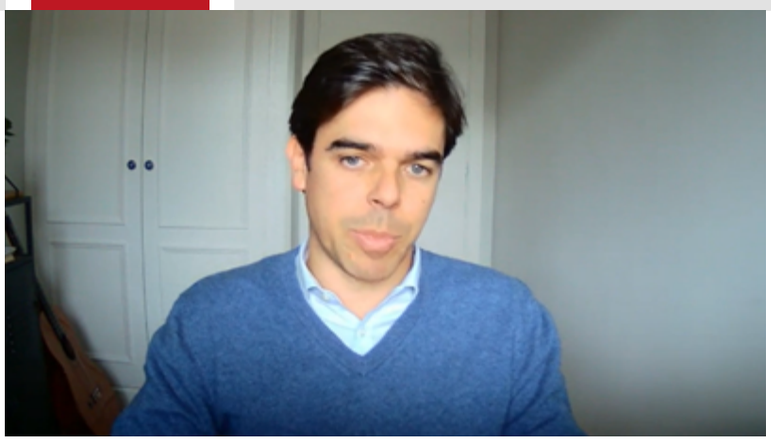
En palabras de Fernando Gutiérrez, “la sanidad no podía estar fuera de esta transformación digital”. La necesidad ha supuesto un acelerón de la digitalización, de eso no hay duda y pasa en general en todos los sectores, pero esta transformación digital ha venido muy propiciada también porque ha habido una digitalización del usuario. “La sanidad se ha encontrado con un ciudadano también más abierto, más preparado para utilizar canales digitales”. En cuanto a las personas mayores, que conforman gran parte de los usuarios de los servicios médicos, ha sido la necesidad de otros sistemas, como las compras online o las videollamadas con la familia, lo que ha conseguido que se digitalizaran.

Según Álvaro Fernández, ha habido sectores que habían avanzado más en su transformación digital porque se había demandado por parte de los usuarios. En el sector de la sanidad, al igual que por ejemplo en el de la educación, quizá no hubo esa demanda, que surgió a raíz de la pandemia y se tuvo que hacer de forma precipitada. “Desde el punto de vista de la seguridad, las prisas son enemigas de la securización. Se han priorizado los servicios perjudicando de alguna forma el hacer esos servicios seguros”. Además, añadía que “la pandemia hizo que todas las organizaciones de salud sin excepción pisasen el acelerador y fuesen a modelos más digitales para poder seguir dando un servicio”. Estas organizaciones están trabajando ahora en terminar de securizar estos servicios y en consolidarlos.

“Siempre se ha tenido el dato en cuenta, pero esta situación de necesidad tan brutal ha puesto de manifiesto la necesidad de apoyarse en el dato para tomar decisiones y para la gestión”

FERNANDO GUTIÉRREZ

Borja Pérez es de la opinión que hay distintos ritmos de transformación digital según las organizaciones. Para explicar su afirmación, saca a colación el PERTE que se ha aprobado para sanidad, el cual está dotado con 1.500 millones de euros y en el que hay cuatro grandes áreas



“Desde el punto de vista de la seguridad, las prisas son enemigas de la securización. Se han priorizado los servicios perjudicando de alguna forma el hacer esos servicios seguros”

ÁLVARO FERNÁNDEZ

de trabajo, una de ellas para la transformación digital en la atención primaria. “Las autoridades son conscientes de que hay que avanzar en ese sentido, pero hoy por hoy la atención primaria por ejemplo todavía adolece de falta de medios”. Después hace referencia a que los envíos de datos no son siempre del todo seguros: “Hay un montón de transferencias de datos en otras áreas y en muchos casos todavía no están debidamente implementados los procesos más seguros y más adecuados”.

¿ESTÁ PREPARADA LA SANIDAD?

La transformación digital de los entornos sanitarios ha supuesto la aceleración e implantación de nuevos modelos de asistencia, la telemedicina, la gestión y análisis de los datos y la securización de todos los sistemas. ¿Realmente está la sanidad preparada para todos estos avances?

En opinión de Vesku Turtia, lo más importante es que las organizaciones sepan lo que tienen en su infraestructura. “La visibilidad y el inventario de lo que tengas es la base para empezar a hacer políticas, segmentaciones de las redes, para intentar estar lo más seguro posible”. Es importante ser consciente de todo lo que hay, para después poder hacer las estrategias e integraciones necesarias para proteger todos los sistemas. “Cuanto más avanzamos en integración tecnológica, más dependientes somos de ella”, comenta David Marco, que añade hablando de la securización de los sistemas: “Rara vez se piensa en la seguridad antes que en el servicio”. El portavoz señala hay pocos servicios sanitarios que tengan un departamento de seguridad, y subraya la importancia de proteger el correo electrónico: “9 de cada 10 ataques de ransomware empiezan por un email, sin embargo solo el 5% de los presupuestos de ciberseguridad se dedican a proteger el correo”.

Álvaro Fernández también pone el punto de mira en la seguridad, cuando habla de la transformación digital acelerada que tuvo que emprender el sector a raíz de la pandemia: “Hay mucho espacio de mejora. Hemos podido salvar el escollo sabiendo que no ha sido todo lo seguro que debiera y hay muchas cosas que hacer”. En su opinión hay diferentes escenarios en cuanto al estado de las organizaciones sanitarias se refiere: “hay algunas que están mejor, otras que están peor, pero por supuesto hay mucho que hacer”.

“Hay concienciación sobre privacidad y confidencialidad de los datos del paciente, pero yo creo que no hay todavía los recursos dedicados a proteger la integridad y a proteger la disponibilidad de los datos”

BORJA PÉREZ

A Borja Pérez no le preocupan tanto estos nuevos servicios como el tema de los datos: “me preocupa más la gestión de datos internamente dentro de las distintas organizaciones”. A la hora de hablar de Big Data, es importante que los datos vayan anonimizados para trabajar con ellos.

Por otra parte, también cree que en el sector hay luces y sombras. "Es un entorno muy heterogéneo e incluso dentro de un mismo hospital hay áreas que están a la última y áreas que están todavía muy atrasadas".

DATOS Y TELEASISTENCIA

La nueva normalidad en la sanidad conlleva una securización del acceso a datos especialmente sensibles y del análisis de los mismos, así como de un nuevo modelo como es el de la teleasistencia, la virtualización o la movilidad que implica la asistencia remota.

Según Vesku Turtia "es muy importante proteger los datos de dentro del hospital con las segmentaciones". Es de la opinión que se está mejorando muchísimo en ese aspecto, y las instituciones, tanto públicas como privadas, están esforzándose muchísimo para proteger nuestros datos aparte de nuestra salud. Sobre todo cree que hay que poner el foco en que la circulación de los datos sea segura.

Javier Rodríguez comenta que "Los centros sanitarios donde hemos hecho despliegues de soluciones de videocolaboración, en barras por ejemplo de última generación, estas barras vienen ya con computación integrada, con inteligencia artificial, y sí que veo a los responsables de los centros sanitarios concienciados con el tema de la seguridad". Señala que hay cierta concienciación, pero está seguro que aún queda mucho por hacer.

En palabras de Fernando Gutiérrez, "en la parte del dato, hay velocidades distintas, no es lo mismo la sanidad pública que la sanidad privada y dentro de cada uno de ellas, hay hospitales y organizaciones en distintos rangos". El objetivo es que también la sanidad siga el concepto de Data Driven Company. También señala que la población cada vez es más digital, pero sigue habiendo una brecha importante que hay que romper.

Para Borja Pérez "Hay concienciación sobre privacidad y confidencialidad de los datos del paciente, pero yo creo que no hay todavía los recursos dedicados a proteger la integridad y a proteger la disponibilidad de los datos". El portavoz subraya que no se trata de un problema exclusivo de España, sino que es un problema a escala mundial. "No se están tratando de forma adecuada esos datos, no se están almacenando adecuadamente".

ÁREAS DE MEJORA

Ante este panorama, ¿cuáles son las principales áreas de mejora que debe considerar la sanidad?

David Marco señala que descuidar la seguridad puede traer tres tipos de consecuencias: en el funcionamiento de la organización, consecuencias legales y para pacientes y empleados. "Si sigo construyendo la casa cogiendo piezas de la parte de abajo para crecer en altura cada vez más, pero usando materiales de abajo, llega un momento en que lo de arriba pesa tanto y lo de abajo es tan débil que no va a aguantar". Hay que avanzar, pero de forma segura.

Donde pone el acento Javier Rodríguez es en la videocolaboración: "Ha habido un despliegue acelerado y masivo de las plataformas de colaboración, pero yo creo que hay mucho campo de mejora en dotar de los dispositivos adecuados para que los equipos médicos puedan colaborar a distancia y al final puedan llegar a diagnósticos entre varios especialistas remotamente, realizar por ejemplo ciertas terapias...". A nivel de teleasistencia sí cree que se han dado pasos agigantados y los pacientes están más concienciados, pero tenemos que dar un salto en la calidad de la tecnología que se utiliza para dar esa asistencia.

Por su parte, Álvaro Fernández señala que las principales áreas de mejora en sanidad son cerrar la brecha que se ha producido entre servicios y seguridad por las prisas con las que se hizo la implementación y dotar a las organizaciones de más personal de IT. "Es uno de los ratios de los diferentes sectores donde menos personal de IT tiene más carga tecnológica para gestionar". ■

MÁS INFORMACIÓN

Retos y Soluciones para una Sanidad en cambio

MAURICIO VALBUENA, RESPONSABLE DE INNOVACIÓN,
DIRECCIÓN DE PROYECTOS Y MEJORA CONTINUA DE LOS HOSPITALES
DEL T2 PÚBLICOS BCN-VALLÉS, QUIRÓN SALUD

“Esta situación vivida ha puesto a prueba la adaptabilidad de las organizaciones”

Tras dos años en el foco de la actualidad, directamente impactado por la pandemia, el sector de la Sanidad ha visto que los proyectos de Transformación Digital han tenido que acelerarse para poder estar a la altura de las demandas de profesionales y pacientes. De la situación actual que vive el sector, así como de los retos pendientes, hemos conversado con Mauricio Valbuena, responsable de innovación, Dirección de Proyectos y Mejora Continua de los hospitales del T2 Públicos BCN-Vallés, Quirón Salud.

¿Cómo valora la situación actual de la Sanidad después de estos dos últimos años de pandemia?

Escenarios como el surgido en Wuhan hace 2 años, que carecieron de un adecuado análisis predictivo integrado por parte de los sistemas de vigilancia epidemiológica a nivel mundial, ha puesto en el punto de mira la fragilidad y las grandes carencias de los ecosistemas sanitarios del siglo XXI. Es importante reconocer que nos queda mucho camino por recorrer no solo en materia de igualdad de derechos, sino también de accesibilidad, de igualdad de oportunidades y de mejorar las coberturas; hay que resaltar que la inversión es importante y que las organizaciones sanitarias deben asumir después de esta situación de emergencia no solo un compromiso, sino el reto de transformarse.

La realidad de los pacientes crónicos y los que se encontraban en listas de espera, el frenazo a la investigación científica al concentrarse fundamentalmente en el Covid-19, el impacto de la

pandemia y sus consecuencias en la salud mental, así como la situación que viven los profesionales sanitarios, ha creado una realidad muy compleja para asumir.

Se hace muy necesario no solo el conocimiento en materia de actualidad sino la capacidad de implementar medidas de cambio agiles y con visión holística, que permitan a los lideres de las organizaciones sanitarias agilizar la adaptación a este período de transición y anticiparse a lo que sucederá en los próximos años. Ha de quedar claro que no solo hablamos de avances en el área tecnológica, sino también en lo relacionado a la adopción de nuevos modelos organizacionales innovadores, más dinámicos y eficientes, centrados en las personas pero que utilizan la tecnología como palanca de aceleración, todos nacidos dentro de la filosofía de cambio implícita en la ola de la transformación digital y que indudablemente están cambiando la manera de funcionar y de gestionar la salud por parte de las organizaciones sanitarias.

¿Considera que esta situación pandémica ha provocado un cambio de paradigma en la Sanidad y, debido a esto, se han acelerado los procesos de Transformación Digital e Innovación en el sector?

La situación vivida ha roto de forma inesperada los esquemas en los que estábamos anclados, ha sido la palanca de cambio perfecta para la irrupción en pleno de este nuevo actor que es la transformación digital. Es tal vez por este motivo que la gestión organizacional de esta situación tan excepcional durante la pandemia ha supuesto una serie de desafíos para los distintos actores implicados, así como la necesidad de planificación de cambios adaptativos, a una velocidad sin precedentes dentro y fuera de los ecosistemas sanitarios. Sería difícil hablar de esta gestión sin resaltar el esfuerzo titánico que esto supuso para las áreas TIC, que han tenido que afrontar con urgencia el despliegue de infraestructuras y herramientas tecnológicas a una escala sin precedentes, para hacer frente a la situación generada por el nuevo escenario que planteo la crisis sanitaria. Cambios que han llevado a rediseñar por completo, no solo la manera de prestar servicios en salud, sino la visión de las organizaciones y sus procesos, para garantizar la continuidad de aquellos servicios que pasaron del formato clásico presencial en su gran mayoría, a ser atendidos por canales digitales de la noche a la mañana.

> “La situación vivida ha roto de forma inesperada los esquemas en los que estábamos anclados, ha sido la palanca de cambio perfecta para la Transformación Digital”

Esta situación de cambio, derivada del afán de la implementación de estrategias de transformación digital, buscando minimizar el impacto de la pandemia en la salud de la población, ha puesto a prueba la adaptabilidad de las organizaciones, que a su vez han puesto el foco en la introducción de cambios tecnológicos, y pueden haber ignorado en algún momento el papel relevante de las personas que conforman los ecosistemas de salud. Las personas son una pieza clave, no solo en la fase de implementación, sino en la consolidación y la evolución del cambio cultural, que pueda garantizar el éxito de este nuevo paradigma que ha traído la transformación digital.

Desde las lecciones aprendidas, ¿cómo considera que deberá evolucionar el sistema sanitario para garantizar una asistencia efectiva y de calidad al paciente? ¿Cuáles deberían ser los pasos siguientes en el camino de digitalización del sector?

Los resultados y las lecciones aprendidas de la pandemia por Sars-Cov-2, en el contexto de su comportamiento impredecible y variable en las distintas olas vividas, muestran un camino claro; lo primero y muy importante es la necesidad de inversión. Y es que ahora es el momento para apostar por la innovación disruptiva, por investigar y desarrollar nuevas tecnologías en

“Asistimos a la era del Dato de calidad como herramienta útil no solo para la medición, sino en la planificación y en la predicción de escenarios fuera de lo común”

materia de atención sanitaria, implantarlas no solo como un eje de crecimiento económico, sino con un serio compromiso social de todos los actores que participan directa o indirectamente en el sector salud.

Un reciente artículo publicado en New Medical Economics comparte cinco recomendaciones que he considerado como líneas estratégicas sobre las cuales evolucionar. Estas líneas, deberían estar muy bien alineadas con las tecnológicas; con la sencilla idea de generar dinámicas que sean favorables y que permitan avanzar en este cambio cultural. Tenerlas en cuenta, garantizará la creación de modelos efectivos que sean capaces de satisfacer las necesidades de las personas integrantes de los sistemas sanitarios y que tengan a su vez un alto impacto positivo sobre el end-user que es el paciente: Formación, visión integral, inversión a largo plazo, políticas público-privadas y comunicación y compromiso.

Por otra parte, es muy necesario que se establezca un foro abierto público-privado, que permita la creación de políticas con líneas estratégicas comunes, bien definidas y que dibujen procesos con métricas claras, que nos permitan trazar dentro de las organizaciones sanitarias la situación real, su evolución y puntos de mejora. Un modelo uniforme y homogéneo que dibuje un engranaje dinámico, que permita la evolución exponencial de los todos los actores involucrados, la creación de alianzas estratégicas con actores tecnológicos que fortalezcan la sostenibilidad y adaptabilidad del modelo al entorno, y que faciliten el camino hacia la verdadera transformación digital que requieren los sistemas de salud hoy.

Es por este motivo que urge trabajar en la búsqueda de modelos innovadores de alto rendimiento, que sean capaces de conectar a todos los actores, que lideren una transformación del sistema con un “scope” holístico, donde se innove en procesos asistenciales, donde se integren nuevas tecnologías y se promueva la salud digital, que faciliten la incorporación de infraestructuras tecnológicas; no solo basados su capacidad de vigilancia y prevención en salud, sino con una alta capacidad para adaptarse y evolucionar según el entorno, que permitan la toma decisiones de alto impacto, en tiempo real, con datos fiables, recopilados de los mismos sistemas sanitarios; pero con una interoperabilidad e interconectividad de alcance global. Modelos que ofrezcan una atención sanitaria adecuada, personalizada, predecible, ágil, segura, y con un alto nivel de calidad tanto para el personal asistencial, como para el paciente.

¿Quieres saber más?

Este texto es un resumen de la entrevista con Mauricio Valbuena. Puedes leer la entrevista completa en este enlace

Desde su punto de vista, ¿cómo puede ayudar la tecnología en la evolución y medición de la calidad de la asistencia sanitaria? ¿Qué herramientas considera que son necesarias para ello?

La importancia que ha adquirido la tecnología en el mundo de la asistencia sanitaria es un hecho indudable; vemos con diferencia cómo este campo se está viendo beneficiado en gran medida por un alto nivel de inversión y por los nuevos avances tecnológicos-científicos. Podríamos decir, sin temor a equivocarnos, que asistimos a la era del Dato de calidad como herramienta útil no solo para la medición, sino en la planificación y en la predicción de escenarios fuera de lo común; sino como una nueva herramienta que juega un papel importantísimo para la

supervivencia y evolución de las organizaciones sanitarias.

Hasta hace muy poco la explotación de los datos se hacía de una forma meramente descriptiva buscando asociar factores de riesgo para plantear acciones preventivas, sobre bases observacionales aplicando estadísticas y probabilidades. Gracias a la irrupción de estas nuevas tecnologías y a su gran capacidad de análisis de grandes volúmenes de datos y prácticamente en tiempo real, es posible construir modelos con un perfil mucho más objetivo y dinámico, con un enfoque predictivo y personalizado, que nos permita abordajes más personalizados y de calidad en materia de diagnóstico, tratamiento y seguimiento de diferentes enfermedades. Los nuevos modelos de análisis predictivo permitirán una anticipación de un modo más real a situaciones como la que se vivió durante esta pandemia.

En este sentido, la aparición de la nueva cultura centrada en los datos, Data Driven, y con herramientas poderosas de análisis, Data Analytics, muestran una alta capacidad para recopilar, clasificar y analizar enormes cantidades de datos generados por dispositivos de todo tipo que son parte del día a día de las personas. El dato de calidad es el actual protagonista del nuevo modelo de atención y gestión de la salud. Gracias a herramientas tecnológicas como la inteligencia artificial y el Big Data, la interpretación y el análisis predictivo de datos está transformando la

> "La inversión es importante y las organizaciones sanitarias deben asumir después de esta situación de emergencia no solo un compromiso, sino el reto de transformarse"

forma de entender y prestar servicios dentro de los ecosistemas sanitarios.

Estamos viviendo un nuevo modelo de asistencia sanitaria... telemedicina, gestión y analítica de datos sensible, securización de infraestructura y accesos ... ¿está la sanidad preparada para soportar estos nuevos modelos? ¿Qué tipo de escenarios de atención al paciente podremos ver que se van a crear en los próximos meses/años?

Digitalmente hablando, la hiperconectividad se ha convertido en un aspecto clave de la transformación de los modelos de negocio y de las organizaciones sanitarias. La innovación y la irrupción en los entornos sanitarios de nuevas tecnologías, los grandes volúmenes de datos generados relativos a las personas plantean muchos interrogantes en materia de seguridad y desde la perspectiva de derechos y libertades. En concreto, en materia de derechos fundamentales como el de la intimidad y la protección de datos personales.

De ahí, que para que este proceso de transformación digital sea confiable y seguro, tiene que ir acompañado del cumplimiento de la normativa aplicable en protección de datos personales, el Reglamento (UE) 2016/679 y la Ley Orgánica 3/2018 de Protección de Datos Personales y garantía de los derechos digitales (no hay que olvidar que no estamos protegiendo datos sino derechos y libertades de las personas físicas) y por la implementación de políticas de seguridad realmente eficientes y que comprometan al conjunto de las organizaciones sanitarias de modo efectivo. En definitiva, cumplir con esta normativa en materia de privacidad y protección de datos, supondrá una mejora en los resultados y la competitividad de las organizaciones sanitarias; que, además, permitirá aportar seguridad y confianza, favoreciendo la transparencia de las organizaciones y fortaleciendo la relación con los usuarios.

Por otra parte, una de las grandes ventajas que aporta la transformación digital a las organizaciones, es precisamente el buen aprovechamiento de la información obtenida de los datos masivos generados gracias a la incorporación de las nuevas tecnologías a los ecosistemas sanitarios. Es así, como en los últimos años se ha visto un crecimiento en la tendencia de invertir en herramientas de inteligencia empresarial, y

analítica de datos; con la consiguiente mejora de resultados comerciales y el incremento directo de beneficios para las organizaciones.

Por último, y como conclusión, ¿cuáles son, desde el punto de vista de la tecnología y su transformación digital asociada, las principales áreas de mejora que debe abordar la Sanidad? ¿Qué tecnologías emergentes o ya consolidadas van a tener un mayor protagonismo en Sanidad en los próximos años?

En líneas generales, esta pandemia podríamos decir que se ha transformado en un catalizador de grandes avances en materia de salud; el cre-cimiento abrumador de tecnologías digitales; el acceso a datos y a su creciente capacidad de análisis, la cultura de empoderamiento del paciente, su autocuidado y su experiencia son factores que juegan un papel importante en los próximos años y aceleraran aún más la transformación de los ecosistemas sanitarios.

Son ya muchas las herramientas tecnológicas nacidas en los entornos digitales forzados por la pandemia, todo ello ha despertado una respuesta de creciente interés por parte actores externos, que buscan activamente incursionar en el mundo sanitario y establecer un nicho de mercado. Muchas de estas tecnologías en los próximos años, se harán cada vez más presentes, consolidando un nuevo modelo de relación médico-paciente. Modelos basados en servicios no presenciales como punta de lanza; veremos una notable mejora no solo en cuanto al alcance de oportunidades y de cobertura de la atención médica, sino también en la gestión de la salud de las personas. Hecho que por otra parte permitirá a los actores del sistema sanitario un cambio de visión, ya que serán más ágiles y/o eficientes en la prevención y detección de ciertas enfermedades o en el seguimiento mismo del enfermo crónico; todos ellos, aspectos que fueron relegados a un segundo plano debido a la situación de colapso de los servicios sanitarios generado durante la reciente pandemia.

Creo que todas las organizaciones sanitarias deberían tomar conciencia a nivel general, que deben seguir apostando por la transformación digital. Que no es cuestión de digitalizar los procesos para generar dinámicas de cambio. Que el mindset digital se logra con un profundo conocimiento de los procesos y de los circuitos a nivel funcional de la organización. Que también resulta imprescindible adoptar un marco adecuado para el proceso de la transformación digital que vincule a las personas. Marco que implica la adquisición de capacidades digitales adecuadas, sistemas de información interconectados e interoperables, la vinculación de tecnología disruptiva e integrable, además de una financiación que habrá de ser sostenida en el tiempo. Solo entonces se podrá desarrollar una planificación clara de cuáles son las posibilidades de la transformación digital y una visión acertada de cómo y dónde verdaderamente puede ayudar la tecnología.

La Transformación Digital supone así, un paso fundamental para alcanzar una atención alineada con la ola de cambio tecnológico y científico que avanza vertiginosamente y que trae implícito un nuevo modelo de atención en salud. Con una mayor cobertura, atención de predominio virtual, el enfoque predictivo, alta capacidad diagnóstica ligada a un abordaje terapéutico en el marco de la medicina 5P, que serán, en definitiva, aspectos a tener en cuenta para que se contribuya de un modo realista y activo a mejorar la salud de las personas. ■

MAURICIO VALBUENA

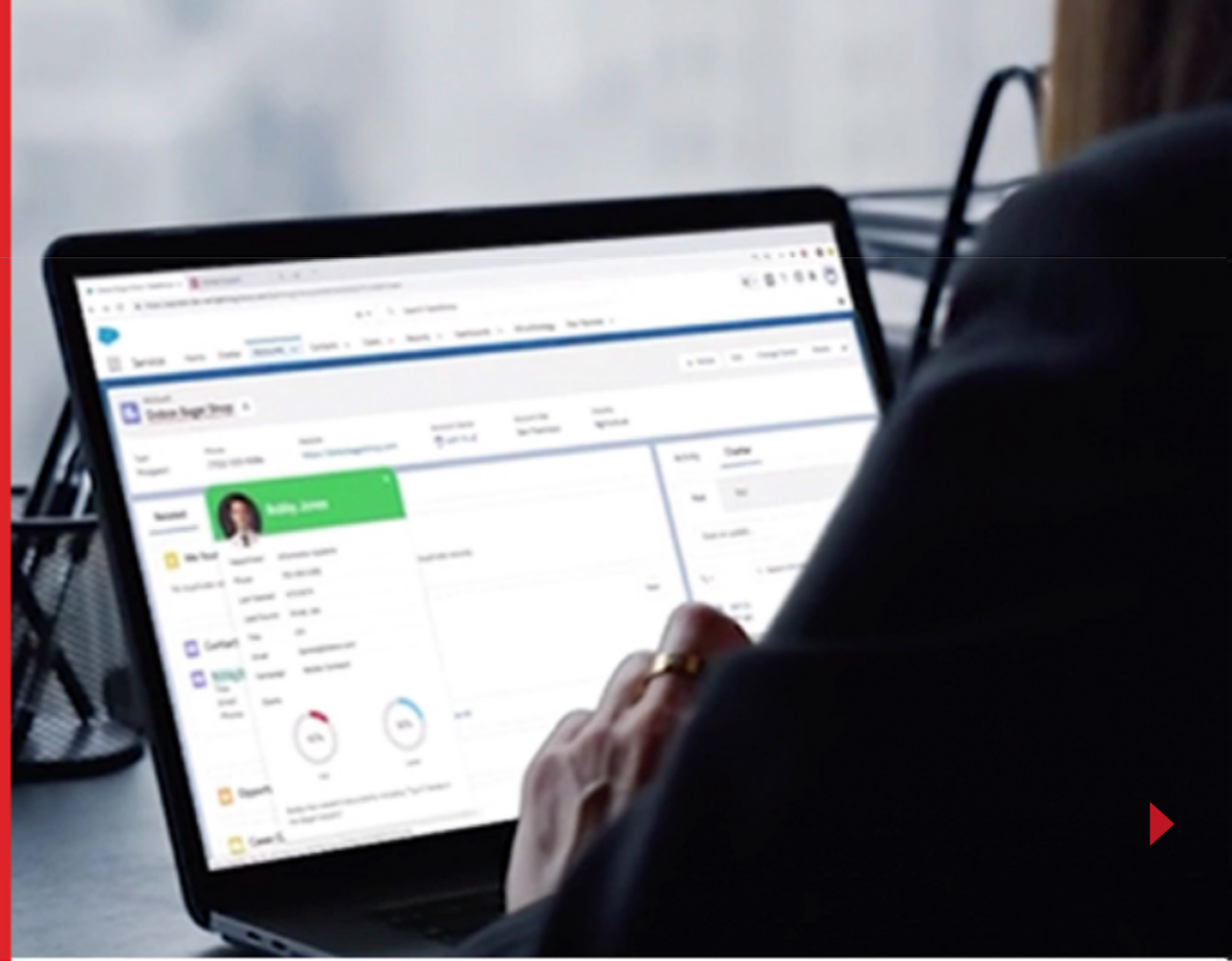
Mauricio Valbuena es médico con Postgrado Ejecutivo en Transformación Digital por IEBS y en Inteligencia Artificial en Salud por la Universidad de Standford.
Actualmente, es responsable de innovación dentro de la Dirección de Proyectos y Mejora Continua de los hospitales del T2 Públicos BCN-Vallés Quiron Salud.

HYPERINTELLIGENCE®

Las respuestas le encontrarán

MicroStrategy®

Intelligence Everywhere



eSalud, clave para la transformación del sector sanitario

JAVIER RODRÍGUEZ,
Senior Key Account Manager de Logitech

La situación de emergencia sanitaria que hemos vivido ha provocado un estado de metamorfosis continua y global, con una urgente necesidad de incluir nuevos modelos de trabajo, de comunicación, de relación o de acceso a servicios primarios, en cualquier momento y lugar.

Bajo estas premisas, la transformación digital se ha convertido en un objetivo inaplazable para cualquier organización y los centros de salud, hospitales y profesionales sanitarios no son ajenos a estos cambios. Y es que, durante la pandemia se han habilitado toda una serie de recursos y herramientas tecnológicas, así como servicios digitales para abordar la transformación digital del sector sanitario de forma acelerada, habilitando las reuniones entre equipos y centros, la discusión de diagnósticos, formaciones o convenciones. Todo ello, no solo internamente entre comunidad médica sino también con pacientes, incorporando la telemedicina para seguimientos, terapias o atención primaria, entre otros usos.

Actualmente estamos en la línea de salida del cambio en el ecosistema de salud que sitúe más cerca de la prevención de enfermedades, que sea más proactivo y que, al final, mejore la calidad de vida de los pacientes, facilitando su acceso y contacto con el sistema sanitario, y asegurando una intervención inmediata, en caso necesario, así como la desaturación de los centros de salud convencionales.

Las tecnologías para el sector salud suponen, además, la aportación de un valor añadido respecto a la cualificación de los sanitarios en el ámbito digital, una inversión a futuro que posiciona España como país referente. Según confirmamos en septiembre del año pasado en un análisis global realizado junto a Scalent sobre la opinión que merecía la atención sanitaria mediante vídeo, la mayoría de sanitarios exponían su preocupación por esta tendencia digital, pues solicitaban tecnologías intuitivas, conexión estable, aparatos de uso sencillo y con calidad de imagen y sonido comparable a lo que podría ser esa misma consulta si se realizara de forma presencial.

Entre 2020 y 2021, equipamos más de 700 centros sanitarios de la capital con sistemas de video colaboración de última generación y liderамos el proceso de digitalización de hasta 100 salas del Hospital Clínic de Barcelona con el fin de facilitar el trabajo colaborativo y el creciente servicio de telesalud al que ya se adscriben más del 57% de los pacientes en todo el mundo. En esta línea, también hemos llevado a cabo un proyecto de eConsulta para dermatología que permite captar imagen y vídeo de las lesiones de los pacientes en alta resolución desde los servicios de atención primaria para, posteriormente, compartir esos recursos gráficos con un especialista. Agilizando, de este modo, la derivación al especialista si éste lo considera oportuno.

Cada avance y cada proyecto que iniciamos comparten siempre un objetivo inamovible, que es el de proveer la mayor cantidad posible de facilidades a las personas para minimizar cualquier

obstáculo existente. Por eso, la digitalización en el sector sanitario debería dividir sus esfuerzos en cuatro ámbitos de igual relevancia: mejorar la calidad de vida de la sociedad, cuidar la experiencia del paciente, motivar la formación de los profesionales sanitarios en cuanto a lo digital y aumentar la eficiencia de los sistemas a través de su modernización.

En este sentido, la tecnología se ha posicionado como aliada indiscutible en el proceso. Propiciar la autonomía de los pacientes al implicarse en la gestión activa de su estado de salud, facilitar el acceso a historiales y datos médicos desde cualquier dispositivo, aumentar la rapidez y disponibilidad para las citas, agilizar los trámites administrativos, medir datos o celebrar formaciones y debates online son solo algunos de los servicios que ofrece la video colaboración.

Para ello es prioritaria la transformación del sistema sanitario, de forma progresiva, segura y efectiva, para habilitar experiencias personalizadas que contribuyan a la mejora de la salud de toda la población, con las innovadoras tecnologías de telemedicina que tenemos a nuestra disposición tanto para modernizar la relación médico-paciente como los métodos de comunicación entre centros o profesionales sanitarios. Es decir, una transformación a través de la tecnología que permita derribar fronteras y abrir puentes en la relación médico-paciente. ■

JAVIER RODRÍGUEZ, SENIOR KEY ACCOUNT MANAGER DE LOGITECH

Nuevos modelos de asistencia sanitaria

La pandemia ha transformado todos los sectores, incluido el sanitario, implicando la irrupción de nuevos modelos de asistencia sanitaria, entre los que destacan los entornos colaborativos y la telemedicina como tecnología emergente.

Según McKinsey, la utilización de la telesalud a diciembre de 2021 era 38 veces mayor que justo antes de la pandemia. Javier Rodríguez, Senior Key Account Manager de Logitech, cree que ha supuesto una aceleración de todos los procesos y ha provocado la creación de nuevos modelos de asistencia sanitaria remota, debido a los confinamientos y a la necesidad de evitar contagios. A pesar de ello, aún hay margen de mejora en cuanto a la calidad y la experiencia que se le ofrece al paciente. Estas soluciones deben contar con tres requisitos básicos: seguridad, integración y facilidad de uso.

Las soluciones Logitech se utilizan en todo tipo de áreas en el sector sanitario, desde la comunicación interna de los equipos de trabajo a la atención a distancia del paciente para tener nuevas vías de interacción. La compañía ofrece soluciones de audio, video y control que funcionan en cualquier plataforma de videocolaboración en la nube y ofrecen una buena experiencia tanto en el puesto de trabajo del personal médico como en las salas de reunión.

La sanidad y el mundo del dato

FERNANDO GUTIÉRREZ,
Account Executive de MicroStrategy

Hoy en día, la información es un activo fundamental de las empresas y la sanidad no es una excepción.

La sanidad maneja uno de los "productos" más preciados por todos, la salud.

El objetivo principal del sistema sanitario es mejorar la salud y por tanto la calidad de vida de la población. Existen también otros objetivos como facilitar el acceso a los servicios de salud, mejorar la calidad y satisfacción del ciudadano, incrementar la eficiencia y efectividad de la infraestructura hospitalaria/centros y un incremento eficiente de los presupuestos.

Como sucede en otras industrias, ese deseo de incremento en diferentes aspectos necesita de nuevas vías más allá de las vías tradicionales. El uso del dato junto con nuevas tecnologías puede permitir al sistema sanitario alcanzar los objetivos anteriormente mencionados.

Una mejora en la gestión del dato del paciente, de los centros de atención y de los procesos tiene una repercusión y un beneficio directo en la salud del ciudadano.

Por tanto, el dato se convierte en un activo fundamental que debe ser utilizado para la obtención de información y aportar ese valor diferencial al ciudadano.

No se trata exclusivamente de ver la información histórica del paciente en el momento de acudir a la consulta y ser reactivo, se trata de ser proactivo para obtener una sanidad preventiva. Las capacidades de inteligencia artificial y machine learning en la sanidad nos permiten poder ofertar una sanidad preventiva que evite problemas mayores en la salud de los pacientes, que permitan una mejor planificación y utilización de los recursos.

Otro de los aspectos que hacen que el dato sea crítico en el sistema sanitario, es el aspecto económico. Un análisis de la actividad operacional del sistema sanitario permitirá un incremento de la eficacia y de la eficiencia de los procesos, lo cual repercutirá directamente en un uso eficiente del presupuesto e indirectamente en la satisfacción del ciudadano al percibir una mejora en la calidad de los procesos, disponer de los medios necesarios y una organización más eficiente.

En los periodos de estrés se pone a prueba todo; los sistemas, los protocolos... se ve de manera clara que cosas son realmente necesarias, que cosas funcionan y que áreas son susceptibles de mejora.

Es por eso que el sistema sanitario se encuentra como muchas empresas y sectores en un proceso de transformación digital, muy encaminado a la calidad del dato y al gobierno del dato, pero también en la analítica y explotación del dato para la obtención de información.

Se podrían mencionar 3 áreas de mejora en lo que al mundo del dato respecta:

1. Uno de los objetivos que se busca con el gobierno y la calidad del dato es tener una visión del paciente 360º, necesidad incrementada con la incorporación de nuevos canales como la teleasistencia.

2. Incorporación de inteligencia artificial y machine learning para una sanidad preventiva y mejora de la operativa de los sistemas sanitarios.

3. Un área donde hay claro margen de mejora es en como facilitar el acceso a la informa-

ción para todo el personal involucrado en la operativa de un hospital o centro; ya personal sanitario, como personal de mantenimiento encargado de la gestión de las maquinas... para ayudarles en la toma de decisiones.

Hoy en día la gran mayoría de decisiones que se toman no van sustentadas en el dato. Existen 3 motivos principales, el dato se encuentra demasiado disperso y no hay tiempo, el segundo motivo es la falta de conocimiento en como acceder a todos esos sistemas y el tercer motivo es utilizar la experiencia

Es por tanto que el acceso a la información debe ser sencillo, rápido, intuitivo y multicanal. De esta manera se asegura que todo el personal dispone esté donde esté de la información relevante para la toma de decisiones. Como sucede en el resto de sectores, la sanidad no podría ser diferente, la tendencia actual es la de convertirse en un sector Data Driven con el menor coste y tiempo posible, es por ello que muchas compañías líderes han recurrido a HyperIntelligence como solución. ■

FERNANDO GUTIÉRREZ, ACCOUNT EXECUTIVE DE MICROSTRATEGY

El dato, fundamental en el sector sanitario

La situación pandémica ha implicado un nuevo modelo de la gestión del dato, tanto en su análisis como en su tratamiento, fundamentalmente dada la sensibilidad de muchos de ellos en un entorno tan específico como el sanitario.

El concepto data driven es completamente aplicable al sector sanitario. Para Fernando Gutiérrez, Account Executive de MicroStrategy, el poder disponer de datos para poder tomar decisiones y mejorar los tiempos de respuesta tiene un impacto en la sociedad brutal. El dato es fundamental para la salud del paciente, tanto en aspectos directamente relacionados con él, como en la gestión y la operación de los centros, que al final también recae en su bienestar. Además, la correcta gestión del dato ayuda a la medicina preventiva.

El objetivo de MicroStrategy es llevar de manera rápida y sencilla esa información recopilada a cualquier persona que en su trabajo requiera tomar una decisión y que pueda resultarle útil, pero de forma completamente segura. También trabaja en proyectos 360 y apuesta por una hiperpersonalización de la teleasistencia, ofreciendo una visión global de cada caso a través del dato. Además, tecnologías como la inteligencia artificial o el machine learning sirven para intentar detectar y ser proactivo ante posibles enfermedades.

El sector sanitario, protección crítica de sus datos

PEDRO DAVID MARCO,
CEO y Fundador de Iberlayer

El sector sanitario ha estado sometido a grandes tensiones durante los últimos dos años. Por las consecuencias de la pandemia de COVID 19, clínicas, centros de atención primaria, hospitales, farmacias y laboratorios farmacéuticos están jugando un papel crítico, y a esta presión se suma el hecho de que este sector, se ha convertido en un objetivo prioritario para los ciberdelincuentes.

La criticidad de los datos que manejan: hospitales y clínicas, con los registros médicos de cada paciente, y laboratorios farmacéuticos, con la documentación confidencial sobre vacunas o medicamentos; o la importancia de asegurar -en todo momento- la disponibilidad de los sistemas de información y la conexión ininterrumpida de los diferentes dispositivos y máquinas de salud, han actuado en su contra.

EL CORREO ELECTRÓNICO EN EL PUNTO DE MIRA

A esta situación se ha unido también el hecho de que el correo electrónico, uno de los servicios más antiguos de Internet y, en el caso del sector sanitario, herramienta crítica de los sistemas de información, se ha convertido en un arma de ataque para los ciberdelincuentes.

Cada vez más, entre todos los correos legítimos que circulan por Internet, se da un mayor número de mensajes SPAM, de correos con virus, troyanos, ransomware o de tipo phishing, en un intento por conseguir información sensible de carácter personal para realizar suplantación de identidad. Esta forma de comunicación no solicitada e ilícita está provocando serios problemas a las organizaciones y usuarios en cuanto a su seguridad y al consumo de recursos informáticos y ancho de banda de comunicaciones.

Las estadísticas de los tres últimos meses en el sector sanitario, al que Iberlayer proporciona su servicio de seguridad y anti-fraude para el correo electrónico en algunas compañías, muestran que en torno al 60% de los correos recibidos son SPAM. Aún más peligroso y preocupante es el hecho de que un 10% son campañas de phishing (en todas sus variantes, incluyendo intentos de fraude) mientras que otro 10% son correos con adjuntos con virus (que descargan ransomware en su mayoría).

El ransomware es un tipo de malware por el que un ciberdelincuente se lucra económicamente extorsionando a compañías a las que amenaza básicamente de dos modos posibles:

1. Cifrando todos sus datos y pidiendo un dinero de “rescate” a cambio de la clave de descifrado

2. Sacando fuera de la compañía enormes cantidades de datos internos y amenazando con hacerlos públicos si no se paga un “rescate”. A menudo, esta modalidad va acompañada de avisos a los propietarios de esos datos: pacientes, clientes, proveedores a los que se advierte que, de no efectuarse el pago, sus datos se harán públicos.

A este respecto aclarar que, en contra de lo que pueda parecer, no existe ninguna ga-

rantía de que, una vez ejecutado el pago, los datos perdidos sean recuperados o sigan permaneciendo secretos.

El sector sanitario es, por desgracia, uno de los objetivos del ransomware, y el correo electrónico es, sin lugar a dudas, el principal vector de entrada al ser los usuarios el eslabón de más débil de la cadena y el más fácil de engañar.

Otra de las amenazas más graves para el sector sanitario es el llamado Fraude del CEO, el cual es un tipo de engaño (y un posible delito a nivel legal) donde los cibercriminales crean cuentas de correo o dominios fraudulentos para hacerse pasar por ejecutivos de la organización, normalmente directores generales, o consejeros delegados, entre otros altos ejecutivos.

El fin último es intentar engañar a un empleado -con poderes para transferir dinero- para que lleve a cabo transferencias bancarias urgentes. Estos correos electrónicos no contienen malware malicioso, ni URL sospechosas; están completamente limpios desde el punto de vista de la seguridad. Por ello, es necesario utilizar una tecnología y un conocimiento especial de las técnicas empleadas por los ciberdelincuentes, para detectarlos y bloquearlos. Asimismo, es preciso poner una capa por encima de esta tecnología con un servicio de aviso personalizado, utilizando canales (para alertar a las posibles víctimas) distintos al del propio correo electrónico. ■

PEDRO DAVID MARCO, CEO DE IBERLAYER

Seguridad para el correo electrónico como servicio

La pandemia del coronavirus ha supuesto un verdadero reto para el sistema sanitario español, pero no solo a pie de campo, sino que sus sistemas informáticos también han visto cómo se han multiplicado los ciberataques amenazando la seguridad de datos muy sensibles, sobre todo a través del correo electrónico.

La forma más fácil de llegar al corazón de las empresas son los usuarios. Dado que la manera más directa de impactar al usuario es mediante el correo electrónico, se ha convertido en uno de los principales vectores de ataque. Pedro David Marco, CEO de Iberlayer, señala que no muchos directivos son conscientes del daño que le puede ocasionar a su compañía un ciberataque, sobre todo en sectores como el sanitario que no cuentan con departamentos específicos dedicados a ello.

Por esta razón Iberlayer ofrece la seguridad del correo como un servicio, lo que permite al cliente abstraerse de esa capa y tener la mayor protección que existe en el mercado sin necesidad de contar con especialistas in house. Además, sus soluciones de seguridad para el correo electrónico realizan un cifrado por defecto, de tal manera que todo el tráfico del cliente pasa a estar protegido.

El sector sanitario tiene graves problemas para detener el ransomware.

El 65% de los ciberataques consiguieron cifrar datos

Sophos Managed Threat Response

Tome medidas contra las ciberamenazas
Un servicio totalmente gestionado con funciones de búsqueda, detección y respuesta ante amenazas las 24 horas.

www.sophos.com/es-es/

SOPHOS
Cybersecurity delivered.

Los atacantes tienen una mayor tasa de éxito en el cifrado de datos sanitarios

JAVIER DONOSO,
Sales Engineer, Sophos

Según El estado del ransomware en la sanidad 2021 de Sophos, entre las organizaciones sanitarias afectadas por el ransomware, el 65% afirmó que sus datos estaban cifrados, en comparación con la media intersectorial del 54%. A nivel mundial, el 39% de las organizaciones fueron capaces de detener el ataque antes de que se cifraran los datos, pero sólo el 28% en el sector sanitario. Esta menor capacidad para detener un ataque puede ser un reflejo de los retos financieros y de recursos a los que se enfrenta el sector sanitario, en parte debido a la reticencia a desviar fondos a la ciberseguridad que podrían utilizarse para la atención de primera línea a los pacientes.

Para que los organismos sanitarios ganen terreno a las nuevas y evolucionadas ciberamenazas, deben seguir ciertas estrategias clave de seguridad para protegerse:

1. Adoptar el modelo de seguridad de confianza cero o Zero Trust. Un informe, muestra que en el sector sanitario hay más infracciones causadas por amenazas internas que externas. Esto puede atribuirse a un error humano, a la falta de supervisión en ciberseguridad o al abuso intencionado del privilegio de acceso a datos y sistemas confidenciales.

Al implementar un enfoque de confianza cero, las organizaciones de salud pueden introducir controles granulares en el tráfico de la red. Esto elimina la oportunidad de que los atacantes y los usuarios deshonestos realicen acciones malintencionadas y obtengan acceso a información personal confidencial de salud mientras permanecen fuera de todas sospecha.

2. Mejorar la ciberseguridad contra los ataques de ransomware. Más de un tercio de las organizaciones sanitarias (34%) fueron atacadas por ransomware el año pasado. Podemos afirmar, que el ransomware es un arma devastadora en manos de los ciberdelincuentes que tienen como objetivo el sector sanitario.

Estos ataques han detenido operaciones sanitarias, han paralizado los dispositivos y sistemas médicos conectados y han cifrado los registros para que el personal sanitario no pueda acceder a ellos. Sophos ofrece una seguridad líder en ransomware con Intercept X Advanced with XDR, la única solución XDR del sector que sincroniza la protección nativa de endpoints, servidores, firewalls, correo electrónico, infraestructura en la nube y M365.

3. Superar la escasez de mano de obra cualificada. La falta de personal con los conocimientos y la experiencia adecuados en materia de ciberseguridad es uno de los principales desafíos para los proveedores de servicios de salud.

Para las organizaciones sanitarias que carecen de recursos en ciberseguridad, Sophos ofrece el servicio de Managed Threat Response (MTR). Este servicio brinda una supervisión eficaz y una evaluación continua de los riesgos gracias al equipo de expertos dedicado las 24 horas del día, los 7 días de la semana. Nuestra solución va más allá de las simples alertas, ya que proporciona una respuesta contra las amenazas, asegurando que el riesgo se identifica, se contiene.

4. Cubrir los puntos ciegos en sus esfuerzos de transformación digital. Las transacciones de información entre los pacientes, los cuidadores, las agencias de seguros y otras partes interesadas deben ser fluidas y seguras. Las redes SD-WAN, con su arquitectura flexible, ha surgido como una muy buena alternativa entre las organizaciones de salud para cumplir con estos requisitos.

Es crucial proporcionar un acceso fiable y seguro a los datos clasificados de la asistencia sanitaria en un momento en que muchos hospitales están adoptando nuevas tecnologías como los dispositivos médicos conectados a la red, la telesalud y aplicaciones médicas como los sistemas de comunicación y archivo de imágenes (PACS).

Sophos, con Sophos Firewall y SD-RED, hace posible conseguir una conectividad SD-WAN en línea con sus objetivos de seguridad y continuidad.

5. Promover la concienciación en ciberseguridad. Otra preocupación importante para el sector sanitario es la falta de formación sobre ciberseguridad y la escasa conciencia sobre la privacidad de los datos entre los empleados.

Es importante tener una cultura de ciberseguridad adecuada para ayudar a reducir la alta susceptibilidad de la sanidad a una amplia gama de sofisticados ciberataques.

Con Sophos Phish Threat, los equipos de seguridad informática pueden simular ataques de phishing con sólo unos pocos clics, y proporcionar formación automatizada e in situ a los empleados de atención sanitaria según sus necesidades. ■

ÁLVARO FERNÁNDEZ, ENTERPRISE ACCOUNT EXECUTIVE DE SOPHOS

Prevención, detección y respuesta

En los últimos dos años los ciberataques hacia el entorno sanitario se han visto multiplicados como consecuencia de la pandemia, con infraestructuras, accesos y datos como principales objetivos. El ransomware es el más notorio, pero detrás de esos ataques hay mucho más.

Muchas veces se entiende el ransomware como un ataque aislado, pero realmente se trata de la última fase de un ataque, antes de aflorar han pasado muchas otras cosas. Como explica Álvaro Fernández, Enterprise Account Executive de Sophos, una vez dentro el atacante va a intentar pasar inadvertido y filtrar información, lo que supone un gran riesgo para un sector como el sanitario, y será después cuando preparará el entorno eliminando las copias de seguridad existentes para poder liberar el ransomware sin problemas y salir a la luz.

Para hacer frente a estos problemas es necesario contar con un plan de respuesta ante este tipo de incidentes. Sophos Rapid response es un servicio específicamente diseñado para este tipo de eventos que cuenta con una fase de neutralización del atacante y otra de monitorización para solucionar cualquier tipo de incidente. La seguridad del entorno sanitario se debe basar en 3 claves: prevención, detección y respuesta.

El impacto de TLStorm

en la seguridad de las organizaciones médicas y sanitarias

OSCAR MIRANDA,
CTO for Healthcare, Armis

TLStorm son un grupo de tres vulnerabilidades críticas, descubiertas por Armis, que afectan a los Smart-UPS de APC. Dos de ellas son vulnerabilidades de ejecución remota de código (RCE) en el código que maneja la conexión a la nube, lo que hace que estas vulnerabilidades sean explotables a través de Internet. La tercera vulnerabilidad es un fallo de diseño, en el que las actualizaciones de firmware de la mayoría de los dispositivos Smart-UPS no están correctamente firmadas o validadas, lo que permite a un atacante cargar firmware malicioso de forma remota y sin validación. Un ataque a estos dispositivos podría llegar a traer consecuencias catastróficas, ya que los Smart-UPS de APC se encuentran en infraestructuras críticas como hospitales, centros de datos e instalaciones industriales.

Estas tres vulnerabilidades de día cero, acuñadas como TLStorm, exponen a más de 20 millones de dispositivos en todo el mundo y podrían permitir a atacantes eludir las funciones de seguridad y controlar o dañar remotamente dispositivos médicos, industriales y enterprise críticos para el funcionamiento de cualquier organización. Datos obtenidos por el equipo de investigadores de Armis, muestran que 8 de cada 10 organizaciones podrían ser vulnerables a TLStorm.

En el sector de la sanidad, esta amenaza pone de manifiesto los riesgos que entrañan los dispositivos médicos conectados y la importancia de la seguridad de los mismos. Con activos como los dispositivos SAI convirtiéndose en un objetivo para los actores maliciosos, es más importante que nunca tener una visibilidad completa de todos los dispositivos conectados a la red, junto con la capacidad de supervisar su comportamiento e identificar los intentos de explotación de cualquier fallo de seguridad, como TLStorm.

Alrededor del 91% de los clientes de Armis del sector sanitario y médico de todo el mundo utilizan algún tipo de SAI, y de ellos el 76% tienen modelos de SAI identificados como vulnerables a TLStorm. Los clientes de la compañía pueden ver inmediatamente los dispositivos vulnerables y parchearlos, pero el alto número de posibles afectados destaca los riesgos potenciales para aquellos que no pueden hacerlo.

El ecosistema de dispositivos en empresas sanitarias va más allá de los dispositivos médicos. Los SAI se utilizan no sólo en los centros de datos sino dentro de los hospitales y clínicas, por lo que un ataque podría afectar significativamente los cuidados y el trato con los pacientes. En resumen, cualquier evento de seguridad que afecte a los dispositivos médicos conectados puede causar una interrupción considerable en la prestación de servicios sanitarios y afectar a la seguridad de los pacientes.

Los hospitales deben identificar qué dispositivos ayudan al flujo de trabajo clínico, aparte de los dispositivos médicos clásicos, y cuáles están conectados a sistemas SAI vulnerables. Solo a través de la identificación y monitoreo continuo de los dispositivos un hospital puede mitigar o remediar el riesgo creado por estos sistemas SAI rápidamente.

Aunque las ventajas de las nuevas tecnologías son evidentes, cada dispositivo médico conecta-

do crea un nuevo objetivo para los malos actores y debe utilizarse en un entorno seguro, con supervisión continua de su actividad.

El descubrimiento de las vulnerabilidades TLStorm subraya la importancia de tener un inventario de dispositivos en entornos como el médico, y de controlar la actividad de todos aquellos dispositivos responsables de mantener la energía y las operaciones críticas en funcionamiento. El uso de dispositivos médicos conectados supone una gran oportunidad para mejorar la atención al paciente en centros hospitalarios y sanitarios, pero los profesionales de la salud deben entender que también crea oportunidades de entrada para actores maliciosos.

Contar con un plan de ciberseguridad para los dispositivos médicos, es fundamental para cualquier organización que utilice el Internet de las cosas médicas, o IoMT. La Agencia de Ciberseguridad de la Unión Europea (ENISA) y la FDA ofrecen directrices para ayudar a los equipos informáticos (TI) a gestionar la seguridad de los dispositivos médicos. Ambas son un buen punto de partida para garantizar la seguridad del IoMT.

La visibilidad es fundamental para que las organizaciones sanitarias se aseguren de que todos los dispositivos están supervisados y protegidos. En la realidad hiperconectada en la que vivimos, tener visibilidad completa y a tiempo real garantiza una protección holística. ■

VESKU TURTIA, REGIONAL DIRECTOR ESPAÑA Y PORTUGAL DE ARMIS

Monitorización continua sin agentes y de forma pasiva

La situación de pandemia vivida en los últimos años ha implicado un nuevo paradigma para sectores como el sanitario, así como la aceleración de nuevos modelos tecnológicos, donde el componente de la ciberseguridad de los diferentes assets juega un papel muy importante.

La aceleración de la digitalización en el sector sanitario es un hecho desde el inicio de la pandemia, lo que ha implicado ciertos retos para los players del sector. Para Vesku Turtia, Regional Director España y Portugal de Armis, el principal reto es que las empresas logren entender qué es todo lo que tienen integrado en su red, para poder hacer políticas de ciberseguridad y proteger los assets de cada centro hospitalario. Además, es muy importante hacer una monitorización continua, sin agentes y de una forma pasiva, para no interferir en posibles procesos hospitalarios importantes.

Armis ha traído al mercado una plataforma que engloba precisamente todas estas cuestiones: inventario, visibilidad, monitorización continua, sin agentes y de forma pasiva, que se integra de forma perfecta con los sistemas del cliente. Además, cuentan con una base de datos en la nube de más de 2 billones de dispositivos distintos perfilados en 20 millones de perfiles, que permite compartir información para estar a la última en protección.

El riesgo de las infraestructuras sanitarias frente a diversos vectores de ataque

BORJA PÉREZ,
Country Manager
Stormshield Iberia

Cada vez más digital e interconectado, el sector sanitario, con los hospitales al frente, lleva tiempo siendo objetivo de ciberataques. La sensibilidad que encierra, lo han convertido en un blanco codiciado para los ciberdelincuentes, quienes lanzan sus amenazas contra estas entidades. No en vano, el sanitario fue, según la Agencia de la Unión Europea para la Ciberseguridad, ENISA, el cuarto sector más atacado durante 2020, registrando 143 incidentes , lo que supone un 47% más que el año anterior. Se trata por tanto de un sector expuesto en el que, además, y a diferencia de lo que ocurría en el pasado, no se enfrenta a un factor de riesgo uniforme, sino que los peligros, cada vez más, proceden de diferentes vectores: redes, software, físicos y humanos.

EN EL CORAZÓN DEL SISTEMA

El rendimiento y la disponibilidad de las redes informáticas de los sistemas de salud son muy importantes, dado que la vida de los pacientes a menudo depende de la información que permiten intercambiar.

Por tanto, salvaguardar esa información confidencial y vital es un tema prioritario, igual que garantizar la disponibilidad de los servicios. La salud vive al ritmo de las emergencias. Por lo tanto, requiere una reacción rápida en caso de incidente, en relación con equipos biomédicos, Gestión Técnica de Edificios (BMS) o Gestión Técnica Centralizada (CTM) del hospital. Estas intervenciones se pueden facilitar proporcionando acceso remoto seguro a técnicos o proveedores externos a través de VPN nómadas, SSL o IPSec y autenticando a los usuarios a través de flujos de red. Dos medidas que también son útiles para fortalecer el mantenimiento a distancia y el desarrollo de la telemedicina.

UN ATAQUE CONTRA EL CEREBRO

Los programas informáticos prestan innumerables servicios en los hospitales, tanto para la gestión interna como externa de la organización. Sin embargo, por su propia naturaleza, también pueden presentar puntos débiles, como lagunas o una obsolescencia, que pueden ser aprovechados por los ciberdelincuentes para acceder a los equipos médicos, informáticos o, incluso a los datos de los pacientes o a las instalaciones sensibles.

Para prevenir los ciberataques de software, es esencial la concienciación de los equipos humanos, así como el cumplimiento de las mejores prácticas en este ámbito: limitar el acceso a la red de las aplicaciones al mínimo, realizar una auditoría del sistema, endurecer las configuraciones y realizar copias de seguridad sin conexión.

TRABAJANDO SOBRE EL TERRENO

Lejos del cliché del ciberdelincuente, aislado tras su pantalla a kilómetros de su víctima, algunos se acercan lo más posible a su objetivo. Su técnica consiste en atacar directamente los equipos hospitalarios, ya sean informáticos, médicos u operativos, y explotar sus vulnerabilidades. Para ello el ciberdelincuente accede físicamente al equipo en cuestión, y se conecta a él para interrumpir su funcionamiento. Tras ello, su impacto puede ser múltiple, desde el sabotaje de la máquina hasta la

alteración -o incluso el robo- de datos sanitarios.

Para protegerse de estos ataques, es necesario salvaguardar las máquinas, como las estaciones de trabajo. Por lo tanto, se recomienda el control de acceso, la gestión de los dispositivos externos e incluso el análisis del comportamiento. Esto puede lograrse con la creación de estaciones blancas que actúan como una descontaminación de llaves USB. Como último recurso, la segmentación de la red para limitar la propagación de la infección, en caso de que esta se produjera.

RIESGO HUMANO, PRINCIPAL PREOCUPACIÓN

Además de los riesgos tecnológicos es importante tener en cuenta los asociados al ser humano, sobre todo con el uso todavía muy extendido de las memorias USB en entornos TI y OT. Por ello, es importante endurecer los puestos de control y supervisión mediante el establecimiento de soluciones de listas blancas o de análisis de dispositivos de almacenamiento, para rechazar cualquier uso de un perfil no autorizado, pero también concienciar a los trabajadores sanitarios de todos los riesgos cibernéticos para evitar cualquier error o acción involuntaria que pueda poner en peligro los datos o la infraestructura.

Adicionalmente, y además de trabajar en esta concienciación, dado que los ataques son cada vez más dirigidos y sofisticados, es fundamental ofrecer soluciones que no dependan del conocimiento que el usuario pueda tener en ciberseguridad. ■

BORJA PÉREZ, COUNTRY MANAGER DE STORMSHIELD

El cifrado de datos, imprescindible

La seguridad del sector sanitario se ha cuestionado a raíz de la pandemia, dado que se ha convertido en uno de los entornos más amenazados por los ciberdelincuentes.

El intercambio de datos sensibles entre distintas áreas del sistema sanitario, como laboratorios, hospitales, clínicas, es continuo, pero no está debidamente securizado. Así lo pone de manifiesto Borja Pérez, Country Manager de Stormshield, señalando que los datos no se están almacenando adecuadamente y el intercambio muchas veces no se hace con las medidas de seguridad suficientes. A pesar de ello, en su opinión los CISOs son conscientes del problema, pero les faltan recursos.

Para Stormshield es fundamental tener todos los datos cifrados y salvaguardados de manera segura, de manera que si se produce una filtración de datos, no se pueda sacar ninguna información útil de esos documentos filtrados. La compañía basa su propuesta en tres principios:

Securización de los datos mediante cifrado de documentos y correo, protección del puesto de trabajo; y segmentación de las redes y securización de cada uno de los servicios que se estén dando en el entorno sanitario.

STORMSHIELD

La opción europea en ciberseguridad

Su socio de confianza para proteger **infraestructuras hospitalarias**

www.stormshield.com

Visibilidad, clave de la seguridad en el entorno sanitario

En el sector sanitario, Armis permite a las organizaciones utilizar la visibilidad en su ecosistema de dispositivos médicos e informáticos, para identificar, evaluar y asegurarse ante riesgos cibernéticos, a la vez que realizar mejoras operativas significativas.

Esta aproximación ofrece un valor clínico y un valor operacional. En el caso del primero, destaca el manejo y seguimiento de inventario; identificar y localizar dispositivos médicos no conectados a la red; alertar sobre dispositivos médicos que abandonen el recinto hospitalario y monitorización del comportamiento de dispositivos en busca de indicadores de mal funcionamiento. Asimismo, sobresale la utilización dirigida hacia la eficacia clínica (tiempos de espera y satisfacción del paciente); mejorar la monitorización de dispositivos de alto valor para controlar tiempos de inactividad y problemas operacionales; identificar tiempos óptimos para el mantenimiento de los dispositivos y alertar de anomalías o usos incorrectos de dispositivos para el cuidado de pacientes. Por último, mejoras de seguridad y calidad, y realizar informes trimestrales con seguimiento de medidas de los órganos reguladores.

Desde el punto de vista operacional, destaca el coste de gestión; asistir a operaciones para realizar previsiones financieras; mostrar dispositivos perdidos para prevenir la compra excesiva; y ayudar a a tomar decisiones de compra informadas al adquirir inventario adicional. Igualmente, ahorro en contratos de mantenimiento, al mostrar datos de utilización y riesgo para optimizar los Acuerdos de Nivel de Servicio (SLA) y los contratos de mantenimiento relacionados con dispositivos médicos y sistema de gestión de edificios. Finalmente, integración con inversiones existentes en TI y Seguridad de la Información como ServiceNow, Biomed CMMS o CMDB, para una mayor visibilidad y precisión de los activos; realización de informes en tiempo real sobre los usos de li-

cencias; simplificación de la implementación de soluciones de Control de Acceso a Red (NAC) (Cisco ISE); aumento de las capacidades de otras soluciones y de administración de vulnerabilidades para dispositivos no gestionados y puntos ciegos de redes; mejora de la visibilidad y alerta en la Gestión de Información y Eventos de Seguridad (SIEM); e identificación de dispositivos perdidos durante proyectos de migración de tecnología – proyectos de migración de servidores y proyectos de renovación de infraestructuras inalámbricas.

CIBERSEGURIDAD Y CONTINUIDAD DE LAS OPERACIONES

Con la Auditoría y Cumplimiento de normativas se crean informes cuatrimestrales de requerimientos regulatorios; cuadros de mando dinámicos en tiempo real para identificar dispositivos que incumplen la normativa; fuentes de información absoluta para la identificación y orquestación de dispositivos; e identificación de riesgos de terceras partes relacionados con el comportamiento de los dispositivos.

Mientras, con la Protección de la Privacidad de los Clientes, se informa de transmisiones de Información de Salud Protegida (PHI) no encriptada a destinaciones internas o externas no autorizadas; se identifican cámaras IP transmitiendo en la red; se alerta de dispositivos afectados con potencial de grabar o impactar la privacidad del paciente; y se crean normativas de seguridad para prevenir la exfiltración de datos.

Por último, con las Políticas de Seguridad y control de Regulaciones (Análisis de Brechas de Seguridad), se crean informes para la identificación de dispositivos sin los controles de seguridad enterprise necesarios como: agentes de protección endpoint, parches/asset management agent (SCCM). Ayuda a fortalecer la seguridad y protección ante ciberataques; y se identifica y ayuda a la remediación de dispositivos personales (BYOD).

ARQUITECTURA DE SEGURIDAD Y OPERACIONES

Con las Operaciones de Seguridad de la Información, se mejora la detección y respuesta del SOC ante ciberataques y detección de ransomware (reduce el tiempo de inactividad del hospital); se aplican políticas de seguridad automáticas para contener y mitigar incidentes (menor tiempo de respuesta y resolución); y se alerta ante comportamientos anómalos como exfiltración de datos, comunicación con IPs internacionales, y conexiones de red no autorizadas.

Con la Gestión de vulnerabilidades y amenazas, se manejan las vulnerabilidades en dispositivos médicos; se realizan y expanden políticas de escaneo de vulnerabilidades para dispositivos nuevos y ya existentes; se asesora sobre riesgos en tiempo real y contextualiza, según tipo de dispositivos, función, comportamiento, y vulnerabilidades; se crean informes y monitorizan en tiempo real los intentos de explotación de vulnerabilidades de día cero en dispositivos médicos y Enterprise; y se crean cuadros de mando de seguimiento de los esfuerzos de remediación.

Por último, con la Capacidad de Respuesta de Incidentes Automatizada, se integra con mallas de ciberseguridad existentes para automatizar respuestas de seguridad; se identifican comportamientos malignos y ejecuta políticas estrictas de firewall para remediarlos; se integra con soluciones NAC para segmentar la red y poner en cuarentena dispositivos; y genera tickets de forma automática para alertas, investigación y seguimiento. ■

MÁS INFORMACIÓN

- Security Operational efficiency
- Securing the patient journey
- Medical device vulnerabilities

La protección de correo electrónico, clave en el sector sanitario

Iberlayer, como compañía centrada exclusivamente en la protección del correo electrónico desde la nube, ofrece una solución en la que han confiado compañías de casi toda Europa, Reino Unido, Estados Unidos y América Latina: Iberlayer Email Guardian.

El correo electrónico es la principal vía y puerta de entrada de aproximadamente 9 de cada 10 incidentes de ciberseguridad, porque el email es la forma más sencilla de llegar al interior de las compañías y a su eslabón más débil: el usuario final. Con solo un 8% del correo electrónico considerado como limpio, todo el resto es correo no deseado, incluyendo correos spam, scam, phishing, fraudes, estafas, y correos con malware, que además de consumir recursos corporativos, como ancho de banda, carga en sistemas, espacio en disco, entre otros, puede suponer un gran riesgo en la seguridad de las propias compañías hasta límites críticos.

Hoy día, las compañías se enfrentan a la necesidad de contar con cuatro elementos fundamentales para mantenerse protegidos:

- Tecnología con años de experiencia con un alto nivel de sofisticación, automatización, disponibilidad, y capacidad de detección de los algoritmos empleados en las campañas de correo no deseado.
- Personal experto en ciber-seguridad que esté constantemente actualizado y constan-

Al tratarse de un servicio y no de un producto, Email Guardian ofrece a las compañías una capa de seguridad completa con una fuerte protección frente a las amenazas que a diario se reciben por email

temente pendiente de todas las amenazas nuevas que a diario van apareciendo...

- Personal experto en el correo electrónico y en el uso y administración de las herramientas de filtrado de correo para su correcto funcionamiento, continuos ajustes y parametrizaciones...
- Personal que esté pendiente de los paneles de control, estado de los sistemas, logs, posibles alertas... y con el nivel de entrenamiento adecuado para distinguir cuando es necesario tomar medidas drásticas.

EMAIL GUARDIAN DE IBERLAYER

Al tratarse de un servicio y no de un producto, ofrece a las compañías una capa de seguridad completa con una fuerte protección frente a las amenazas que a diario se reciben por email y sin necesidad de gestionar todas las anteriores necesidades mencionadas. Como servicio completo de protección del correo electrónico desde la nube, impide que posibles amenazas a través de este vector, lleguen hasta los usuarios, protegiéndolos contra ransomware y malware de todo tipo, Spam, Scam, Phishing, Fraudes, Estafas, y un largo etcétera.

IBERLAYER DOMAIN GUARDIAN

Uno de los principales métodos utilizados para ataques de Phishing es la suplantación de identidad. Resulta sencillo y económico registrar un dominio similar al de la víctima para hacernos pasar por un alto cargo y realizar un fraude de CEO. En muchos casos se suplantan dominios de reconocidas marcas para que resulte mucho más creíble el origen del correo. De este modo, el usuario confía en el emisor y no sospecha de un posible ataque.

El sistema de vigilancia de dominios, incluido en el servicio Iberlayer Email Guardian, monitoriza la creación de nuevos dominios similares. De este modo, se puede anticipar a una posible suplantación de identidad permitiendo tomar las medidas necesarias en un tiempo mínimo.

El laboratorio de Iberlayer vigila, monitoriza, estudia y analiza constantemente la actividad mundial relativa al email, incluyendo un servicio de vigilancia de dominios, para, no solo bloquear todo tipo de amenazas, sino también tratar de adelantarse a ellas lo antes posible. Dada la inmediatez del peligro, a través de Domain Guardian, Iberlayer es capaz de monitorizar posibles abusos, avisando al cliente de manera directa, incluso vía telefónica en casos urgentes, de aquellas actividades sospechosas de posibles fraudes o ataques dirigidos. ■

MÁS INFORMACIÓN

Iberlayer

Email Guardian

Soluciones para una telesalud de calidad

Logitech está promoviendo la adopción y eficacia de la telesalud trabajando para crear una atención médica innovadora que mejore la calidad de vida y la interacción entre pacientes, proveedores y profesionales sanitarios. Logitech permite a las organizaciones de atención médica brindar atención de alta calidad independientemente de su ubicación a través de un conjunto de soluciones de videocolaboración fundamentales y fáciles de administrar.

A medida que la telesalud continúa transformándose e innovándose, Logitech busca desarrollar soluciones que se integren fácilmente en la sanidad con el objetivo de ofrecer experiencias excepcionales a todas las personas involucradas en los servicios sanitarios a través de atención vanguardista y centrada en el paciente.

Para los profesionales, sus pacientes y los equipos de TI, las soluciones de videocolaboración de Logitech proporcionan experiencias de telesalud de alta calidad para repensar las posibilidades y necesidades de todos ellos. Logitech ayuda a las organizaciones de atención médica de todo el mundo a brindar atención de alta calidad de forma remota, mejorando los resultados, reduciendo los costes y elevando la experiencia de atención sanitaria para todos los involucrados.

De cara al paciente, las soluciones de Logitech le conectan con su especialista médico al instante y le permiten evitar desplazamientos innecesarios, porque su examen y control se realizan en modo remoto, a través de vídeo y evitando cualquier riesgo de contagio potencial.

En el día a día de los profesionales sanitarios, estas soluciones modernizan las salas de reuniones, los despachos y demás ubicaciones de los diferentes equipos multidisciplinares (MDT). Asimismo, permiten equipar las salas de los centros favoreciendo la consulta entre el personal médico y potenciar la formación a distancia, habilitando a los médicos y enferme-

Para los profesionales, sus pacientes y los equipos de TI, las soluciones de videocolaboración de Logitech proporcionan experiencias de telesalud de alta calidad para repensar las posibilidades y necesidades de todos ellos

ras la observación de cirugías y procedimientos en remoto de otros hospitales o centros de investigación.

Herramientas como webcams, auriculares y otras soluciones profesionales para equipar el espacio de trabajo personal sanitario, como es el caso de Logitech Brio, una webcam que permite habilitar cualquier espacio en una sala de consulta remota para conectar al personal médico con los pacientes, y estos con sus familiares en casos de ingreso prolongado. La implementación de auriculares con micrófono como los Logitech Zone con cancelación de ruido con el objetivo de mejorar la experiencia de los pacientes y los médicos con un audio claro y de alta calidad. O, el uso de Logi dock para simplificar la organización del espacio de trabajo del especialista, reducir la acumulación de cosas en el escritorio y contribuir a su productividad.

Además de la apuesta por avanzadas soluciones de videocolaboración para consultas o salas de formación, como es el caso de Rally Bar, una barra de video todo en uno, que facilita el acercamiento de equipos que están en diferentes centros, con el fin de reducir el número de viajes para el seguimiento de los pacientes o la puesta en común de casos prácticos. Todo ello a partir de un sistema de doble cámara y tecnología de encuadre automático RightSight 2, que además permite elegir la vista para resaltar al orador activo, la vista de grupo para capturar a todos los presentes en la sala o combinar las dos vistas para una experiencia inmersiva y atractiva; y, Tap Scheduler, un panel de programación enfocado a gestionar de forma más eficiente los espacios de reunión. Esta solución se ha diseñado para facilitar su visualización y uso, con una instalación sencilla y una experiencia de usuario intuitiva que impulsan una rápida implantación y adopción.

En resumen, todo tipo de soluciones para impulsar la digitalización del sector sanitario, compatibles con todas las plataformas de vídeo en la nube del mercado, que permitan tender los puentes necesarios de cara a mantener unidos a todos los profesionales del ámbito sanitario y apostar por una nueva relación entre médico-paciente. ■

MÁS INFORMACIÓN

- El futuro de la atención virtual conectada
- Lecciones del COVID 19

ARMIS®

Fortalece la seguridad de tus pacientes obteniendo visibilidad completa de todos tus dispositivos

Armis ofrece visibilidad completa e información precisa sobre todos los dispositivos administrados y no autorizados de tu red.

Descubre nuestra solución en
www.armis.com/medical-device-security/

Soluciones para convertir a las sanitarias en compañías Data Driven

MicroStrategy es una empresa con foco en el sector analítico, siendo una arquitectura orientada a objetos su mayor diferenciador con el resto de soluciones analíticas, una arquitectura que le permite el gobierno de la información y ofrecer una visión única de la verdad a lo largo de la toda la compañía.

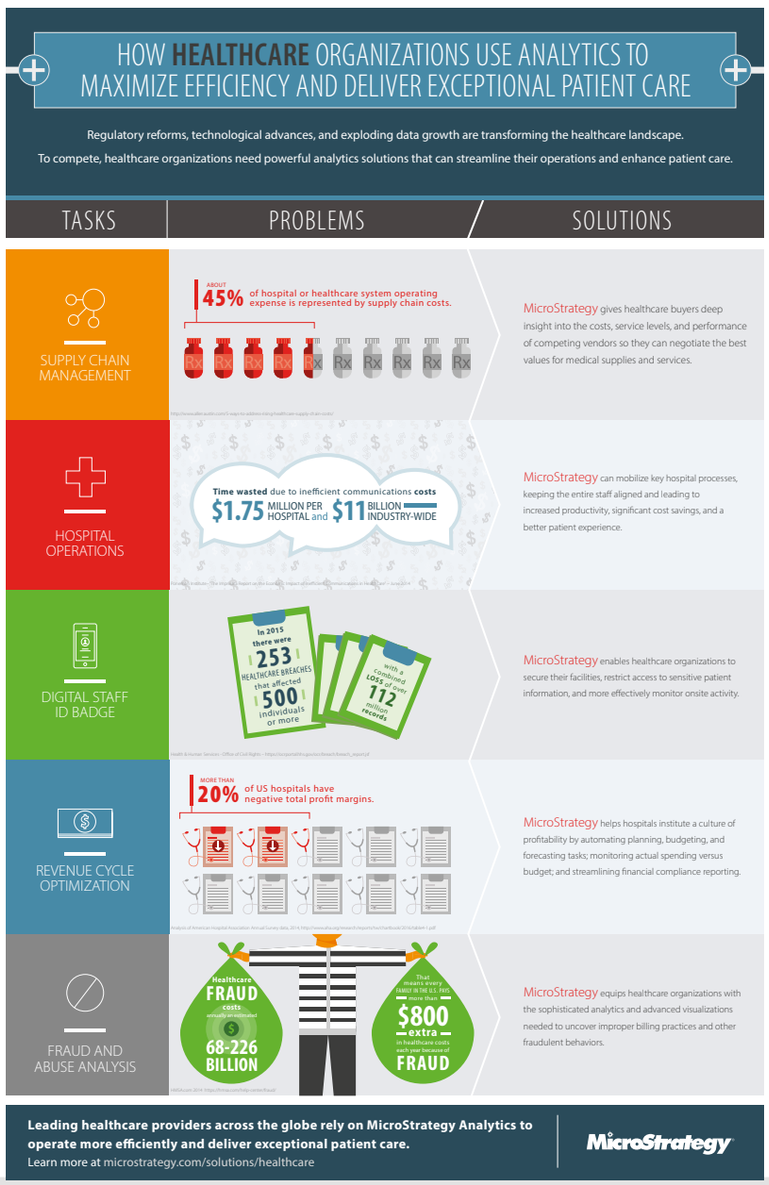
Se trata de una plataforma escalable, tanto en usuarios como en datos, que cubre cualquier caso de uso que planteen los consumidores de información sin necesidad de añadir más herramientas y por tanto pudiendo reaprovechar los desarrollos en cualquiera de los canales por los que el usuario consume la información, dando una sensación de omnicanalidad y reduciendo los costes de gestión.

Otro de los diferenciales principales de MicroStrategy es su dedicación plena a la analítica, esto hace que sea una empresa cercana con sus clientes, lo que le permite dar una atención y escucha diaria de las necesidades y tendencias. Es por eso que, desde hace unos años MicroStrategy ha trabajado en 3 áreas principalmente:

❖ **Área Corporativa.** Esto es, seguir trabajando en las capacidades para dar un servicio empresa-

rial, es decir, capacidades de gobierno del dato, de una visión única, de escalabilidad de datos y usuarios y de una seguridad centralizada.

❖ **Una arquitectura abierta.** MicroStrategy ha apificado prácticamente toda la plataforma, ha incluido un motor RestAPI para no solo poder consumir de cualquier sitio, si no para poder inyectar datos en cualquier sitio.



❖ **Modernizar la plataforma** para dar respuesta a esas necesidades de negocio modernas, como son autoservicio, pero un autoservicio gobernado, intuitivo y sin líneas de código. Dentro de la modernización, dispone de una tecnología que permite el acceso rápido, sencillo e intuitivo a la información, que se conoce con el nombre de HyperIntelligence.

Hyperintelligence es una tecnología que permite romper la brecha digital con los usuarios consumidores, y ayuda a acelerar el proceso de ser una compañía Data Driven.

El objetivo principal de Hyperintelligence es facilitar de manera rápida, sencilla e intuitiva la información a los usuarios con cero clics. Esto es, permite que los usuarios sin realizar clics con tan solo situarse sobre las palabras, conceptos de negocio que son importante para él, le abra una tarjeta que trae los datos relevantes de 1 o varias fuentes. De esta manera, la tarjeta permite consolidar los datos más importantes de múltiples sistemas, lo que acelera enormemente la productividad y permite que las decisiones estén apoyadas en los datos.

La otra gran característica de Hyperintelligence es su tiempo de despliegue, en tan solo unos días es posible tener las tarjetas disponibles, las cuales aparecerán sobre cualquier solución de mercado o aplicación desarrollada internamente que corra sobre navegador o móvil principalmente. ■

Hyperintelligence es una tecnología que permite romper la brecha digital con los usuarios consumidores, y ayuda a acelerar el proceso de ser una compañía Data Driven

MÁS INFORMACIÓN

- Healthcare Pharmaceuticals
- The Hyperintellicenge Pilot
- Health Solution Map
- Caso de éxito: Derbyshire NHS
- Caso de éxito: AllScripts
- HyperIntelligence

Seguridad Sophos para Sanidad

Sophos cuenta en su oferta tecnológica con soluciones de seguridad que aplican en el mundo de la Sanidad. Conozcamos algunas de ellas.

❖ **Sophos Intercept X EDR/XDR.** Es un sistema de protección endpoint que engloba la protección tradicional (firmas), junto con protección "next-gen" (Inteligencia Artificial, anti exploit, análisis de comportamiento, anti ransomware y anti hacking) así como protecciones complementarias (control web, control de aplicaciones, cifrado, DLP...) y, por supuesto, EDR o, a día de hoy, XDR, gracias a la integración cruzada de datos con sus firewalls, su servicio de correo, su UEM para la gestión de los dispositivos móviles y los sistemas de protección cloud. Su gestión se realiza a través de Sophos Central, lo que permite la interacción con otros productos de Sophos y gracias a su API, con cualquier fabricante.

❖ **Sophos MTR y Rapid Response**. Sophos Managed Threat Response (MTR) es un servicio gestionado de respuesta frente a amenazas, que ofrece a las empresas funciones de búsqueda, detección y respuesta ante posibles amenazas 24/7. Formado por un equipo de detección de amenazas y profesionales expertos en investigaciones avanzadas dando respuesta a los ciberataques y tomando medidas para neutralizar incluso las amenazas más sofisticadas. Sophos puede dar respuesta, apoyándose en el agente de Sophos para realizar las acciones oportunas para la detección y la mitigación de la amenaza. Cualquier empresa que sufra un ataque activo puede recurrir a Sophos Rapid Response, que es capaz de realizar un despliegue rápido del producto y su equipo de expertos en ciberseguridad son capaces de ver cuál es la situación dentro de la compañía, detener el ataque y, si es posible, detectar por dónde ha venido, a quién ha afectado y limpiar todo lo que haya sido dañado para que pueda volver a la normalidad lo antes posible.

❖ **Sophos Firewall.** La seguridad de red desde la compra de Astaro en 2008 por Sophos ha seguido evolucionando hasta llegar a los nuevos Sophos Firewall, que son gestionados de forma centralizada desde Sophos Central, se integran con el Endpoint y con el servicio MTR. Además, son capaces de hidratar el lago de datos, englobándose dentro de su estrategia XDR. La arquitectura de Xstream de Sophos Firewall protege la red de las amenazas más recientes, al tiempo que acelera el tráfico importante de SaaS, SD-WAN y aplicaciones en la nube.

❖ **Sophos Zero Trust:** Sophos ZTNA se basa en los principios de Zero Trust: no confiar en nada y verificarlo todo. Los usuarios y dispositivos se convierten en su propio perímetro microsegmentado, con lo que se validan y verifican constantemente. Con Zero Trust,

los usuarios ya no se encuentran “en la red” con la confianza y el acceso implícito que habitualmente conlleva. Sophos ZTNA es la única solución Zero Trust Network Access que se integra perfectamente con un producto para endpoints next-gen: Sophos Intercept X.

❖ **Sophos Email.** Seguridad del correo electrónico más inteligente con IA. Las actuales amenazas para el correo electrónico evolucionan rápidamente, y las empresas en expansión necesitan una seguridad predictiva para el email, es decir, que combata las amenazas de hoy día sin perder de vista el mañana.

❖ **Sophos Cloud Optix.** Conscientes de que cada vez más la infraestructura de TI está migrando a la nube, Sophos lleva tiempo hablando de CSWP y CSPM gracias al agente para servidores y a Cloud Optix, el cual audita los recursos que se tengan sobre proveedores de nube pública como AWS, Azure o Google Cloud. Además, se integra con XDR y con servicios como MTR, lo que proporciona más visibilidad e información que será recogida en el lago de datos. ■

MÁS INFORMACIÓN

- Ramsonware in Healthcare
- Adaptative Security
- Guía para la adquisición de servicios de detección

Las actuales amenazas para el correo electrónico evolucionan rápidamente, y las empresas en expansión necesitan una seguridad predictiva para el email

Seguridad de Stormshield para el sector sanitario

Stormshield cuenta con una serie de soluciones diseñadas para ayudar a las empresas del entorno sanitario a enfrentarse a los retos de ciberseguridad que tienen por delante.

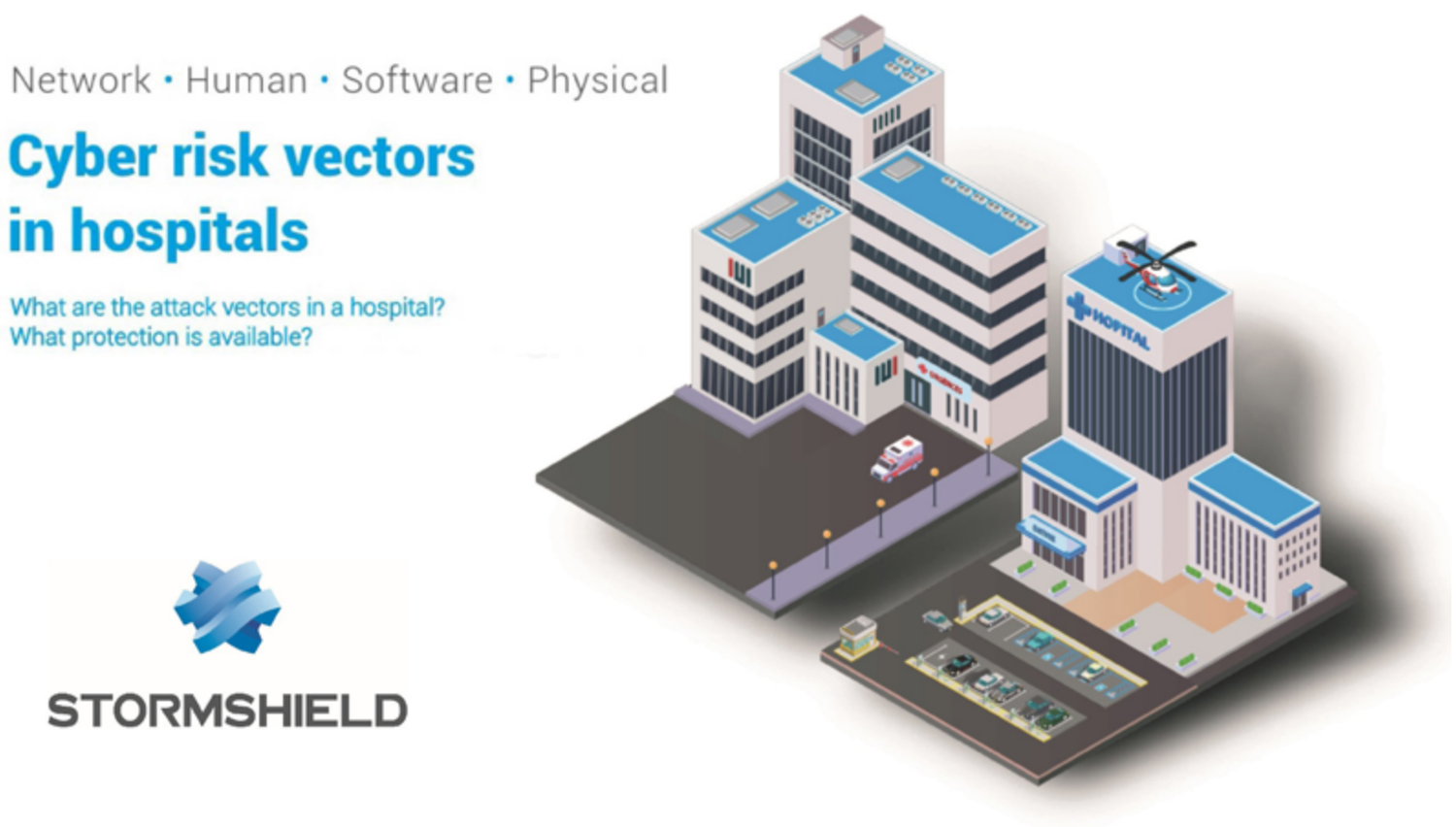
SNI20. FIREWALL A MEDIDA PARA ENTORNOS SANITARIOS

El firewall industrial SNi20 ofrece una integración de red única y completa (enrutamiento y NAT) y seguridad avanzada. Asimismo, proporciona una inspección profunda de paquetes (análisis basado en el contexto), permitiéndole proteger protocolos de comunicación de telemedicina, BMS (Building Management Systems) y CTM (Centralized Technical Management). El firewall garantiza la confiabilidad operativa de su infraestructura y una continuidad de negocio óptima en todo momento, incluso en caso de avería, gracias al sistema de alta disponibilidad y modo de seguridad de la red operativa.

El cortafuegos SNi20 ha sido diseñado para cumplir con los estándares de certificación más estrictos del mercado.

SNI40. FIREWALL PARA SISTEMAS SANITARIOS

El cortafuegos SNi40 está especialmente diseñado para proteger equipamiento médico (respiradores, imágenes médicas...) y equipamiento técnico como reguladores de presión, temperatura o gases y ofrece una amplia gama de funciones: segmentación de red, control de acceso por filtrado de direcciones IP o MAC, análisis contextual de paquetes, control de mensajes operativos y cumplimiento de protocolos (IPS) y comunicaciones seguras de mantenimiento remoto (VPN). Además, este equipo se puede integrar fácilmen-



te en su entorno, especialmente en sus armarios de control (sobre rieles DIN), gracias a un sencillo procedimiento de puesta en marcha.

El SNi40 garantiza la continuidad de la actividad gracias, en particular, a su sistema de alta disponibilidad y al modo de seguridad de la red operativa, que mantiene sus sistemas de producción funcionando sin interrupción, incluso en caso de fallo.

El SNi40 es un cortafuegos certificado al más alto nivel europeo. Ha recibido la certificación y calificación CSPN a nivel elemental, emitida por ANSSI. Por ello, si elige esta solución de Stormshield Network Security, puede estar seguro de que su infraestructura industrial estará cubierta por la mejor protección posible.

STORMSHIELD ENDPOINT SOLUTION (SES)

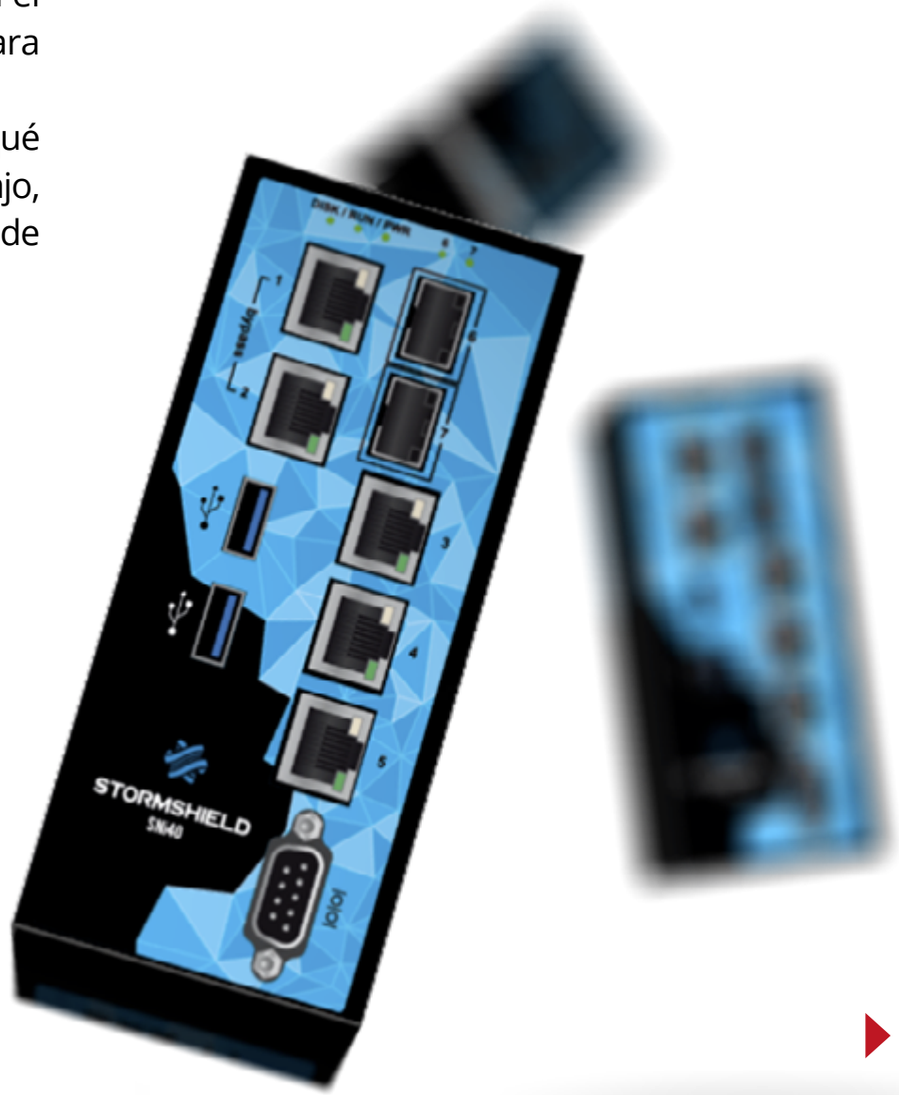
A menudo considerados como los eslabones más débiles en la seguridad de TI, los terminales incluyen todos los dispositivos que se conectan a la red central de una organización sanitaria: ordenadores de escritorio y portátiles, tabletas, teléfonos inteligentes, impresoras y todos los demás dispositivos (inteligentes o no) que se nos requiera conectar a la red interna. Sin embargo, todos estos terminales podrían ser secuestrados y utilizados por los ciberdelincuentes como un punto de entrada para penetrar en su sistema informático con el fin de instalar malware u obtener acceso a sus datos. Desde ellos, pueden saltar a la red hospitalaria provocando graves daños.

SES tiene características que lo hacen especialmente adecuado para el entorno sanitario: protege sistemas operativos obsoletos que siguen operando en redes de imágenes médicas, por ejemplo, como puede ser Windows XP. Por otra parte, SES no está basado en firmas ni necesita conexiones al exterior para su correcto funcionamiento. Por último, hay que destacar sus capacidades de creación de listas blancas, que no son manejables en el mundo IT pero sí en el sanitario, donde las aplicaciones necesarias para los puestos son mínimas y estables.

SES también controla qué dispositivos y a qué redes puede conectarse cada puesto de trabajo, bloqueando, por ejemplo, el uso no deseado de dispositivos USB. ■

MÁS INFORMACIÓN

- Telemedicina y ciber-riesgos
- Cómo prevenir ataques de ransomware
- Vulnerabilidades en la infraestructura de un hospital
- DPI Systems Network Security
- Context/Behavior-aware Endpoint Protection and response to meet digital and hybrid workforce requirement



IBERLAYER

Cloud Email Security

9 de cada 10 incidentes de
ciberseguridad empiezan por email

¿Cuánto le preocupa la seguridad del suyo?

WWW.IBERLAYER.COM

Protección total contra Spam, Phishing, Ransomware, Malware,
APTs, Scam, Fraudes de CEO, Fraudes Bancarios ...