TECNOLOGIA Y SANIDAD:

la mejora en la atención del usuario

Patrocinadores:

COMMSCOPE® RUCKUS®

GRENKE

SOPHOS

S21SEC

Las TIC en Sanidad: el paciente como eje central de las nuevas tecnologías

En un mundo impulsado por la digitalización, la integración de la tecnología es prioritaria, más si cabe en un sector como el de la sanidad, sometido a significativos cambios durante el último año.

La pandemia generada por el Coronavirus SARS-CoV-2 ha puesto de manifiesto la importancia de contar con un sistema sanitario eficaz, accesible y resiliente, no solo a nivel de capacitación de los profesionales, sino también en lo referente a infraestructuras, servicios de alto valor, y, por supuesto, mejores tecnologías.

Y es que, como en todo, aunque en el sector sanitario con más razón, la adopción de nuevas tecnologías, sobre todo de las centradas en la Información y la Comunicación (TIC), puede aportar un valor diferencial. La Socie-

dad Española de Informática de la Salud (SEIS) considera las TIC, "imprescindibles para afrontar los retos actuales de los sistemas de salud en sus procesos de modernización y racionalización, y para lograr la transformación digital del sector. Además, su utilización intensiva favorece el tejido industrial, la innovación y la economía del país" .

Sin embargo, en este contexto de evolución digital, es importante tener en cuenta que la transformación tecnológica del sector sanitario debe ir más allá de la mera digitalización de los procesos; también implica ofertar nuevos productos y servicios digitales a los pacientes, además de acercar capacidades de diagnóstico, tratamiento y seguimiento a millones de personas, sin importar su ubicación.

Precisamente, y a lo largo del último año, con el sistema de salud colapsado a causa de la Covid-19, el redireccionamiento de la asistencia a los pacientes a través de la atención y el seguimiento a distancia ha sido más trascendental que nunca, convirtiéndose en muchos casos en la única alternativa, bien como primera capa informativa o canal de comunicación bidireccional entre el usuario y los diferentes profesionales de los distintos niveles asistenciales.

En este sentido, y junto a la telemedicina, Internet se ha alzado como medio idóneo para que los pacientes puedan acceder a asistencia médica sin tener que pasar por hospitales y centros de salud. Así, sistemas de videoconsulta, videollamadas, aplicaciones móviles o chatbots están siendo muy utilizados. También, otras tecnologías como Inteligencia Artificial, Machine Learning, Big Data o la analítica avanzada de datos están permitiendo progresar en cuanto a detección temprana y previsiones de evolución del coronavirus, entre otras. Y, por supuesto, IoMT, el Internet de las Cosas Médicas, un sistema de dispositivos médicos interconectados que utilizan sensores informáticos para así poder intercambiar datos a través de Internet. Con esta tecnología es posible conocer con mayor precisión la situación del paciente, aplicar tratamientos más efectivos y facilitar la prevención.

No obstante, y pese a estos avances, el sistema sanitario español, sobre todo la sanidad pública, sigue aquejado de una escasez de recursos de distinta índole. Años de falta de inversión, barreras administrativas, desajustes estructurales y una segmentación política incesante han lastrado su digitalización, actuando como verdaderos inhibidores. A este respecto, el Índice SEIS 2019 cifra la inversión sanitaria actual en TIC en España en 707.344 euros, un 3% menos que en 2018, mientras que el personal especializado en TIC y el gasto global en plataformas tecnológicas también se ha reducido un 1,86% y un 8,19% respectivamente.

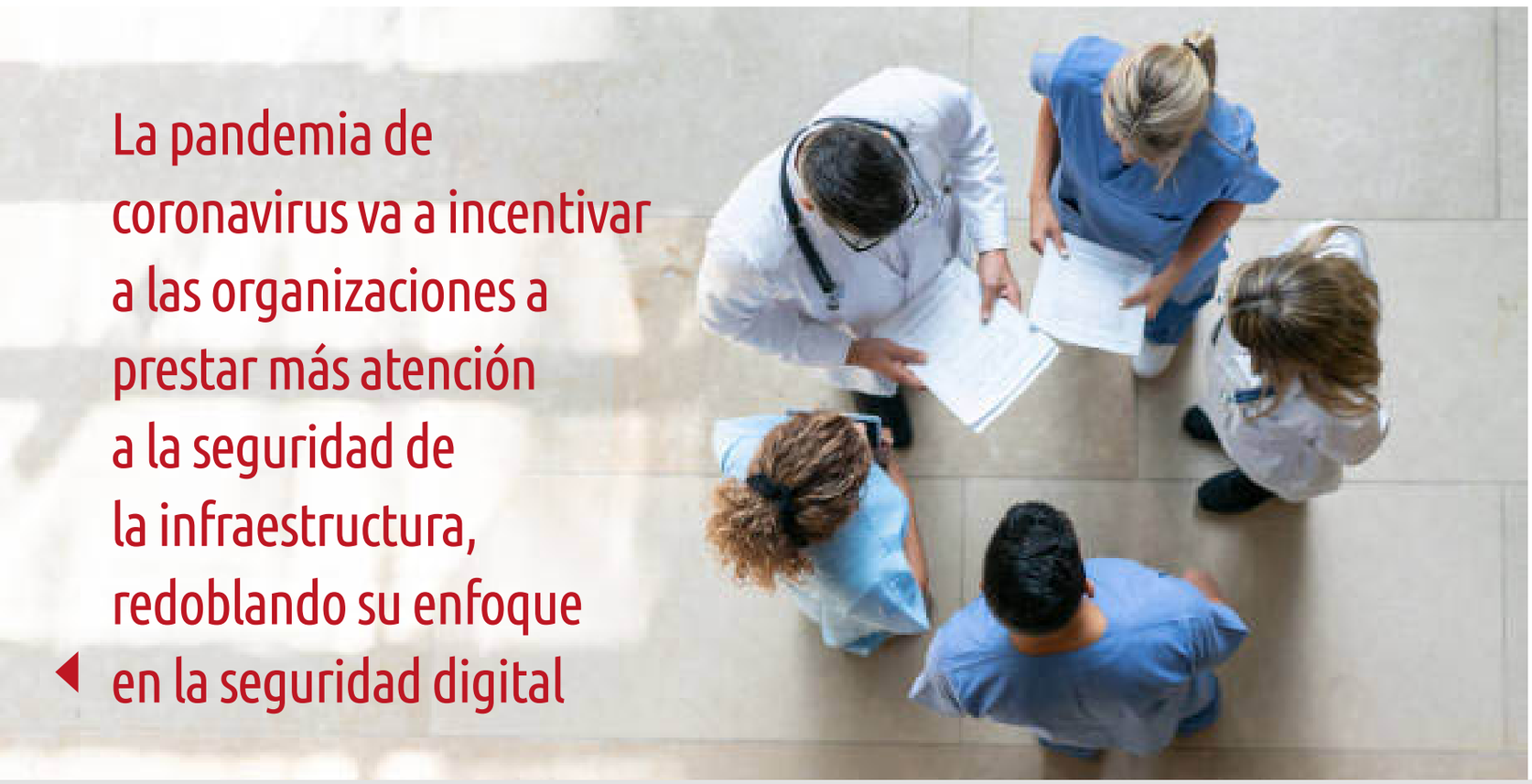
En la actualidad, y tras lo acontecido a lo largo del último año, es de esperar que la tendencia cambie: la Covid-19 ha acelerado la adopción digital en todos los ámbitos, incluido el sanitario, por lo que las TIC se hacen imprescindibles para afrontar los retos actuales.

IMPULSAR UNA ESTRATEGIA DE SALUD DIGITAL

Sobre este necesario avance, la ministra de Sanidad, Carolina Darias, adelantaba el pasado mes de febrero los principales puntos que constituyen la hoja de ruta de su Ministerio para los próximos años y entre los que se encuentran, la digitalización y la innovación de la sanidad. Adicionalmente, el Gobierno de España ha incluido en los Presupuestos Generales del Estado (PGE) para 2021 una dotación de 400 millones de euros para la Renovación de Tecnologías Sanitarias en el Sistema Nacional de Salud (SNS), además de 295,5 millones destinados a acelerar la estrategia digital del SNS.

A nivel privado, empresas como Accenture ya valoran que las empresas sanitarias preparadas para el futuro implementen estrategias digitales más innovadoras. Ya se trate de aplicaciones móviles, nube, EHR o wearables, las organizaciones líderes pueden cambiar fundamentalmente la forma en que se presta la atención médica.

Es de prever, por tanto, que estas iniciativas, y otras que estén por venir, potenciarán la innovación del sector sanitario, un nicho que hasta ahora se ha centrado mayoritariamente en integrar tecnologías dirigidas a modernizar el propio sistema en sí, como la Receta Electrónica o el acceso a la historia clínica electrónica por parte de los facultativos, más que en otras dirigidas a cubrir las necesidades reales de pacientes y profesionales.



La pandemia de coronavirus va a incentivar a las organizaciones a prestar más atención a la seguridad de la infraestructura, redoblando su enfoque en la seguridad digital

Preciso es también procesar adecuadamente los volúmenes masivos de información que caracterizan la actividad propia de los servicios de salud y que bien aprovechados pueden generar enormes beneficios.

EL DATO, EL ACTIVO MÁS SENSIBLE

La digitalización de los dispositivos utilizados en el entorno de la sanidad genera una ingente cantidad de información sensible sobre el ser humano. Se estima que en 2020 se alcanzaron los 25.000 petabytes de datos en el entorno sanitario, una cifra que sigue incrementándose de forma exponencial, influida también por el desarrollo de dispositivos IoT, que están contribuyendo a que los datos crezcan a una escala nunca vista.

Tal acumulación masiva de datos hace imposible su gestión a través de sistemas tradicionales, por lo que tecnologías como Big Data, Business Intelligence o la analítica de datos ofrecen nuevas posibilidades para la elaboración de modelos predictivos, patrones de comportamiento o para la provisión de servicios más personalizados en tiempo real. Igualmente sientan la base para la interoperabilidad electrónica de la información sanitaria y allana el acceso a la tan ansiada Medicina 5P (Personalizada, Predictiva, Preventiva, Participativa y Poblacional); el cruce entre la sanidad y Big Data.

El análisis de grandes conjuntos de datos también ha servido como base para la aplicación de la Inteligencia Artificial, Machine Learning o Deep

TECNOLOGIA Y SANIDAD: la mejora en la atención del usuario

Learning en el campo de la salud, como una herramienta fundamental de la medicina personalizada. Estas tecnologías pueden ampliar la analítica con el aprendizaje continuo y los análisis, derivando en una ventaja para el ser humano gracias a mejoras en el diagnóstico precoz de enfermedades, los tratamientos a medida, y una mejor administración eficaz de recursos sanitarios.

Por tanto, no hay duda de que el tratamiento global y sistemático de los datos ha abierto un nuevo mundo en distintas áreas. Sin embargo, el acceso a datos personales por parte de facultativos, máquinas y demás responsables no gusta a todos por igual.

En este contexto, satisfacer las expectativas sobre la privacidad y seguridad de los datos se hace clave para impulsar la sanidad digital. Sin duda, el conocimiento por parte del paciente de la finalidad del uso de sus datos y de los mecanismos de protección empleados incrementará la confianza en la sanidad digital.

PROTEGER Y CUIDAR LOS DATOS

La información confidencial que maneja el sector sanitario es de gran interés para la ciberdelincuencia por lo que se ve continuamente sometida a ataques, además de ser víctima de brechas o fugas de información que generan un gran coste económico (5,8 millones de euros, en 2020, según Data Breach Report publicado por IBM). Y es que, por su importante información, los registros médicos de pacientes tienen un valor en el mercado negro hasta 50 veces superior al de la información financiera personal, lo que explica que los ataques contra el sector sanitario se incrementen sin medida. No hay más que ver que el número de intentos de ataque contra empresas de la salud aumentó a nivel mundial un 45% durante los dos últimos meses de 2020, según indica Check Point, más del doble de lo que creció en todos los sectores a nivel mundial. En el caso de España, el número de ataques contra infraestructuras sanitarias también se duplicó en ese periodo, tal y como revela dicha fuente.

Las amenazas más comunes que afectan al sector salud tienen su origen en el correo electrónico: suplantación de identidad, campañas de phishing, adjuntos maliciosos, aunque es el ransomware el que muestra el mayor aumento, sobre todo la variante Ryuk. Los cibercriminales saben que una interrupción del servicio en un hospital puede ser crítico, por lo que apuntan sus objetivos a estos blancos, más propensos a satisfacer sus demandas de rescate.

SIN VACUNA PARA LOS ATAQUES

En cuanto a las tendencias, es de esperar que la pandemia de Covid-19 siga actuando sobre la mayoría de las amenazas y riesgos, muchos de estos directamente relacionados con el aumento del teletrabajo. En este sentido, el mayor uso de soluciones en la nube, conexiones VPN, servicios de escritorios VDI, redes de confianza cero y gestión de identidades, servicios y tecnologías

La pandemia de coronavirus va a incentivar a las organizaciones a prestar más atención a la seguridad de la infraestructura, redoblando estas su enfoque en la seguridad digital

para el acceso remoto, uso de herramientas colaborativas o aplicaciones de videoconferencia generará que los ataques a estos entornos, en especial a los sistemas públicamente expuestos, sigan creciendo . También los ataques y vulnerabilidades relacionados con redes domésticas o dispositivos personales y los dirigidos contra farmacéuticas, laboratorios de investigación dedicados a la Covid-19. Asimismo, y en relación a los ataques de ransomware, es necesario señalar una tendencia, ya consolidada, como es la sofisticación de dichos ataques.

Sin duda, la medicina se usará como señuelo al menos hasta el final de la pandemia. El factor humano es uno de los componentes más importantes de muchos ataques, y la información sobre nuevas restricciones regulatorias, tratamientos potenciales y la salud del paciente seguirá atrayendo la atención de los usuarios. Los expedientes médicos filtrados también se convertirán en parte del gancho de los ataques dirigidos, ya que la información precisa del paciente hará que los mensajes falsos sean mucho más creíbles.

No obstante, también hay buenas noticias. La pandemia de coronavirus va a incentivar a las organizaciones a prestar más atención a la seguridad de la infraestructura, redoblando estas su enfoque en la seguridad digital. Es más, según se desprende del Informe de Ciberpreparación de Hiscox 2020, la industria española de Pharma y Salud ha mejorado con respecto a 2019 tanto su ciberpreparación, incrementándose desde el 4% al 12% el número de empresas calificadas como expertas, como la inversión en TI. Las compañías participantes han pasado de invertir el 4,6% del presupuesto de TI en ciberseguridad al 13,73% en 2020. Además, más de la mitad (56%) dicen integrar aspectos de ciberseguridad en todos los procesos y proyectos desarrollados en su plan de negocio, convirtiendo esta área en una variable transversal a toda la organización.

A raíz de esta situación, no hay duda de que las TIC juegan y jugarán un papel determinante en las organizaciones sanitarias, para facilitar la gestión eficiente de los servicios ofrecidos a la ciudadanía y la capacidad asistencial. La necesidad de comunicarse de manera efectiva con los pacientes es una prioridad, como ha quedado demostrado. Por tanto, hay que seguir trabajando para aumentar las conexiones digitales con los pacientes (más datos y análisis en tiempo real) para mejorar la calidad asistencial mediante una medicina basada en la evidencia y en al análisis del dato para la toma de decisiones adecuadas. Es hora de desarrollar una medicina personalizada con la ayuda de las TIC. ■

MÁS INFORMACIÓN

- Índice SEIS 2019
- Hoja de ruta del Ministerio para digitalizar e innovar en Sanidad
- Renovación de Tecnologías Sanitarias en los Presupuestos Generales del Estado
- IBM Data Breach Report
- Incremento de ataques a organizaciones sanitarias por la Covid19

Una infraestructura de red inteligente mejora los resultados, las operaciones y la seguridad a todos los niveles.

Los centros de atención médica super conectados del mañana ofrecen oportunidades casi ilimitadas para potenciar la conectividad universal (cableada, Wi-Fi y celular en interiores) para construir una red estable de servicios, aplicaciones y herramientas que sirven como base de la evolución de su red a largo plazo. Desde la oficina más pequeña hasta el laboratorio de investigación más avanzado y el campus hospitalario más grande, existen nuevas y emocionantes formas de mejorar la atención sanitaria y la eficiencia operativa.

Conozca las soluciones de CommSCope para el Sector Sanitario: **Click aquí**

Transformación tecnológica como paso previo hacia un nuevo modelo de sanidad

El de la Sanidad es un segmento especial, tanto por la necesidad de inmediatez en la respuesta como por la sensibilidad de los datos que manejan. Por ello, este sector debe poner todo de su parte para ofrecer un servicio continuado, pero sin descuidar aspectos como la seguridad de la información o la protección de los dispositivos de salud. Los retos, por tanto, no dejan de crecer. ¿Está la Sanidad española preparada para superarlos?

Para hablar de estos temas y analizar otras cuestiones como el estado actual de la inversión en la Sanidad, nuevas formas de financiación y servicio o conocer qué se está haciendo, tanto desde la sanidad pública como privada para proteger los datos y luchar contra el incremento de ciberataques, hemos contado con la participación en esta #MesaRedondaIT de Bernardo Gómez, territory account manager Iberia de CommScope; Marco Frühauf, vicepresidente de Grenke; e Iván Mateos, Ingeniero preventa de Sophos. Asimismo, incluimos las opiniones y valoraciones de Jairo Alonso, ICS security consultant de S21Sec, quien por problemas de última hora no pudo conectarse al debate.

ESTADO DE SALUD TECNOLÓGICO

Sin duda, y en lo que respecta a la adopción de Tecnologías de la Información y la Comunica-

TECNOLOGÍA Y SANIDAD: mejora en la atención al paciente

“La situación actual puede repetirse, y hay que estar preparados. No obstante, el ritmo de inversión se ralentizará a medio plazo, porque las inversiones se han adelantado. En un año hemos avanzado lo que en condiciones normales hubiese llevado entre tres y cinco”

BERNARDO GÓMEZ, TERRITORY ACCOUNT MANAGER IBERIA DE COMMSCOPE

ción, el sector sanitario ha dado un gran paso de gigante a lo largo del último año. En este contexto, Bernardo Gómez considera que la situación provocada por la pandemia ha servido como “catalizador para impulsar la adopción de este tipo de tecnologías y si bien aún queda mucho camino por recorrer, el sanitario se encuentra en un punto significativamente desarrollado”.

Algo distinto ocurre en lo concerniente a los flujos de caja, donde Marco Frühauf, evidencia algunos desafíos: “durante el último año, algunos subsectores, como el de las farmacias, han tenido que hacer frente a una falta de tesorería, al no recibir, o fluir más lenta, la financiación proveniente de las Administraciones Públicas”. Por tanto, y aunque por su trascendencia este sector demanda estar perfectamente equipado, “también requiere estar bien financiado, y aquí todavía hay aún muchos retos”.

“La rápida digitalización de principios de 2020 abrió la puerta a nuevos riesgos en ciberseguridad, que han tenido que ir mitigándose”, reconoce Iván Mateos. Sin embargo, y aunque la situación actual es más positiva de lo que se preveía, el sector sanitario sigue en el punto de mira de muchos atacantes. No obstante, “las empresas están actuando, tomando decisiones a corto y medio plazo y en ese sentido no vamos por mal camino, aunque hay que seguir avanzando”.

“La sanidad española dispone de prácticamente los últimos dispositivos del mercado”, destaca Jairo Alonso, por lo que, a nivel de equipamiento tecnológico está bastante actualizada para hacer frente a los problemas de ciberseguridad. Sin embargo, “esto no significa que no existan otros equipos y dispositivos tradicionales que sigan funcionando perfectamente”, reconoce este responsable.

INVERSIÓN SIN PLANIFICACIÓN

A raíz de lo comentado, no hay duda de que la inversión en tecnologías a lo largo del último año ha sido muy importante en Sanidad. Sin embargo, ¿se han hecho estas adquisiciones en base a una planificación o las empresas se han dejado llevar por la alarma del momento?

Aunque, en los primeros meses, la aceleración en los procesos de digitalización llevó a muchas empresas a realizar una inversión tecnológica no planificada, Marco Frühauf considera que según se fue avanzando, y teniendo acceso a más información, la situación varió. “Las grandes inversiones se han hecho bien, han sido planificadas. Sin embargo, sobre todo al principio, se tomaron decisiones precipita-

das; se adquirió equipamiento que no era necesario o que no era la solución adecuada, debido a una gran desinformación".

En la misma línea, Iván Mateos coincide en destacar cierta improvisación a la hora de adquirir equipamiento, porque al principio lo que primaba era la productividad. "Hoy con el conocimiento de que esta situación aún se va a extender en el tiempo se impone la planificación, ajustar los presupuestos a las necesidades, ya sin prisa. En su momento se cometieron muchos fallos, se abrieron más puertas de las necesarias y esto trajo distintas consecuencias. "Lo peor ya pasó y ahora estamos intentando hacerlo todo mejor".

Sobre las infraestructuras de comunicaciones, Bernardo Gómez destaca que se han acelerado los tiempos de despliegue de las agendas de digitalización ya preestablecidas, variando las prioridades. "Si antes de la pandemia, hospitales y residencias apostaban por el desarrollo de las redes de uso interno, con la integración de tecnologías como IoT, la nueva situación ha llevado a priorizar las redes de accesos para los pacientes. "Hemos pasado de la incertidumbre a la racionalización de la tecnología, una vez entendido a qué nos enfrentamos".

La adquisición de tecnología debe responder a un plan ya previsto. Así, Jairo Alonso se muestra convencido de que la aceleración en los procesos de digitalización provocada por la Covid-19, ha comprometido la planificación necesaria en cualquier proyecto de digitalización. Es más, según este responsable, "en el mundo de la seguridad la falta de planificación acaba pasando factura a largo plazo, bien sea en forma de ataque, que no sería lo deseado, o bien obligando a las empresas a incrementar sus presupuestos para optimizar su seguridad".

> "La tecnología tiene que ser flexible. Tenemos que poder cambiarla cuando nos convenga. Por ello, tenemos que adoptar un enfoque de pago por uso, y para ello, debe darse un cambio de mentalidad"
>
> MARCO FRÜHAUF, VICEPRESIDENTE DE GRENKE

CIBERSEGURIDAD

Con una amalgama de empresas públicas y privadas, el de la Sanidad es un segmento especial, tanto por la necesidad de inmediatez en la respuesta como por la sensibilidad de los datos que manejan. ¿Son los retos en ciberseguridad los mismos para la sanidad pública y privada?

Independientemente de que sea público o privado, el sector sanitario tiene que ofrecer un servicio continuado. Por ello, Iván Mateos explica que "enseguida entiendes su forma de trabajar". Para el personal de IT, la ciberseguridad es importante, pero lo es más que un dispositivo no funcione o que falle una conexión entre máquinas. "Así, es necesario elevar el nivel de ciberseguridad, pero sin olvidar sus requisitos. Los fabricantes debemos poner ciberseguridad sin implicar dificultad, una vez que lo comprendes, el planteamiento coge buen rumbo".

Sobre esta necesidad de elevar la seguridad, Bernardo Gómez destaca que esta exigencia

es igual tanto en la sanidad pública como en la privada. La diferencia fundamental estriba en la velocidad con la que se adopta y adapta la tecnología, que sin duda es mucho más rápida en el sector privado. No obstante, no hay que olvidar que "la información es crítica, y cada vez hay más dispositivos conectados en el entorno sanitario, por lo que hay muchos riesgos a los que hacer frente".

Para Marco Frühauf la sanidad pública y la privada abordan sus retos de forma totalmente distinta. Así, "hay enormes diferencias en cuanto a la rapidez en la adopción de medidas o en la toma de decisiones, aunque las necesidades sean las mismas". Respecto a la financiación de la tecnología, el sector privado está mucho más abierto a nuevos métodos más alejados de las tradicionales. "Los retos y las posibilidades se entienden mejor y se pueden dar soluciones de un modo mucho más eficiente".

Por su parte, Jairo Alonso reconoce que además de ser un segmento esencial, gran parte de la sanidad, tanto pública como privada, se considera infraestructura crítica. "Esa significación conlleva que deben aplicarse medidas de seguridad más concretas y que apoyen y favorezcan en todo momento la prestación del servicio".

Ahora bien, ¿por qué hay tanta diferencia a la hora de afrontar un escenario de ciberseguridad?

Según Marco Frühauf este contraste se debe principalmente a que el sector público es mucho más complejo. "Hay que lidiar con distintas administraciones y organismos por lo que el proceso de toma de decisiones es mucho más largo y difícil, además de existir cierta opacidad a la hora de interpretar por dónde va la cosa".

En cuanto al ritmo de digitalización, ¿es de esperar que continúe en la misma línea tras la pandemia?

Sobre esta cuestión, Bernardo Gómez observa que esta nueva aproximación a la digitalización se mantendrá. "La situación actual puede repetirse, y hay que estar preparados". No obstante, el ritmo de inversión se ralentizará a medio plazo, porque las inversiones se han adelantado. "En un año hemos avanzado lo que en condiciones normales nos hubiese llevado entre tres y cinco".

Pese a estos avances, toca saber si el dato, está adecuadamente protegido.

El sector sanitario debe gestionar información muy sensible, que no es fácil de manejar, y que si se filtra o se pierde puede traer graves consecuencias. Por ello, Iván Mateos apunta a que es necesario buscar soluciones concretas: "El primer paso es identificar el riesgo, y luego querer abordarlo. Buscar una solución de seguridad concreta para ese problema es más sencillo".

Muy importante es también cumplir con las distintas normativas para la seguridad de la información. En este punto, Jairo Alonso afirma que a nivel TI, normas de seguridad como la ISO 27001 son seguidas ampliamente en el sector, "el problema viene cuando el sector se olvida de su parte industrial, de cumplir con normas como IEC 62443 que afectan a los dispositivos médicos y a sus redes.

"La seguridad como servicio puede suplir muchas carencias, pero la falta de conocimientos y experiencia de los usuarios no es uno de ellos. El factor humano suele ser casi siempre el eslabón débil de la cadena, por lo que es necesaria una capacitación en seguridad"

JAIRO ALONSO, ICS SECURITY CONSULTANT DE S21SEC

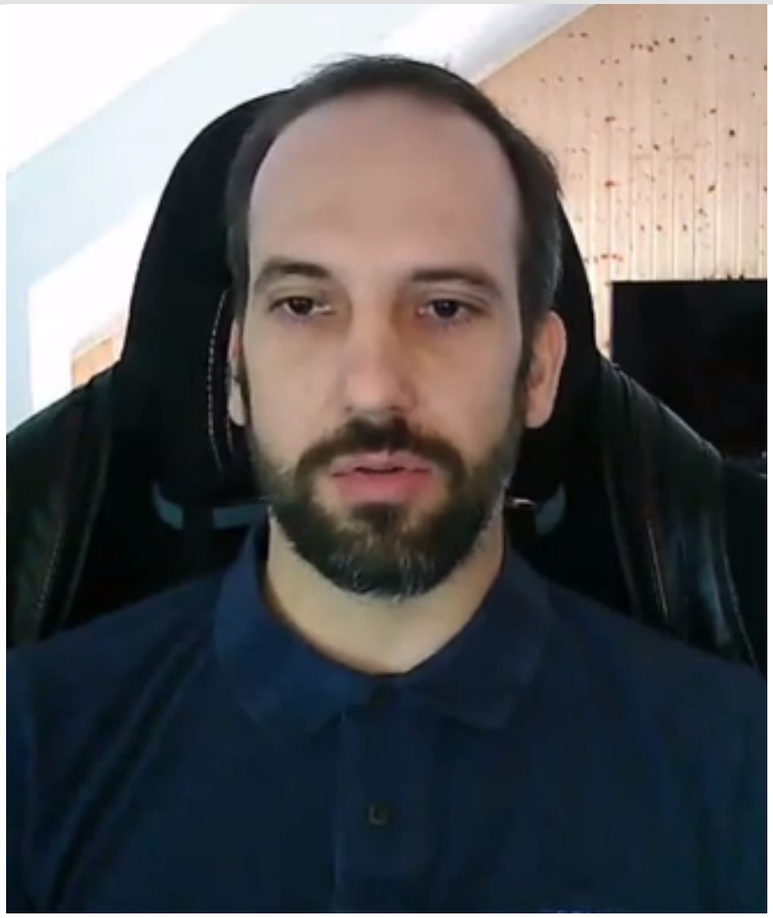
PRINCIPALES RETOS EN SANIDAD

La telemedicina ha llegado para quedarse, tanto en el sector público como privado, por lo que hay que adaptar las infraestructuras para ofrecer un servicio de calidad al usuario.

Así, según Bernardo Gómez es necesario poner los recursos para el personal sanitario en

“Para el personal de IT, la ciberseguridad es importante, pero lo es más aún que un dispositivo no funcione o que falle una conexión entre máquinas. Es necesario elevar el nivel de ciberseguridad, pero sin olvidar sus requisitos”

IVÁN MATEOS, INGENIERO PREVENTA DE SOPHOS



su dispositivo, dotar de conectividad a todo el equipamiento con el que cuentan los centros sanitarios, para que la información fluya libremente, además de garantizar su seguridad: “No solo preocupa que alguien pueda acceder a la información, sino también que pueda modificarla. Estos son los grandes retos”.

Por su parte, Marco Frühauf considera que “la inversión tiene que continuar”, pero es necesario que quienes controlan el dinero, los financieros, cambien su enfoque hacia uno centrado en el pago por uso. “La tecnología tiene que ser flexible. Tenemos que poder cambiarla cuando nos convenga. Por ello, tenemos que adoptar un enfoque de pago por uso, y para ello, debe darse un cambio de mentalidad, que en España está costando bastante”.

Según Iván Mateos, el principal desafío es que el sector sanitario pueda seguir avanzando tecnológicamente, sin incurrir en un riesgo para la seguridad. Una vez llevado este riesgo al mínimo exponente, se podrán ofrecer soluciones en todos los ámbitos: software, hardware y servicios. El reto por tanto pasa porque “tecnológicamente el servicio pueda crecer, que se pueda dar sin interrupción y que la ciberseguridad no sea un problema, para que los trabajadores puedan dedicarse a su trabajo”.

Asegurar una compartición segura de los datos para que los pacientes puedan ser atendidos en cualquier lugar o incluso en remoto y el médico pueda disponer de todo el historial clínico es el principal reto, según considera Jairo Alonso. “Tampoco debe ignorarse la seguridad de los dispositivos que monitorizan y controlan la salud de los pacientes, tanto los que pueden llevar en su propio cuerpo como los utilizados en quirófanos y UCI”.

TECNOLOGÍA Y SEGURIDAD COMO SERVICIO

¿Es el sector sanitario un buen escenario para el despliegue de tecnología como servicio?

Sobre este aspecto Bernardo Gómez reconoce que el sector privado está empezando a desplegar este modelo por su bajo impacto presupuestario y por la rápida evolución de las tecnologías, lo que permiten estar siempre actualizados. A la contra el sector público sigue anclado en el modelo presupuestario tradicional y se muestra más reticente a este tipo de inversiones. “Es una tendencia que acabará cambiando, pero queda tiempo para este cambio de mentalidad”.

En la misma línea, Marco Frühauf también reconoce el avance de la sanidad privada en este punto, sin embargo, valora que el cambio en el sector público tardará bastante tiempo

en producirse. “Con intereses y procesos que cambian, y atrapadas en concursos públicos y partidas presupuestarias ya fijadas, las administraciones públicas son presas de sus propios métodos y o te adaptas a ellos o no juegas. Al contrario que en la privada, es complicado cambiarles el paso”.

Para Iván Mateos ofrecer la tecnología como servicio es la respuesta, también en ciberseguridad. Ante la falta de capacidades tecnológicas y de expertise, la opción más adecuada es contratar un servicio que se dedique a vigilar la infraestructura, implementar soluciones de pago por uso, sencillas de utilizar y que no afecten a la operativa diaria. “Como fabricantes tenemos que facilitarles el trabajo, ofrecerles una tecnología sencilla, que le permita centrarse en su trabajo. Cuanta más tecnología se tiene, más eficiente se vuelve el sector sanitario”.

Por su parte, Jairo Alonso también señala que el sector sanitario es un buen escenario para el despliegue de seguridad como servicio, no obstante, considera que la falta de conocimientos y experiencia de los usuarios no es uno de ellos. “El factor humano suele ser casi siempre el eslabón débil de la cadena, por lo que es necesaria una capacitación en seguridad”. ■

MÁS INFORMACIÓN

Tecnología y Sanidad: mejora en la atención al paciente

Un mensaje para los responsables tecnológicos

Tras el empujón en inversión tecnológica vivido a lo largo del último año, es de esperar que todo esto siga mejorando de cara a maximizar los resultados. ¿Cómo puede lograrse? Sobre este hecho, “es importante aprovechar la inercia”, reflexiona Bernardo Gómez, “continuar invirtiendo en dos líneas críticas a nivel de infraestructura: la digitalización de los procesos de los centros hospitalarios, pero sin olvidar al paciente, a fin de darle capacidad de comunicación en los centros hospitalarios y en las residencias de mayores cuando se encuentre en ellos”.

Asimismo, Marco Frühauf también aboga por sacar partido de la experiencia, aprovechar todas las herramientas existentes para flexibilizar el modelo de gestión de las tecnologías para una mejor toma de decisiones. “Aprovechar la experiencia y el conocimiento para poder tomar las decisiones adecuadas y ser flexibles, manteniendo una inversión permanente”.

Dialogar, escuchar las necesidades de los responsables de tecnología y ciberseguridad es imprescindible para mantener esta tónica de implementación tecnológica, reconoce Iván Mateos. “A lo largo del último año se han visto los beneficios de implementar tecnología; ante un problema, se puede seguir trabajando e incluso la productividad se incrementa. Tanto técnicos como personal sanitario son igual de importantes para que el servicio no se detenga”.

Por último, Jairo Alonso concluye este bloque con un mensaje similar dirigido a las organizaciones de salud, “que no tengan miedo en contactar con empresas de seguridad. Estamos para ayudarles y podemos identificar sus necesidades principales a nivel de seguridad”.

GRENKE

FAST // FORWARD // FINANCE

¿TUS CLIENTES QUIEREN TU TECNOLOGÍA PERO NO TIENEN LA LIQUIDEZ PARA PAGARLA?

CONTACTA CON NOSOTROS

916305672

O CONTIGO@GRENKE.ES

Estar a la vanguardia tecnológica para ser más competitivo es una necesidad, pero en ocasiones resulta complicado sin que esto afecte a la liquidez de tu negocio.

Gracias al renting tecnológico y de equipamiento de GRENKE podrás ayudar a tus clientes a conseguirlo. Ellos pagan cómodas cuotas mensuales, en lugar de desembolsar el total, mientras tu cobras el 100 % de tu factura en 24 horas. ¡Así de fácil!

WWW.GRENKE.ES

JUAN DIZ, ASESOR SÉNIOR TIC SANIDAD

“Hemos visto que la sanidad va retrasada en la Transformación digital y eso conlleva escasa cartera de servicios digitales no presenciales”

La sanidad es un ecosistema de muy diversos actores y muy complejo y por tanto es difícil generalizar con sus profesionales, pero digamos que buscan una excelente usabilidad y movilidad de los sistemas de información

En su opinión, ¿qué carencias desde el punto de vista tecnológico ha destapado la situación de pandemia que estamos viviendo en las Infraestructuras sanitarias?

La obsolescencia de los actuales sistemas de información y la baja calidad del dato han quedado al descubierto con esta pandemia. Asimismo, hemos visto como la sanidad va retrasada en la Transformación digital y eso conlleva escasa cartera de servicios digitales no presenciales, lo que en casos como esta pandemia ha colapsado y retrasado toda la actividad no “covid” existente, impidiendo la accesibilidad y equidad del sistema.

Teniendo en cuenta la criticidad de la Infraestructura sanitaria, ¿qué ventajas aporta la tecnología a los profesionales del sector, tanto desde el punto de vista sanitario como de gestión?

Las tecnologías que subyacen en la Transformación Digital son claves para apuntalar la transformación de la sanidad a la medicina 5P. Los sistemas de “Big Data” son vitales para una medicina poblacional y predictiva, las aplicaciones móviles y portales web son esenciales para una sanidad participativa y preventiva y el “Deep learning” y la Inteligencia Artificial dan soporte a la medicina de precisión o personalizada.

¿Cuáles son las principales demandas tecnológicas de los profesionales del sector sanitario?

La sanidad es un ecosistema de muy diversos actores y muy complejo y por tanto es difícil generalizar con sus profesionales, pero digamos que buscan

“La Sanidad se tiene que transformar a una sociedad digital y eso requiere consensos que permitan cambiar las organizaciones, procesos y por último sistemas”

una excelente usabilidad y movilidad de los sistemas de información que realmente le descargue de tareas burocráticas y de sus procesos, así como que le asista en su actividad profesional de una manera “responsive” no intrusiva y que aprenda y se adapte a cada profesional y su contexto de manera dinámica e incremental

Poniendo en el centro la atención al paciente/usuario, ¿cuáles son las tecnologías más relevantes que impactan en esta atención?

Aquellas que le apoyen en su rol de medicina participativa mediante aplicaciones móviles, asistentes virtuales, portales de paciente y “wearables” sanitarios, los cuales deben aportar datos objetivos de los pacientes. Muchas veces los pacientes y los profesionales establecen una relación de manera verbal con indicación de percepciones que no ayudan a acotar los problemas de salud con eficiencia. Los datos recogidos y cuantificables (hábitos de sueño, actividad, pulsaciones durante las 24h, así como saturación de oxígeno pueden dar una dimensión objetiva de los problemas de salud y son además susceptibles de ser gestionados por sistemas de “machine learning” que descarguen al profesional de tareas de poco valor. La calidad y cantidad de los datos aportan mejor información y como ultimo mejoran el conocimiento de los ciudadanos y sus dolencias.

¿Hasta qué punto la Transformación Digital es una realidad en el entorno Sanitario? ¿Podemos diferenciar entre Sanidad Pública y Privada?

La Transformación Digital en este sector tiene que ser precedida de una Transformación de la Sanidad. La Sanidad se tiene que transformar a una sociedad digital y eso requiere consensos que permitan cambiar las organizaciones, procesos y, por último, sistemas.

La Sanidad en general va atrasada en esta transformación, si bien es cierto que hay tanto en el sector Público como Privado excepciones, pero en todo caso es un proceso muy complejo y lento.

¿Hacia dónde debe evolucionar la Sanidad y cuáles son los aspectos más críticos de mejora?

La sanidad debe y está evolucionando hacia las líneas estratégicas que indica la Sanidad 5P antes mencionada (Poblacional, Preventiva, Participativa, Preventiva y de Precisión/personalización) con el último objetivo de ser medida en base e a resultados de salud, a su valor aportado a la sociedad.

Sin embargo, en tecnología en sistemas de información en Sanidad existen elementos tan básicos por mejorar como la simple identidad única del paciente o la obsolescencia del puesto de trabajo, así como la capacitación digital de profesionales y pacientes, además de escasez de profesionales TIC con experiencia en Sanidad. No tenemos que olvidarnos que venimos de una escasez de financiación TIC en Sanidad que de manera crónica ha retrasado su evolución. Esperamos que los anunciados Fondos Europeos en sanidad transformen para bien un sector tan crítico y esencial como es la sanidad y que la pandemia ha subrayado. ■

Juan Diz, asesor sénior TIC Sanidad

Master en Dirección de Sistemas y Tecnologías de la Información y Comunicaciones de la Salud por la ENS Escuela Nacional de Sanidad del Instituto Carlos III, e ingeniero de Telecomunicaciones Universidad Politécnica de Madrid. Más de 32 años de experiencia en empresas de equipamiento médico de alta tecnología médica, empresas de soluciones digitales de Imagen Medica, así como consultoras TIC de Sanidad.

Las redes de atención sanitaria obtienen más beneficios de una solución de infraestructura llave en mano

COMMSCOPE®
RUCKUS®

Internet de las cosas (IoT) está revolucionando innumerables sectores de la industria, permitiendo una automatización más avanzada y un mayor control de todo tipo de aplicaciones IT y OT. Estas incluyen iluminación, sistemas de seguridad y climatización (HVAC). Si bien casi todas las industrias pueden beneficiarse del IoT, la atención sanitaria ofrece un conjunto particularmente diverso de casos de uso.

Aunque esto supone un futuro apasionante para la evolución de las redes de atención sanitaria, también introduce un considerable nivel de complejidad que puede impedir que una organización médica aproveche plenamente la eficiencia operativa, la mejora de la seguridad y la ampliación de las capacidades que posibilita el IoT, o como se suele denominar en el contexto de las redes sanitarias, el Internet de las cosas médicas (IoMT).

IOMT APORTA UNA ENORME DIVERSIDAD DE APLICACIONES

Pocos espacios comerciales pueden siquiera acercarse al tipo de necesidades de procesamiento de datos de una moderna institución sanitaria u hospital. El movimiento fiable y rápido de información es de misión crítica, la seguridad física y de los datos debe cumplir con estrictos estándares regulatorios, el personal y los pacientes ampliamente distribuidos requieren una conectividad de gran alcance, y tanto el inventario como los equipos deben ser minuciosamente gestionados de forma cercana.

Algunos ejemplos específicos de los dispositivos que responden a estas necesidades son:

- Cámaras y sensores de seguridad conectados por IP en todas las instalaciones
- Señalización digital para dirigir a pacientes y visitantes a sus destinos
- Sistemas de gestión de alerta de cama y desplazamientos que mantienen a los pacientes seguros

“Dado que las instalaciones médicas y sus áreas estériles son lugares difíciles para instalar la infraestructura de red, una solución sencilla y llave en mano puede contribuir a que su inversión en red tenga un retorno de la inversión positivo más pronto”

❖ Acceso a la información y entretenimiento en la habitación a través de la red

❖ Botones de llamada del paciente y alarmas de pánico para garantizar que la ayuda llegue rápidamente

❖ Gestión de inventario mediante RFID o Tags activos WiFi para asegurar que las existencias sean adecuadas y que las auditorías sean sencillas

❖ Automatización de edificios con la integración de las cerraduras de las puertas de acceso con tarjetas, via WiFi, Zigbee y BLE

❖ Software de gestión automatizada de infraestructuras (AIM) que supervisa y protege todas las conexiones de red en tiempo real, automatiza las alarmas y administra toda la documentación de la red en tiempo real para asegurar los datos y garantizar la privacidad de los pacientes

Mirando todas estas funciones, aplicaciones y servicios, parece una tarea casi imposible integrar tantos tipos diferentes de conectividad en una sola infraestructura de red. Sin embargo, eso es exactamente lo que CommScope ofrece a las redes de salud de todo el mundo.

Una infraestructura de red llave en mano que es simple, fiable y adaptable

Con tantas piezas móviles, una red que permita el IoMT no puede permitirse ser una solución fragmentada. Unir un mosaico de tecnologías de infraestructura no solo degrada el rendimiento general, sino que también aumenta el tiempo y los problemas de instalación. Dado que las instalaciones médicas y sus áreas estériles son lugares difíciles para instalar la infraestructura de red (abrir techos y paredes a menudo requiere cerrar partes necesarias y rentables de las instalaciones), una solución sencilla y llave en mano puede contribuir a que su inversión en red tenga un retorno de la inversión positivo más pronto. ■

La comunicación como puntal para la telemedicina

El sector sanitario, sobre todo en lo que tiene que ver con tecnología, ha vivido una catarsis a lo largo del último año. A este respecto, Bernardo Gómez, territory account manager Iberia de CommScope, considera que las agendas tecnológicas sobre digitalización que tanto la sanidad pública como privada tenían concretadas se han acelerado, permitiendo que en poco tiempo se haya avanzado lo que en circunstancias normales habría llevado cuatro o cinco años. Sin duda la tecnología aplicada al sector sanitario ha acelerado este proceso de adopción.

Ahora bien, pese a este paso de gigante en cuanto a adopción de tecnologías, lo cierto es que el sector sanitario tiene por delante aún muchos retos, desafíos que bien encarados, gracias al apoyo de empresas especializadas, pueden suponer no desandar lo ya andado.

Sobre estos retos, Bernardo Gómez reconoce que el principal es que ha cambiado el modelo de negocio de la sanidad. Cada vez surgen nuevas aplicaciones en el entorno sanitario, como la telemedicina, que está muy ligada a la infraestructura de comunicaciones y es precisamente ahí donde CommScope puede aportar valor al sector sanitario, tanto en la parte de infraestructura con redes de cableado y fibra, para toda la parte de comunicaciones de los centros sanitarios; como en lo que concierne a la infraestructura activa con la conectividad inalámbrica y las redes LAN, requisitos indispensables para poder ofrecer un servicio de telemedicina de forma adecuada.

Asimismo, Gómez razona que para desarrollar este modelo de telemedicina es ineludible interconectar todos los centros de toma de decisiones con los puntos donde se genera la información. Esto en el entorno sanitario es crítico porque hay que conectar un ecógrafo o un equipo de radio diagnóstico con un médico que trabaja desde su casa dando tele asistencia a sus pacientes. Es decir, la información generada en diferentes sistemas tiene que fluir de una manera eficiente y de manera segura. Por tanto, es crítico dotar de infraestructuras de comunicaciones robustas y seguras a los centros sanitarios para poder trabajar en este nuevo modelo de servicio.

VALOR DIFERENCIAL

Cuando se plantea una estrategia de comunicación, un director de IT de un centro sanitario tiene que pensar tanto en la conectividad de las personas como en la conectividad de las cosas. Son las dos líneas de actuación críticas, y que permitirán que un médico pueda acceder a toda la información relevante de un paciente.

Para ayudar a las organizaciones del sector sanitario a dar este paso, desde CommScope consideran que estas entidades deben realizar una actualización de sus redes de comunicación empresariales, evolucionando desde una arquitectura tradicional de un punto de acceso inalámbrico, o punto de acceso WiFi, hacia un modelo de nodos de comunicaciones convergentes. En estos nodos de comunicaciones no solo se va a poder dar conectividad WiFi al usuario, a un dispositivo concreto, sino que también va a ser posible adoptar nuevas tecnologías sobre todo del espectro de IoT dentro de esta propia infraestructura.

Gracias a esta correlación, las organizaciones podrán reforzar sus redes LAN para convertirlas en redes multiservicio, dada la convergencia hacia el mundo IT, principalmente hacia el mundo IoT.

Tecnología para una sanidad más eficiente

JUAN CARLOS FARIÑAS, Área Manager de GRENKE España

La pandemia de Covid-19 ha dejado lecciones muy valiosas para el futuro de la sociedad. Una de ellas es la importancia de la tecnología como una herramienta necesaria para la gestión del sistema sanitario. En España, la Sanidad ha visto cómo los avances en materia tecnológica se han convertido en sus mejores aliados durante los meses más virulentos del coronavirus.

Desde las video llamadas, que consiguieron conectar a familiares con enfermos aislados, hasta la telemedicina, una forma de recibir prescripción médica que algunas comunidades autónomas ya han implantado en sus sistemas sanitarios.

La pandemia ha acelerado la puesta al día de la Sanidad con una revolución tecnológica de la que se había quedado descolgada, si la comparamos con otros sectores donde las soluciones y herramientas IT están a la orden del día.

De esta manera, empresas e instituciones sanitarias han visto la necesidad de utilizar esta vanguardia tecnológica para ofrecer una mejor atención al paciente y mejorar el trabajo del profesional.

Conseguir la implementación de los avances tecnológicos en la sanidad es la función de empresas como GRENKE, donde lo que aportamos se traduce en agilizar el trabajo de los sanitarios al favorecer y mejorar el seguimiento de los pacientes con herramientas que pueden evitar que tengan que acudir en repetidas ocasiones a los centros de salud.

Así, ciencia y tecnología se conjugan al cuidado de la salud para el diagnóstico, vigilancia y tratamiento de diversas enfermedades.

“La tecnología sanitaria es, en la actualidad, un instrumento esencial en la asistencia sanitaria, ya que consigue aliviar el dolor, las lesiones y la discapacidad de los pacientes, al tiempo que mejora la eficacia de las prestaciones sanitarias”

Gracias a ella, se obtienen diagnósticos precoces y más certeros, tratamientos menos invasivos y se reduce el tiempo de hospitalización y de rehabilitación, mejorando así la calidad de la atención sanitaria y aumentando la esperanza de vida de los pacientes.

La tecnología sanitaria es, en la actualidad, un instrumento esencial en la asistencia sanitaria, ya que consigue aliviar el dolor, las lesiones y la discapacidad de los pacientes, al tiempo que mejora la eficacia de las prestaciones sanitarias.

Beneficia a miles de millones de personas en todo el mundo, no solo en los hospitales, sino también en residencias y en el propio hogar. Forman parte de ella desde material desechable, como agujas o test de embarazo, hasta sofisticados equipos de diagnóstico, glucómetros, desfibriladores, robots quirúrgicos menos invasivos, máscaras de oxígeno, marcapasos, y un largo etcétera.

El futuro ya está aquí con los avances en tecnología sanitaria centrados en la robótica aplicada a la atención médica, la biotecnología, la telemedicina, los chatbots entre médico y paciente o las aplicaciones móviles orientadas a la salud, entre otros.

TECNOLOGÍA MÉDICA ACCESIBLE

Así y todo, el talón de Aquiles de toda esta revolución tecnológica viene siendo su financiación. No obstante, y al mismo tiempo, la inversión en nuevas tecnologías es fundamental para mantener el ritmo del progreso de las ciencias médicas modernas y para afrontar los retos que se ciernen sobre el sector. Los hospitales, centros clínicos y farmacias experimentan la presión de mejorar la experiencia de los pacientes en lo que se refiere al tratamiento, el diagnóstico, la atención y la comunicación.

Desde GRENKE aportamos soluciones que permiten un acceso a la tecnología de forma asequible y sin castigar su cuenta de resultados; y a sus pacientes disfrutar de lo último en tecnología sanitaria.

La apuesta es sencilla: un amplio portfolio de alternativas a la financiación tradicional de equipos médicos. Hay distintas soluciones de arrendamiento disponibles, y cada una de ellas se puede estructurar de forma diferente para ajustarse a necesidades concretas, ya sea en términos de presupuesto o de uso previsto. El arrendamiento ayuda a garantizar un acceso a las mejores y más recientes tecnologías sanitarias sin necesidad de una inversión sustancial por adelantado.

Y ya hay soluciones reales que van más allá del simple arrendamiento y que cubren toda la gestión del ciclo de vida de los equipos. Algunas de ellas pueden ser el pago por escaneo, los servicios de equipos gestionados y el mantenimiento inclusivo. Un aspecto crucial es que estas soluciones se ocupan del activo al final de su vida útil, de modo que los métodos de reciclaje y eliminación segura no son responsabilidad del cliente.

Al final de lo que se trata es de brindar el acceso a la tecnología repartiendo los costes y el presupuesto con más eficacia. ■

Financiación flexible al servicio de la sanidad

Tecnología y sanidad van de la mano. Sin embargo, en ocasiones el acceso a la tecnología puede ser un proceso complicado bien por la inversión que conlleva o porque el proceso de gestión se torne farragoso. Para ayudar a las empresas sanitarias en su digitalización, existen soluciones financieras flexibles capaces de adaptarse a las distintas necesidades que presentan estas organizaciones. Marco Frühauf, vicepresidente de Grenke, aborda estas alternativas y explica cómo han ido ganando en importancia a lo largo de estos últimos meses.

Desde el inicio de la pandemia, el modo de adquirir tecnología ha ido cambiando. Durante una primera fase el sector sanitario, como tantos otros, se lanzó a adquirir equipamiento tecnológico para dar respuesta a las nuevas necesidades que iban surgiendo a causa del confinamiento, para después, tras unos meses de grandes inversiones, volver a un periodo de mayor moderación. Se ha pasado por tanto de un escenario de prisas y desorganización, de compra y financiación sin análisis previo de las necesidades reales, a otro de mayor mesura y examen, avanzando ya lo que podría ocurrir después del confinamiento.

A este respecto, Marco Frühauf reconoce que ha sido una época de grandes cambios para las empresas del sector sanitario, pero también para compañías como la suya, dedicadas al renting tecnológico, y que han tenido que adaptar sus sistemas y modelo de negocio a cada nueva situación surgida.

En este punto, y teniendo en cuenta, además, que la solvencia de las empresas se ha ido debilitando a causa de las grandes inversiones iniciales, desde Grenke se aboga por que las organizaciones del sector sanitario avancen hacia nuevas fórmulas de financiación que les permitan superar estos y otros escollos que les afectan de cara a adquirir tecnología. En este contexto, los principales desafíos a los que tienen que hacer frente estos actores tienen que ver con su necesidad de hacer inversiones y su incapacidad para realizarlas con las herramientas que normalmente utilizan; una financiación tradicional.

Por eso, Marco Frühauf expone la importancia de que estos agentes, no solo grandes hospitales, comunidades autónomas, sanidad pública, sino también sanidad privada, doctores o farmacéuticos conozcan nuevos métodos de financiación con los que invertir en tecnología y adaptar sus negocios a la situación actual, como puede ser el pago por uso, que permite disponer del uso de tecnología y bienes de equipo sin aumentar el endeudamiento de la empresa.

PAGO POR USO COMO SOLUCIÓN

Ahora bien, ¿es esta situación de pago por uso igual cuando se habla de grandes clientes, pequeños clientes, sector público, privado…?

Por su dimensión, se trata de realidades muy distintas, ya que, por ejemplo, mientras una pequeña farmacia tiene que subsistir con la tesorería que genera, un gran hospital, ya sea público o privado, cuenta con un importante respaldo económico.

No hay que olvidar que el sector sanitario es muy tradicional en cuanto a la gestión y manejo de los fondos y los recursos económicos. Esto le da una gran dependencia de la financiación tradicional, que está en manos de bancos, ya sean comerciales o especializados.

No obstante, toda la banca tradicional está ahora exigiendo un nivel de solvencia o unos requerimientos para ofrecer financiación muy altos, también sobre la documentación a aportar. Por ello, y cuando se trata de operaciones más sencillas, con una menor cuantía para hacer la inversión, el cierre de la operación puede depender más de cómo se gestione la documentación de la financiación que de la propia decisión del dueño del pequeño negocio y del fabricante de hacer la instalación. De este modo, y en un sector en el que se exige que todo sea rápido y sencillo, Gerke apuesta por simplificar este proceso. Realizar una gestión en minutos, sin un solo papel y de forma digital.

Ciberseguridad y funcionalidad, el futuro de los entornos OT

JAIRO ALONSO, ICS Security Consultant, S21sec

Desde la pandemia, el sector sanitario ha cobrado más relevancia que nunca y ha experimentado un rápido proceso de transformación digital. Sin embargo, esto ha provocado que el sector se exponga a importantes riesgos de ciberseguridad, cuya solución requiere de una mayor colaboración entre las empresas de ciberseguridad y el sector sanitario, en especial, los fabricantes de dispositivos médicos. La evolución tecnológica ha ayudado a los hospitales y al personal sanitario a proporcionar una mejor atención a los pacientes, pero la situación de emergencia ha provocado también que se pasen por alto ciertos protocolos de ciberseguridad necesarios en el sector sanitario. Esto no solo supone un riesgo para los trabajadores de los hospitales, sino que también puede repercutir en la salud de los pacientes.

Es comprensible que los fabricantes quieran presentar sus productos al mercado lo antes posible para llevar ventaja con respecto a la competencia, pero, en ocasiones, esa urgencia hace que se salten el primer paso de trabajar conjuntamente con las empresas de seguridad ya que, en un inicio, ahorran tiempo y costes. Aun así, sus productos quedan expuestos innecesariamente a riesgos de ciberseguridad. Además, tampoco suele tenerse en cuenta que al aplicar la seguridad más adelante, dichos dispositivos requerirán de recertificaciones, cuyos procesos suelen ser todavía más lentos y costosos. Es cierto que existen limitaciones a la hora de aplicar ciertas medidas de seguridad en este

“Una de las tácticas más eficaces para prevenir ciberataques es la formación. Es fundamental promover la concienciación entre el personal sanitario acerca de los riesgos informáticos a los que se expone el sector”

tipo de dispositivos, dado que podrían afectar a su funcionalidad. No obstante, este riesgo se puede solventar integrando la ciberseguridad desde la etapa más temprana: su diseño.

La seguridad de los dispositivos médicos es de vital importancia, y la única forma de garantizarla es haciendo que los fabricantes y las empresas de ciberseguridad trabajen de manera conjunta desde un primer momento, para así evitar costes adicionales y otros problemas más graves, como pueden ser los ciberataques. De hecho, desde S21sec hemos tenido constancia de varios ataques de ransomware dirigidos al sector sanitario que implicaban el secuestro de equipos o cifrado de datos, y ha sido una de las razones por las que la ciberseguridad se ha convertido ahora en una preocupación global para los profesionales del sector.

El aumento de la conectividad entre dispositivos, el uso de tecnologías estándar y la acelerada digitalización de los sistemas de automatización, ha provocado que muchos sectores queden expuestos a riesgos de ciberseguridad. En este caso, los ciberataques son una amenaza todavía mayor para el sector de la atención sanitaria, ya que un ataque que interrumpa cualquier actividad puede suponer una cuestión de vida o muerte. Por ello, desde S21sec consideramos que el sector sanitario debe implantar determinadas estrategias con el objetivo de protegerse.

Para empezar, una de las estrategias más eficaces a adoptar es el modelo de ciberseguridad de confianza cero o Zero Trust. En los entornos OT, es básico separar las comunicaciones propias de Internet de la red IP corporativa y de los dispositivos médicos. El enfoque de confianza cero también recomienda y se basa en implementar controles en el tráfico de la red con el fin de evitar y contener ataques de usuarios que aprovechan estas vulnerabilidades para, en el mejor de los casos, hacerse con información personal y confidencial de salud.

Es crucial que el sector sepa cómo protegerse de los ataques de ransomware ya que, como he mencionado anteriormente, desde S21sec hemos detectado varios ataques a centros hospitalarios, infectando sus equipos informáticos y extrayendo información confidencial para posteriormente reclamar un rescate económico. En este sentido, los empleados deben saber qué acciones suyas pueden poner en riesgo la ciberseguridad de la infraestructura y, en última instancia, facilitar una brecha que los atacantes aprovechen para desplegar un ramsomware.

Es por ello, que una de las tácticas más eficaces para prevenir ciberataques es la formación. Es fundamental promover la concienciación entre el personal sanitario acerca de los riesgos informáticos a los que se expone el sector, como estafas en materia de ciberseguridad o tácticas de phishing. Es alarmante que exista tal desinformación en este aspecto, pues la realidad es que hay vidas que dependen de un dispositivo médico, ya sea en su hogar, o en el propio hospital. Ya que es complicado superar la escasez de perfiles cualificados en seguridad, es importante formar al personal y además, confiar en empresas de ciberseguridad que puedan proporcionar respuestas de incidentes desde un SOC-OT.

En definitiva, además de apostar por la formación en ciberseguridad en entornos sanitarios, los fabricantes de los dispositivos médicos y las empresas de seguridad deberían trabajar conjuntamente para diseñar dispositivos óptimos, velando por la seguridad de los pacientes y empleados de los centros sanitarios. En S21sec contemplamos un futuro cercano donde será posible lograr este objetivo que podrá reducir tiempo y costes y, lo más importante, priorizar la seguridad, ante todo. ■

Seguridad y concienciación para evitar ataques

Tres son los retos que tiene el sector sanitario en estos momentos: asegurar la confidencialidad de los datos, proteger la red de comunicaciones y salvaguardar los dispositivos de salud. Para afrontarlos, se debe establecer una estrategia basada en la seguridad de esos activos, pero sin descuidar la formación de las personas.

El sector sanitario se ha alzado como uno de los principales objetivos de los ataques cibernéticos, incrementándose el número de ofensivas alarmantemente. Por este motivo, Jairo Alonso, consultor de sistemas de control industrial de S21sec, explica qué acciones son necesarias para proteger datos y recursos adecuadamente, además de ofrecer otra serie de recomendaciones de seguridad a llevar a cabo.

Efectivamente, por las actuales circunstancias, el sector sanitario se enfrenta a tres retos principales: asegurar la confidencialidad de las historias médicas, proteger su propia red corporativa de comunicaciones, y salvaguardar los dispositivos de salud destinados a monitorizar las constantes vitales de los pacientes cuando están ingresados en un centro médico.

La historia médica no deja de ser información que debe resguardarse ya que se trata de datos críticos que pueden determinar en muchos casos acciones respecto a una persona.

En base a ello, se hace imperativo que esa información no quede alojada en cualquier servidor, sino en servidores internos corporativos. Los datos tampoco deben estar publicados en Internet, ni ser accesibles desde el exterior, y cuando sea necesario realizar un intercambio de información, por un tema de pacientes o similar, utilizar siempre canales seguros. Asimismo, y siempre que sea posible, es recomendable utilizar redes propias, y no recurrir a servicios de terceros que puedan poner en riesgo la información de los pacientes.

No obstante, y pese a seguir estas recomendaciones los datos pueden enfrentarse a amenazas que, como el ransomware, están golpeando con fuerza desde hace meses al sector sanitario.

Como medidas de seguridad y de protección ante este tipo de amenaza, Jairo Alonso recomienda, como primer punto, la formación, a fin de que las personas sean capaces de identificar por dónde puede entrar un ataque de ransomware y notificar cada vez que detectan una brecha. También es muy importante disponer de herramientas de monitorización de la red del sistema sanitario en general, para que al menor indicio de una posible brecha de seguridad o de un ataque, se tenga constancia, y pueda contenerse. El objetivo es evitar por todos los medios que el ransomware se expanda a otros servicios y que los ciberatacantes consigan cifrar historias clínicas de pacientes, lo que impediría tratar adecuadamente a estos usuarios. Además de acciones para luchar contra el ransomware, Jairo Alonso ofrece tres recomendaciones de seguridad a llevar a cabo.

La primera de tiene que ver con la separación o aislamiento de diferentes componentes que integran la infraestructura tecnológica, como son la red que da servicio a los dispositivos de monitorización de salud, la red en la que se incluyen las herramientas de trabajo habituales del sector (correo electrónico, páginas web, etc.), y las historias clínicas y su acceso. Adicionalmente, es muy importante crear políticas y procedimientos que permitan asegurar y elevar el nivel de seguridad sanitario, imponiendo medidas que impliquen mejoras de dispositivos o adquisición de nuevos elementos de seguridad, entre otros.

El último es la concienciación. Es fundamental que todo el personal, esté muy concienciado y comprenda de dónde puede venir un ataque, y qué medidas se pueden tomar para prevenirlo y que no se produzca.

Ciberseguridad en el sector sanitario en pandemia

IVAN MATEOS, Ingeniero Preventa, Sophos

El sector de la salud es hoy muy vulnerable. En medio de una de las peores crisis sanitarias que ha golpeado a la sociedad moderna, los ciberatacantes están explotando hechos como el aumento del teletrabajo, que en muchos casos se ha iniciado con poca o ninguna experiencia y planificación previa, miedo y ansiedad, y una fuerza laboral médica con exceso de trabajo.

El fallo de los sistemas de atención médica puede tener consecuencias nefastas: problemas en ordenar medicamentos, perder el historial médico de un paciente, programar operaciones o hacer que las ambulancias no estén disponibles a tiempo durante las emergencias. Por otro lado, los ciberdelincuentes aprovechan cada vez más la mayor dependencia de la atención médica de herramientas y dispositivos digitales. Se han aprovechado de esta crisis global lanzando ciberataques a través de correos electrónicos de phishing con temas relacionados con la pandemia, ataques de ransomware spear-phishing, que paralizan la atención médica y comprometiendo emails empresariales.

Además, para adaptarse al número de infecciones en rápido aumento y para respaldar la infraestructura de atención médica existente, muchos países han tenido que crear instalaciones médicas temporales para albergar a los pacientes infectados por COVID-19 o para atender los turnos de vacunación. Dado que estas instalaciones se crean rápidamente y la prioridad es brindar atención al paciente, la seguridad se convierte en una prioridad menor, y se pasan por alto muchos pasos cruciales para proteger las redes y los dispositivos y la información que estos manejan

Un resultado de la pandemia también ha sido el aumento significativo en la cantidad de datos de salud de los pacientes almacenados por el gobierno y las organizaciones de salud. Los datos personales como los parámetros de salud diarios, el estado de salud comórbido, los proveedores de seguros, así como el seguimiento de todos aquellos que entran en contacto con una persona infectada, pueden explotarse para el robo de identidad y venderse por un alto valor en la dark web.

Para que las organizaciones de salud ganen terreno a las ciberamenazas modernas, deben seguir ciertas estrategias clave de seguridad para protegerse correctamente contra posibles ciberataques. A continuación, damos cinco consejos de seguridad para intentar conseguirlo:

1. ADOPTAR EL MODELO DE SEGURIDAD DE CONFIANZA CERO O ZERO TRUST

Un informe reciente 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 limita la oportunidad de que los atacantes y los usuarios deshonestos obtengan acceso a información personal confidencial de salud (PHI) mientras permanecen bajo el radar.

2. MEJORAR LA CIBERSEGURIDAD CONTRA LOS ATAQUES DE RANSOMWARE

El ransomware es un arma devastadora en manos de los ciberdelincuentes que tienen como objetivo el sector sanitario, y es responsable de más del 70% de los brotes de malware en el sector.

Estos ataques han detenido operaciones sanitarias, han paralizado los dispositivos y sistemas médicos conectados y han cifrado los registros sanitarios para que los sanitarios no puedan acceder a ellos.

Sophos no sólo ofrece una seguridad líder en ransomware, sino que también realiza un seguimiento del desarrollo de ransomware mediante una rigurosa investigación de SophosLabs. Sophos Intercept X con EDR y Sophos XG Firewall trabajan conjuntamente para interrumpir y rechazar los ataques avanzados de ransomware.

3. SUPERAR LA ESCASEZ DE PERSONAL CUALIFICADO

La falta de personal contratado con los conocimientos y la experiencia adecuados en materia de ciberseguridad es uno de los principales desafíos para los proveedores de servicios de salud. Esto es especialmente un dolor de cabeza para aquellos que no tienen un experto en seguridad a tiempo completo.

Para las organizaciones sanitarias que carecen de recursos en ciberseguridad, Sophos ofrece el servicio de Managed Threat Response (MTR). Este servicio ofrece una supervisión eficaz y una evaluación continua de los riesgos, así como un equipo de expertos dedicado las 24 horas del día, los 7 días de la semana a mitigar y resolver cualquier ataque.

> "Para que las organizaciones de salud ganen terreno a las ciberamenazas modernas, deben seguir ciertas estrategias clave de seguridad para protegerse correctamente contra posibles ciberataques"

Nuestra solución va más allá de las simples alertas, ya que proporciona una respuesta a incidentes reales contra las amenazas, asegurando que el riesgo se identifica, se contiene y que se toman medidas correctivas de inmediato.

4. CUBRIR LOS PUNTOS CIEGOS EN SUS ESFUERZOS DE TRANSFORMACIÓN DIGITAL

Las transacciones de información entre los pacientes, los cuidadores, aseguradoras y otras partes interesadas deben ser fluidas pero tambien seguras.

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 sus últimos dispositivos XG Firewall y SD-RED, hace posible conseguir una conectividad en línea con sus objetivos de seguridad y continuidad. Se permite no solamente enrutar tráfico a nivel de aplicación o usuario sino también aprovechar todas las ventajas de la seguridad sincronizada de Sophos en entornos SD-WAN

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.

Las organizaciones de atención sanitaria deberían realizar campañas periódicas de sensibilización para que sus empleados, socios y proveedores sean más conscientes de las últimas estafas y de las tácticas de phishing, y así estar mejor preparados para tomar las medidas adecuadas cuando se encuentren con malware o phishing.

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

Mantener el servicio activo protegiendo la información

Los ciberataques contra el sector sanitario se han multiplicado en el último año, y este sector se enfrenta al reto de proteger sus activos. Abordando esta realidad, Iván Mateos, Sales Engineer de Sophos, explica por qué el sector socio sanitario está recibiendo más ataques que ninguna otra industria, y ofrece las claves para mantener la actividad diaria sin alteraciones mientras se aseguran todos los activos.

Efectivamente, por las actuales circunstancias, el sector sanitario, no solo hospitales sino también los laboratorios o las farmacéuticas, se ha convertido en una realidad muy visible, hecho que no pasa desapercibido para los ciberatacantes.

En este sentido, Iván Mateos considera que además de lanzar su artillería en modo de ciberataques contra organizaciones, también lo han hecho contra los usuarios, que a diario reciben emails de phishing, con la excusa de una vacuna o de cualquier otro tema sanitario.

Por tanto, y para frenar esta incertidumbre, el sector sanitario tiene que poner remedio, y afrontar algunos retos, siendo el principal el de mantener el servicio lo más activo y productivo posible, pero sin olvidar que lo que manejan y gestionan es información muy sensible: los datos de los usuarios o de los pacientes. De este modo, esta digitalización que está acometiendo el sector sanitario para mejorar la infraestructura debe ir acompañada innegablemente de ciberseguridad, que debe ser tomada como un valor elemental.

DISPOSITIVOS IOT

Importante es también custodiar los dispositivos que manejan datos sensibles, como los dispositivos IoT, que pueden recolectar cantidades significativas de información sobre sus usuarios y su entorno. Por ello, es imperativo minimizar los riesgos de sufrir un incidente de seguridad, protegiendo tanto el dispositivo como la información que gestiona. A este respecto, es necesario salvaguardar la conexión a la red de estos dispositivos, limitar su acceso, (el qué y quién puede acceder a qué).

Hoy en día, en el mercado, ya existen soluciones de segmentación de red, firewalls, y dispositivos de protección que ya tienen en cuenta los equipos de IoT, por lo que es perfectamente compatible la integración de este tipo de dispositivos con la parte de ciberseguridad.

Por último, Iván Mateos lanza también unas cuantas recomendaciones para que los responsables de IT mantengan la seguridad a raya. Entre ellas destaca la importancia de no alargar la vida de equipos que están fuera de soporte, aplicaciones antiguas, sistemas operativos obsoletos. En este sentido reconoce que, aunque es difícil el cambio, hay que entender que estos son problemas de seguridad. Por tanto, hay que intentar mantener aplicativos y sistemas lo más actualizados posibles, optar por soluciones de ciberseguridad que permitan un manejo sencillo, como es el caso de Sophos, que cuenta con una consola para todos los productos, lo que simplifica la ecuación.

Adicionalmente, y para mejorar esta seguridad, Mateos sugiere aplicar el concepto de las tres Cs: cifrado de los dispositivos, con el objetivo de que si se pierde un dispositivo que no se pierda la información; cambio de contraseñas; y, por supuesto, concienciación, con recursos didácticos y de entrenamiento. Si se consigue eso, si se acompañan las herramientas de nueva generación con concienciación, todo puede ser mucho más efectivo.

S21 SEC

CIBERSEGURIDAD INDUSTRIAL

Servicios enfocados a una gestión eficiente de los riesgos de ciberseguridad industrial.

Conoce tus sistemas de automatización y control mejor que el enemigo.

Ahuyenta a potenciales atacantes de tus instalaciones industriales.

Vigila a tu enemigo en los procesos industriales.

Lucha contra el enemigo de tus instalaciones industriales.

Para más información puedes visitar www.s21sec.com/es/ciberseguridad-en-el-sector-industrial/ o escribir un correo a marketing@s21sec.com

Los cuidados sanitarios deben dejar atrás las redes heredadas

Nadie duda de que en plena pandemia es más complicado planificar una actualización tecnológica de amplio espectro en la red de su organización de cuidados sanitarios. Sin embargo, de algún modo, el estrés experimentado por los proveedores de cuidados sanitarios hace que ahora sea el momento perfecto para observar cómo funciona la red desde un nuevo ángulo y determinar qué nuevas e inteligentes posibilidades surgen a raíz de la pandemia

Si hay algo que hemos aprendido todos desde comienzos de 2020 es que la adaptabilidad y la flexibilidad de las redes es incluso más importante de lo que se creía antes. Las redes de atención sanitaria a menudo se ven limitadas por sistemas antiguos ineficaces y aislados que resultan difíciles de mejorar y, algunas veces, imposibles de integrar. Ahora que las normas de atención sanitaria han cambiado radicalmente, estos límites resultan más costosos e insostenibles. Si la eficacia operativa se ve mermada, también se resiente el estado operativo de su organización.

LOS RETOS DEL FUTURO Y LOS QUE YA ESTÁN AQUÍ

El rápido cambio realizado para adoptar interacciones de telemedicina, los servicios digitales de hospitalización y la conexión al Internet de las Cosas Médicas (IoMT) crean nuevos requisitos para la red y su infraestructura.

Para seguir el ritmo y abordar la necesidad de disponer de redes fiables, adaptables y seguras, la actualización de la red es la única opción que permite la forma de suministrar atención médica al paciente. Al mismo tiempo, los elevados costes asociados a la actualización pueden resultar abrumadores y los proveedores de servicios sanitarios deben sopesar las opciones de soluciones con sus necesidades. La inversión debe estar justificada por la duración de la solución, y dicha duración puede determinarse en función de lo sólida y adaptableque sea.

OPORTUNIDADES DISPONIBLES CON LA INFRAESTRUCTURA DE RED ACTUALIZADA

Una red preparada para el futuro es algo más que una infraestructura física más rá-

pida. Supone analizar las estrategias y las soluciones para mejorar el modo en el que se ofrecen los servicios sanitarios y se utilizan las instalaciones. Las soluciones adecuadas pueden hacer posibles nuevos enfoques, arquitecturas y capacidades, como los que se describen a continuación:

- **Capacidades de edificio inteligente** que conectan los sistemas de calefacción, refrigeración, iluminación y otros servicios ambientales y de seguridad a un gestor de redes automatizado que maximiza el bienestar y reduce los costes
- **Robótica y realidad aumentada** impulsadas por redes con ultra alta velocidad que realizan procedimientos complejos para ofrecer decisiones mejor informadas y resultados óptimos para los pacientes
- **Sistemas blockchain seguros** que permiten realizar un registro preciso del inventario y la cadena de suministro, las transacciones financieras, los tratamientos de los pacientes, el procesamiento de reclamaciones de seguros sanitarios y mucho más
- **Plataformas de aprendizaje mejoradas** necesarias para que los médicos y el personal puedan adoptar estas múltiples y beneficiosas prácticas de manera rápida y eficaz y disfrutar así de un uso compartido de datos más eficaz tanto en el ámbito de la práctica médica como en el de la investigación
- **Informática en la nube** que proporciona una plataforma más sólida que la que se obtendría in situ y que aumenta las oportunidades de procesamiento analítico, automatización operativa y comunicación del personal
- **Redes 5G** que ofrecen lo más novedoso en alta velocidad, rendimiento de baja latencia en interiores y exteriores para conectar a médicos, personal, pacientes, visitas y dispositivos IoMT conectados como dispositivos “wearable” para los pacientes
- **Plataformas interoperables** que conectan disciplinas y departamentos con el objetivo de simplificar el uso compartido de información crítica y la toma de decisiones
- **Sistemas basados en IA** que ayudan a obtener diagnósticos precisos y tratamientos eficaces
- **Soluciones de procesamiento del lenguaje natural (PLN**) que pueden generar notas médicas precisas a partir detexto hablado
- **Análisis médicos** que pueden procesar de manera eficaz enormes cantidadesde datos no estructurados para revelar patrones ocultos en tratamientos y resultados de pruebas
- **Análisis operativos** que pueden informar a los responsables de la toma de decisiones del flujo de trabajo, la seguridad, la sostenibilidad y los procesos logísticos para aumentar la eficacia operativa de todos los aspectos del centro

Estas son solo algunas de las nuevas herramientas disponibles para los proveedores de servicios sanitarios que, en una realidad post pandémica, serán cada vez más importantes para el funcionamiento eficaz de una organización de servicios médicos, tanto en el caso de prácticas médicas individuales como hospitales y centros de investigación.

No obstante, el único prerrequisito que comparten todas ellas es una infraestructura de red unificada, sólida y preparada para el futuro, y aquí es donde más destaca el exclusivo valor de CommScope como Partner de soluciones. ■

MÁS INFORMACIÓN

- Soluciones CommScope para el sector sanitario
- Infografia de la Solución de Healthcare
- Infografía de la Solución de Redes

GRENKE. Una amplia experiencia en renting

GRENKE es una compañía especializada en ofrecer a las pequeñas y medianas empresas, y a toda empresa en expansión, el renting como alternativa a la financiación tradicional para la adquisición de tecnología y equipamiento.

Los esfuerzos de GRENKE, van enfocados a combinar el negocio innovador del renting con la rapidez, la confianza y la cercanía, manteniendo siempre vivo nuestro espíritu emprendedor.

La adquisición de equipamiento tecnológico a través del renting es un modelo en alza por sus claras ventajas financieras, fiscales y operativas: Se paga a medida que se usa el bien, no en el momento de la adquisición; las cuotas mensuales son deducibles al considerarse gasto; y al finalizar el contrato se pueden renovar los equipos para así estar siempre a la vanguardia y ofrecer una inmejorable imagen al cliente.

Sabemos que hoy por hoy la tecnología es clave y gracias a nuestras soluciones de renting queremos hacer llegar a todas las empresas, pertenezcan al sector o industria que pertenezcan, la posibilidad de crecer, adaptarse o innovar.

GRENKE permite que el cliente, ya sea un autónomo, una empresa, un organismo público o una startup, pueda arrendar prácticamente todo el equipamiento necesario para el desarrollo de la actividad de su negocio incluyendo software, iluminación, TPV, robots o cualquier otro equipamiento. También permite al cliente obtener una planificación realista gracias a las cuotas fijas y una optimización de su tesorería, mejor pagar por uso que hacer un gran desembolso inicial.

GRENKE ofrece a clientes dos grandes líneas de soluciones:

Contrato Classic: Con esta solución cualquier empresa o negocio podrá adquirir el equipamiento que necesite en un momento dado. Desde una máquina de café hasta un equipo de resonancia.

Póliza Máster: Si la empresa requiere el renting de equipos con regularidad, enton-ces la opción perfecta es nuestra línea de renting,

permitiéndole ahorrar dinero y ofreciéndole ventajosas condiciones.

De esta forma cuidamos y ayudamos a nuestros clientes o partners. Ya que consi-de-ramos cada relación única, debido a que cada negocio tiene necesidades particulares que suponen para nosotros retos distintos cada vez. Por ello trabajamos día a día en soluciones de renting tecnológico y de equipamiento que se adapten 100 % a cada necesidad: contratos desde 500 euros, respuesta a las operaciones en 20 minutos con la mínima documentación y, por supuesto, firma electrónica de los contratos.

En este sentido primero ofrecimos la firma digital eSignature, con la que se pueden firmar los documentos contractuales directamente en pantalla y devolverlos firmados vía digital en un abrir y cerrar de ojos, de forma segura y jurídicamente vinculante. Desde casa, desde la oficina o en movimiento. Todo lo que se necesita es un ordenador, un portátil o un Smartphone, y acceso a internet.

Y ahora, adicionalmente a la firma digital eSignature, nuestros clientes y partners pueden optar por la firma del contrato a través nuestra Signing App. Una carpeta virtual que permite firmar los contratos de manera electrónica sin perder el contacto cercano entre ambas partes.

De esta forma podemos alcanzar nuestro objetivo que no es más que facilitar a los empresarios la puesta en marcha de sus ideas y proyectos. Después de todo, GRENKE también comenzó siendo solo una idea. Cuando empresarios y emprendedores necesitan adaptar la tecnología de su negocio y no disponen de solvencia para hacerlo, el renting de GRENKE es la solución perfecta.

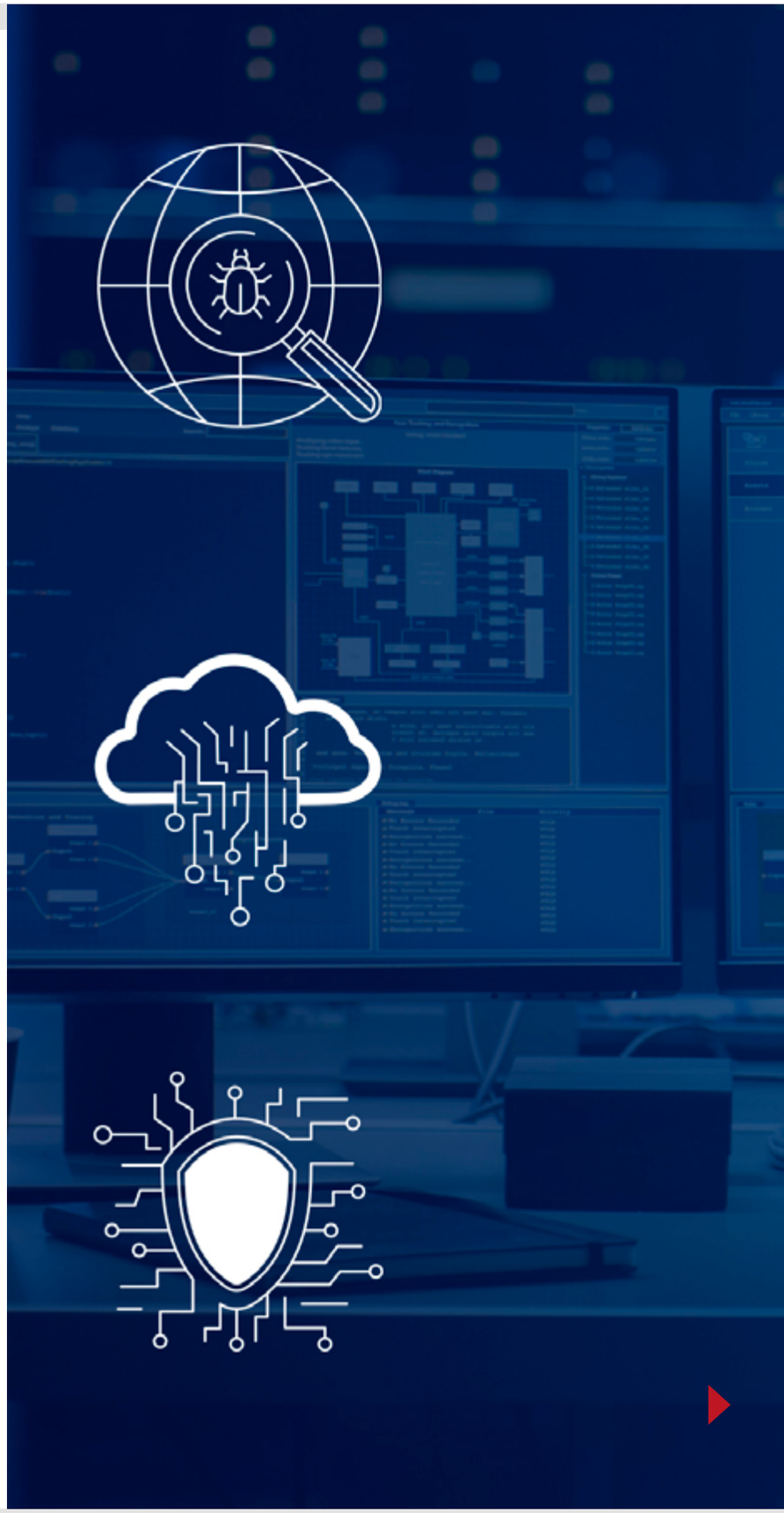
Algo que ya muestra nuestro propio eslogan de marca «Fast. Forward. Finance». Ofrecemos un valor añadido a nuestros clientes porque son nuestra prioridad. ■

MÁS INFORMACIÓN

- Información para partners
- Información renting tecnológico
- Información Productos
- Información Contrato Classic
- Información Póliza Máster
- Información Rent Back
- Información GRENKE para la sanidad

La detección y prevención, claves en la protección

S21sec es la compañía pure-player de ciberseguridad más grande de Iberia con una dilatada experiencia en el sector, lo que le permite ofrecer una cobertura completa de riesgos de ciberseguridad en los procesos de negocio de las organizaciones.



El desarrollo de un mundo cada vez más hiperconectado, en el que las empresas enfrentan complejos procesos de transformación digital y dependen de un mayor de dispositivos conectados a Internet, resulta clave proteger los datos de las organizaciones, así como la operatividad de sus sistemas y cumplimiento con el RGPD.

Una plantilla de más de 410 expertos reflejan las capacidades de S21sec para investigar, detectar y prevenir amenazas; piezas clave para reaccionar con mayor rapidez ante cualquier ataque e identificar, diagnosticar y remediar eventuales incidentes en el menor tiempo posible.

Perteneciente al grupo Sonae, S21sec es líder sectorial en España y Portugal por historia, formación, infraestructura y equipo. Está entre las cinco principales compañías de ciberseguridad de Europa, con la aspiración de liderar el mercado europeo a medio plazo.

Además, cuenta con el primer SOC de España, convertido ahora en un multiSOC global distribuido en cuatro localizaciones, que garantiza la integridad de más de 500 organizaciones en España, Portugal y México.

Su porfolio, que aúna soluciones diferentes de manera transversal, está diseñado en torno a cinco necesidades:

1. Identificar: análisis de riesgos y plan general de ciberseguridad, cumplimiento regulatorio, ciberseguridad en la nube y programas de transformación y Red Team.

2. Proteger: diseño y despliegue de arquitecturas y tecnologías, servicios de forma-

El desarrollo de un mundo cada vez más hiperconectado, en el que las empresas enfrentan complejos procesos de transformación digital y dependen de un mayor de dispositivos conectados a Internet, resulta clave proteger los datos de las organizaciones

ción y concienciación, gestión de dispositivos de seguridad, seguridad de la información y seguridad ATM.

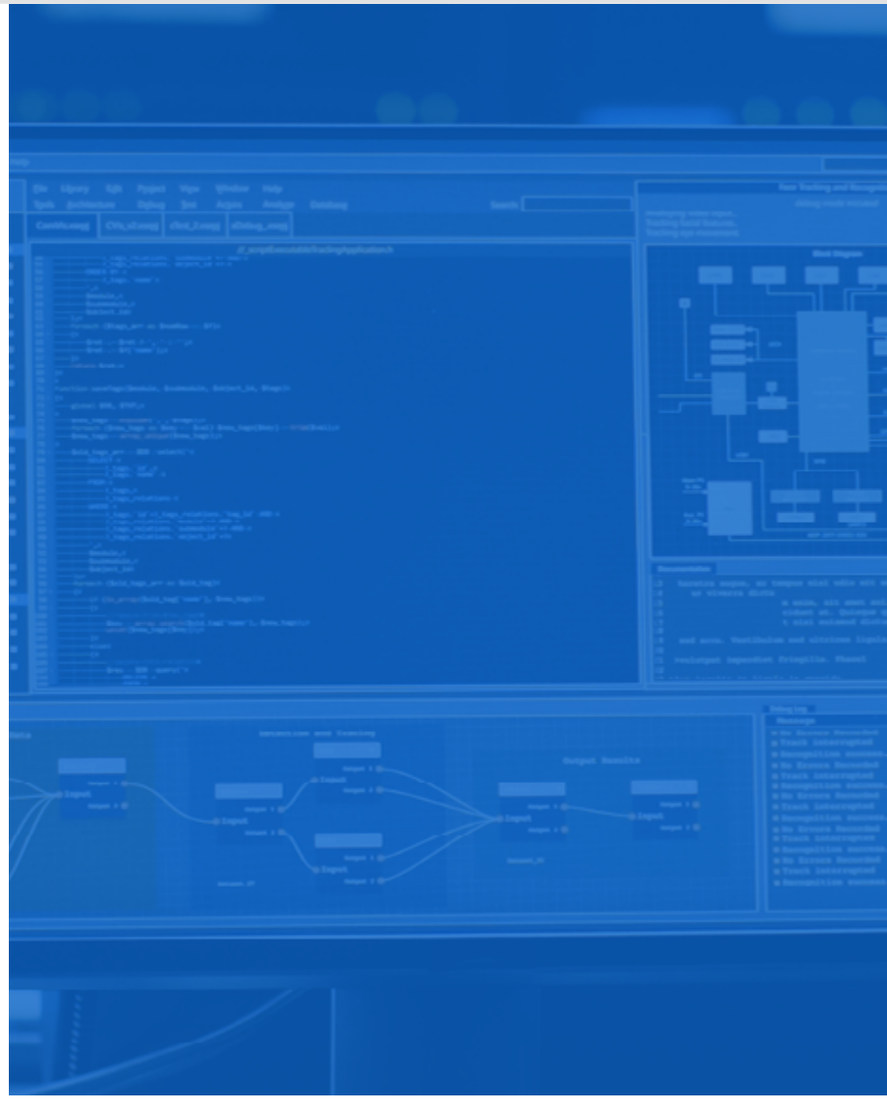
3. Detectar: SOC gestionado y SIEM como servicio, Unidad de Inteligencia de Ciberamenazas, EDR - Detección y respuesta End Point.

4. Responder: CSIRT - Gestión de incidentes de ciberseguridad 24x7, DFIR - Análisis forense digital y respuesta ante incidentes, plataforma de respuesta ante incidentes, SOAR - Automatización, Remediación y Orquestación de la Ciberseguridad y amenazas emergentes - evaluación y perfilación.

5. Recuperar: Continuidad de negocio y planes de respuesta ante ciber-desastres.

Por último, S21sec se guía por una serie de valores clave a la hora de desarrollar e implementar sus soluciones con éxito:

* **Transparencia:** se pone a disposición la información necesaria para la colaboración y la toma de decisiones colectivas.
* **Excelencia:** se persigue ofrecer la más alta calidad gracias a encontrarse en un continuo proceso de aprendizaje.
* **Trabajo en equipo:** se dedica esfuerzo para encontrar la mejor forma de ayudarse entre sí, poniendo el rendimiento de la compañía por encima del rendimiento individual.
* **Innovación:** se busca la diferenciación a través de implementar cambios que mejoran su eficiencia y ventaja competitiva.
* **Confianza:** se construyen relaciones con las personas y las organizaciones basadas en la confianza y la honestidad.
* **Pasión:** se disfruta del trabajo porque siempre se busca de manera proactiva diferenciarse. ■



MÁS INFORMACIÓN

- Rediseños de arquitectura de red en SCI
- Detección de anomalías
- Evaluación y gestión de vulnerabilidades
- Inventario de activos

Proteger las TI a partir del conocimiento de las amenazas

La ciberdelincuencia está cambiando y los ciberdelincuentes cada vez están más preparados y coordinados entre sí, utilizando herramientas muy sofisticadas y difíciles de detectar y de parar, por lo que hay que estar constantemente monitorizando y conocer cuál es la situación de la empresa ante cualquier potencial amenaza.

Las soluciones de Sophos destacadas este año y las que mayor crecimiento están demostrando son:

SOPHOS EDR/XDR

Un completo sistema de protección endpoint que engloba la protección tradicional (firmas), junto con protección "next-gen" (Inteligencia Artificial, anti Exploit, 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 nuestros firewalls y 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, MTR-E 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

Sophos dispone de un ZTNA para securizar, las conexiones de usuarios remotos así como los accesos a servicios en nube

posibles amenazas 24/7. Está formado por un equipo de detección de amenazas y expertos en dar respuesta, capaz de tomar medidas para neutralizar incluso las amenazas más sofisticadas. El factor diferencial de esa solución es que, cuando otros sólo notifican, Sophos puede dar respuesta, apoyándose en el agente de Sophos para realizar las acciones oportunas para la detección y mitigación de la amenaza.

Si aún no es cliente de Sophos, cualquier empresa que sufra un ataque activo puede recurrir a Sophos Rapid Response. Un conjuntode productos y un equipo de expertos que son capaces de ver cuál es la situación dentro de la compañía, detener el ataque, si es posible, y detectar cómo ha venido, a quién ha afectado y limpiar para que pueda operar lo antes posible.

SOPHOS ZTNA

Sophos dispone de un ZTNA para securizar, las conexiones de usuarios remotos, así como los accesos a servicios en nube. Todo ello gestionado desde Sophos Central, integrándose con el cliente de Seguridad Endpoint para facilitar los despliegues y adopción de las nuevas metodologías de conexión, evitando los problemas “habituales” de los sistemas VPN y SD-WAN tradicionales. El modelo Zero-Trust Network Access permite a los usuarios conectarse de forma sencilla a los recursos corporativos desde cualquier ubicación y al mismo tiempo mejora su seguridad al verificar de manera constante al usuario y validar el estado y el cumplimiento del dispositivo, así como la red desde donde se conecta.

SEGURIDAD SINCRONIZADA

Sophos lleva ya más de 5 años conectando a través de su Seguridad Sincronizada los distintos sistemas de protección, compartiendo información.

SOPHOS CLOUD OPTIX

Conscientes de que la TI está migrando a la nube, Sophos propone CSWP y CSPM gracias tanto al agente para servidores como a Cloud Optix, el cual audita los recursos que tengamos sobre proveedores de nube pública como AWS, Azure, Google Cloud o Kubernetes tanto en cualquiera de estos entornos como locales. Además, se integra tanto con la protección de instancias y servicios como MTR, lo que proporciona más visibilidad e información que será recogida en el DataLake.

SOPHOS FIREWALL

La seguridad de red no queda desatendida en Sophos. Desde la compra de Astaro en 2008, la han seguido evolucionando hasta llegar a los modernos Sophos Firewall, gestionados de forma centralizada desde Sophos Central, integrándose con el Endpoint y servicios como MTR así como hidratando el lago de datos para permitir detectar, englobándose dentro de nuestra estrategia XDR. ■

MÁS INFORMACIÓN

- Informe de Amenazas 2021
- La evolución de la ciberseguridad: el impacto empresarial de Sophos
- Guía de respuesta a incidentes

El sector sanitario está en el punto de mira de los ciberdelincuentes

Sophos Endpoint

Intercept X with EDR

Impida que su organización se vea afectada por el ransomware.

Sophos Endpoint incluye tecnología antiransomware que detecta procesos de cifrado malicioso y los neutraliza antes de que puedan propagarse por la red.

SOPHOS

Cybersecurity evolved.