¿Estamos seguros en la nueva era de la atención médica?

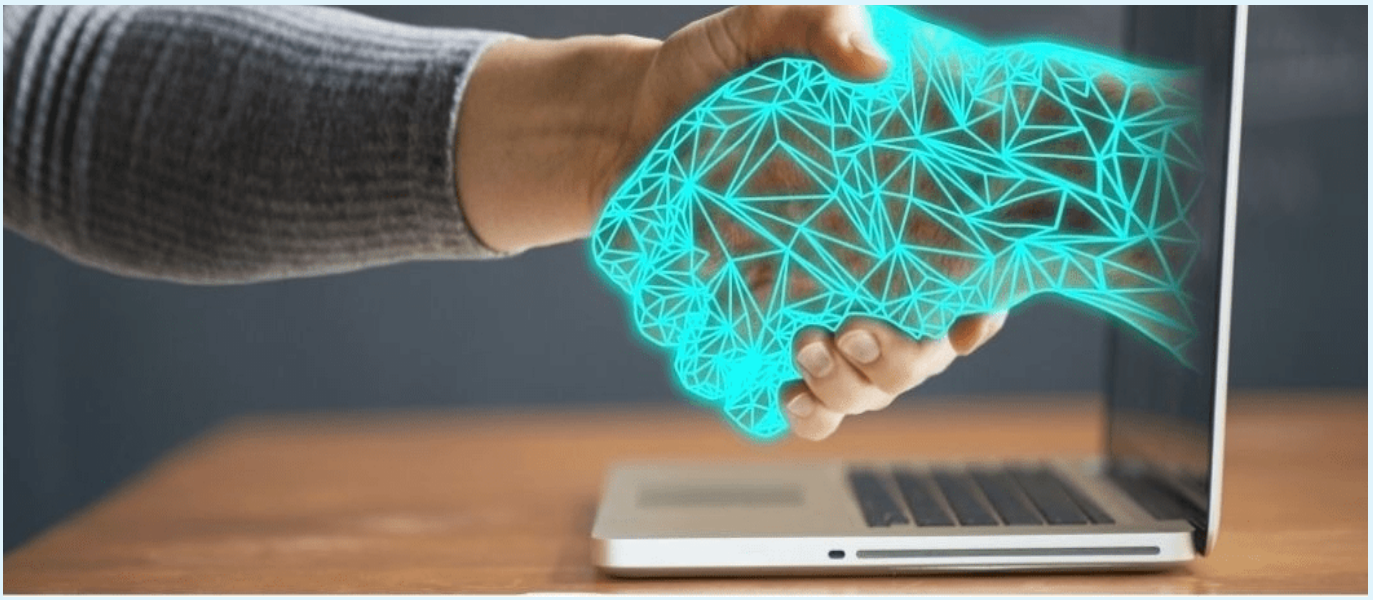
Si tenemos que elegir un sector que haya sufrido en especial grandes cambios, seguro que muchos de nosotros elegiríamos al sector sanitario. Su momento de enorme demanda, cargas de trabajo nunca vistas y su obligada resiliencia así lo ponen de manifiesto.

Como sector esencial en cualquier sociedad, su necesidad de afrontar los continuos retos de seguridad buscando la excelencia es una obligación en la que “no se pueden poner de perfil”.

Ya antes de la pandemia, se esperaba que el mercado del sector salud digital europeo alcanzara un valor de 145. 000 millones de euros en el año 2025, por lo tanto estamos quizás, ante el mayor periodo de crecimiento transformador en el que se ha visto inmerso en los últimos 15 años.

Forbes pronosticó hace unos meses que la cantidad de datos dentro del sector se doblará cada 73 días anualmente. A este aumento de generación de datos también contribuirá la actual crisis sanitaria, con una cifra cercana a los 3 millones de casos notificados solo en la UE hasta ahora.

Este aumento de demanda de la atención , de los datos que se manejan, del uso de las comunicaciones externas y el del IOT en el ámbito sanitario obliga a responder de forma contundente a la necesidad de garantizar que el entorno sanitario posea la infraestructura de seguridad necesaria para abordar este crecimiento.



Con la pandemia, la proliferación de las consultas virtuales y atender a los pacientes a distancia, está empujando al sector a cambiar su forma de trabajar, siendo aún más dependiente, casi de una forma crítica, de dos aspectos importantes y viejos conocidos para el sector:

- La energía
- La infraestructura digital.

En el caso de la conectividad e IOT, el aumento sigue una carrera a altas velocidades, en 2025 se esperan más de 10 millones de dispositivos conectados en el entorno sanitario europeo, eso supone multiplicar por 5 la cifra que teníamos en 2019.

La Ciberseguridad tiene que venir por defecto.

Es obvio que todos los factores y aspectos de los que he hablado, aumentan exponencialmente la superficie de ataque actual del sector en lo que a ciberseguridad se refiere. Las puertas de acceso para los ciberdelincuentes se han multiplicado de forma significativa.

Es verdad que antes de la pandemia la ciberseguridad ya era un gran área de preocupación, pero, la exigencia actual generada por la innovación tecnológica asociada a la inteligencia artificial y modelado 3D en el diagnóstico, la sonorización a gran escala, la protección de datos, software existente y el asociado a equipamiento de última generación.....están poniendo a prueba las capacidades de seguridad física y lógica que este sector debe tener.

La seguridad por defecto en toda la infraestructura de hardware y software y en general a todo el equipamiento médico susceptible de convertirse en una puerta de acceso al entorno, debe ser una prioridad para la industria que abastece a todo el entorno sanitario. Sin duda alguna, la red de partners tecnológicos especializados se enfrentan a una gran oportunidad pero también tienen una gran responsabilidad que no pueden eludir. Concienciar al sector y al usuario es clave para evitar grandes incidentes y ataques que doy por seguro que se van a generar por los ciberdelincuentes, la pregunta es ¿CUÁNDO?, por lo tanto hay que estar preparados y trabajar hacia la minimización del riesgo y la obtención de grandes capacidades de resiliencia.

La monitorización y la gestión de incidencias- incidentes-eventos 24/7/365, auditorias y evaluaciones de riesgos continuas para toda la infraestructura de red y de IOT (digital) así como en los dispositivos y equipamientos médicos de un entorno sanitario se hacen imprescindibles y de obligado cumplimiento en las políticas de gestión de este sector.

Carlos Aguayo
CEO Intelsynet