Puliendo diamantes

Los datos cada vez cobran mayor relevancia. De hecho, se podría llegar a decir que los datos son el nuevo lenguaje que tienen que hablar los negocios hoy en dia. Los datos conducen a la comprensión y gracias a ello las organizaciones disponen de nuevas herramientas para poder tomar decisiones de negocio.

Las personas creamos datos constantemente aunque no nos demos cuenta de ello. Ya no solo a través de las redes sociales, sino que estamos constantentemente recibiendo y enviando información. (Incluso cuando nuestros dispositivos están en estado de reposo)

La cantidad de datos que producimos cada día es realmente sorprendente. Cada día generamos aproximadamente 2,5 quintillones de bytes pero con el crecimiento del Internet de las Cosas (IoT) esta cifra pronto quedará obsoleta. Sólo en los dos últimos años hemos generado el 90 por ciento de todos los datos generados a lo largo de la historia. [1]

De acuerdo a un análisis realizado por la consultora Domon durante el año 2018 [2], cada minuto se envían medio millón de tuits a través de la red y se reproducen aproximadamente 750.000 canciones de Spotify. Gestionar este volumen de datos resulta bastante complicado.

La obtención de los datos y su preparación para el análisis es una de las tareas más tediosas a las que se enfrentan las organizaciones en la actualidad. Los analistas dedican mucho tiempo a buscar y reunir los datos adecuados. De hecho, por promedio, los analistas dedican entre el 60 y el 80 por ciento de su tiempo a la preparación de los datos en lugar del análisis.

Además, todos lo datos no poseen el mismo valor ni presentan un formato adecuado. Es por ello que a la hora de analizar los mismos es necesario atender a un aspecto importante: la **calidad**.

Pero… ¿qué es la calidad de los datos?

La calidad de los datos o “Data Quality”, en inglés, hace referencia a una percepción o una evaluación de la idoneidad de los datos para cumplir su

propósito en un contexto dado. Esta puede estar determinada por factores como la exactitud, la integridad, la confiabilidad, la relevancia o cómo de actualizados se encuentran. [3]

De hecho, hacer uso de datos de baja calidad puede conllevar a la elaboración de informes erróneos o a estrategias mal planteadas. El daño económico provocado por estos problemas puede ir desde gastos adicionales o hasta multas por la elaboración de informes financieros inadecuados.

Según datos de IBM [4], en el año 2016 el coste anual de los problemas generados por la mala calidad de los datos en Estados Unidos se situó alrededor de los 3,1 trillones de dólares. La razón por la cual los datos con poca calidad cuestan tanto es que estos en muchas ocasiones presentan errores y ante una fecha límite crítica, muchos trabajadores simplemente hacen correcciones ellos mismos para completar la tarea en cuestión.

En este mundo plagado de datos, lo importante no es solo tener una gran cantidad de datos, sino contar con datos de calidad que permitan llevar a cabo análisis exhaustivos con los que obtener los mejores beneficios. En un panorama saturado de datos como el que tenemos actualmente, buscar datos de calidad resulta imprescindible.

Debido a este fenómeno, incluso han comenzado a proliferar start-ups encargadas del procesamiento de los datos. Liberando así a las compañías de realizar estas arduas tareas. De hecho, disponer de datos de calidad resulta esencial a fin de poder realizar análisis correctos.

Puede que al principio los datos no parezcan relevantes pero puliendolos un poco pueden llegar a convertirse en diamantes.

Referencias

[1] “How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read”, Forbes, consultado el 15 de enero de 2020, https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/

[2] “Data Never Sleeps 6.0”, Domo, acceso el 15 de enero de 2020, https://www.domo.com/learn/data-never-sleeps-6

[3] “¿Qué es Data Quality y por qué es importante?”, Elternativa, acceso el 15 de enero de 2020, https://www.elternativa.com/blog/index.php/2019/04/03/que-es-data-quality-y-por-que-es-importante/

[4] “Bad data costs the US 3 trillion per year”, Harvard Business Review, acceso el 15 de enero de 2020, https://hbr.org/2016/09/bad-data-costs-the-u-s-3-trillion-per-year

---

El poder del diseño

El diseño es algo de lo que ya he hablado en otros artículos de este blog: diseño aplicado como seguridad en dispositivos médicos, la relevancia de aplicar técnicas de diseño accesibles,… Sin embargo, el diseño no solo se limita al ámbito tecnológico. Todas las personas diseñamos. Diseñamos como queremos que sea nuestra vida en el futuro, diseñamos como queremos que sea nuestra casa, diseñamos como queremos que sea nuestra familia,…

Nos pasamos la vida diseñando y cuando se trata de conversaciones, en cambio, solemos dejar que la improvisación predomine.

Diseñar conversaciones resulta importante para poder alcanzar nuestros objetivos. Manteniendo mejores conversaciones generamos emociones más positivas tanto a nivel individual como social que permiten obtener relaciones interpersonales de mejor calidad.

Es por ello que resulta necesario adquirir competencias conversacionales para lograr nuestro bienestar tanto en el ámbito personal como en el profesional.

¿Pero qué es una conversación?

Tal y como lo define la RAE, [1] una conversación es la “acción y efecto de hablar familiarmente una o varias personas con otra u otras”. No obstante, esta definición resulta bastante pobre.

Una conversación no es solo un intercambio de ideas, sino que constituye una actividad comunicativa en la cual destaca su función socializadora. Las conversaciones nos permiten a las personas socializar y desarrollarnos tanto individualmente como socialmente.

Una conversación no consiste en atacar o en dar por supuesto el punto de vista de las demás personas. Una conversación es más una multiplicación de ideas en la que predomina el concepto de nosotros frente al concepto de uno mismo. [2]

Detrás de las conversaciones verdaderas no hay ganadores ni perdedores sino que hay personas que interactúan.

¿Y cómo diseñamos estas conversaciones?

Para poder mantener mejores conversaciones, estas tienen que estar correctamente **estructuradas**, es decir, requieren de una argumentación sólida. Debemos conocer el mensaje que queremos transmitir para poder estructurar las conversaciones de tal forma que el mensaje quede claro y no resulte ambiguo.

Además, las conversaciones requieren de **empatía**, es decir, ponernos en el lugar de los demás interlocutores. Gracias a la empatía se pueden estructurar las conversaciones de tal forma que no resulten ofensivas, se puede elegir el mejor momento en el cual mantenerlas,…

Según la escritora y presentadora Celeste Headlee, [3] estas son las 10 claves para poder mantener una buena conversación:

1. Debemos concentrarnos en la conversación y hacer sentir a los demás que estamos ahí, es decir, que nos interesa lo que nos están contando.
2. No debemos ser intransigentes.
3. Debemos pensar en el quién, el qué, el cómo, el cuándo y el porqué a la hora de diseñar nuestras conversaciones.
4. Debemos respetar el ritmo de la conversación.
5. Si no sabemos que significa algo o no hemos entendido algo, tenemos que decirlo.
6. No debemos comparar nuestra experiencia a la de los demás. No consiste en demostrar lo genial que somos o lo mucho que hemos sufrido.
7. Aunque a veces resulte complicado, no debemos repetirnos.
8. No debemos enredarnos. Esto va unido a lo mencionado previamente:

tenemos que estructurar las conversaciones para no perder el hilo conductor de lo que queremos transmitir.
9. Debemos escuchar atentamente lo que exponen los demás.
10. Debemos ser breves. Como dice el refrán lo bueno, si breve, dos veces bueno.

Estamos todo el tiempo comunicándonos, incluso cuando estamos en silencio. El lenguaje verbal, el lenguaje gestual, … son distintas formas de expresarnos. Sin embargo, resulta importante equilibrar las dos principales etapas de la comunicación: la escucha y el habla. Si mantenemos conversaciones internas mientras dialogamos con otros, seguramente que perdamos información que pueda ser relevante o dejemos de percibir cómo están recibiendo nuestros mensajes las demás personas.

El habla resulta una forma de interacción más natural para las personas que la interacción con el ratón. Las personas nos sentimos más cómodas hablando que haciendo click ya que esta es la forma inherente que tenemos los seres humanos de comunicarnos.

Marketing conversacional, Interfaces Conversacionales,… cada vez son más los ámbitos en los cuales se aplican todos estos conceptos. Y esto es debido al poder que tienen las buenas conversaciones y para las cuales el diseño previo resulta fundamental.

Y hasta aquí el post de hoy, espero que os haya gustado.

¡Hasta la próxima!

Referencias

[1] <<Conversación>>, RAE, acceso el día 26 de diciembre del 2019, https://dle.rae.es/conversación

[2] <<El poder de una conversación. Álvaro González Alorda>>, Youtube, acceso el día 26 de diciembre del 2019, https://www.youtube.com/watch?v=tW0elgW7SZY

[3] <<10 ways to have a better conversation>>, Ted, acceso el día 26 de

diciembre del 2019, https://www.ted.com/talks/celeste_headlee_10_ways_to_have_a_better_conversation

---

Que no hackeen tu corazón

Esto va llegando a su fin. Hasta ahora hemos visto los **riesgos** que presentan los dispositivos médicos y hemos establecido una serie de posibles **controles** a fin de mitigar los mismos. Además, hemos observado la relevancia de la cual disponen este tipo de dispositivos en la industria.

En este post me gustaría hacer énfasis sobre algunos de los problemas más sonados en los últimos años en cuanto a dispositivos médicos respecta. No con el objetivo de asustaros o alarmaros sino de concienciar sobre la relevancia de todo lo expuesto hasta la fecha y la necesidad de informar a las autoridades pertinentes sobre este tipo de situaciones. Además, me gustaría exponer algunos de los motivos principales por los cuales el sector de la salud resulta el objetivo de tantos ataques.

¿Os acordáis de la empresa Medtronic?

En el tercer post hablamos sobre cómo esta empresa tuvo que retirar del mercado algunas bombas de insulina ya que resultaban vulnerables a ataques. No obstante, este tipo de vulnerabilidades no solo se limitan a las bombas de insulina.

A principios de este mismo año, por ejemplo, el Departamento de Seguridad Nacional de EE.UU advirtió sobre una vulnerabilidad crítica en el sistema de transmisión de datos de los implantes cardíacos de Medtronic. Este fallo permitía a los hackers modificar la configuración de los mismos. [1]

Si retrocedemos un poco más en el tiempo, en el año 2017 la FDA emitió la retirada de seis modelos de marcapasos producidos por la compañía Abbott debido a la presencia de una serie de vulnerabilidades. Estas vulnerabilidades permitían que usuarios no autorizados accedieran al

dispositivo y modificaran el funcionamiento del marcapasos implantado. Esto podría resultar en daños para el paciente debido a un rápido agotamiento de la batería o a la modificación en la gestión de los latidos del paciente.

A fin de solucionar este problema la compañía desarrolló y validó una actualización correctiva para todos los dispositivos afectados. En este caso en concreto no resultó necesario intervenir a los pacientes a fin de retirar los marcapasos afectados. Sin embargo, al igual que con cualquier actualización de firmware la FDA informó sobre la existencia de una serie de riesgos asociados a la instalación incorrecta de esta actualización. Entre estos riesgos se mencionaba la posibilidad de la pérdida de la configuración del dispositivo o incluso la pérdida completa de la funcionalidad del mismo. [2]

¿Y qué debe hacer una compañía ante estas situaciones?

A fin de detectar posibles problemas de seguridad relacionados con los dispositivos médicos, la FDA requiere la utilización de "Informes de Dispositivos Médicos". Los fabricantes están obligados a reportar eventos adversos a través de este tipo de informes. Mientras que se alienta a profesionales sanitarios, cuidadores o pacientes a presentar informes voluntarios sobre posibles eventos adversos que estos puedan apreciar. [3]

Uno de los errores más comunes que cometen los fabricantes a la hora de comunicar la situación a las organizaciones correspondientes es esperar demasiado. Y esto puede resultar comprensible hasta cierto punto. Las compañías pueden tener miedo a hacer público este tipo de situaciones debido a las consecuencias sobre su imagen corporativa, a las consecuencias económicas,…

Pero en realidad informar sobre los peligros no solo demuestra un buen hacer por parte de la compañía sino que demuestra una preocupación por la salud de sus clientes.

Los fabricantes necesitan entender que **alertar a las organizaciones pertinentes** acerca de problemas potenciales no siempre posee como desencadenante una retirada del producto del mercado. No hacerlo puede conducir, a su vez, a una mayor desconfianza por parte de los clientes o incluso a tener que hacer frente a multas cuantiosas.

Otro punto importante a considerar es la **transparencia**. Los fabricantes de dispositivos médicos deben ser francos sobre la verdadera naturaleza de la situación. Este no es el momento de endulzar los problemas. Los fabricantes deben estar preparados para divulgar el peligro potencial así como su alcance e impacto. [4]

Es importante entender que este tipo de organizaciones permiten actuar de forma más rápida al poder llegar a un mayor número de afectados.

¿Y porqué se producen tantos ataques contra este sector?

Después de investigar he podido encontrar una serie de razones [5] por las cuales el sector de la salud y por consiguiente, el de los dispositivos médicos, representan uno de los mayores objetivos para los hacktivistas:

- **La información privada de los pacientes posee alto valor económico para los atacantes:** Los hospitales almacenan una ingente cantidad de datos. Datos confidenciales que valen mucho dinero y que pueden ser vendidos fácilmente, lo que convierte a la industria médica en un objetivo cada vez más relevante.
- **Dispositivos médicos como punto de entrada:** Los dispositivos médicos como los rayos X, las bombas de insulina o los desfibriladores desempeñan un papel fundamental en la atención médica moderna. Sin embargo, este tipo de dispositivos pueden ser utilizados para lanzar un ataque sobre dispositivos mayores como pueden ser los servidores de un hospital. Incluso en el peor de los casos, los hackers pueden hacerse con el control completo de un dispositivo médico, impidiendo que las organizaciones sanitarias proporcionen a los pacientes la atención que requieren.
- **Acceso a datos remotos:** Conectarse a una red de forma remota puede resultar peligroso en caso de que no se tomen las medidas oportunas. De esto hablamos también en el post anterior, en el cual mencioné la necesidad de hacer uso de canales de comunicación seguros.
- **Los profesionales sanitarios no están concienciados sobre los múltiples riesgos tecnológicos existentes:** Cuando hablamos de seguridad, el eslabón más débil suele ser el empleado. El personal sanitario suele estar demasiado ocupado como para mantenerse informado sobre las últimas amenazas correspondientes a los dispositivos médicos. Sin embargo con que un solo dispositivo se vea comprometido, toda la red puede haber sido vulnerada.

Y ahora que ya tenemos una visión completa, me gustaría decir que a pesar de que los dispositivos médicos presenten múltiples riesgos y resulten

vulnerables a ataques también facilitan la vida de muchas personas y permiten que muchas personas continúen con vida. Con el transcurso del tiempo cada vez obtendremos dispositivos médicos más seguros, eficaces y efectivos.

Ojala yo hoy no tuviera contenido para escribir este post, ya que eso implicaría que los dispositivos médicos serían completamente seguros. Ya es imposible cambiar el pasado y solo nos queda aprender de él para evolucionar hacia el futuro.

Ha sido un placer escribir para todos vosotros durante este tiempo pero esto ha llegado a su fin. Ha sido un periodo corto pero espero que os haya gustado. Como se suele decir coloquialmente "lo bueno, si breve, dos veces bueno".

PD: Aunque se salga un poco de la línea argumental seguida durante este recorrido, no me gustaría acabar este post sin hacer mención a la necesidad de continuar investigando. Hace relativamente poco, por ejemplo, fue el día del cáncer de pulmón, una enfermedad que representa el 20,55% de defunciones en el territorio nacional. Además de resultar uno de los cánceres más letales, la calidad de vida de la cual disponen los pacientes supervivientes se ve considerablemente mermada. Es por ello que a través de este post me gustaría dar visibilidad a todas esas personas que sufren cada día las consecuencias de enfermedades como esta y recalcar la necesidad de continuar investigando. No solo en esta temática en concreto sino en la medicina en general. Solo a través de la investigación conseguiremos erradicar o paliar las consecuencias de este tipo de enfermedades y la tecnología puede resultar una gran fuente de ayuda. La investigación y cooperación son pilares fundamentales para continuar prosperando.

Y ahora sí que sí…**THE END**

Referencias

[1] <<Medtronic Conexus Radio Frequency Telemetry Protocol>>, CISA, acceso el día 30 de noviembre del 2019, https://www.us-cert.gov/ics/advisories/ICSMA-19-080-01

[2] <<Firmware Update to Address Cybersecurity Vulnerabilities Identified in Abbott's (formerly St. Jude Medical's) Implantable Cardiac Pacemakers: FDA Safety Communication>>, FDA, acceso el día 30 de noviembre del 2019,

https://www.fda.gov/medical-devices/safety-communications/firmware-update-address-cybersecurity-vulnerabilities-identified-abbotts-formerly-st-jude-medicals

[3] <<Medical Device Reporting (MDR): How to Report Medical Device Problems>>, FDA, acceso el día 30 de noviembre del 2019, https://www.fda.gov/medical-devices/medical-device-safety/medical-device-reporting-mdr-how-report-medical-device-problems

[4] <<Software is a top cause of medical device recalls: Here's what you can do>>, Medical Design & Outsourcing, acceso el día 30 de noviembre del 2019, https://www.medicaldesignandoutsourcing.com/software-leading-cause-medical-device-recalls/

[5] <<9 reasons why healthcare is the biggest target for cyberattacks>>, Swivel Secure, acceso el día 30 de noviembre del 2019, https://swivelsecure.com/solutions/healthcare/healthcare-is-the-biggest-target-for-cyberattacks/

Cuando se habla de salud, aceptar riesgos no es una opción

En el anterior artículo pudimos ver como los dispositivos médicos pueden manipularse para administrar dosis fatales de insulina, para robar datos de pacientes o incluso para directamente dejarlos inoperativos. Estos escenarios no son ciencia ficción. Son muy reales y cada vez son más los dispositivos médicos como marcapasos, bombas de insulina o máquinas de resonancia magnética vulnerables a sufrir ataques.

Mientras investigaba me he encontrado con un artículo [1] en el cual se recoge como varios investigadores emularon el funcionamiento de un dispositivo médico en un sistema de señuelo. En el transcurso de seis meses, los malhechores se conectaron con éxito en más de 55.000 ocasiones al sistema e instalaron más de 300 malwares. Esto refleja lo expuestos que estamos ante este tipo de ataques. Los dispositivos médicos están constantemente en peligro de ser comprometidos y es por ello que todo lo expresado hasta este post cobra especial relevancia.

Cuando hablamos de temas tan sensibles como es el caso de la salud de las personas, aceptar los riesgos no es una opción.

¿Y entonces qué hacemos?

Tenemos que gestionar dichos riesgos. La seguridad del paciente debería ser ante todo la prioridad de todos los fabricantes de dispositivos médicos.

Esta gestión, además, no resulta opcional sino que es un requisito reglamentario en todo el mundo. La FDA de los EE.UU. lo exige en el Reglamento del Sistema de Calidad. Europa, a su vez, lo requiere en el nuevo Reglamento de Dispositivos Médicos.

Asimismo, Japón, Canadá, Australia, Brasil y todos los demás mercados importantes también requieren la aplicación de la gestión de riesgos, a la cual se hace referencia en sus reglamentos nacionales o en la norma **ISO 13485:2016**. [2] Esta norma internacional respalda la obligación de los fabricantes de asegurarse de que los productos cumplen sistemáticamente los requisitos normativos aplicables y las exigencias del cliente. [3]

Sin embargo, todos ellos se rigen por la norma **ISO 14971**, norma mundial para la gestión de riesgos de los dispositivos médicos. Esta norma aprobada por la FDA, especifica el proceso de gestión de riesgos mediante el cual un fabricante puede identificar los peligros asociados con su dispositivo médico, estimar y evaluar los riesgos, **controlar** estos riesgos y supervisar la eficacia de los controles a lo largo del ciclo de vida del producto. [4]

Parece fácil, ¿verdad? No obstante, la realidad es que la gestión de riesgos es uno de los aspectos más complejos del cumplimiento de las regulaciones.

En este post, en concreto, nos vamos a centrar en los controles para mitigar los riesgos asociados a este tipo de dispositivos.

¿Pero qué es un control?

Un control es un proceso en cual se toman decisiones y se aplican medidas que permiten reducir los riesgos a niveles especificados.

Para cada uno de los riesgos es necesario estimar el **grado de impacto** así como la **probabilidad** de que este ocurra. A partir de estos valores se puede estimar si el riesgo resulta crítico, moderado o bajo pudiendo detectar aquellos riesgos sobre los cuales deberemos aplicar controles. [5]

¿Os acordáis de los riesgos que mencionamos en el anterior artículo?

Los hemos mencionado un poco antes: accesos no autorizados, ataques contra la disponibilidad, robo de datos, cambio de ajustes de configuración, software y firmware no probado o defectuoso …

Ahora vamos a intentar establecer una serie de controles para mitigar dichos riesgos: [6][7]

- **Establecer controles de acceso:** Consiste en limitar el acceso al dispositivo médico conectado a través de técnicas como la doble autenticación, uso de tecnologías NFC, establecimiento de contraseñas,… Este tipo de medidas permiten reducir el número de accesos no autorizados, reduciendo de esta forma también las posibilidades de sufrir un robo de datos. Sin embargo, este tipo de medidas pueden resultar polémicas en determinados casos: ¿Establecemos una contraseña de acceso en un marcapasos? De esto hablaremos un poco más adelante.
- **Realizar actualizaciones periódicas:** Es necesario aplicar parches de seguridad al dispositivo médico con frecuencia de acuerdo con las pautas posteriores a la comercialización emitidas por la FDA.
- **Aplicar estándares de codificación:** Muchos ciberataques exitosos han explotado vulnerabilidades presentes en el código que no han sido probadas rigurosamente antes de su implementación en un entorno activo. Una de las normas más importantes de la industria es la emitida por la Comisión Electrotécnica Internacional (IEC), IEC 62304. Este estándar proporciona una serie de características robustas sobre cómo desarrollar mejor el código.
- **Aplicar la seguridad mediante el diseño:** Es fundamental la gestión adecuada del ciclo de vida del dispositivo médico. Tener en cuenta la seguridad desde el primer momento en el cual se va a diseñar el dispositivo resulta fundamental.
- **Hacer uso de canales de comunicación cifrados:** Los dispositivos deberían hacer uso de canales de comunicación debidamente encriptados a fin de comunicarse con el mundo exterior.

Pero los controles no solo se deben establecer, estos a su vez deben ser **auditados**. Realizar auditorías periódicas de los procesos y de la tecnología ayuda a identificar las amenazas y permite mitigar los riesgos. Esta labor recae sobre los **auditores,** es decir las personas responsables de velar por la cumplimentación de las regulaciones correspondientes y de evaluar los procedimientos llevados a cabo por la organización.

Cuando se trata de auditorías de dispositivos médicos, las **pruebas de penetración** son un enfoque recomendado. Estas pruebas ayudan a evaluar lo fácil que es para los hackers violar la seguridad de los dispositivos para obtener recursos tales como datos, interrumpir operaciones o modificar sistemas que podrían afectar la salud del paciente.

Además, establecer controles no solo implica establecer iniciativas que solucionen el problema. Debemos ser conscientes también del ámbito en el cual se aplican. El otro día me enviaron una noticia en la cual el titular decía

“Investigadores muestran la relación entre las brechas de datos y las tasas de mortalidad hospitalaria”. [8] Al principio pensé que la relación entre ambos factores sería las consecuencias generadas por el ataque. Sin embargo, la relación que establecía el estudio yacía en las contramedidas aplicadas por los hospitales y su consecuente aumento en los tiempos de atención a los pacientes.

Al final intentamos blindar los dispositivos y se nos olvida que en este sector en concreto se necesita de dispositivos seguros y efectivos pero que a su vez resulten rápidos en caso de emergencia. Imaginaros un médico que tuviera que estar introduciendo una contraseña mientras el paciente se está muriendo.

¿Y qué pasaría si al profesional sanitario se le ha olvidado la contraseña?

Somos humanos, estas cosas pueden pasar. Desde un punto de vista tecnológico esto supone un reto ya que cualquier mala implementación posee como resultado lo mencionado en el artículo, un aumento en la tasa de mortalidad.

Es por ello que se debe establecer una alineación entre las medidas aplicadas y el ámbito del mismo. ¿De que sirve blindar un dispositivo si en caso de emergencia no podemos acceder a él? ¿Tal vez tengamos que hacer uso de nuevas tecnologías? Y estas tecnologías a su vez, ¿ qué riesgos presentarían?

Muchas preguntas a contestar cuyas respuestas no resultan sencillas. Sin embargo lo que sí sé es que necesitamos dispositivos seguros, efectivos y alineados con el trabajo que realizan los profesionales del sector. En el momento en que se consiga alcanzar todo ello será cuando este sector alcance su máximo esplendor, pudiendo todos los ciudadanos aprovechar las ventajas que nos aporta la tecnología sin miedo a que nuestra vida corra peligro.

Y hasta que el post de hoy.

Referencias

[1] <<Closing the Gap in Medical Device Cybersecurity>>, Knowledge Leader, acceso el día 22 de noviembre del 2019, https://www.knowledgeleader.com/knowledgeleader/content.nsf/web+content/hotissueclosingthegapinmedicaldevicecybersecurity

[2] <<ISO 14971 and the Basics of Medical Device Risk Management Explained>>, Oriel, acceso el día 22 de noviembre del 2019, https://www.orielstat.com/blog/iso-14971-basics-explained/

[3] <<ISO 13485 Certificación para los productos sanitarios>>, Lloyd's register, acceso el día 23 de noviembre del 2019, https://www.lr.org/es-es/iso-13485/

[4] <<Case study – Risk management for medical devices (based on ISO 14971)>>, IEEE Xplore, acceso el día 20 de noviembre del 2019, https://ieeexplore.ieee.org/document/5754492

[5] <<The definitive guide to ISO 14971 risk management for medical devices>>, Green Light, acceso el día 22 de noviembre del 2019, https://www.greenlight.guru/blog/iso-14971-risk-management

[6] <<The Internet of Medical Things – Anticipating the Risk>>, ISACA, vol 4 (2019): 27-32

[7] <<Medical device cyber security guidance for industry>>, Australian Government, acceso el día 22 de noviembre del 2019, https://www.tga.gov.au/sites/default/files/medical-device-cyber-security-guidance-industry.pdf

[8] <<Researchers Show Link Between Data Breaches and Hospital Mortality Rates>>, CPO Magazine, acceso el día 20 de noviembre del 2019, https://www.cpomagazine.com/cyber-security/researchers-show-link-between-data-breaches-and-hospital-mortality-rates/?mc_cid=61cc16581e&mc_eid=5a73407028

Con la salud no se juega

¿Con ganas de seguir profundizando en el ámbito de los dispositivos médicos? Ojalá que así sea.

Antes de empezar me gustaría recapitular un poco. En el primer post pudimos obtener una visión general sobre el amplio mundo del IoMT, mientras que en el segundo post profundizamos en mayor medida en la relevancia de la cual disponen este tipo de dispositivos en la industria. En este post, sin embargo, nos vamos a centrar más en sus riesgos.

¿Os lo podrías imaginar no? A pesar de disponer de múltiples beneficios, los riesgos son una cuestión importante a tener en cuenta.

Algunos de los principales riesgos asociados a los dispositivos médicos son los **riesgos cibernéticos**. El ataque WannaCry, por ejemplo, muestra cómo la interconexión de los sistemas de salud y las **débiles prácticas de seguridad** pueden poner en riesgo tanto a las organizaciones como a los pacientes. Este malware afectó a dos hospitales de EE. UU, en los cuales los atacantes aprovecharon las vulnerabilidades conocidas en el software de los dispositivos para atacar. Muchos dispositivos en todo el sistema sanitario utilizan software antiguo que es difícil de actualizar, lo que significa que están indefensos a que actores maliciosos los exploten. [1]

En junio de este mismo año, por ejemplo, la empresa Medtronic tuvo que retirar del mercado algunas bombas de insulina ya que resultaban vulnerables a ataques, siendo imposible su enmienda a través de una actualización. Este tipo de dispositivos estaban siendo utilizados por alrededor de 4000 pacientes, pudiendo cualquier persona que no fuese cuidador o proveedor de atención médica conectarse de forma inalámbrica y cambiar la configuración de la bomba. Esto podría permitir a cualquier persona administrar insulina en exceso a un paciente (lo que llevaría a un nivel bajo de azúcar en sangre) o a detener la administración de insulina (lo que podría conllevar a una cetoacidosis diabética). [2]

En octubre, hace escasamente un mes, la Administración de Drogas y Alimentos (FDA) emitió una advertencia a los consumidores sobre posibles fallos de ciberseguridad en algunos dispositivos médicos. Los investigadores identificaron 11 vulnerabilidades que permitían que cualquier persona tomara el control de los dispositivos médicos a distancia y cambiara su función, causara fugas de información o incluso causara un ataque de denegación de servicio inhabilitando el dispositivo. [3]

Además, las compañías de dispositivos médicos poseen datos sensibles y de alto valor que los ciberdelincuentes o los hacktivistas pueden intentar robar. **La información de identificación personal** (IIP) como los **datos clínicos** de los pacientes son un objetivo primordial a proteger. Estos datos no solo deben ser protegidos antes atacantes externos, sino que también se

deben controlar los accesos internos realizados por empleados a los datos sensibles y restringir aquellos accesos no autorizados.

Según un estudio realizado en 2016 por el Ponemon Institute, que incluyó a empresas de dispositivos médicos, el 90 por ciento de las organizaciones de salud habrían sufrido una violación de datos en los dos años previos a la realización del estudio. Ponemon estima que estos incidentes le costaron a la industria de la salud 6.200 millones de dólares. [1]

¿Y cuales son los mayores riesgos que presentan actualmente los dispositivos médicos?

De acuerdo al informe realizado por el instituto ECRI con vistas al año 2020 acerca de los peligros tecnológicos más candentes en cuanto a dispositivos médicos se refiere, [4] se pueden resaltar los siguientes:

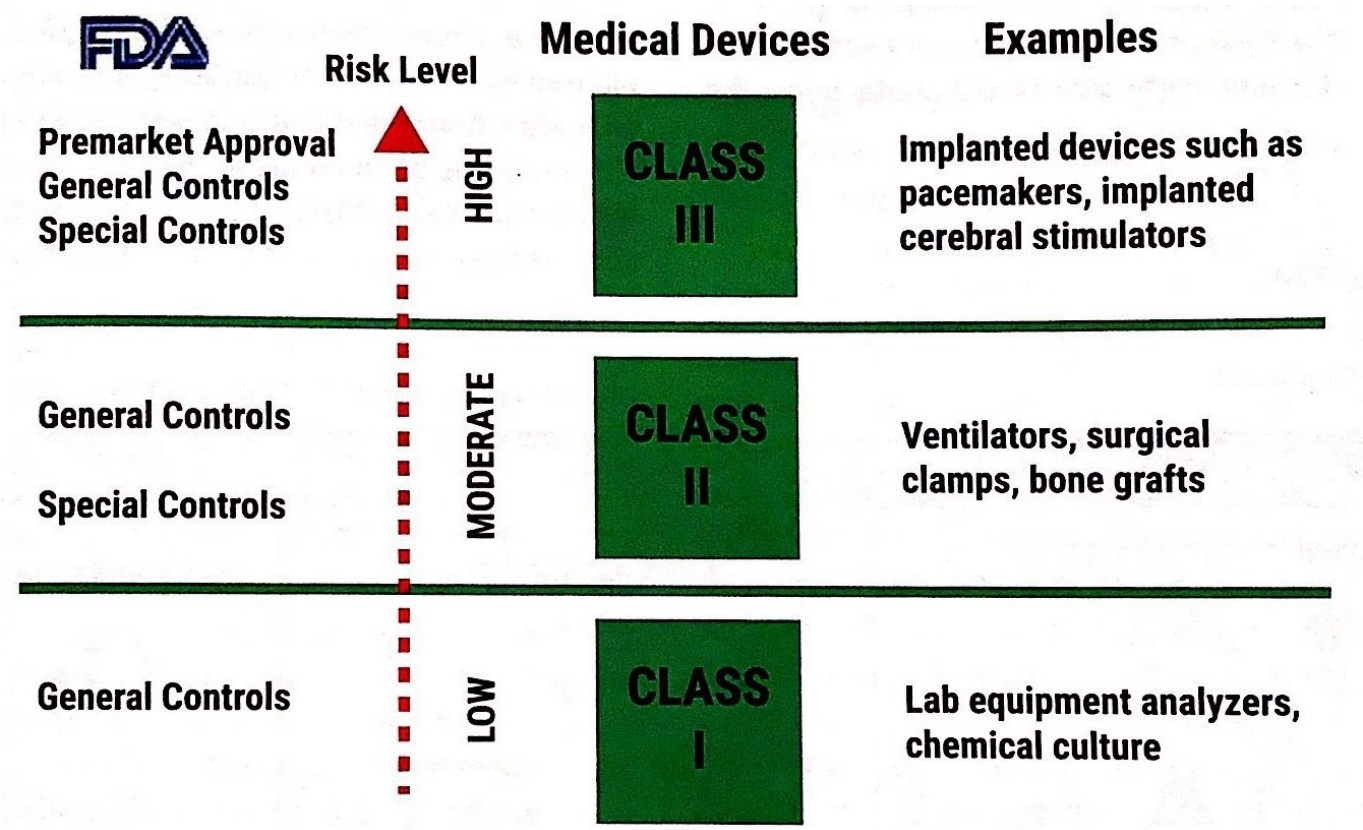
- **Procedimientos quirúrgicos robóticos no probados:** Los centros de salud necesitan procesos robustos para aprobar la aplicación de robots quirúrgicos en nuevos procedimientos, así como programas integrales de capacitación y acreditación para cirujanos y personal de quirófano.
- **Sobrecarga de alarmas, alertas y notificaciones:** Se necesita un enfoque global que tenga en cuenta todas las fuentes de datos a fin de evitar la sobrecarga cognitiva que puede distraer o desensibilizar a los médicos. Esto puede hacer que profesionales sanitarios ignoren notificaciones relevantes.
- **Riesgos de la ciberseguridad en el entorno de atención sanitaria a domicilio:** Al igual que con cualquier dispositivo médico en la red, los dispositivos médicos utilizados en el hogar deben estar protegidos contra amenazas que puedan interrumpir el flujo de datos, alterar o degradar el rendimiento del dispositivo o exponer información médica protegida.
- **Las tuercas y tornillos sueltos:** Las tuercas y tornillos que sujetan los componentes de los dispositivos médicos pueden aflojarse con el tiempo. Si no se reparan o reemplazan estos mecánicos, se pueden producir consecuencias graves. Los dispositivos pueden volcarse, caerse o colapsar durante su uso, lo cual puede provocar lesiones o incluso la muerte de pacientes.

En este estudio también se contemplan otro tipo de peligros que no corresponden explícitamente al ámbito tecnológico, por lo que no los he tenido en cuenta en este artículo.

Ante este contexto, en 2014 la FDA (Food and Drug Administration) por primera vez en su historia y como el primer organismo regulador del mundo, identificó y abordó el riesgo de la ciberseguridad asociada a los dispositivos médicos. Esta fue la primera mejora para proteger a los pacientes desde la perspectiva de la ciberseguridad de los dispositivos médicos. [5]

Vale, bien… ¿Y cómo podemos clasificar los dispositivos médicos?

De acuerdo a la FDA, los dispositivos médicos pueden ser clasificados de acuerdo a su riesgo de la siguiente forma: [6]



Clasificación de dispositivos médicos en base a riesgos (ISACA)

- **Dispositivos clase I:** Estos dispositivos presentan un **potencial mínimo de daño** al usuario y a menudo tienen un diseño más simple que los dispositivos de Clase II o Clase III. Por ejemplo, se pueden incluir dentro de esta clasificación dispositivos como los estetoscopios.
- **Dispositivos clase II:** La mayoría de los dispositivos médicos se consideran dispositivos de Clase II. Estos dispositivos disponen de un **riesgo moderado** y dentro de esta clase se pueden incluir dispositivos como las sillas de ruedas eléctricas o dispositivos de rayos X.
- **Dispositivos clase III:** Estos tipos de dispositivos normalmente son responsables de mantener con vida al paciente, son implantados o

> presentan **un riesgo potencial** de enfermedad o lesión. Ejemplos de dispositivos de Clase III pueden ser los marcapasos implantados.

Dado que la clasificación de los dispositivos médicos se basa en el riesgo, es importante entender el nivel de riesgo y, lo que es más importante, para qué se va a utilizar el dispositivo desde el punto de vista médico y su alcance.

Espero que con este artículo os haya quedado más claro la ingente cantidad de riesgos a los cuales están expuestos los dispositivos médicos (control remoto no autorizado, robado de información personal, ataques a la disponibilidad,…) y cómo podemos clasificarlos de acuerdo a su riesgo para luego poder establecer **controles**.

Pero de esto hablaremos en mayor profundidad en el siguiente post, espero que os haya gustado.

Referencias

[1] <<Life Sciences, Pharmaceutical and Medical Device Companies Need to Trust Less and Question More to Keep High-Value Data Safe>>, Knowledge Leader, acceso el día 15 de noviembre del 2019, https://www.knowledgeleader.com/knowledgeleader/content.nsf/web+content/hotissuekeephighvaluedatasafe

[2] <<Medtronic recalls some insulin pumps as FDA warns they can be hacked>>, CNBC, acceso el día 15 de noviembre del 2019, https://www.cnbc.com/2019/06/27/medtronic-recalls-some-insulin-pumps-as-fda-warns-they-can-be-hacked.html

[3] <<FDA issues warning on medical devices that are vulnerable to takeover from hackers>>, CNBC, acceso el día 16 de noviembre del 2019, https://www.cnbc.com/2019/10/01/fda-issues-warning-on-medical-devices-that-are-vulnerable-to-cyberattacks.html

[4] <<Top 10 Health Technology Hazards for 2020>>, ECRI Institute, acceso el día 16 de noviembre del 2019, https://assets.ecri.org/PDF/White-Papers-and-Reports/ECRI-Top-10-Technology-Hazards-2020.pdf

[5] <<The Internet of Medical Things – Anticipating the Risk>>, ISACA, vol 4 (2019): 27-32

[6] <<Classify Your Medical Device>>, FDA, acceso el día 17 de noviembre del 2019, https://www.fda.gov/medical-devices/overview-device-regulation/classify-your-medical-device

---

Tecnología al servicio de la salud: relevancia en la industria

Bueno aquí estamos otra vez, ¿con ganas de conocer cómo de relevantes resultan los dispositivos médicos en la industria? Espero que sí.

Una vez habiendo comprendido de qué trata el amplio mundo del IoMT, es momento de centrarnos en como de relevantes resultan este tipo de dispositivos en el sector.

Durante el siglo XX, los avances científicos, médicos y de salud impulsaron la primera revolución de la longevidad en los Estados Unidos: un aumento de más de 30 años en la esperanza de vida. [1] Gracias a los seguimientos clínicos realizados sobre los pacientes, los expertos de la salud se volvieron más eficientes en la determinación sobre cuando tienden a surgir las enfermedades, que factores de riesgo contribuyen a su aparición y progresión,…

Sin embargo, las estadísticas no capturan lo que realmente está sucediendo dentro de nuestros cuerpos. Gracias a los avances tecnológicos (como pueden ser los rayos X, las tomografías computarizadas, cirugía laparoscópica,…), los médicos no sólo pueden diagnosticar con mayor certeza, sino también detectar posibles enfermedades antes de que los síntomas se manifiesten. Yendo un poco más allá, la tecnología no solo ha permitido facilitar las labores de diagnóstico sino tomar una posición activa en el tratamiento de determinadas patologías.

Mientras investigaba he podido observar una serie de casos que me han parecido interesantes y que me gustaría compartir con vosotros.

En el ámbito de las enfermedades torácicas, por ejemplo, se puede observar cómo la tecnología ha facilitado la vida de los pacientes hospitalizados que requieren de drenajes pleurales. Gracias a la creación de dispositivos denominados "Thopaz", los pacientes disponen de mayor movilidad, prescindiendo así de la restricción de quedarse postrados en la cama durante el proceso. Este dispositivo no solo aporta beneficios palpables a los pacientes sino que mejora la atención sanitaria proporcionada por los profesionales médicos. Entre los múltiples beneficios que proporciona este dispositivo se podría destacar una mejora en la planificación del alta, una simplificación en el consenso entre diferentes observadores gracias a la supervisión precisa de las fugas de aire,… [2] En el Hospital Universitario Cruces, por ejemplo, los pacientes que requieren este tipo de intervenciones hacen uso de este tipo de dispositivos.

Sin embargo, imaginaros que podría pasar si el dispositivo no garantizase un correcto hermetismo e introdujese aire al pulmón o si el sistema fuese hackeado. Las consecuencias podrían ser catastróficas, pudiendo llegar incluso a provocar la muerte del paciente. De esto hablaremos en mayor profundidad durante el siguiente post.

Asimismo, en el ámbito de los trastornos neurológicos y neuropsiquiátricos la empresa norteamericana NeuroSigma ha desarrollado un tratamiento no farmacológico a fin de ofrecer una alternativa con bajo riesgo y sin medicamentos a aquellos niños que sufren de Trastorno por Déficit de Atención con Hiperactividad (TDAH). Haciendo uso de estimulación eléctrica de bajo nivel, el dispositivo intenta ser una alternativa al tratamiento con medicamentos actual. Este dispositivo ha recibido este año la aprobación por parte de la FDA. [3]

¿Pero qué es la FDA?

La FDA (Food and Drug Administration) es la agencia del gobierno de los Estados Unidos responsable de proteger la salud pública al garantizar la seguridad, eficacia y protección de los medicamentos, los cosméticos, … Y también de los dispositivos médicos [4]

En el caso del mercado europeo, los fabricantes de dispositivos médicos deben cumplir con el Reglamento sobre Dispositivos Médicos 2017/745 establecido como una enmienda a la Directiva 93/42/CEE de la UE. [5]

Esto permite disponer y hacer uso de dispositivos avalados y homologados por las autoridades de la salud.

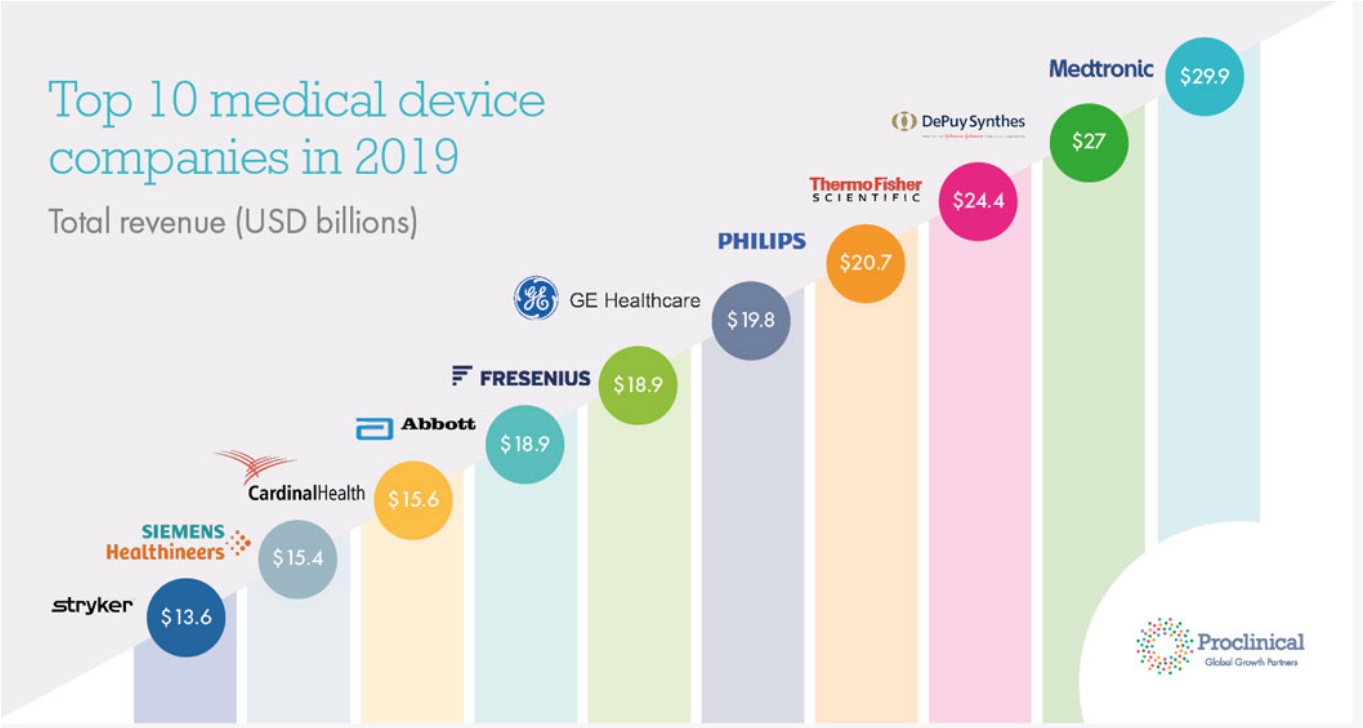
La tecnología avanza a un ritmo frenético, que duda cabe de ello. Atendiendo a los avances mencionados previamente resulta difícil augurar con seguridad el límite hasta el cual seremos capaces de llegar los humanos.

Recuerdo que cuando yo empecé a estudiar la carrera, un profesor nos dijo: "El único límite que tenéis es vuestra imaginación". Y qué razón tenía… Siempre que seamos capaces de imaginarlo seremos capaces de hacerlo. Puede que el resultado sea mejor o peor, o puede ser que aún no estemos preparados para llevarlo a cabo pero que una década nuestras ideas ambiciosas resulten un simple juego de niños. ¿Realidad virtual que acelere la curación de la rehabilitación? ¿Dispositivos de ultrasonido que nos eviten tener que realizarnos pruebas de diagnóstico más invasivas?

¿Quien sabe como será nuestra atención sanitaria dentro de unas décadas?

Atendiendo a un informe realizado por la consultora KPMG respecto a la situación de los dispositivos médicos en el año 2030, [6] se prevé que la industria de dispositivos médicos incremente sus ventas anuales en un 5 por ciento cada año, alcanzando la cifra de US$800 mil millones para el año 2030. Estas proyecciones reflejan una creciente demanda de nuevos e innovadores dispositivos (como pueden ser las prendas de vestir) y nuevos servicios (Procesos de intervención quirúrgicos innovadores, mecanismos de imagen innovadores, …)

Actualmente, las principales compañías que operan dentro de este sector son las siguientes:



Reparando al gráfico realizado por la compañía Proclinical [7], se puede observar cómo la empresa Medtronic es la compañía de dispositivos médicos más grande del mundo que genera la mayoría de sus ventas y ganancias del sistema de salud de los EE. UU. Esta es una de las principales compañías encargadas de desarrollar sistemas de soporte vital, bombas de insulina,…

Tal es el aumento de este sector que también han comenzado a proliferar múltiples startups destinadas a resolver problemas de salud haciendo uso de tecnologías avanzadas. Entre estas startups innovadoras podemos destacar Transplant Biomedicals, la cual ha desarrollado un nuevo sistema de transporte de órganos. Durante el proceso de transplante resulta vital reducir los tiempos de espera y conseguir la mayor calidad en el transporte. [8]

Desde mi punto de vista, a este sector aún le queda un largo camino por recorrer y los ciudadanos seremos partícipes de una nueva sanidad en la cual la tecnología cobrará un papel protagonista. Para mi siempre y cuando se garantice que los dispositivos creados no resulten perjudiciales para la salud y se contemplen los posibles riesgos asociados a los mismos estableciendo salvaguardas para evitarlos, bienvenidos serán.

Espero que este post os haya resultado interesante y os haya permitido obtener una visión más completa sobre la relevancia que están cobrando este tipo de soluciones en la sociedad. Y por supuesto, si tenéis cualquier tipo de duda siempre me podéis dejar un comentario. Yo encantado de contestaros.

!Nos vemos¡

Referencias

[1] <<The Future of Smart Health>>, IEEE Xplore Digital Library, acceso el día 9 de noviembre del 2019, https://ieeexplore.ieee.org/document/7742289

[2] <<Sistema de supervision y drenaje torácico digital Thopaz>>, Medela Healthcare, acceso el día 8 de noviembre del 2019, https://www.medelahealthcare.es/soluciones/drenaje-cardiotoracico/thopaz

[3] <<Aprobado por la FDA el primer dispositivo médico para el tratamiento del TDAH>>, IM Médico Hospitalario, acceso el día 8 de noviembre del 2019, https://www.immedicohospitalario.es/noticia/16368/aprobado-por-la-fda-el-primer-dispositivo-medico-para-el-tratamiento

[4] <<What we do>>, U.S Food and Drug Administration, acceso el día 7 de noviembre del 2019, https://www.fda.gov/about-fda/what-we-do

[5] <<Medical Devices>>, European Commission, acceso el día 8 de noviembre del 2019, https://ec.europa.eu/growth/sectors/medical-devices_en

[6] <<Medical Devices 2030>>, KPMG, acceso el día 9 de noviembre del 2019, https://assets.kpmg/content/dam/kpmg/xx/pdf/2017/12/medical-devices-2030.pdf

[7] <<The top 10 medical device companies (2019)>>, Proclinical, acceso el día 9 de noviembre del 2019, https://www.proclinical.com/blogs/2019-5/the-top-10-medical-device-companies-2019

[8] <<3 startups que están revolucionando los avances en el sector de la salud>>, Emprendedores, acceso el día 9 de noviembre del 2019, https://www.emprendedores.es/ideas-de-negocio/a25638554/startups-salud-revolucionan-avances-tecnologia-sector-medicina/

Destino: satisfacción del cliente

Hace unos días comentábamos en clase la relevancia que ciertas startups están cobrando últimamente en sectores tradicionales como pueden ser la banca o los seguros. Términos como Fintech o Insurtech cada vez cobran mayor relevancia en el mercado, ¿pero a qué se debe este fenómeno?

Debido a la proliferación de nuevas tecnologías, se han generado nuevos modelos de negocio con el objetivo de suplir las carencias presentes en las compañías tradicionales. Mediante la utilización de la tecnología, estas empresas son capaces de ofrecer a sus clientes productos y servicios innovadores. Estas nuevas soluciones destacan por su transparencia, grado de personalización, costes y por ser productos enfocados en el usuario.

Es importante resaltar que para estas empresas el foco es el **cliente**, mientras que en la banca tradicional o en los seguros el foco era el **producto**. Debemos ser conscientes que para poder ofrecer a los usuarios una correcta experiencia, es necesario diseñar soluciones que conecten con el usuario y le acompañen en todo el proceso. Puede resultar obvio pero los negocios requieren de clientes, requieren de personas que adquieran un producto o se suscriban a un servicio. Es por ello que desatender sus necesidades o no prestarles la atención que se merecen puede provocar insatisfacción, repulsión o incluso la pérdida perenne de un cliente.

¿Y como podemos analizar la experiencia que ofrecemos a los clientes?

Para poder comprender mejor las necesidades de los usuarios, se pueden llevar a cabo tres tipos diferentes de investigación: [1]

- **User Research (Investigación de usuarios):** Permite comprender en mayor profundidad la problemática que se desea solucionar. A través de este tipo de investigaciones, se puede profundizar sobre las personas y sus circunstancias e identificar sobre qué ámbito debemos centrar nuestra atención.
- **UX Testing (Testing asociada a la experiencia de los usuarios):** Permite evaluar si la experiencia ofertada resulta óptima. Un producto complejo e inentendible puede producir rechazo y hacer que los clientes opten por productos de la competencia. Gracias a este tipo de pruebas, podemos

obtener más información sobre cómo de fácil resulta comprender y usar aquello que buscamos construir.
- **Customer Experience Research (Investigación de la experiencia de los clientes):** Esto permite entender por qué nos aman los clientes y de la misma forma, por qué los clientes deciden darse de baja o abandonar la compañía. Gracias a este tipo de investigaciones, se pueden establecer posibles vías de mejora y evaluar la situación actual de la compañía desde un punto de vista menos económico y más social.

Pero la experiencia de cliente no es solo usabilidad y un diseño atractivo.

Cuando se diseña un producto resulta necesario prestar atención a todos los detalles incluidos aquellos que conciernen a los usuarios pertenecientes a sectores minoritarios. En muchas ocasiones, no se presta atención a aquellas personas que presentan algún tipo de discapacidad. La accesibilidad representa una de las grandes temáticas olvidadas de la tecnología.

¿Cuántas veces hemos desarrollado una solución que resulte accesible para todo el mundo?

Yo desde luego que pocas veces, seguramente que ninguna. Pensando en él motivo por el cual nunca lo he hecho, se me han venido a la cabeza varias cuestiones: falta de tiempo, ignorancia,…. Sin embargo, esto no son más que excusas que establecemos para justificar la carencia de la aplicación asociada a los principios de accesibilidad. Hoy en día, podemos acceder a cualquier tipo de información con un mero click y con la accesibilidad ocurre exactamente lo mismo.

No se nos puede olvidar que la accesibilidad no es un funcionalidad extra que se agrega a un proyecto, sino que es un **derecho**. Si nos pusiéramos en el lugar de todas esas personas que cada día afrontan múltiples adversidades, es cuando verdaderamente nos daríamos cuenta de lo complicado que resulta poder realizar actividades que para nosotros resultan cotidianas. Hace poco pude ver en Internet un movimiento tecnológico que abogaba por la inutilización del cursor en nuestros ordenadores personales, obligándonos así a las personas a interactuar únicamente con el teclado. Creo que os podéis imaginar el resultado: múltiples páginas inaccesibles, sistemas mal estructurados, …

Como desarrolladores es nuestra **responsabilidad** no realizar distinciones de ningún tipo en los productos que desarrollamos.

Pero la experiencia de usuario no es solamente aplicable al mundo tecnológico. ¿Os acordáis de cuando Coca Cola comenzó su campaña #ShareACoke? Mediante esta campaña se incitaba a las personas a compartir una Coca Cola con la persona cuyo nombre apareciese escrito en el envase. Puede parecer una tontería, pero Coca Cola consiguió convertir una acción ordinaria de consumo en una experiencia de cliente personalizable y compartible. Gracias a esta iniciativa su presencia en redes sociales se multiplicó y sus ventas aumentaron por primera vez en 10 años. [2]

Es por todo eso que debemos darnos cuenta sobre el carácter social que poseen los negocios y dotar de relevancia a los clientes. Nuestra labor como profesionales debería consistir en acompañar a los mismos en todo el proceso y preocuparnos por su satisfacción. El director ejecutivo de Amazon, Jeff Bezos, manifestó la siguiente frase haciendo referencia a su compañía: "Nosotros vemos a nuestros clientes como los invitados de una fiesta en la que nosotros somos los anfitriones. Nuestro trabajo es hacer que la experiencia del cliente sea un poco mejor cada día".

Observando el éxito de Amazon, puede que no estén equivocados.

Y hasta aquí el post de hoy, ¡que tengáis un buen día!

Referencias

[1] <<De qué se tratan y por qué son tan importantes el User Research, UX Testing y CX Research>>, Octuweb, acceso el día 30 de octubre del 2019, https://octuweb.com/user-research-ux-testing-y-cx-research/

[2] <<5 ejemplos de «experiencia del cliente» ganadoras que inspirarán tu estrategia de marketing>>, Blog Digimind, acceso el día 30 de octubre del 2019, https://blog.digimind.com/es/insight-driven-marketing/5-estrategias-de-experiencia-del-cliente

---

Tecnología al servicio de la salud: introducción al mundo IoMT

Internet of things in healthcare, Medical Internet of Things, IoMT,… podemos encontrar multitud de términos que hacen referencia a una misma realidad. ¿Pero sabemos verdaderamente a que se refieren?

No se si alguna vez habréis escuchado estos términos o si los habréis leído en alguna noticia, pero tal vez si os hablo del Apple Watch o de las pulseras Fitbit la cosa cambie. Estos dispositivos además de proporcionar funcionalidades como la consulta de notificaciones o el envío de mensajes, permiten **monitorizar** el estado físico del usuario a través de un conjunto de sensores.

Si nos abstraemos de estos ejemplos concretos, el Medical Internet of Things o en su forma abreviada IoMT se podría definir como el conjunto de aplicaciones o dispositivos médicos que digitalizan y transforman la atención sanitaria. [1] Dicho de otra manera, se podría definir como un tipo de tecnología formada usualmente por un conjunto de sensores, los cuales aprovechando el poder de las comunicaciones se integran con otro tipo de sistemas a fin de promover un nuevo modelo médico más moderno.

Este tipo de tecnologías no solo permiten **monitorizar**, **informar** o **notificar** a los ciudadanos sobre estilos de vida poco saludables, sino que también pueden proporcionar a los proveedores de atención médica datos reales con el objetivo de **identificar** posibles problemas antes de que se vuelvan críticos.

Este tipo de dispositivos no pretenden sustituir a los proveedores sanitarios, sino que tratan de proporcionar datos para reducir las ineficiencias y el derroche en el sistema sanitario.

Gracias a la ingente cantidad de datos que fluyen continuamente desde este tipo de dispositivos, los facultativos médicos pueden llegar a conclusiones más rápidas y veraces. Por ejemplo, la famosa empresa de Cupertino, Apple, ha anunciado este año el lanzamiento de tres estudios innovadores en el sector de la salud, en los cuales se hará uso de los datos capturados por los dispositivos de la compañía. [2]

Dentro de este ámbito, podemos distinguir dos áreas principales: [3]

- **Dispositivos wearable:** Hace referencia a aquellos dispositivos electrónicos que pueden ser ubicados en alguna parte de nuestro cuerpo. De esta forma, el usuario puede interactuar con ellos en múltiples contextos. Ejemplo de este tipo de dispositivos pueden ser las pulseras de actividad, monitorizadores del estado de salud, …
- **Dispositivos non wearable:** Dispositivos que se encuentran en hospitales o clínicas. Se trata de dispositivos más específicos y que bien por su precio o su complejidad requieren de manipulación por parte de profesionales sanitarios.

Pero… **¿Es esto una moda pasajera o el inicio de un nueva forma de hacer medicina?**

La medicina es una ciencia que se remonta a la antigua Grecia, motivada inicialmente por la necesidad de curar las heridas de guerra. [4] Una de las principales figuras en este ámbito debido a sus aportaciones y su conocimiento es Hipócrates, quien alegaba que “Debemos volvernos a la naturaleza misma, a las observaciones del cuerpo en cuanto a salud y enfermedad, para aprender la verdad”.

Por lo tanto, la medicina es una ciencia antigua que ha ido evolucionando y mejorando a lo largo de la historia. De la misma forma, la tecnología también ha evolucionado a un ritmo vertiginoso haciendo que su uso se vea extendido a casi todos los ámbitos de la vida. Y la medicina, como no, es uno de ellos. Si bien la tecnología no puede detener el envejecimiento ni erradicar las enfermedades crónicas de momento, al menos pretende facilitar la labor de diagnóstico y control ejercida por los profesionales sanitarios.

De acuerdo a un estudio realizado por la consultora Frost & Sullivan, [5] se estima que para el año 2024 el mercado asociado a este tipo de dispositivos alcance la cifra de 10.9 billones. Asimismo, se prevé que para ese mismo año el mercado IoMT crezca en un 30,29%.

Por lo que los dispositivos conectados médicos están aquí para quedarse y no hay vuelta atrás. Sin embargo, no es oro todo lo que reluce. Este tipo de tecnologías plantean una serie de **riesgos** siendo necesario establecer una serie de **controles** a fin de garantizar tanto la integridad de los datos de los pacientes así como su integridad física. No se nos puede olvidar que este ámbito resulta muy sensible. Es por ello que se requiere de cierto tipo de regulaciones que permitan garantizar su correcto uso.

En mi opinión, la tecnología aún tiene mucho que aportar a este sector tan poco explotado y los beneficios asociados a este tipo de avances pueden resultar inmensurables. No obstante, estamos hablando de la salud de las personas por lo que toda cautela es poca.

Y bueno si queréis saber más acerca de la relevancia que tienen este tipo de tecnologías en la industria…

¡Nos vemos en el siguiente post!

PD: Para terminar, me gustaría dejaros aquí una frase que me ha invitado a reflexionar sobre la importancia que tiene estar sanos y como este tipo de tecnologías pueden ayudarnos a alcanzar dicho objetivo:

“La salud no lo es todo pero sin ella, todo lo demás es nada.”

Arthur Schopenhauer, filósofo alemán

Referencias

[1] <<¿Que es la IoMT?>>, Blog de Kiversal, acceso el día 20 de octubre del 2019, https://blog.kiversal.com/que-es-la-iomt/

[2] <<Apple announces three groundbreaking health studies>>, Apple Newsroom, acceso el día 20 de octubre del 2019, https://www.apple.com/newsroom/2019/09/apple-announces-three-groundbreaking-health-studies/

[3] <<The Internet of Medical Things – Anticipating the Risk>>, ISACA, vol 4 (2019): 27-32

[4]<<La medicina en la Grecia antigua: el nacimiento de una ciencia>>, National Geographic, acceso el día 20 de octubre del 2019, https://www.nationalgeographic.com.es/historia/grandes-reportajes/la-medicina-en-la-grecia-antigua_7023/6

[5] <<2019 Healthcare predictions unleashed – Growth opportunities, technology and trends>>, Frost & Sullivan, acceso el día 20 de octubre del 2019, https://apacmed.org/content/uploads/2019/03/Frost-Sullivan-2019-Medical-Devices-Outlook_20190227.pdf