CIBERSEGURIDAD EN EL SECTOR SALUD

Claudia Andrea Cortés Cedeño Jesús Alejandro Sevilla Patiño
Claudia Marina Vicario Solórzano

Instituto Politécnico Nacional
UPIICSA

andyceden90@gmail.com jsevillap1700@alumno.ipn.mx cvicario@ipn.mx

Resumen

En la última década, los avances tecnológicos han ayudado a la humanidad a facilitar sus actividades cotidianas y profesionales, donde el uso del internet e inteligencia artificial han hecho facilitar el acceso a información de cualquier área en específico o incluso de empresas o instituciones, pero esta libertad de poder encontrar información importante en ocasiones trae consecuencias que puede poner en riesgo la privacidad y seguridad de personas o, si fuera el caso, de las mismas organizaciones, a esto le llamamos ciberseguridad, es una de las herramientas más importantes y fundamentales dentro de una empresa o institución, pues protege los archivos de los usuarios, datos personales, información de vital importancia, e información crucial para una empresa, es de los pocas áreas en las que no se escatima en gastos, pues podría generar pérdidas millonarias en caso de que pudiera filtrarse algún tipo de información logrando incluso la quiebra y desaparición de esta misma empresa; por tanto en el caso del sector salud es mucho más importante, ya que la información de las cuentas de millones de usuarios están salvaguardadas por un sistema de ciberseguridad que puede repeler casi cualquier ataque.

Palabras claves: ciberseguridad, sector salud, inteligencia artificial, big data, dispositivos médicos.

ABSTRACT

In the last decade, technological advances have helped humanity to facilitate their daily and professional activities, where the use of the internet and artificial intelligence have made it easier to access information from any specific area or even from companies or institutions but this freedom to find important information sometimes brings consequences that can put at risk the privacy and security of people or, if it were the case, of the same organizations, we name this cybersecurity, it is one of the most important and fundamental tools in a company or institution, as it protects user files, personal data, vital information, and crucial information for a company, it is one of the few areas in which no expense is spared, as it could generate millions in losses in the event that some type of information could leak, even achieving the bankruptcy and disappearance of this same company; therefore, in the case of the health sector it is much more important, since the information in the accounts of millions of users are safeguarded by a cybersecurity system that can repel almost any attack.

Keywords: cybersecurity, health sector, artificial intelligence, big data, medical device.

I. Introducción

La ciberseguridad es un elemento importante dentro de cualquier institución o empresa ya que, si no se le da la atención y el seguimiento necesario puede ser el causante de problemas económicos, políticos, sociales, etc., es por esto que muchas empresas e instituciones desaparecen por la divulgación de datos e información importante que no fueron protegidos debidamente, hoy en día existen métodos para que esto no suceda que pueden ser desde un antivirus hasta programas complejos que garantizan la protección de toda la información de las organizaciones.

II. Ciberseguridad

En la actualidad más del 50% de la población mundial hace uso de alguna de las muchas tecnologías que tenemos hoy en día, y se sabe que todas las empresas de nivel mundial tienen sus datos almacenados en algún lado, es por esto que hay personas que se dedican a tratar de robar tan preciada información de estas empresas o incluso de usuarios, generando pérdidas para los usuarios y para las empresas, llegando incluso a demandas por parte de los usuarios debido al bajo sistema de seguridad que resguarda su información; estas personas son expertos en informática mejor conocidos como “Hackers”. “La cantidad de incidentes de ciberseguridad que afectan a empresas de todos los tamaños demuestra que nuestra postura actual de ciberseguridad no es del todo exitosa y que las empresas están pasando lentamente de una postura de evitación de riesgos a una estrategia de mitigación de riesgos” (Murphy y H. Murphy, 2013, p. 91.). Es por esto que las empresas deben considerar dentro de sus estrategias un sistema adecuado y eficaz para que toda la información esté resguardada y se eviten hackeos.

Una de las maneras más conocidas y más usadas por los usuarios, es el uso de antivirus, que son programas que detectan el uso de “malware informáticos”, que pueden venir adjuntos a los enlaces de alguna página web, aplicaciones, o incluso videos. En el caso de las empresas, los sistemas más comunes para la protección de sus datos e información son los Firewall (Cortafuegos), este sistema es uno de los más usados y más básicos a la hora de proteger la empresa. Por otro lado, tenemos el llamado Sistema IDS/IPS, que son sistemas que detectan si algún usuario quiere intervenir en algún dispositivo sin autorización. Actualmente existen personas con experiencia dedicadas a enseñar a jóvenes a mejorar los sistemas de ciberseguridad que son llamados defensores de la ciberseguridad que son “un subconjunto de profesionales de la seguridad que promueven, educan y motivan la adopción de las mejores prácticas y tecnologías de seguridad como un componente importante de sus trabajos”(Haney y Lutters, 2019, p. 112).

La privacidad en los sistemas de información, los dispositivos tecnológicos, las redes sociales, las bases de datos, etc., es uno de los problemas principales en la informática, donde los usuarios están expuestos a que la información y datos sean revelados ante el público, una de las soluciones para esta situación es la privacidad diferencial, la cual consiste en garantizar la

protección de información mediante algoritmos matemáticos, aplicaciones y optimización. "La privacidad diferencial ha surgido como un enfoque matemáticamente riguroso que ofrece sólidas garantías de privacidad. En particular, tiene varias propiedades útiles, incluida la resistencia tanto al posprocesamiento como al uso de información secundaria por parte de los adversarios". (Han y Pappas, 2018, p. 326)

III. Los piratas cibernéticos en el sector salud.

Una de las mayores preocupaciones a la hora de meter datos personales en una aplicación, página web, etc., es el robo de información, pues con él se puede provocar mucho mayor daño que si hubiera un robo físico de un aparato electrónico o dinero en efectivo; en el sector salud es mucho más peligroso, ya que mientras las personas están esperan un servicio óptimo y de la mejor calidad posible, los piratas informáticos se encargan de que algunas personas no lo pasen así, pues el robo acceso a la información (tarjetas de crédito, cuentas, direcciones, tratamientos, etc.) es uno de los temas en donde se debe de poner mucha mayor atención. Además, en los últimos años se han implementado distintas aplicaciones que ayudan de cierta forma a las personas en la salud y de hecho, "según una encuesta de BMJ Open, hubo más de 100,000 aplicaciones para teléfonos inteligentes enfocadas en la salud en 2016"(Paolotti et al., 2019, p. 5.), pero como en todas las aplicaciones se debe proporcionar información personal, y en este caso información médica.

Se han dado casos en los que la información de los pacientes es robada y vendida en el mercado negro, sus tratamientos son cambiados, sus dósis son alteradas, o hasta se cambia su nombre, provocando problemas legales; a los cuales no se les ha prestado mucha atencion, es por esto que se debe realizar un indice de ciberseguridad el cual es "una encuesta que mide la preparación y las capacidades de seguridad de un país u organización y un índice se compone de una serie de preguntas, a menudo divididas en categorías" (Burke et al., 2019, p. 6) todo con el fin de realizar un análisis acerca de la ciberseguridad en el sector salud.

IV. Avances tecnológicos en la medicina

En la última década la tecnología ha afectado aspectos de gran importancia dentro de la medicina, por ejemplo, las aplicaciones, programas o plataformas usadas para la vigilancia de enfermedades, dar posibles diagnósticos y seguimiento de tratamientos a pacientes con casi cualquier tipo de padecimiento, además de incluir información para prevenir distintas enfermedades, y para el uso de estas aplicaciones es necesario aportar información personal y médica de cada paciente, este avance tecnológico ha mejorado la atención médica de muchas personas, ya que en los últimos años se ha reportado que los hospitales, principalmente los públicos, se encuentran sin espacio para todos los pacientes por lo tanto esta innovación a sido un logro que debe seguirse mejorando. "Los desarrollos prometedores incluyen sistemas híbridos que combinan datos de vigilancia tradicionales con datos de consultas de búsqueda, publicaciones en redes sociales y crowdsourcing" (Aiello et al., 2020, p. 115)

Países con tecnología muy desarrollada como China donde se han propuesto, creado e implementado dispositivos enfocados en la salud como EmotionSense que es una propuesta de un aparato capaz de reconocer las emociones de las personas utilizando sensores que registra desde los gestos hasta las actividades físicas como caminar o sentarse, para finalmente realizar un análisis del comportamiento del paciente, y se determinó que "una precisión del 74,3% para 30 participantes demuestra que el sistema propuesto puede reconocer las emociones humanas de forma eficaz" (Wang et al., 2020, p. 14), si este dispositivo fuera aprobado, se tendría que pensar en las posibles desventajas técnicas del uso de estos aparatos, por ejemplo, la privacidad de los datos adquiridos y de la información personal, los posibles hackeos de los dispositivos, etc., todas estas posibilidades tienen que ser vigiladas y garantizar la protección de toda la información. Este último punto no ha sido determinado por los creadores del dispositivo.

"En salud pública, el análisis de redes se ha utilizado para estudiar principalmente la transmisión de enfermedades, transmisión de información, difusión de innovaciones; el papel del apoyo social y el capital social" (Luke y Harris, 2007, p. 83). Por lo tanto, las redes sociales han sido influencia en la medicina, usualmente utilizada para la investigación y la recopilación de datos mediante encuestas, entrevistas, etc., también han sido de gran ayuda para difundir información rápidamente a todo el país, por desgracia no toda esta información es totalmente verídica y en ocasiones es alterada para dar un mensaje diferente, ya que en ocasiones en las redes sociales no sabe con exactitud quien es la persona que controla dicha red.

V. Big data en la salud

"Los sistemas de vigilancia de salud pública monitorean las tendencias en la incidencia de enfermedades, los comportamientos de salud y las condiciones ambientales con el fin de asignar recursos para mantener poblaciones saludables" (Mooney y Pejaver, 2018, p. 98). La recopilación de datos es un procedimiento necesario para la investigación, la realización de hipótesis, toma de decisiones, etc., en el sector salud se obtiene el registro de datos de cientos de pacientes de diferentes hospitales, clínicas e incluso consultorios médicos que son utilizados para realizar análisis de enfermedades con diferentes motivos, por ejemplo, el descubrimiento de una cura y tratamientos, la determinación de síntomas, prevención, o incluso el descubrimiento de otras enfermedades, entre otras. Estos análisis son realizados a nivel nacional, internacional, etc, muchos de estos son dados a conocer al público en general, principalmente para que estén informados.

"La vigilancia es una parte integral de la práctica de salud pública. La capacidad de obtener información precisa y oportuna sobre los patrones de incidencia de enfermedades y mortalidad es un objetivo central de la salud pública" (Virnig y McBean, 2001, p. 221). Sin embargo, una de las preocupaciones que muchos médicos y científicos han tenido en los últimos años es que estos datos de gran importancia en ocasiones han sido robados por maleantes para hacer cosas malintencionadas, por ejemplo, se ha dado el caso de personas que interfieren en las bases de datos para alterar información y perjudicar a pacientes comúnmente por problemas personales

o simplemente porque quieren hacerle daño a cualquier persona o incluso se ha dado el caso de personas que alteran las cantidades de medicamento administrado a un paciente. Es por esto que es indispensable la protección y privacidad de esta información mediante herramientas y aplicaciones tecnológicas para evitar estas situaciones que ponen en riesgo la identidad de las personas y de las organizaciones.

Conclusiones

Podemos decir que los ciberataques en hospitales resultan en extremo peligrosos para los pacientes no solo por tener acceso a la información médica, sino también por involucrarse en los tratamientos y dispositivos médicos que finalmente puede traer consecuencias catastróficas.

Los avances tecnológicos han sido de gran ayuda para la medicina, pero en ocasiones no se considera que estos dispositivos o bases de datos pueden ser manipulados por personas con el objetivo de cometer algún crimen a pequeños o grandes rasgos.
Al analizar a fondo, nos damos cuenta de que muchas veces lo más importante no es tener vigilancia las 24 horas para prevenir algún robo, y no siempre los robos son por cuestiones materiales, en ocasiones los robos son de datos personales que pueden valer varias decenas de veces más que un dispositivo electrónico y pueden provenir de cualquier lugar.

Referencias

Beth A Virnig y Marshall McBean (2001). Datos administrativos para la vigilancia y planificación de la salud pública, 213-230. Consultado el 12 de noviembre de 2020 en https://www.annualreviews.org/doi/abs/10.1146/annurev.publhealth.22.1.213

Daniela Paolotti, Umair A Shah, Michael Edelstein, Onicio Leal Neto, Patty Kostkova, Caroline Wood, (2019). Innovación en salud digital: de la prueba de concepto al valor público, 1-5. Consultado el 11 de diciembre de 2020 en https://doi.org/10.1145/3357729.3357764

Diane R. Murphy y Richard H. Murphy (2013). Enseñanza de la ciberseguridad: protección del entorno empresarial, 88-93. Consultado el 11 de diciembre de 2020 en https://doi.org/10.1145/2528908.2528913

Douglas A. Luke y Jenine K. Harris (2007). Análisis de redes en salud pública: historia, métodos y aplicaciones, 69-93. Consultado el 13 de noviembre de 2020 en https://www.annualreviews.org/doi/abs/10.1146/annurev.publhealth.28.021406.144132

E. Aiello, A., Renson, A., & N. Zivich, P. (2020). Vigilancia de enfermedades basada en redes sociales e Internet para la salud pública, 101-118. Consultado el 1 de noviembre de 2020 en https://www.annualreviews.org/doi/abs/10.1146/annurev-publhealth-040119-094402

Julie M. Haney ,Wayne G. Lutters (2019). Motivar a los defensores de la ciberseguridad : implicaciones para el reclutamiento y la retención 109-117. Consultado el 11 de diciembre de 2020 en https://doi.org/10.1145/3322385.3322388

Shuo Han y George J. Pappas (2018). Privacidad en sistemas dinámicos y de control, 309-332. Consultado el 16 de noviembre de 2020 en https://www.annualreviews.org/doi/abs/10.1146/annurev-control-060117-105018

Stephen J. Mooney y Vikas Pejaver (2018). Big Data en salud pública: terminología, aprendizaje automático y privacidad, 95-112. Consultado el 12 de noviembre de 2020 en https://www.annualreviews.org/doi/abs/10.1146/annurev-publhealth-040617-014208

Wendy Burke, Taiwo Oseni, Alireza Jolfaei, Iqbal Gondal (2019). Índices de ciberseguridad para eHealth, 1-8. Consultado el 11 de diciembre de 2020 en https://doi.org/10.1145/3290688.3290721

Zhu Wang, Zhiwen Yu, Bobo Zhao (2020). EmotionSense: un sistema de reconocimiento de emociones adaptable basado en dispositivos inteligentes portátiles, 13-20. Consultado el 13 de noviembre de 2020 en https://dl.acm.org/doi/10.1145/3384394