Farmacia Hospitalaria 48 (2024) 195–197

Farmacia HOSPITALARIA
Órgano oficial de expresión científica de la Sociedad Española de Farmacia Hospitalaria
www.elsevier.es/farmaciahospitalaria

Editorial

Ciberseguridad, una prioridad de los servicios de farmacia en la era de la inteligencia artificial

Cybersecurity, a priority for pharmacy services in the age of artificial intelligence

En la era digital los hospitales se encuentran en una encrucijada: por un lado, la adopción de tecnologías de vanguardia ha revolucionado la atención médica, mejorando la precisión de los diagnósticos, la eficiencia de los tratamientos y la calidad de vida de los pacientes. Por otro lado, esta digitalización ha abierto las puertas a ciberamenazas cada vez más sofisticadas, poniendo en riesgo los datos sensibles de los pacientes, la continuidad de la atención médica e incluso la vida de las personas[1].

Por todo ello, la información sanitaria se vuelve cada vez más valiosa y codiciada. Un claro ejemplo de esto es la entrada de grandes corporaciones, tradicionalmente dedicadas a otros sectores, en el ámbito de la sanidad, estableciendo divisiones específicas para el sector sanitario, las cuales están aumentando continuamente su volumen de negocio.

Por este motivo, la ciberseguridad se ha convertido en un aspecto cada vez más importante y que genera mayor preocupación en el entorno sanitario. Hemos experimentado ataques significativos que han afectado gravemente a los sistemas de información de hospitales y, por ende, a la prestación de servicios de salud esenciales. Un reciente estudio realizado en Estados Unidos demuestra que en los últimos años se ha incrementado la frecuencia, sofisticación y duración de los ciberataques a instituciones sanitarias[2].

Los hospitales suelen estar preparados para afrontar contingencias puntuales, que afectan a sistemas concretos y durante un período de tiempo limitado. Sin embargo, los ciberataques pueden afectar a todos los sistemas y datos alojados en los servidores del hospital y, además, pueden prolongarse durante largos períodos de tiempo. A menudo, el ciberataque se prepara durante semanas o meses, y estos son los más peligrosos, debido a que las copias de seguridad de sistemas y datos están infectadas desde mucho tiempo antes de que se evidencie el ataque y se pueda actuar[3].

La importancia de la ciberseguridad en los servicios de farmacia

Los servicios de farmacia hospitalaria (SFH) deben enfrentar importantes desafíos durante un ciberataque, lo que requiere la identificación de roles clave y procedimientos estandarizados para superar los efectos de dichas violaciones de seguridad. El SFH desempeña un papel crucial en la evaluación de los sistemas afectados y su impacto, la estimación de la duración de la inactividad y la planificación de los períodos de recuperación, para mantener lo mejor posible el circuito del medicamento[4].

Algunos de los principales efectos de un ciberataque en un SFH son[4]:

- Interrupción de sistemas críticos: pérdida de acceso a la historia clínica electrónica, sistema de admisión, sistema de gestión del SFH, prescripción electrónica y herramientas de soporte a las decisiones clínicas, registro de administración de medicamentos, armarios de dispensación automatizada y software de dispensación, entre otros.
- Intensificación del trabajo manual: la interrupción de la automatización hace necesario llevar a cabo las actividades de forma manual, lo que puede ser laborioso e inseguro para los pacientes al aumentar el riesgo de cometer errores.
- Impacto en productividad y eficiencia: la falta de sistemas funcionales dificulta la disponibilidad de información y ralentiza el proceso de validación de órdenes médicas, que debe realizarse manualmente. Esto también afecta al tiempo de respuesta en la entrega de medicamentos y al seguimiento farmacoterapéutico de pacientes.
- Desafíos en la gestión de inventarios: es necesario generar listados de forma manual y coordinar con los proveedores la entrega en el SFH.
- Problemas de comunicación: la interrupción de los sistemas ordinarios de comunicación (correo electrónico, teléfono o aplicaciones de mensajería) puede retrasar la transmisión de información crítica.
- Retos en la documentación y registro: la necesidad de documentar manualmente las órdenes médicas incrementa el riesgo de errores y omisiones, lo que puede afectar la calidad del cuidado al paciente.
- Reorganización del equipo de trabajo: se requiere una colaboración estrecha entre el equipo de farmacia, médico, enfermería, administrativo y de otros servicios y departamentos, así como la redistribución del personal y adaptación a nuevas responsabilidades y procedimientos temporales.

En el contexto de un ciberataque, resulta fundamental la colaboración multidisciplinar para una gestión efectiva de los medicamentos en el hospital y garantizar una atención farmacéutica segura al paciente. Para ello, los SFH deben establecer protocolos detallados y actualizados, así como desarrollar planes de contingencia para mitigar riesgos y mantener una atención de calidad al paciente[4,5]. Asimismo, conviene realizar regularmente una autoevaluación de los riesgos de ciberseguridad, así como llevar a cabo simulacros para

https://doi.org/10.1016/j.farma.2024.08.001

mantener al equipo siempre preparado para dar respuesta a un posible ataque[6]. Si bien resulta inasumible realizar estos simulacros reproduciendo situaciones de afectación real, podría establecerse un calendario de ejercicios para reproducir situaciones con un grado de afectación menor y, por tanto, más manejable.

La ciberseguridad en la era de la inteligencia artificial

En el mundo de la salud, como en prácticamente todos los sectores, la implementación de la inteligencia artificial (IA) está impactando enormemente, lo que conlleva importantes implicaciones (positivas y negativas) en el ámbito de la ciberseguridad.

Las implicaciones positivas son diversas y significativas:

- Permite detectar amenazas avanzadas a través del análisis predictivo, analizando patrones de comportamiento y prediciéndolas antes de que ocurran. Además, mejora la capacidad de responder rápidamente a las amenazas en tiempo real, reduciendo el impacto de los ataques.
- Facilita la automatización de tareas de seguridad, incluyendo monitorización continua, vigilancia constante de sistemas y redes, identificación de anomalías y comportamientos sospechosos, todo sin necesidad de intervención humana.
- Automatiza la gestión de incidentes de seguridad, abarcando la identificación, clasificación y mitigación de amenazas.
- Análisis de grandes volúmenes de datos. La IA es capaz de manejar y analizar los datos generados por los sistemas de salud, identificando patrones y tendencias que pueden señalar brechas de seguridad. Además, tiene la capacidad de correlacionar eventos de múltiples fuentes para proporcionar una visión integral de la seguridad.
- Contribuye significativamente a la mejora en la protección de datos. Los algoritmos pueden desarrollar técnicas de cifrado más robustas para proteger la información sensible. Además, facilita sistemas de autenticación y autorización más seguros, mediante el uso de biometría y análisis de comportamiento, asegurando un nivel de seguridad superior.

No obstante, la implementación de la IA presenta también riesgos y desafíos significativos. Uno de los principales riesgos es la dependencia de la IA. Los algoritmos no son infalibles y pueden cometer errores en la identificación de amenazas, lo que podría resultar en falsos positivos o falsos negativos. Además, la eficacia de estos algoritmos depende de los datos de entrenamiento. Si estos datos están sesgados, los sistemas de IA podrían desarrollar prejuicios, afectando así su precisión y eficacia.

Otro desafío son los ciberataques específicos contra sistemas de IA. Los atacantes pueden manipular datos para engañar a los sistemas de IA, impidiendo que detecten las amenazas correctamente (ataques adversariales). Si los atacantes descubren vulnerabilidades en los sistemas de IA, pueden explotarlas para infiltrarse en los sistemas de salud.

La privacidad es también un aspecto crítico. La IA necesita acceso a grandes volúmenes de datos para ser efectiva, incrementando el riesgo de exposición de datos sensibles. Es crucial cumplir con las regulaciones de protección de datos, lo que puede resultar complejo en el ámbito de la IA[7].

El mantenimiento y actualización de sistemas de IA representa otro desafío, ya que requieren actualizaciones y mantenimiento constantes para adaptarse a nuevas amenazas, lo que implica recursos y costes adicionales. Además, se necesita personal altamente capacitado para gestionar y operarlos y puede representar un desafío para muchas organizaciones de salud.

Finalmente, es fundamental que estos sistemas sean transparentes y que sus decisiones puedan ser explicadas y comprendidas por los profesionales de la salud y los gestores de seguridad. Los usuarios deben tener confianza en que los sistemas de IA protegerán sus datos y no comprometerán su privacidad[8].

Para abordar estos desafíos y riesgos asociados con la implementación de la IA en la ciberseguridad sanitaria, es fundamental adoptar estrategias integrales y rigurosas, tales como la evaluación continua de riesgos, realizando evaluaciones regulares para identificar y mitigar posibles vulnerabilidades en los sistemas. Es esencial llevar a cabo pruebas de penetración y simulacros de ataques para evaluar la efectividad de los sistemas de IA y fortalecer las defensas contra posibles amenazas. Además, los algoritmos deben actualizarse regularmente para adaptarse a nuevas amenazas y reducir el riesgo de explotación de vulnerabilidades. Establecer un sistema de monitorización continua para detectar y responder a anomalías y amenazas en tiempo real, garantiza una vigilancia constante[9].

Por otra parte, se debe ofrecer formación continua sobre las capacidades y limitaciones de los sistemas de IA, así como sobre buenas prácticas de ciberseguridad y fomentar la concienciación sobre amenazas, informando a los usuarios sobre ellas y cómo pueden afectar a los sistemas de salud, promoviendo una cultura de seguridad[7,8].

Por último, la colaboración y el cumplimiento normativo no pueden ser subestimados. Es necesario asegurarse de que todos los sistemas y procesos cumplan con las normativas de privacidad y seguridad aplicables, así como colaborar con otras instituciones y organismos reguladores para compartir información sobre amenazas y mejores prácticas, fortaleciendo así la defensa colectiva contra ciberataques[7].

Implementando estas estrategias, las organizaciones de salud pueden mejorar significativamente la seguridad de sus sistemas de IA y proteger mejor los datos sensibles de los pacientes.

Declaración de contribución de autoría CRediT

Cayetano M. Hernández Marín: Writing – review & editing, Writing – original draft, Conceptualization. **Emilio Monte-Boquet:** Writing – review & editing, Writing – original draft, Project administration, Conceptualization. **José Luis Poveda Andrés:** Validation, Supervision.

Bibliografía

1. Wasserman L, Wasserman Y. Hospital cybersecurity risks and gaps: review (for the non-cyber professional). Front Digit Health. 2022;4, 862221. doi: 10.3389/fdgth.2022.862221.
2. Neprash HT, McGlave CC, Cross DA, Virnig BA, Puskarich MA, Huling JD, et al. Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016-2021. JAMA Health Forum. 2022;3(12), e224873. doi: 10.1001/jamahealthforum.2022.4873.
3. Sullivan N, Tully J, Dameff C, Opara C, Snead M, Selzer J. A national survey of hospital cyber attack emergency operation preparedness. Disaster Med Public Health Prep. 2023;17(e363):1–4. doi: 10.1017/dmp.2022.283.
4. Santalo O, Perez G, Lorich C, Greenberg M, Hernandez JM, Bohorquez R, et al. Defining key pharmacist and technician roles in response to a hospital downtime or cyberattack. J Am Pharm Assoc. 2023;62(5):1518–23. doi: 10.1016/j.japh.2022.03.027.
5. Alanazi AT. Clinicians' Perspectives on healthcare cybersecurity and cyber threats. Cureus. 2023;15(10), e47026. doi: 10.7759/cureus.47026.
6. Burke W, Stranieri A, Oseni T, Gondal I. The need for cybersecurity self-evaluation in healthcare. BMC Med Inform Decis Mak. 2024;24:133. doi: 10.1186/s12911-024-02551-x.
7. Esmaeilzadeh P. Challenges and strategies for wide-scale artificial intelligence (AI) deployment in healthcare practices: a perspective for healthcare organizations. Artif Intell Med. 2024;151, 102861. doi: 10.1016/j.artmed.2024.102861.

8. Nifakos S, Chandramouli K, Nikolaou CK, Papachristou P, Koch S, Panaousis E, et al. Influence of human factors on cyber security within healthcare organisations: a systematic review. Sensors. 2021;21(15):5119. doi: 10.3390/s21155119.
9. Bhagat SV, Kanyal D. Navigating the future: the transformative impact of artificial intelligence on hospital management – a comprehensive review. Cureus. 2024;16(2), e54518. doi: 10.7759/cureus.54518.

Cayetano M. Hernández Marín[a]
[a]*Subdirección de Sistemas de Información, Hospital Universitario y Politécnico La Fe, Valencia, España*

Emilio Monte-Boquet[b]*
[b]*Servicio de Farmacia, Hospital Universitario y Politécnico La Fe, Valencia, España*
*Autor para correspondencia.
Correo electrónico: monte_emi@gva.es

José Luis Poveda Andrés[c]
[c]*Dirección, Hospital Universitario y Politécnico La Fe, Valencia, España*