Atencion Primaria 56 (2024) 102854

Atención Primaria

www.elsevier.es/ap

ARTÍCULO ESPECIAL

Ciberseguridad y uso de las TIC en el Sector Salud

Alejandro Cervera García y Alyson Goussens*

L'Equip d'Atenció Primària de Figueres (EAP Figueres), Institut Català de la Salut, Girona, España

Recibido el 1 de noviembre de 2023; aceptado el 12 de diciembre de 2023
Disponible en Internet el 13 de enero de 2024

PALABRAS CLAVE
Ciberseguridad;
Ransomware;
eSalud;
Tecnologías de la información y la comunicación;
TIC

Resumen La ciberdelincuencia en el sector salud es una creciente amenaza en la era digital. Con la informatización de registros médicos y la telemedicina en aumento, los ataques cibernéticos pueden tener consecuencias devastadoras. La filtración de datos sensibles o el secuestro de sistemas pueden comprometer la privacidad de los pacientes y poner en peligro la atención médica. Para contrarrestar esta amenaza, se requieren medidas de ciberseguridad sólidas como medida protectora.

Este artículo pretende exponer los principales peligros y amenazas que enfrentan las tecnologías de la información y la comunicación (TIC), así como presentar la ciberseguridad con sus implicaciones bioéticas y, finalmente, el esquema ideal para esta en el sector de la salud con el fin de crear un entorno más seguro y eficiente. Este artículo busca abordar estos temas y proporcionar una visión integral de cómo la ciberseguridad y las TIC pueden coexistir de manera segura y efectiva en el ámbito sanitario.

KEYWORDS
Cybersecurity;
Ransomware;
eHealth;
Information and communication technologies;
ICT

Cybersecurity and use of ICT in the health sector

Abstract Cybercrime in the health sector is a growing threat in the digital age. With computerization of medical records and telemedicine on the rise, cyberattacks can have devastating consequences. Leaking sensitive data or hijacking systems can compromise patient's privacy and jeopardize healthcare. To counter this threat, robust cybersecurity measures are required as a protective measure.

This article aims to expose the main dangers and threats faced by ICT, as well as present cybersecurity with its bioethical implications and, finally, the ideal scheme for it in the health sector in order to create a safer and more efficient environment. This article aims to address these issues and provide a comprehensive view of how cybersecurity and ICT can coexist safely and effectively in the healthcare field.

* Autor para correspondencia.
Correo electrónico: agoussens.girona.ics@gencat.cat (A. Goussens).

https://doi.org/10.1016/j.aprim.2023.102854

Introducción

Las tecnologías de la información y la comunicación (TIC) han revolucionado numerosos sectores y la atención médica no es una excepción. Desde la gestión de registros de pacientes hasta la telemedicina y los diagnósticos asistidos por inteligencia artificial, las TIC han desempeñado un papel clave en la optimización de servicios, la mejora de los resultados y la seguridad para los pacientes[1]. Sin embargo, la adopción de estas tecnologías también ha abierto nuevas vías para potenciales amenazas, poniendo en riesgo tanto la integridad de la información como la confianza y seguridad del paciente.

A medida que la tecnología avanza, también lo hacen las amenazas cibernéticas siendo cada vez más sofisticadas[2]. Dado que los sistemas de salud almacenan gran cantidad de datos sensibles, se convierten en un blanco atractivo para ciberdelincuentes. Uno de los aspectos más preocupantes es el robo de datos médicos. La información de los pacientes, como historiales médicos, resultados de pruebas y datos personales, es altamente valiosa en el mercado negro digital. Los ciberdelincuentes pueden utilizar esta información para cometer fraudes, extorsiones o venderla a terceros, llevando a consecuencias devastadoras, poniendo en riesgo la privacidad de los pacientes, la integridad de los datos médicos y, en última instancia, la vida de las personas.

De aquí surge la importancia de la ciberseguridad en los diferentes ámbitos de la sociedad, dándole suma importancia en el sector de la salud, para poder protegerla y preservarla. En la era digital en la que vivimos, los sistemas de información y la tecnología desempeñan un papel fundamental en el sector sanitario, permitiendo la gestión eficiente de la información médica, la comunicación entre profesionales de la salud y el acceso a los registros de pacientes.

Peligros asociados con el uso de las TIC en salud

Vulnerabilidad a los ataques cibernéticos y principales amenazas

El sector sanitario es particularmente susceptible a ataques cibernéticos debido a varias razones intrínsecas. La información de salud y los datos sanitarios son extremadamente valiosos para los ciberdelincuentes ya que pueden ser utilizados para el robo de identidad, fraudes médicos o incluso extorsión, tanto a las empresas proveedoras como a los pacientes.

Así pues, entra en valor la tríada de Confidencialidad, Integridad y Disponibilidad (CIA), siendo el modelo que guía las políticas de seguridad de la información en una organización, fundamental en el ámbito de la ciberseguridad y la protección de datos. Cualquier amenaza cibernética puede afectar a alguno de estos pilares básicos, teniendo consecuencias tanto en el funcionamiento de la empresa como en la confianza y seguridad de los pacientes.

La confidencialidad se refiere a la protección de la información para que solo sea accesible para personas autorizadas. La confidencialidad se puede ver comprometida con el acceso no autorizado a los datos. Debe tenerse en cuenta el control de acceso, el cifrado de datos, la autenticación de usuarios y las políticas de privacidad. Por ejemplo, en un hospital, los registros médicos solo deben estar disponibles para el personal médico autorizado que asista al paciente en cuestión.

La integridad de datos asegura que la información es precisa, fiable y que no ha sido alterada de manera no autorizada. De lo contrario, no se mantienen la consistencia, la exactitud ni la confiabilidad de los datos. Esta debe conservarse a través de controles como sumas de verificación, hashes criptográficos y políticas de control de cambios. Por ejemplo, en un contexto médico, es vital que los datos de los pacientes no se alteren de forma incorrecta ya que esto podría afectar el tratamiento y la atención.

La disponibilidad de datos se refiere a que la información y los sistemas de registros médicos estén siempre en línea y accesibles para el personal cuando la necesiten. Debe asegurarse la infraestructura de red, implementando soluciones de respaldo y recuperación de datos, y manteniendo los sistemas actualizados y protegidos contra ataques como el *Distributed Denial of Service* (DDoS), que se refiere a las acciones maliciosas que buscan colapsar la infraestructura de sistemas de salud con tráfico web excesivo, paralizando la disponibilidad de servicios y datos críticos[3].

A continuación, se explica el funcionamiento de los principales ataques cibernéticos que pueden alterar la tríada CIA:

En primer lugar, como ya se ha objetivado, los sistemas de información en salud suelen ser complejos y multidisciplinarios. Así pues, existen varias formas de vulnerar los pilares básicos a través de los diferentes sistemas o aplicaciones informáticas; la historia clínica electrónica del paciente, los dispositivos de monitorización de los mismos o las diferentes aplicaciones de salud, lo que genera múltiples puntos de entrada para posibles ataques.

Además, el personal sanitario o administrativo no siempre está suficientemente formado en buenas prácticas de ciberseguridad, lo que aumenta el riesgo de errores humanos que pueden resultar en brechas de seguridad como la pérdida o robo de dispositivos[4].

Los principales ataques que ponen en riesgo los sistemas de salud son el *phishing*, el *ransomware* y el *malware*. Otras amenazas son las filtraciones de datos, que consisten en la exposición accidental de información médica confidencial a personas no autorizadas (muchas veces obtenida dicha información con los ataques anteriormente citados); el robo de identidad o los ataques DDoS[5]. Véase el Anexo 1.

Las vulnerabilidades en dispositivos médicos conectados a Internet, como los marcapasos y las bombas de insulina, pueden ser explotadas también por ciberdelincuentes para recaudar o modificar datos y causar daños.

La empresa IBM realiza un resumen anual del que, si bien es un estudio plurinacional y es complicado extrapolarlo a nuestra realidad de forma completa, se pueden sacar diversas ideas que orientan sobre lo que suponen los ciberataques al sector salud. El *phishing* y las credenciales robadas o comprometidas fueron responsables de 16 y 15% de las brechas, respectivamente. Una mala configuración de la nube fue identificada como el vector inicial para 11% de los ataques, seguido del compromiso del correo electrónico empresarial con 9%.

El coste promedio de un ataque que ponga en compromiso los datos (*data breach*) en 2023 es de 4,45 M USD, sin embargo, en el sector salud, este coste incrementa de media hasta 10,93 M USD, siendo el sector al que más dinero cuesta una brecha y siguiendo una tendencia ya presente en 2022. Pese a que los sistemas no son infalibles, se reporta una media de reducción de daños de 1,76 M USD por ataque en caso de usar sistemas de ciberseguridad basados en inteligencia artificial (IA) y sistemas automáticos, siendo esta media global y no sectorizada (por tanto, es posible que sea mayor en el sector salud). Este informe destaca que, desde 2020, los costes por una brecha de seguridad en el sector salud se han incrementado 53,3%[6].

Compromiso de la privacidad de los usuarios

La digitalización de la información médica supone significativos desafíos en la privacidad de los datos. Los sistemas de salud manejan información personal y sensible que varía desde diagnósticos médicos hasta detalles financieros, constituyendo así un tesoro de datos potencialmente explotable. A pesar de la existencia de leyes y regulaciones como el reglamento general de protección de datos (GDPR) en Europa o la *Health Insurance Portability and Accountability Act* (HIPAA) en Estados Unidos, las brechas de privacidad siguen siendo una preocupación real[7].

Además, la creciente adopción de dispositivos de salud conectados, como monitores de ritmo cardíaco y aplicaciones móviles de seguimiento de salud, complica aún más el panorama. Estos dispositivos, que a menudo carecen de medidas de seguridad robustas, pueden recopilar más datos de los estrictamente necesarios para su funcionamiento, lo cual pone en riesgo la privacidad de los usuarios y agrava las vulnerabilidades ya existentes[8].

Mirando al futuro cercano, la creciente dependencia en tecnologías digitales para la atención médica augura que los desafíos en torno a la privacidad de los datos se intensificarán. Los avances en dispositivos conectados y aplicaciones móviles de salud, aunque ofrecen mejoras significativas en el cuidado de los pacientes, seguirán ampliando el espectro de riesgos para la privacidad. La naturaleza cada vez más interconectada de estos sistemas puede potenciar los puntos vulnerables existentes, lo que complica aún más la tarea de mantener la confidencialidad e integridad de la información personal y médica.

Ciberseguridad y ética

La salud, desde la antigüedad con el juramento hipocrático hasta la actualidad regida por la bioética, se fundamenta en la práctica ética y moral para su protección y preservación. La bioética, de acuerdo con la Enciclopedia de la Bioética del Instituto Joseph y Rose Kennedy[9], es el análisis sistemático de la conducta humana en ciencias biológicas y salud, bajo la lente de valores morales.

Los cuatro principios bioéticos esenciales para la toma de decisiones clínicas y el cuidado del paciente, propuestos por Beauchamp y Childress, son: el principio de no maleficencia –entendido como el hecho de no infringir ningún daño intencionadamente–; el principio de beneficencia –el hecho de prevenir o eliminar el daño o hacer el bien a terceras personas–; el principio de autonomía –que consiste en que cada persona es autodeterminante y libre para decidir–; y, finalmente, el principio de justicia –entendido como el tratamiento y cuidado equitativo entre personas–[10]. Estos principios adquieren nuevas dimensiones con la transformación digital en salud. La generación, gestión y circulación de datos digitales plantean retos éticos emergentes, especialmente en ciberseguridad. Las diferentes amenazas a las que se enfrentan las TIC pueden influir en los mismos de la siguiente forma:

- **No maleficencia**: las brechas de seguridad en las TIC pueden llevar a fugas de datos, exponiendo a los pacientes a riesgos de privacidad y potencialmente a daños físicos si la información médica se ve comprometida o alterada. Esto viola el principio de no maleficencia, ya que el sistema de salud, inadvertidamente, puede causar daño al paciente.
- **Beneficencia**: los ciberataques pueden limitar el acceso a sistemas críticos de salud, retrasando o impidiendo tratamientos y diagnósticos vitales. Esto atenta contra el principio de beneficencia porque impide a los profesionales de la salud realizar su trabajo de prevenir daños, eliminar sufrimientos y promover el bienestar del paciente.
- **Autonomía**: las violaciones de la ciberseguridad pueden resultar en la pérdida del control del paciente sobre su información personal de salud. Esto socava el principio de autonomía al privar a los pacientes del derecho a controlar quién accede a su información y cómo se utiliza.
- **Justicia**: si las TIC no están diseñadas o protegidas adecuadamente, es posible que surjan desigualdades en el acceso a la atención médica. Los ciberataques pueden afectar de manera desproporcionada a ciertas poblaciones, especialmente a aquellas con menos recursos para proteger sus datos o recuperarse de un ataque. Esto va en contra del principio de justicia, que busca un acceso y tratamiento equitativo en la atención de salud.

Actualmente nos encontramos con un nuevo paradigma, por un lado, evolucionando hacia una medicina más participativa en la toma de decisiones y, por otro, frente a la veloz transformación digital, la creación de datos digitales, así como su gestión, almacenamiento y su circulación, hecho que hace evidente que la tecnología revoluciona desde la manera en la que nos comunicamos y nos desenvolvemos hasta el cómo tomamos decisiones. La velocidad con la que se producen cambios en la sanidad va de la mano con nuevas amenazas a la ética médica y a la práctica asistencial. Esta evolución constante plantea nuevos retos como son la revisión de los objetivos de las TIC, los riesgos de seguridad asociados a su uso y su estrecha relación con la ética de la salud[9,11,12].

Los principales fines del buen uso de las TIC en la salud son la eficiencia, la calidad de los servicios, la privacidad y confidencialidad, la usabilidad de los diferentes servicios y la ciberseguridad. Estos objetivos se pueden relacionar directamente con los cuatro principios éticos anteriormente citados[10] pero también dependen de la disponibilidad, accesibilidad, aplicabilidad y otros valores ético-morales como son la libertad y el consentimiento, la privacidad y la con-

fianza, la dignidad y la solidaridad, y la justicia y la igualdad. Por lo tanto, los sistemas de información son –intencional o involuntariamente– desarrollados tomando los valores morales de sus creadores[13]. Este hecho nos puede proporcionar una idea inicial de cómo los valores morales pueden entrar en conflicto entre sí. Por ejemplo, el hecho de compartir datos e información personal puede llevar a que la tecnología sea una herramienta más eficiente y precisa para los intereses del usuario, pero, a su vez, que la ciberseguridad se vea comprometida poniendo en peligro la privacidad de los datos tratados.

En los últimos años se ha observado un aumento de casos de ciberataques, especialmente *ransomware* en diversos sistemas sanitarios. El mundo de la salud se ha convertido en un objetivo atractivo para el cibercrimen debido a que es una fuente muy rica en datos valiosos y sus defensas, por diversas razones, son mejorables. Estas amenazas impactan directamente y de forma agresiva en la práctica asistencial, reduciendo la confianza de los pacientes, paralizando los sistemas de salud y siendo una amenaza para la seguridad y la vida de los usuarios.

Según datos de la Agencia de la Unión Europea para la Ciberseguridad (ENISA), se han registrado incidentes que tienen como consecuencia desde las pérdidas económicas hasta el cese total o parcial de la actividad de los centros[14]. Otro tipo de ataque muy frecuente son los métodos de *phishing* a gran escala, donde los atacantes utilizan correos electrónicos para difundir *malware* y robar datos confidenciales para su reventa. A menudo, son una puerta de entrada para la inyección de *ransomware*.

Queremos recordar casos como el secuestro de los servidores del Hospital Universitario de Düsseldorf (Alemania), que provocó el cierre de sus emergencias y la primera muerte documentada secundaria a un ataque *ransomware* de una paciente, ya que no pudo obtener el ingreso que requería[15]. Otro ejemplo es el reciente ataque al Hospital Clínic de Barcelona (España), en el que se secuestraron diversos datos sistema, amenazando posteriormente con su venta a terceros, pidiendo un rescate económico para paralizarla, causando una interrupción generalizada del sistema y la cancelación de diferentes procesos e intervenciones a pacientes. Sobre este caso, consta una comunicación del centro fechada en julio de 2023 donde se reconoce el filtrado de historias clínicas asistenciales y de investigación[16].

Hechos como la primera muerte documentada secundaria a un ciberataque o chantajes realizados a partir de datos robados evidencian que la cultura de la ciberseguridad se debe convertir en una parte integral del concepto de ética asistencial y de seguridad del paciente.

A continuación, se plantean algunas preguntas éticas cruciales relacionadas con la ciberseguridad en el ámbito de la salud que abordan aspectos importantes de la relación entre la primera y la ética en el campo mencionado, cuya discusión es vital para desarrollar prácticas más seguras y éticas en este ámbito.

a. Sobre la financiación de la ciberseguridad. ¿Quién debería ser responsable de financiar la ciberseguridad en el sector sanitario? ¿Deben los gobiernos, las instituciones de salud o los proveedores de tecnología asumir esta responsabilidad?

La financiación de la ciberseguridad en el sector sanitario es un tema complejo que implica múltiples partes interesadas, cada una con roles y responsabilidades diferentes.

En primer lugar, destacarían los gobiernos, quienes desempeñan un papel crucial en este tema. Pueden proporcionar fondos directos para mejorar la infraestructura de ciberseguridad, especialmente en instituciones públicas de salud, además de establecer las normativas y estándares, garantizando un nivel mínimo de protección en todas las instituciones de salud[17].

En segundo lugar, las instituciones de salud, tanto públicas como privadas, deben priorizar y asignar fondos para sus necesidades de ciberseguridad. Esto incluye la protección de datos de pacientes, sistemas de información hospitalaria y dispositivos médicos conectados.

También deben estar involucrados los proveedores de tecnología y *software* ya que tienen la responsabilidad de garantizar que sus productos y servicios sean seguros. Esto incluye el desarrollo de sistemas seguros y la actualización regular para abordar vulnerabilidades conocidas.

Asimismo, se destacan las colaboraciones entre el sector público y privado las cuales pueden incluir la inversión compartida en infraestructura de ciberseguridad, desarrollo de talento e investigación.

Finalmente, las instituciones de salud también tienen la opción de escoger seguros de ciberriesgos, que pueden ayudar a mitigar los costos financieros de un incidente de ciberseguridad.

En resumen, la financiación de la ciberseguridad en el sector de la salud es una responsabilidad compartida. La colaboración entre gobiernos, instituciones de salud, proveedores de tecnología y otros actores es fundamental para garantizar una protección eficaz y sostenible en este sector.

b. En el caso de un ciberataque, ¿es ético negociar con los atacantes?

La respuesta a un ciberataque en el sector de la salud plantea dilemas éticos y operativos significativos, especialmente cuando la vida de los pacientes está en juego. La decisión de negociar con los atacantes, como en el caso de un ataque de *ransomware*, es particularmente controvertida.

Negociar con los atacantes puede ser visto como un mal necesario para proteger la vida y el bienestar de los pacientes. Sin embargo, también establece un precedente peligroso y puede financiar y alentar más actividades delictivas.

Cada situación es única y debe evaluarse en función de su gravedad, el riesgo para la vida de los pacientes y la viabilidad de las alternativas. La decisión debe involucrar a la alta dirección, los equipos de seguridad de la información y, en algunos casos, a las autoridades legales y de aplicación de la ley.

En resumen, la decisión de negociar con los atacantes es compleja y debe tomarse con cautela, evaluando todos los riesgos y consecuencias. En general, las recomendaciones de las agencias nacionales de ciberseguridad y de los expertos suele ser no negociar, entre otros, por el efecto de mantenimiento económico de la actividad delictiva. Sin embargo, la protección de la vida y la seguridad de los pacientes debe

ser siempre la prioridad y por ello los autores entendemos que sea algo posible una vez se ha producido un ataque de grave alcance[18,19].

Modelo ideal de ciberseguridad en salud

Políticas y normativas de seguridad

En un mundo ideal, la ciberseguridad en el sector salud debería ser una extensión natural de las políticas de seguridad existentes y estar alineada con regulaciones y estándares nacionales e internacionales. Un enfoque comprensivo y estandarizado podría minimizar los riesgos y establecer un marco coherente de mejores prácticas[20]. Este implica la necesidad de actualizar regularmente las políticas de seguridad para adaptarlas a un entorno digital en constante cambio.

La formación continua del personal médico y administrativo en buenas prácticas de ciberseguridad es crucial. De igual importancia son las auditorías de seguridad recurrentes y los ejercicios de simulación para evaluar y fortalecer las defensas existentes. Una estrategia de «defensa en profundidad» debería ser adoptada, empleando múltiples capas de medidas de seguridad para proteger tanto los sistemas como los datos[21].

Un modelo de ciberseguridad óptimo también debería contar con un equipo dedicado de respuesta a incidentes de seguridad cibernética, capaz de actuar de manera rápida y efectiva ante cualquier tipo de amenaza, mitigando así los riesgos asociados con posibles brechas de datos y garantizando la continuidad del servicio de atención médica.

También debería imponerse por normativa un control de acceso riguroso a los datos del paciente, con los métodos analizados en el siguiente apartado.

Se debe recomendar no utilizar el correo electrónico para intercambiar datos de salud de forma general. En caso de ser imprescindible, siempre debe hacerse entre cuentas corporativas de la organización, firmando y cifrando los datos, así como evitar almacenar en el disco duro datos sensibles de trabajadores o pacientes, especialmente de forma no cifrada. El trabajador debe conocer cuáles son las buenas prácticas de navegación por Internet y ser instigado a no usar las herramientas de navegación de la organización para motivos no laborales; por ejemplo, hacer clic en una ventana emergente de un anuncio encontrado en una red social, puede poner en peligro la seguridad y la privacidad de toda la organización y, con ello, de los datos sanitarios. Al aplicar estas prácticas, las instituciones de salud pueden aprovechar las ventajas de las TIC, manteniendo al mismo tiempo la confidencialidad y la privacidad de los datos de los pacientes[22].

Tecnologías y herramientas de protección

Para alcanzar un modelo de ciberseguridad óptimo en el sector sanitario, es imperativo incorporar tecnologías y herramientas específicas que provean una defensa integral. Entre las tecnologías clave se incluyen los *firewalls* de última generación, que no solo bloquean tráfico no autorizado, sino que también inspeccionan el contenido para evitar *malware* y ataques dirigidos. Además, sistemas de detección y prevención de intrusiones (IDPS) pueden monitorizar el tráfico de red en tiempo real, permitiendo la identificación y la mitigación proactivas de amenazas potenciales.

La encriptación de datos, tanto en reposo como en tránsito, es crucial para asegurar la confidencialidad y la integridad de la información sensible del paciente[23]. Otra capa vital de protección es el uso de autenticación de múltiples factores que consiste en no confiar solo en una contraseña que puede ser robada, sino añadir una capa más (generalmente una aplicación o una llave física de seguridad), para garantizar que únicamente el personal autorizado tenga acceso a los sistemas y datos relevantes. Actualmente, una solución posible para la autentificación de doble factor es el uso del certificado digital que dispone medicina o enfermería para esta doble autentificación[22]. También existen los hashes criptográficos, que son huellas digitales que se utilizan para identificar datos que son difíciles de modificar o falsificar, por ejemplo, un sistema puede generar un hash de una contraseña para protegerla.

Asimismo, deben realizarse copias de seguridad regulares y contar con sistemas de recuperación de datos para minimizar la pérdida de información y el tiempo de inactividad en caso de un ataque, así como realizar auditorías regulares de seguridad y monitorear los sistemas para detectar cualquier actividad sospechosa o violación de datos. Otra medida preventiva consiste en la evaluación de riesgos del *software* utilizado y pruebas de penetración para identificar y corregir vulnerabilidades[21].

Finalmente, las soluciones de gestión de vulnerabilidades, que incluyen evaluaciones regulares y parches de seguridad, son fundamentales para mantener una postura de seguridad sólida. Todas estas tecnologías deben integrarse en una estrategia holística que permita flexibilidad para adaptarse a nuevas amenazas y cambios en el panorama de la ciberseguridad en salud.

Educación y conciencia sobre ciberseguridad

Uno de los pilares fundamentales en cualquier estrategia de ciberseguridad en el ámbito sanitario es la educación y la concienciación del personal. No basta con tener las mejores herramientas y tecnologías si los usuarios no entienden la importancia de seguir prácticas seguras. La formación continua del personal en ciberseguridad es esencial para minimizar los errores humanos, a menudo el eslabón más débil en la cadena de seguridad[24].

Los programas de formación deben ser prácticos y adaptarse a las diferentes funciones dentro del sector sanitario. Los módulos de formación en línea y las charlas de expertos pueden ser recursos útiles para mantener al personal actualizado sobre las últimas amenazas y estrategias defensivas. Un elemento crítico para el éxito a largo plazo es el compromiso y la participación de la alta dirección en la formación y la concienciación, ya que esto envía un fuerte mensaje sobre la importancia de la ciberseguridad en la organización.

Se debería realizar una formación obligatoria en ciberseguridad a todo personal sanitario, siendo obligatoria su renovación cada cierto tiempo dado el carácter cambiante de las amenazas afrontadas[22].

Conclusión

La implementación de un modelo sólido de ciberseguridad en el ámbito sanitario es una tarea multifacética que requiere enfoques integrales y coordinados. Nuestra revisión sugiere que tal modelo debe fundamentarse en tres pilares principales: políticas y normativas robustas, tecnologías y herramientas avanzadas de protección, y una educación y concienciación continuada del personal sanitario.

Las políticas y normativas efectivas proporcionan el marco necesario para desarrollar estrategias de seguridad coherentes y eficaces. A su vez, el uso de tecnologías y herramientas de punta como *firewalls* de última generación y sistemas de detección y prevención de intrusiones, es crucial para garantizar la integridad de los sistemas y la confidencialidad de los datos.

Por último, pero no menos importante, la educación y concienciación de los profesionales de la salud sobre riesgos y prácticas seguras en ciberseguridad son imperativos para minimizar la vulnerabilidad humana, que a menudo es el error más frecuente en la cadena de seguridad.

La adopción de estas medidas no es solo recomendable sino vital, dada la creciente complejidad y sofisticación de las amenazas cibernéticas que enfrenta el sector sanitario. Fallar en establecer un modelo de ciberseguridad robusto pone en riesgo la integridad de los sistemas y la confidencialidad de los datos, así como también la calidad y la continuidad de la atención al paciente.

Es imperativo que las organizaciones sanitarias tomen medidas proactivas para mitigar estas vulnerabilidades. La inversión en formación de personal, la actualización de infraestructuras y sistemas de detección y la respuesta ante incidentes cibernéticos son pasos esenciales para minimizar los riesgos asociados con la vulnerabilidad a los ataques cibernéticos. Abordar estas amenazas es crucial para garantizar la seguridad de los datos de salud y la integridad de los dispositivos médicos.

Financiación

Este artículo no se ha realizado bajo ninguna subvención ni financiación.

Conflicto de intereses

Los autores no declaran tener ningún conflicto de intereses.

Anexo 1. Tablas

Tabla 1. Principales amenazas cibernéticas

Phishing	Engaño para obtener información confidencial, como contraseñas o datos bancarios, a través de correos electrónicos o sitios web falsificados.
Malware	Software malicioso diseñado para dañar, explotar o robar datos de sistemas informáticos.
Ransomware	*Malware* que encripta los archivos de la víctima y exige un rescate, generalmente en criptomoneda, para desbloquearlos.
Ataque de denegación de servicio (*DDoS*)	Inundación de un sistema o red con tráfico falso para sobrecargarlo y hacerlo inaccesible para los usuarios legítimos.
Ataque de fuerza bruta	Método para descifrar contraseñas o claves de cifrado mediante la prueba exhaustiva de todas las combinaciones posibles.
Spoofing	Falsificación de identidad en comunicaciones digitales para engañar a los usuarios y obtener acceso no autorizado a sistemas.
Troyano	Tipo de *malware* que se disfraza de software legítimo para engañar a los usuarios y obtener acceso a sus sistemas.
Ataque de colisión hash	Los ciberdelincuentes intentan encontrar dos conjuntos de datos diferentes que tienen el mismo hash. Si tienen éxito, pueden utilizar el hash común para engañar a un sistema que confía en el hash para verificar la integridad de los datos.

Bibliografía

1. Ossebaard HC, van Gemert-Pijnen L. eHealth and quality in health care: implementation time. Int J Qual Health Care. 2016;28:415–9.
2. Consejo de la Uniçón Europea. Ciberseguridad: cómo combate la UE las amenazas cibernéticas. [Internet]. [Consultado 22 Nov 2023]. Disponible en: https://www.consilium.europa.eu/es/policies/cybersecurity/
3. Coventry L, Branley D. Cybersecurity in healthcare: A narrative review of trends, threats and ways forward. Maturitas. 2018;113:48–52.
4. Argaw ST, Bempong NE, Eshaya-Chauvin B, Flahault A. The state of research on cyberattacks against hospitals and available best practice recommendations: a scoping review. BMC Med Inform Decis Mak. 2019;19:10.
5. Cano J. Seguridad y Ciberseguridad en los dispositivos médicos. Sistemas. 2018;149:55–67.
6. IBM. Cost of Data Breach Report 2023. [Internet]. [Consultado 20 Nov 2023]. Disponible en: https://www.ibm.com/reports/data-breach
7. Martínez-Pérez B, de la Torre-Díez I, López-Coronado M. Privacy and security in mobile health apps: A review and recommendations. J Med Syst. 2015;39:181.
8. Al-Muhtadi J, Shahzad B, Saleem K, Jameel W, Orgun MA. Cybersecurity and privacy issues for socially integrated mobile healthcare applications operating in a multi-cloud environment. Health Informatics J. 2019;25:315–29.
9. Herrera-Romero M.F.P. Revolución 4.0 y Ciberseguridad - Implicaciones éticas. Repositorio Institucional E-docUR. 2018. [Internet]. [Consultado 11 Sep 2023]. Disponible en: https://repository.urosario.edu.co/items/31c89dc3-603d-4063-a29c-7c7fbc816468
10. Siurana-Aparisi JC. Los principios de la bioética y el surgimiento de una bioética intercultural. Veritas. 2010;22:121–57.
11. Christen M, Gordijn B, Weber K, van de Poel I, Yaghmaei EA. Review of value-conflicts in cybersecurity. ORBIT J. 2017;1:1–19.
12. Weber K, Kleine N. Cybersecurity in Health Care. The International Library of Ethics, Law and Technology: Christen M, Gordijn B; 2020. [Internet]. [Consultado 11 Sep 2023]. Disponible en:

https://link.springer.com/chapter/10.1007/978-3-030-29053-5_7
13. Weber K, Loi M, Christen M, Kleine N. Digital medicine, cybersecurity, and ethics: An uneasy relationship. Am. J. Bioeth. 2018;18:52–3.
14. ENISA European Union Agency for Cybersecurity. Lista de las 15 amenazas principales. Panorama de Amenazas de ENISA [Internet]. [Consultado 01 Oct 2023]. Disponible en: https://www.enisa.europa.eu/publications/report-files/ETL-translations/es/etl2020-enisa-list-of-top-15-threats-ebook-en-es.pdf
15. ETKHO. Los ciberataques a la sanidad: un problema creciente. ETKHO Hospital Engineering - Seguridad eléctrica para instalaciones hospitalarias. [Internet].[Consultado 12 Oct 2023]. Disponible en: https://doi.org/10.1016/j.aprim.2023.102854
16. Hospital Clínic de Barcelona (n.d.). Comunicado legal 5 julio de 2023. [Internet]. [Consultado 12 Oct 2023]. Disponible en: https://www.clinicbarcelona.org/ca/premsa/ultima-hora/ciberatac-a-lhospital-clinic-barcelona
17. Comisión Europea. Configurar el futuro digital de Europa. [Internet]. [Consultado 20 Nov 2023]. Disponible en: https://digital-strategy.ec.europa.eu/es/policies/22-cybersecurity-projects-selected
18. SOPHOS. The State of Ransomware 2023. [Internet]. [Consultado 20 Nov 2023]. Disponible en: https://assets.sophos.com/X24WTUEQ/at/c949g7693gsnjh9rb9gr8/sophos-state-of-ransomware-2023-wp.pdf
19. NoMoreRansom. ¿Debo pagar el rescate si he sido infectado? 2023. [Internet]. [Consultado 20 Nov 2023]. Disponible en: https://www.nomoreransom.org/es/ransomware-qa.html
20. Kruse CS, Frederick B, Jacobson-Taylor DK. Cybersecurity in healthcare: A systematic review of modern threats and trends. Technol Health Care. 2017;25:1–10.
21. Argaw ST, Troncoso-Pastoriza JR, Lacey-Darren MV, Calcavecchia F, Anderson D, Burleson W, et al. Cybersecurity of Hospitals: discussing the challenges and working towards mitigating the risks. BMC Med Inform Decis Mak. 2020;20:146.
22. Sánchez-Henarejos A, Fernández-Alemán JL, Toval A, Hernández-Hernández I, Sánchez-García AB, Carrillo de Gea JM. Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario en atención primaria. Elsevier Atención Primaria. 2014;46:214–22.
23. Williams P, Woodward A. Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem. Med Devices. 2015;20:305–16.
24. Nifakos S, Chandramouli K, Nikolaou CK, Papachristou P, Koch S, Panaousis E, et al. Influence of human factors on cyber security within healthcare organizations: A systematic review. Sensors (Basel). 2021;21:5119.