COMUNICACIÓN CORTA / BRIEF REPORT

DOI: https://doi.org/10.20453/rmh.v35i1.5298

Ciberseguridad en servicios de apoyo al médico ocupacional de la ciudad de Lima. Estudio piloto

Cybersecurity in the support services to occupational physicians in the city of Lima. A pilot study

Raúl Gomero-Cuadra[1,2,a], *David Sánchez-Calle*[2,b]

[1] Universidad Peruana Cayetano Heredia
[2] Sociedad de Medicina Ocupacional y Medio Ambiente
[a] Médico con especialidad y maestría en Medicina Ocupacional y del Medio Ambiente
[b] Médico egresado de la Maestría de Medicina Ocupacional y Medio Ambiente de la Universidad Peruana Cayetano Heredia

Citar como:
Gomero R, Sánchez D. Ciberseguridad en servicios de apoyo al médico ocupacional de la ciudad de Lima. Estudio piloto. Rev Méd Hered. 2024; 35(1): 38-43. DOI: https://doi.org/10.20453/rmh.v35i1.5298

Recibido: 11/09/2023
Aceptado: 22/01/2024

Declaración de financiamiento y de conflictos de intereses:
El estudio fue financiado por los autores. En relación con conflictos de interés, RG labora en el Proyecto donde se realizó la investigación.

Contribución de autoría:
RG: Contribuyó en la concepción y diseño del estudio; en la recolección y análisis de los datos; redactó el informe final y revisión y aprobación de la versión final.
DS: Contribuyó en la concepción y diseño del estudio; en la recolección y análisis de los datos, y revisión y aprobación de la versión final.

Correspondencia:
Raúl Gomero Cuadra
Dirección: Calle Paseo de Aguas Mz D Lote 18, La Molina. Lima, Perú.
Email:
Raul.gomero.c@upch.pe

RESUMEN

Recientes investigaciones destacan la importancia de la ciberseguridad en la creciente era digital. El 83% de las organizaciones han experimentado brechas de seguridad en el 2022, costándoles en promedio 4,35 millones de dólares americanos por incidente. En Perú, la ciberseguridad está regulada por diversas normas, estableciendo medidas de protección de datos y la seguridad informática. ***Objetivo***: Describir la situación de la ciberseguridad en los servicios de apoyo al médico ocupacional (SAMO). ***Material y métodos***: Se incluyeron 11 SAMO. Se elaboró un cuestionario no validado para recolectar la información consentida sobre la gestión de la ciberseguridad de los SAMO que brindaban servicio a un importante proyecto de construcción en Lima Metropolitana. ***Resultados***: La mayoría de los establecimientos de salud (más del 80%) tuvo planes de respuesta a incidentes de seguridad cibernética para garantizar una respuesta rápida ante un ataque cibernético; realizaban copias de seguridad de los datos críticos con regularidad y los almacenaban en un lugar diferente a establecimiento; y actualizaban regularmente los sistemas operativos y programas de softwares buscando asegurar que se utilizan versiones seguras. ***Conclusión***: Existe una gestión de la seguridad informática predominantemente reactiva. El reporte discute la importancia de la ciberseguridad, resaltando la exposición de la información médica y los servicios a riesgos cibernéticos y planteamos retos futuros para la ciberseguridad, subrayando la importancia de la preparación ante amenazas futuras en un entorno en constante transformación digital.

PALABRAS CLAVE: Ciberseguridad, salud ocupacional, medicina del trabajo.

SUMMARY

Recent investigations emphasize the importance of cybersecurity in the growing digital era; 83% of organizations experienced breaks in cyber security in 2022, spending a mean of 4,35 million dollars per incident. Cybersecurity in Peru is regulated by legal norms aimed at protecting data and providing informatic security. ***Objective***: To describe cybersecurity in the support services to occupational physicians (SSOP) in the city of Lima. ***Methods***: A non-validated survey was created and distributed to 11 SSOPs in Lima that provide a service to an important building project in Lima. ***Results***: More than 80% of health care establishments had a response plan against cybernetic attacks; security copies of the data were done regularly storing them in a different place than the establishment and regularly updated security software's. ***Conclusion***: The cybersecurity program is reactive. We discuss the importance of cybersecurity and analyze future challenges as well as emphasize the importance of preemptive preparedness in an environment of constant digital transformation.

KEYWORDS: Computer security, occupational health, occupational medicine

INTRODUCCIÓN

Según un informe publicado por el Instituto Ponemon y la Corporación IBM, el 83% de 550 organizaciones estudiadas reportaron haber tenido más de una brecha de seguridad en el 2022. Además, se estimó que el costo promedio de una brecha de seguridad para una organización fue de 4,35 millones de dólares, incluyendo gastos de remediación, pérdida de datos y daños a la reputación. Estos datos resaltan la creciente importancia de la seguridad informática en un entorno cada vez más digitalizado.[1]

En América Latina, la situación en materia de ciberseguridad también presenta desafíos significativos. Según un estudio realizado por la empresa ESET en 2022, el 48% de las empresas latinoamericanas experimentaron al menos un incidente de seguridad en el último año, con un promedio de 3,9 incidentes por empresa. El país con la mayor cantidad de detecciones fue Perú (18%), seguido por México (17%), Colombia (12%), Argentina (11%) y Ecuador (9%) [2]. Además, el costo promedio de una brecha de seguridad en la región fue de 1,16 millones de dólares, un valor que puede ser especialmente gravoso para las pequeñas y medianas empresas. En el caso de Perú, los resultados de la 22° Encuesta Global de Seguridad de la Información de EY señalan que solo el 36% de las organizaciones incluyen la ciberseguridad como parte de su iniciativa de crecimiento empresarial.[3]

En el Perú, la normativa en ciberseguridad se encuentra principalmente regulada por la Ley N° 29733, Ley de Protección de Datos Personales, y su reglamento aprobado por el Decreto Supremo N° 003-2013-JUS. Estas normativas establecen los principios y requisitos para el tratamiento de datos personales, incluyendo medidas de seguridad que las organizaciones deben implementar para proteger la confidencialidad, integridad y disponibilidad de la información[4]. Además, existen otras regulaciones sectoriales que abordan aspectos específicos de la seguridad informática en salud, como la Ley N° 30024, Ley que Crea el Registro Nacional de Historias Clínicas Electrónicas, y su reglamento aprobado por Decreto Supremo N° 009-2017-SA.[5]

El objetivo de este estudio fue describir, de manera inicial, la situación actual de la ciberseguridad en Perú, evaluando el panorama de amenazas y las vulnerabilidades existentes en una muestra de servicios de apoyo al médico ocupacional de la ciudad de Lima para un Proyecto ferroviario. También, identificar las principales áreas de mejora en términos de prevención, detección y respuesta a incidentes de seguridad cibernética.

MATERIAL Y MÉTODOS

Estudio piloto de serie de casos basado en la recolección de información a través de un aplicativo desarrollado por los investigadores, que contenía 10 preguntas sobre los elementos relacionados con la Ley de Portabilidad y Responsabilidad de Seguros de Salud de 1996 (Health Insurance Portability and Accountability Act - HIPAA), para proveedores de salud que realizan procesos a través de tecnología de información.[6]

El cuestionario no validado elaborado para el estudio incluyó las siguientes preguntas:

Pregunta 1. ¿Tiene la clínica una política de seguridad de la información o gestión de riesgos que abarque aspectos relacionados con la seguridad cibernética?
Pregunta 2. ¿Se han realizado evaluaciones de riesgos de seguridad cibernética para identificar los activos de información críticos y las amenazas potenciales?
Pregunta 3. ¿Se han establecido medidas de control para minimizar los riesgos de seguridad cibernética, como el cifrado de datos, el control de acceso y la monitorización de la actividad de la red?
Pregunta 4. ¿Se realizan pruebas de penetración periódicas para identificar vulnerabilidades en la infraestructura de TI de la clínica?
Pregunta 5. ¿Se proporciona formación en seguridad cibernética a todo el personal de la clínica para concientizar sobre las amenazas y los riesgos de seguridad cibernética?
Pregunta 6. ¿Se dispone de planes de respuesta a incidentes de seguridad cibernética para garantizar que la clínica esté preparada para responder de manera rápida y efectiva en caso de un ataque cibernético?
Pregunta 7. ¿Se realizan copias de seguridad de los datos críticos con regularidad y se almacenan de forma segura en un lugar alejado de la clínica?
Pregunta 8. ¿Se actualizan regularmente los sistemas operativos y los programas de software para asegurar que se estén utilizando las versiones más seguras?
Pregunta 9. ¿Se realiza una auditoría periódica de la seguridad cibernética para evaluar y mejorar la efectividad de las medidas de control establecidas?
Pregunta 10. ¿La clínica cuenta con un equipo dedicado a la seguridad de la información y la ciberseguridad?

Las respuestas para cada pregunta fueron estructuradas de la siguiente manera:
1. No, porque no es necesario; 2. No, pero podría ser necesario en los siguientes años; 3. No, pero está programado; 4. Sí, pero no está actualizada; y 5. Sí, es revisada periódicamente.

Se incluyeron en el estudio 11 establecimientos de salud acreditados como Servicios de Apoyo al Médico Ocupacional por la Dirección General de Salud Ambiental (DIGESA) que brindaron servicio de evaluaciones médicas ocupacionales a un Proyecto de metro subterráneo de la ciudad de Lima durante el año 2023 y que aceptaron participar voluntariamente. Previo al llenado del cuestionario, se convocó a los directores médicos y su respectivo responsable tecnología de información para una reunión presencial con exposición del objetivo y cuestionario del estudio. Posterior a la reunión se envió el consentimiento informado y el cuestionario para su llenado con plazo de entrega de 7 días.

La información fue recolectada en una hoja de cálculo del programa de Microsoft Excel 365, elaborada desde el aplicativo, para, luego, obtener las frecuencias de las respuestas y realizar el análisis descriptivo correspondiente.

Al momento del reporte, existían 160 establecimientos de salud acreditados por DIGESA en Lima.

RESULTADOS

Luego de recibir las respuestas, se determinaron las frecuencias (gráfico 1), observándose que, más del 80% de los establecimientos de salud tuvieron planes de respuesta a incidentes de seguridad cibernética para garantizar una respuesta rápida ante un ataque cibernético; realizan copias de seguridad de los datos críticos con regularidad y los almacenan en un lugar diferente a establecimiento; y actualizan regularmente los sistemas operativos y programas de softwares buscando asegurar que se utilizan versiones seguras.

También, se evidenció que, 72,7% contaba con una Política de Seguridad de la Información en diferentes estados de implementación. Las medidas implementadas con más frecuencia fueron la actualización de sistemas operativos (90,9%), copias de seguridad de datos críticos (90,9%), planes de respuesta frente incidentes de seguridad informática (81,8%) y medidas de control para minimizar riesgos de ciberseguridad (81,8%). Sin embargo, actividades como auditoria periódica de la ciberseguridad (63,7%), contar con un equipo dedicado a seguridad de la información (63,6%) y realizar pruebas de penetración periódicas (54,5%), son poco conocidas o implementadas, lo que podría generar un alto riesgo para su gestión global de la seguridad de la información (gráfico 2).

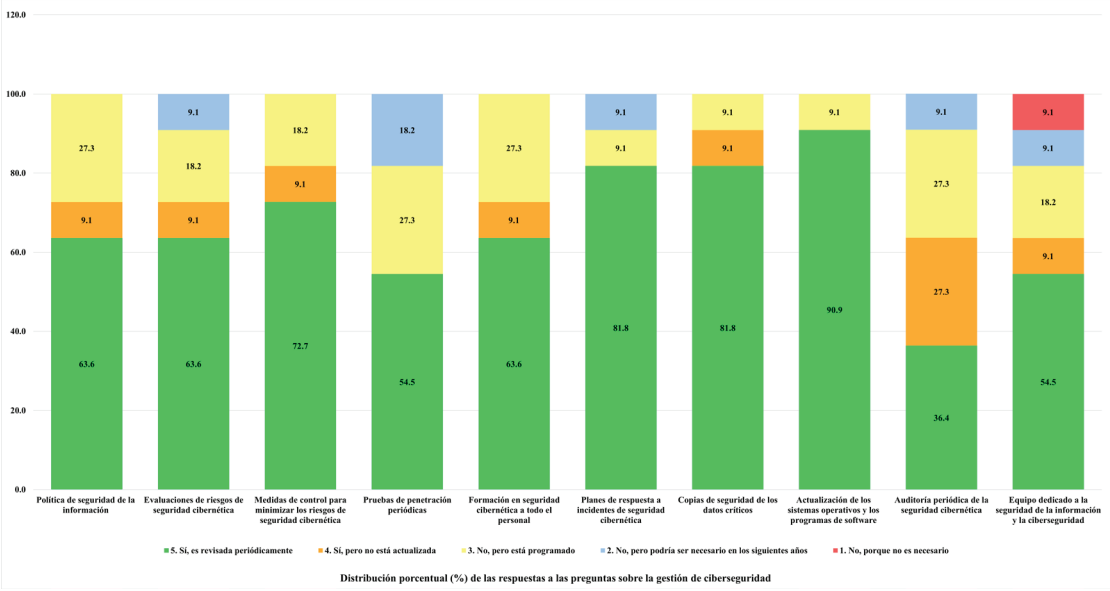

Gráfico 1. Distribución de las respuestas a las preguntas sobre la gestión de ciberseguridad.

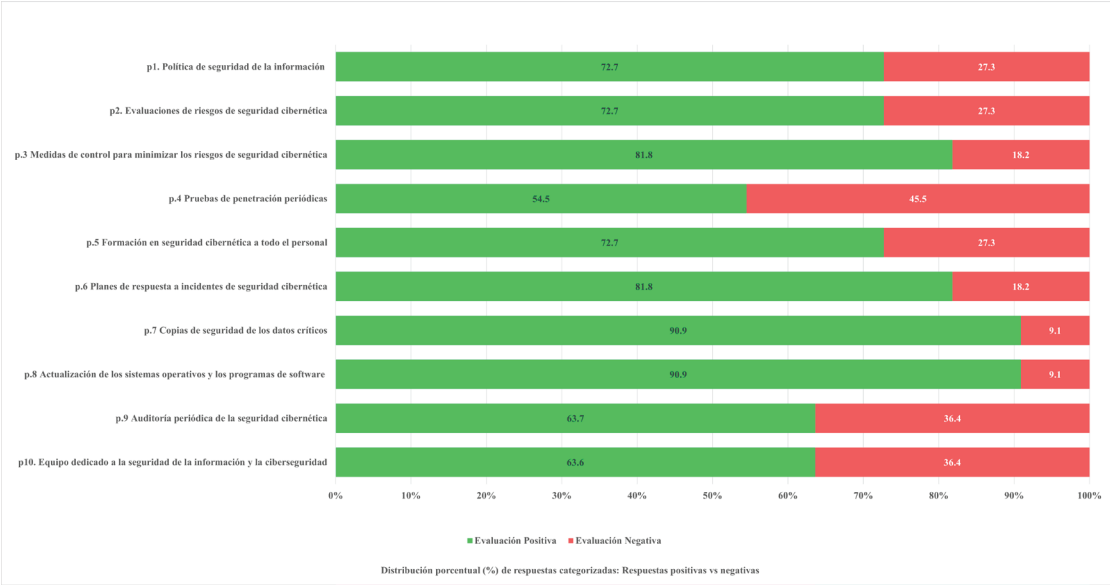

Gráfico 2. Distribución de las respuestas categorizadas en evaluación positiva o negativa.

DISCUSIÓN

Nuestros hallazgos sugieren que existe una gestión a la seguridad informática predominantemente reactiva. Ello podría deberse a que algunos de los establecimientos evaluados habían sufrido ataques cibernéticos. Además, los clientes o potenciales clientes de estos servicios están incluyendo recientemente criterios de seguridad informática para la licitación de sus servicios, como la certificación en ISO 27001:2013.

Según información del diario El Peruano[7], entre enero y abril del 2022, las pequeñas y medianas empresas (PYMES) del Perú sufrieron tres amenazas: el Troyano-PSW, los ataques de internet y los ataques al Protocolo de Escritorio Remoto. Estas amenazas permiten a los ciberdelincuentes acceder a la red corporativa y afectar de diversas maneras el negocio que, según una conocida empresa de seguridad, puede llevar a pérdidas económicas y de reputación hasta por 155 000 dólares[7]. Según el Reporte sobre entidades públicas que implementaron una respuesta ante incidentes de seguridad digital, solo 117 de 2 363 informaron tenerlo implementado, llamando la atención que la Autoridad Nacional de Datos Personales, el Congreso de la República, el Consejo Nacional de Ciencia, Tecnología e Innovación Tecnológica, la Contraloría General de la República, el Despacho Presidencial, la Fuerza Aérea del Perú, entre otros, estaban pendientes.[8]

La ciberdelicuencia también alcanza al sector Salud. En Latinoamérica se conoce el ataque informático a plataformas públicas del sector salud en Costa Rica en el 2022, así como ataque cibernético al sitio web del Instituto Nacional de Vigilancia de Medicamentos y Alimentos en Colombia[9]. En opinión de expertos, el riesgo no solo es el robo de información, sino también la alteración en la operación del sistema. Entonces, en el marco de la transformación digital, se debe considerar los perfiles adecuados para los profesionales de salud que accederán a la red de información dentro de la gestión de ciberseguridad[9]. En nuestro reporte, el 64% de los establecimientos de salud respondieron que se proporciona formación en seguridad cibernética a todo el personal de la clínica para concientizar amenazas y riesgos.

La interconexión de sistemas y el almacenamiento de datos médicos en formato electrónico han aumentado la eficiencia en la atención médica, pero también han expuesto a las instituciones de salud a una serie de riesgos cibernéticos. El marco normativo peruano, compuesto por leyes como la Ley 30096, Ley 29733, Ley 26842 y otras, establece la base legal para la protección de datos personales, la regulación de firmas y certificados digitales, y la prevención de delitos informáticos[5,10-14]. La norma técnica peruana NTP ISO IEC 27001:2022 proporciona directrices para establecer sistemas de gestión de seguridad de la información, lo que es esencial para la protección de datos médicos confidenciales y la infraestructura tecnológica en el sector salud.[15]

Debido a que desarrollamos un estudio piloto, la principal limitación de nuestra investigación es que no podemos generalizar los resultados; sin embargo, consideramos que es una primera aproximación a la problemática de la ciberseguridad en relaicón con la evaluación médica ocupacional. Sería interesante que estudios posteriores validen el instrumento propuesto y consideren una muestra extrapolable.

En conclusión, la transformación digital plantea desafíos en ciberseguridad para el sector salud, debiendo considerarse la protección de la privacidad de los pacientes y la integridad de los servicios médicos en un entorno digital en constante cambio. Los retos futuros incluyen entre otras las amenazas cibernéticas más sofisticadas, protección de dispositivos médicos conectados, cumplimiento normativo constante, escasez de profesionales de ciberseguridad en el sector salud, entre otros.

REFERENCIAS BIBLIOGRÁFICAS

1. IBM Corporation, Ponemom Institute LLC. Cost of a Data Breach Report 2022 [Internet]. 2022 [citado el 5 de junio 2023]. Disponible en: https://www.ibm.com/reports/data-breach
2. ESET. Security Report Latinoamérica 2022 [Internet]. 2022 [citado el 5 de junio 2023]. Disponible en: https://www.eset.com/ve/security-report/
3. Cama E. El 51% de las compañías en el Perú sostienen que la relación entre ciberseguridad y sus líneas de negocio es inexistente o neutral [Internet]. Boletín de Prensa EY. 11 de junio de 2020 [Citado el 5 de junio de 2023]. Disponible en: https://www.ey.com/es_pe/news/2020/06/ciberseguridad-lineas-negocio-neutral
4. Congreso de la Republica de Perú. Ley N.° 29733 - Ley de Protección de Datos Personales [Internet]. 2013. [Citado el 15 de agosto 2023]. Disponible en: https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/243470-29733

5. Ministerio de Salud. Ley 30024 - Ley que Crea el Registro de Nacional de Historias Clínicas Electrónicas. El Peruano; 2013. Disponible en: https://www.gob.pe/institucion/minsa/normas-legales/240527-30024
6. Centers for Disease Control and Prevention. Health Insurance Portability and Accountability Act of 1996 (HIPAA). [Citado el 15 de agosto del 2023]. Disponible en: https://www.cdc.gov/phlp/publications/topic/hipaa.html
7. Pichigua S. ¡Pymes en la mira de la ciberdelincuencia! Modalidades de cibercrimen más frecuentes. El Peruano. 13 de julio de 2022. [Citado el 15 de agosto del 2023]. Disponible en: https://elperuano.pe/noticia/168541-pymes-en-la-mira-de-la-ciberdelincuencia-modalidades-de-cibercrimen-mas-frecuentes
8. Presidencia del Consejo de ministros del Perú. Reporte sobre entidades que implementaron su equipo de respuestas ante incidentes de seguridad digital. 31 de agosto de 2023. [Citado el 15 de septiembre del 2023]. Disponible en: https://www.gob.pe/institucion/pcm/informes-publicaciones/2605569-reporte-sobre-entidades-que-implementaron-su-equipo-de-respuestas-ante-incidentes-de-seguridad-digital
9. Ciberseguridad en el sector Salud. El Peruano. 27 de febrero de 2023. [Citado el 15 de agosto del 2023]. Disponible en: https://elperuano.pe/noticia/206491-ciberseguridad-en-el-sector-salud
10. Ministerio de Salud. Ley 26842 - Ley General de Salud. Ciudad de Lima. El Peruano; 1997. Disponible en: https://www.gob.pe/institucion/minsa/normas-legales/256661-26842
11. Congreso de la República del Perú. Ley 27269 - Ley de Firmas y Certificados Digitales. Ciudad de Lima. El Peruano; 2000. Disponible en: https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/292289-27269
12. Congreso de la República del Perú. Ley 26842 - Ley de Protección de Datos Personales. Ciudad de Lima. Diario Oficial El Peruano; 2011. Disponible en: https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/243470-29733
13. Ministerio Público Fiscalía de la Nación. Ley 30096 – Ley de Delitos Informáticos. Ciudad de Lima. Diario Oficial El Peruano; 2021. Disponible en: https://www.gob.pe/institucion/mpfn/informes-publicaciones/1678028-ley-n-30096
14. Congreso de la República. Ley 27309 - Ley que incorpora los delitos informáticos al Código Penal. Ciudad de Lima. Diario Oficial El Peruano; 2. Disponible en: https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/292284-27309
15. INDECOPI. Norma Técnica Peruana "NTP ISO IEC 27001:2022 Seguridad de la información, ciberseguridad y protección de la privacidad. Sistemas de gestión de la seguridad de la información. Requisitos. 3ª Edición"