Vectores de ataque en Colombia: análisis de vulnerabilidades críticas en el sector salud

Attack vectors in Colombia: analysis of criticalvulnerabilities in the healthcare sector

Ivonne Rocío Bernal Núñez[1]

Yenny Stella Núñez Álvarez[2]

Universidad Nacional Abierta y a Distancia, Colombia

Resumen

La acelerada digitalización del sector salud en Colombia ha incrementadola exposición de sus activos críticos al riesgo de ciberataques. Este estudioexamina las vulnerabilidades específicas explotadas por los ciberdelincuentes en el contexto nacional, identificando los vectores de ataque predominantes y evaluando tanto el estado actual de la administración de riesgos como las prácticas de aseguramiento de la información. A través de un análisis detallado de casos y una revisión exhaustiva de la literatura, se proponen estrategias para mitigar riesgos y gestionar incidentes informáticos, con el fin de robustecer la ciberseguridad en las instituciones de salud colombianas. La investigación contribuye a una comprensión más profunda de las amenazas cibernéticas en el sector salud del país y brinda recomendaciones prácticas para optimizar la protección de la información de los usuarios y garantizar la continuidad de los servicios de salud.

Palabras clave: ciberseguridad, gestión de incidentes, protección de datos, sector salud,vulnerabilidades informáticas.

Abstract

The rapid digitalization of the healthcare sector in Colombia has increased the exposure of its critical assets to cyberattack risks. This study examines the specific vulnerabilities exploited by cybercriminals in the national context, identifying the predominant attack vectors and assessing the current state of risk management and information security practices. Through a detailed case analysis and a comprehensive

[1] Estudiante en la Especialización en Seguridad Informática, UNAD, https://orcid.org/0009-0005-1222-1227 / irbernaln@unadvirtual.edu.co

[2] Ingeniera de sistemas, especialista en seguridad informática, magister en ciberseguridad, UNAD, https://orcid.org/0000-0002-6868-6278 / yenny.nunez@unad.edu.co

literature review, strategies are proposed to mitigate risks and manage cyber incidents, aiming to strengthen cybersecurity in Colombian healthcare institutions. This research contributes to a deeper understanding of cyber threats in the country's healthcare sector and offers practical recommendations to enhance information protection for users and ensure the continuity of health services.

Keywords: Cybersecurity, incident management, data protection, healthcaresector, vulnerabilities.

1. Introducción

Los ciberataques han convertido la seguridad de la información en una preocupación primordial para las organizaciones a nivel mundial, y el sector salud colombiano no es la excepción. La pandemia aceleró la digitalización de los procesos, incrementando la superficie de ataque y exponiendo a las instituciones de salud a un riesgo cada vez mayor. Este trabajo de investigación se centra en analizar el panorama de la respuesta a incidentes de seguridad de la información (SI) en las organizaciones del sector salud colombiano. Se busca comprender cómo estas instituciones están gestionando los ciberataques, identificando las principales brechas y vulnerabilidades que explotan los cibercriminales. Para ello, se analizarán los principales vectores de ataque, las vulnerabilidades más comunes y las prácticas de gestión de incidentes implementadas por las organizaciones. Los resultados de esta investigación permiten identificar las fortalezas y debilidades en la gestión de la seguridad de la información, así como proponer recomendaciones para mejorar la resiliencia de las instituciones de salud frente a las ciberamenazas. La importancia de este estudio radica en la frecuencia y constante avance de los ataques cibernéticos en Colombia. Según datos recientes del CCIT, las pérdidas económicas asociadas a estos incidentes pueden ser significativas, afectando la continuidad de los servicios y la reputación de las organizaciones. Además, el sector salud maneja información sensible de los pacientes, lo que convierte a los ciberataques en una amenaza directa para la privacidad y la seguridad de los ciudadanos.

2. Metodología

2.1 Panorama de la gestión de seguridad informática en el sector salud

En los últimos años, el sector salud se ha convertido en un blanco frecuente de ciberataques. Un ejemplo significativo es el ataque alHospital Clínic de Barcelona en marzo de 2023, en el cual los sistemas fueron encriptados, forzando la cancelación de servicios de urgencias, laboratorio y farmacia. Como resultado, se suspendieron más de 4.000 análisis de pacientes ambulatorios, 300 intervenciones quirúrgicas y 11.000 consultas externas en un solo día (Europapress, 2023). Este tipo de

impacto suele generarse mediante técnicas que explotan software desactualizado, ataques de *phishing* para comprometer cuentas de usuario, y una gestión limitada de incidentes. Otro caso relevante fue el ciberataque al Hospital Universitario de Düsseldorf (UHD) en 2020, que provocó fallos progresivos en sus sistemas y en el acceso a los datos. El malware afectó servicios de correo electrónico y telefonía, además de degradar otras funciones de TI, lo cual obligó al hospital a desviar pacientes a otras instituciones, suspender emergencias y reprogramar cirugías planificadas (Silomon, 2020). Ambos ataques fueron casos de ransomware. Según la XXI Encuesta Nacional de Seguridad Informática, el 72 % de las organizaciones reportaron incidentes de seguridad informática (SI) en 2021, un incremento del 4 % respecto al año anterior (Almanza, 2023). Los incidentes más comunes incluyen errores humanos, *phishing* y accesos no autorizados, aunque solo el 28 % de las empresas reporta estos incidentes a las autoridades. De acuerdo con la Policía Nacional, también ha aumentado el número de denuncias, aunque solo una minoría de empresas realiza reportes formales (Mintic, 2021). La Organización Panamericana de la Salud resalta la necesidad de un marco normativo coherente en América Latina para la protección de datos, proponiendo estrategias que equilibren privacidad y accesibilidad. También identifican brechas significativas en políticas públicas, capacitación en ciberseguridad y mecanismos de detección y respuesta a incidentes. En el sector salud, se observa una creciente tercerización de servicios de ciberseguridad y una escasez de personal especializado. En este contexto, resulta fundamental implementar políticas claras de seguridad de la información y una adecuada gestión de riesgos para mitigar amenazas como ataques a dispositivos médicos e infraestructura crítica (revistahospitalaria,2024). Las GAP en ciberseguridad presentes en el sector salud surgen principalmente de la falta de políticas públicas adecuadas y de un conocimiento limitado sobre las tendencias de ataque, lo que obstaculiza la formulación de estrategias efectivas para la seguridad de la información. Aunque Colombia cuenta con el CAI Virtual y el CSIRT para informar y asesorar sobre incidentes, la información generada no siempre impulsa decisiones estratégicas. La Organización Panamericana de la Salud y la Encuesta Nacional de Seguridad Informática revelan también carencias en capacitación, lo que compromete la primera línea de defensa: los usuarios (no está en las referencias).Además, la tercerización es común en ciberseguridad debido a la escasezde personal especializado, y las funciones suelen mezclarse con las áreas de TI, dejando en segundo plano la seguridad de la información. Existenademás deficiencias en gestión de riesgos, y temas críticos como la protección de dispositivos médicos y la infraestructura en la nube quedanexpuestos a amenazas avanzadas y fuga de información.

3. Discusión

3.1 Principales vectores de ataque en el sector salud

La pandemia aceleró la transformación digital en Colombia, impulsando aun 91 % de organizaciones a adoptar modalidades de teletrabajo o trabajo

híbrido en 2020, incrementando los colaboradores remotos en un 71 %. Sin embargo, muchas carecían de medidas de ciberseguridad adecuadas, lo cual facilitó el abuso de protocolos como el RDP, impulsando el aumento del cibercrimen, en especial ataques de ingeniería social, APT, *ransomware* y *phishing*, con un incremento en denuncias del 46 %. Estudios recientes destacan que el sector salud ha sido vulnerable a ataques como el *ransomware* y *spoofing*, afectando servicios críticos como el Ministerio de Salud (Castañeda Pérez, 2022). El informe nacional de ciberseguridad de MinTIC 2023-2026 resalta que el malware es una amenaza significativa, atribuida en parte a la falta de prácticas de seguridad básica, como el uso de antimalware y contraseñas seguras. Colombia aún enfrenta debilidades en su índice de ciberseguridad y carece de liderazgo gubernamental efectivo en este ámbito. De igual manera, técnicas como el credential stuffing, ataques a la cadena de suministro y la creación de dominios malignos proliferaron, aprovechando el escaso monitoreo y actualizaciones de sistemas críticos (Mintic, 2023). La inteligencia artificial también ha mejorado ataques de phishing y suplantación, mientras que los ataques avanzados como el ransomware emplean técnicas como Mimikatz, PowerShell y PsExec para obtener acceso y comprometer datos de entidades públicas y privadas en toda Colombia. Para el sector salud, informes recientes han mostrado que los vectores de ataque más comunes incluyen ransomware, phishing, y explotación de vulnerabilidades en sistemas sin parches. Los datos de ataques en el sector salud en Colombia y Latinoamérica sonespecialmente altos debido a la sensibilidad de los datos médicos y a la infraestructura tecnológica limitada en ciberseguridad en muchas instituciones. Los ataques de ransomware en el sector salud se han incrementado globalmente, con un aumento en Colombia de más del 100 % en algunos años recientes, lo que afecta tanto a hospitales como a empresas de servicios médicos. Kaspersky reportó en el último año más de 2.4 millones de intentos de phishing en el sector de la salud en Colombia, promovidos por temas sensibles. Se estima que más del 30 % de las entidades de salud carecen de un mantenimiento de parches adecuado, lo que las hace vulnerables a exploits conocidos. Un ejemplo fue el ataque de ransomware a IFX Networks, que comprometió múltiples servicios hospitalarios (Kaspersky,2024).

3.2 *Factores que facilitan ciberataques exitosos*

Diversos factores facilitan la ocurrencia de ciberataques o crean oportunidades para que un adversario identifique vulnerabilidades o fallos de ciberseguridad. Entre estos factores destaca la falta de políticas públicas adecuadas, así como la dificultad para adaptarse a un entorno en constante cambio. Además, muchos profesionales del sector salud carecen de la capacitación necesaria en seguridad de la información, limitando su capacidad para prevenir y detectar incidentes. La escasez de mecanismos gubernamentales efectivos para la detección y respuesta ante incidentes, junto con una gestión de riesgos insuficiente, restringe la

identificación y mitigación de amenazas. Finalmente, la vulnerabilidadde los dispositivos médicos conectados introduce nuevos riesgos, que requieren medidas de seguridad especializadas para su adecuada protección.

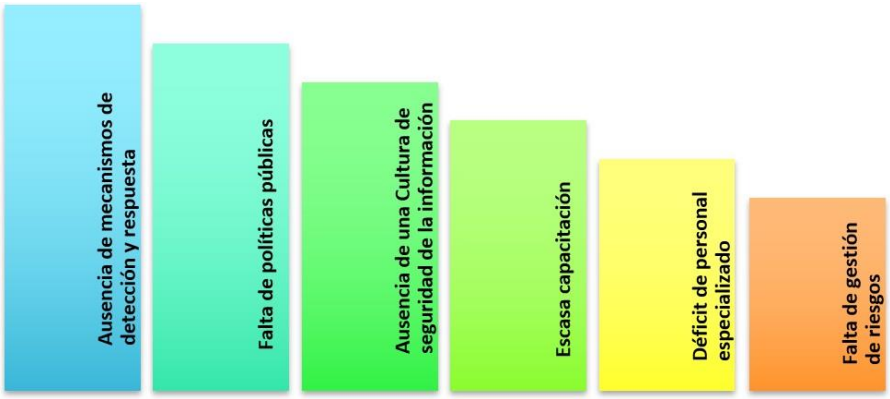

Figura 1. Factores que facilitan ciberataques*.* Nota: elaboración propia.

4. Conclusiones

Desde el inicio de la pandemia, los ciberataques en el sector salud en Colombia han aumentado significativamente, especialmente mediante ransomware, que presenta un alto impacto y facilidad de ejecución. La sofisticación de estos ataques resalta la necesidad de capacitar a los colaboradores y mejorar la adopción de prácticas de ciberseguridad. Además, se observa que las vulnerabilidades más explotadas en el país tienen un promedio de 7 años de antigüedad, lo cual revela deficiencias en la gestión de parches y en la actualización tecnológica de las organizaciones. En el sector salud, también existen brechas para alinear los controles técnicos con los normativos y la estrategia organizacional.

El Gobierno colombiano ha comenzado a implementar resoluciones, comolas emitidas por MinSalud, para fortalecer la seguridad de los datos de salud por ejemplo la resolución número 00500 de marzo 10 de 2021 "Porla cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital", mientras que MinTIC proporciona guías para la gestión de incidentes. Aunque el país ha avanzado en la adopción de buenas prácticas en la última década, aún persisten importantes desafíos en ciberseguridad, particularmente en la gestión de activos, riesgos e incidentes. Se requiere un compromiso de la dirección y la inclusión de la ciberseguridad en la agenda estratégica, especialmente en el sector salud, para lograr avances en el corto y mediano plazo.

Referencias

Almanza J., A. R. (14 de diciembre de 2023). XXIII Encuesta Nacional de Seguridad Informática. Valor y beneficio de la ciberseguridad. *Revista Sistemas, 169*. https://sistemas.acis.org.co/index.php/sistemas/article/view/Inve

stigaci%C3%B3n%20169

Ataque masivo de suplantación de diferentes juzgados de Colombia | Quiero ser UNAB. (18 de septiembre de 2023). *Quiero ser UNAB*.https://unab.edu.co/ataque-masivo-de-suplantacion-de-diferentes-juzgados-de-colombia

Bautista García, F., & Mesa Guzmán, L. (2022). *Estudio trimestral de ciberseguridad. Ataques a entidades de gobierno*. CCIT. https://www.ccit.org.co/wp-content/uploads/estudio-trimestral-de-ciberseguridad-ataques-a-entidades-de-gobierno-safe-bp.pdf

CAI Virtual. (s.f.). *Balances anuales del cibercrimen* | CAI Virtual. CAI Virtual. https://caivirtual.policia.gov.co/observatorio/analisis-cibercrimen