Ciberataque en el sistema general de seguridad social en Salud y su Impacto micro y macro Económico en las entidades de salud y como afectaron a la Superintendencia Nacional de Salud y EPS sanitas

Cyberattack on the general system of social security in health and its micro and macro economic impact on health entities and how it affected the National Superintendence of Health and EPS sanitas.

Carlos David Castañeda Morales
Especialización en gerencia en servicios de salud
Institución Universitaria Colegios de Colombia
ccastanedam@unicoc.edu.co

Resumen

Desde 2019, el sector salud en Colombia ha sido un objetivo cada vez más frecuente de ciberataques, lo que ha impactado de manera severa la operación de entidades tanto públicas como privadas. Esto ha comprometido la atención a los usuarios, la gestión institucional y la seguridad de la información. Este artículo se enfoca en los efectos micro y macroeconómicos que han surgido a raíz de estos ataques, destacando casos representativos como EPS Sanitas, la Superintendencia Nacional de Salud, el Ministerio de Salud y Salud Total EPS. A través de una revisión de documentos y un análisis de eventos ocurridos entre 2020 y 2024, se identificaron impactos significativos en la continuidad de la atención, pérdidas económicas tanto directas como indirectas, deterioro de la reputación y la interrupción de procesos críticos. En el ámbito microeconómico, los ataques resultaron en pérdidas operativas, un aumento en gastos inesperados y una disminución en la confianza de los usuarios. A nivel macroeconómico, se hizo evidente la necesidad de redirigir recursos públicos, una caída en la productividad del sistema y una creciente dependencia de la tecnología internacional. Los tipos de ataque más comunes fueron ransomware, phishing y malware, que afectaron bases de datos clínicas, plataformas de agendamiento y sistemas de supervisión estatal. Los hallazgos indican una cultura organizacional débil en ciberseguridad, una preparación preventiva escasa y una limitada colaboración entre los actores del sistema. Finalmente, se sugieren estrategias para fortalecer las instituciones, como la inversión continua en infraestructura tecnológica, la capacitación del personal, auditorías de vulnerabilidad y la creación de un centro nacional de respuesta ante incidentes cibernéticos en el sector salud. Estas acciones buscan proteger la continuidad operativa, salvaguardar la vida de los pacientes y asegurar la resiliencia digital del Sistema General de Seguridad Social en Salud en Colombia.

Palabras clave: Ciberseguridad, Sector Salud, Ransomware, EPS Sanitas, Supersalud, impacto económico, seguridad informática.

Abstract:

Since 2019, the healthcare sector in Colombia has become an increasingly frequent target of cyberattacks, severely impacting the operations of both public and private entities. These attacks have compromised user care, institutional management, and information security. This article focuses on the micro- and macroeconomic effects resulting from these incidents, highlighting representative cases such as EPS Sanitas, the National Superintendency of Health, the Ministry of Health, and Salud Total EPS. Through a document review and analysis of events that occurred between 2020 and 2024, significant impacts were identified in care continuity, direct and indirect economic losses, reputational damage, and the interruption of critical processes.

At the microeconomic level, the attacks led to operational losses, increased unplanned expenses, and a decline in user trust. From a macroeconomic perspective, they revealed the need to redirect public resources, a decrease in system productivity, and a growing dependency on international technology providers. The most common types of attacks included ransomware, phishing, and malware, which affected clinical databases, appointment scheduling platforms, and state supervision systems.

Findings indicate a weak organizational culture in cybersecurity, insufficient preventive preparedness, and limited collaboration among system stakeholders. Finally, this paper suggests strategies to strengthen institutional resilience, such as sustained investment in technological infrastructure, continuous staff training, periodic vulnerability audits, and the creation of a national cyber incident response center for the health sector. These actions aim to protect operational continuity, safeguard patient lives, and ensure the digital resilience of Colombia's General System of Social Security in Health.

Keywords: Cybersecurity, Health Sector, Ransomware, EPS Sanitas, Supersalud, economic impact, information security.

Introducción

Durante la época de la transformación digital, el ámbito del sector salud ha conseguido posicionarse como uno de los objetivos más vulnerables y rentables para los criminales informáticos debido al gran volumen de información sensible que gestiona. Historias clínicas electrónicas, datos personales, financieros y administrativos representan un valor incalculable tanto para el funcionamiento institucional como para el crimen organizado. Organismos internacionales como la Organización Mundial de la Salud (OMS, 2022) han advertido que los sistemas de salud en el mundo enfrentan una amenaza cibernética que pone en jaque tanto la privacidad de los pacientes como la continuidad y seguridad de los servicios médicos. Esto se ha vuelto mucho más agudo en países donde la infraestructura tecnológica es débil (como Colombia), donde persisten fallas estructurales en ciberseguridad, gobernanza digital, funcionabilidad y cultura organizacional frente a la gestión del riesgo digital.

La Agencia Nacional Digital (2023) ha expuesto que más del 60% de las instituciones públicas de salud en Colombia utilizan software obsoleto, que no cuenta con protocolos para las actualizaciones ni para las copias de seguridad. Esto incrementa la vulnerabilidad técnica que tienen estas instituciones, ya que hay baja cualificación del talento humano que las opera y escasa articulación entre las distintas entidades que componen el sector salud. En un entorno de alta vulnerabilidad técnica, sumado a la baja cualificación del talento humano y los fracasos de la articulación entre entidades del sector salud, se genera un contexto de alta vulnerabilidad ante ataques de ransomware, phishing, malware o DoS (denegación del servicio o DDoS). IBM Security (2023) establece que el sector salud es el que tiene el mayor coste medio por brecha de seguridad en el mundo, por una cuantía que supera los USD 10,9 millones por incidente, superando incluso al sector que ocupa el segundo lugar, que es el bancario o el de las telecomunicaciones. Este dato puede resultar especialmente alarmante cuando se considera que la mayoría de las entidades de salud no tienen ni estrategias preventivas implementadas ni planes de contingencia ante eventos de esta magnitud.

Definida desde una vertiente teórica, la gestión del riesgo cibernético en salud puede ser contemplada como una función transversal de la gerencia institucional y de sus operaciones, la protección de la información no es el único objetivo sino que debe ser abordada la gestión de la continuidad operativa, la confianza que genera en el usuario, así como la manera de afrontar la continuidad financiera. Heeks & Cuganesan (2020) sugieren que los sistemas de salud digital deben construirse desde los modelos de “resiliencia adaptativa” en el que los actores de la tecnología, el capital humano y la regulación son las bazas en la defensa de la seguridad cibernética. En este sentido, la falta de normas jurídicas, la escasa inversión en tecnologías de la información y el conocimiento de mecanismos reactivos ante incidentes cibernéticos o de ciberseguridad permiten evidenciar un entorno débil.

En Colombia, han ocurrido eventos como el ciberataque a la EPS Sanitas en 2023 que, de por sí sólo, llevó a la completa paralización de las plataformas de atención

y a pérdidas operativas directas por un valor estimado de más de USD 1.5 millones (ConsultorSalud, 2023), o el ciberincidente de la Superintendencia Nacional de Salud, comprometiendo su capacidad supervisora por varias semanas (MinSalud, 2021), entre otros, que han puesto el acento en el impacto real de estas amenazas en lo institucional y lo sistémico. Además, otras EPS como Salud Total o el evento en el Ministerio de Salud, han servido para reflejar el estado de fragilidad del ecosistema digital sanitario nacional. La ausencia de un plan nacional de ciberseguridad para el sector sanitario, como también de un centro coordinador de respuesta ante incidentes cibernéticos, es un hecho que refuerza la necesidad urgente de estas acciones estructurales.

En respuesta a esto, la presente investigación tiene como objetivo general indagar sobre la afectación que produce los ciberataques a las entidades de salud, y en concreto cómo impactaron a la Superintendencia Nacional de Salud y EPS Sanitas desde el punto de vista micro y macroeconómico, dadas las medidas de ciberseguridad. A través de un análisis de documentación y casos, ocurridas entre 2020 y 2024, se busca identificar aquellas consecuencias de naturaleza operativa y financiera más relevantes, así como sugerir estrategias que permitan fortalecer la resiliencia institucional frente este tipo de amenazas, garantizando así la protección de los datos, la sostenibilidad del servicio, y por encima de todo la vida y bienestar de los pacientes.

Metodología

El diseño del presente estudio pertenece a un enfoque mixto, en el que se dan cita los métodos cualitativos y cuantitativos a través de un planteamiento descriptivo y exploratorio que se orientará a analizar el impacto de los ciberataques en el sector salud colombiano durante el periodo 2019-2024. La población de interés está conformada por documentos oficiales, por literatura científica y por reportes periodísticos relacionados con incidentes de ciberseguridad en instituciones del sistema general de seguridad social en salud de Colombia y de otras experiencias comparadas internacionalmente. La muestra fue elegida de forma intencionada para incluir aquellos documentos que resultan relevantes y que estén actualizados para que puedan ser sometidos a un análisis del fenómeno.

Principalmente, se utilizaron tres instrumentos para la recolección de datos: (1) la revisión documental pormenorizada de la literatura académica que está indexada en bases de datos como PubMed, Scielo, Google Scholar; (2) el análisis documental de caso de estudios concretos extraídos de entidades oficiales de salud pública, como la Superintendencia Nacional de Salud (Supersalud) y el Ministerio de Salud y Protección Social (MinSalud), así como de medios de comunicación reconocidos, como El Tiempo, Semana, ConsultorSalud; finalmente, (3) la evaluación del impacto económico en base a la información oficial y a los estudios de consultoras especializados en salud y en ciberseguridad. El análisis cualitativo ayudó a

identificar las pautas comunes, las vulnerabilidades estructurales/organizativas y las respuestas institucionales, mientras que el análisis cuantitativo hizo énfasis en la cuantificación de las pérdidas económicas directas/indirectas, los costos operativos y los cambios en los indicadores de gestión y de confianza. Este enfoque consolidado obtuvo como resultado una profunda y multidimensional comprensión del fenómeno y sustenta la propuesta de recomendación orientadas a la mejora de la ciberseguridad en el sistema de salud colombiano.

Resultados:

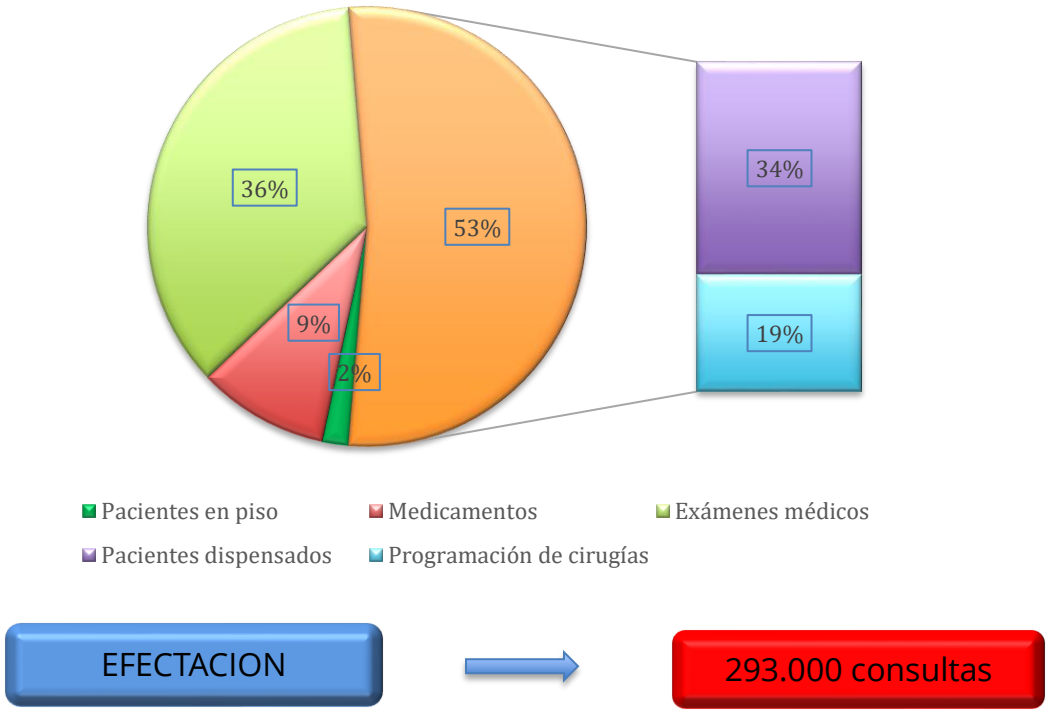
De acuerdo con los objetivos específicos planteados para la presente unidad de trabajo garantizando una adecuada redacción científica a partir de los conocimientos adquiridos, se presentan, a continuación, los resultados del análisis realizado a casos con ciberataques representativos en el sector salud en Colombia recogidos entre los años 2019 y 2022, así como el análisis del impacto, tanto microeconómico como macroeconómico que estos pueden haber tenido sobre el gasto total en salud; es importante tener en cuenta que los ciberataques no solo tuvieron su pico máximo, es decir, a partir de la pandemia por Covid-19 y su posterior adopción de herramientas tecnológicas en el ámbito de la salud, sino que también pueden haber tenido lugar durante los años de 2019 a 2022.

Resultados: Casos Clave y Análisis Económico

Caso 1. EPS Sanitas (2023) El ataque tipo ransomware, mediante el uso del malware White Rabbit, generó una paralización total de los sistemas internos, afectando de tal manera la programación de citas y de los diferentes exámenes médicos, condicionando con ello el seguimiento clínico de los pacientes. En cuanto al costo directo, este se estimó en USD 1.5 millones, más un considerable costo indirecto por desatención y la generación de un impacto negativo en la calidad del servicio (ConsultorSalud, 2023). Desde la práctica institucional, la EPS logó migrar cautivamente sus canales de atención, pero allí se presentó una considerable pérdida de reputación e incrementos importantes en las quejas de los usuarios. (Figura 1)

Figura 1

Análisis porcentual de alteraciones por el ciber ataque a EPS sanitas



Caso 2. Superintendencia Nacional de Salud (2020). El evento impactó la capacidad de monitorear y controlar el sistema general de salud, provocando averías en la interoperabilidad de la información crítica para la supervisión. Aunque no hay estimaciones oficiales del costo económico, se hace referencia a que la interrupción del compromiso de los procesos esenciales duró en torno a semanas, con consecuencias en la supervisión de los prestadores, lo que originó un incremento en las sanciones y las demandas dirigidas a instituciones defectuosamente reguladas (Ministerio de Salud, 2021). Se destinaron más recursos a fortalecer los sistemas tecnológicos de la entidad.

(Figura 2 y 3)

Figura 2

Plan de inversion estrategico de tecnologias

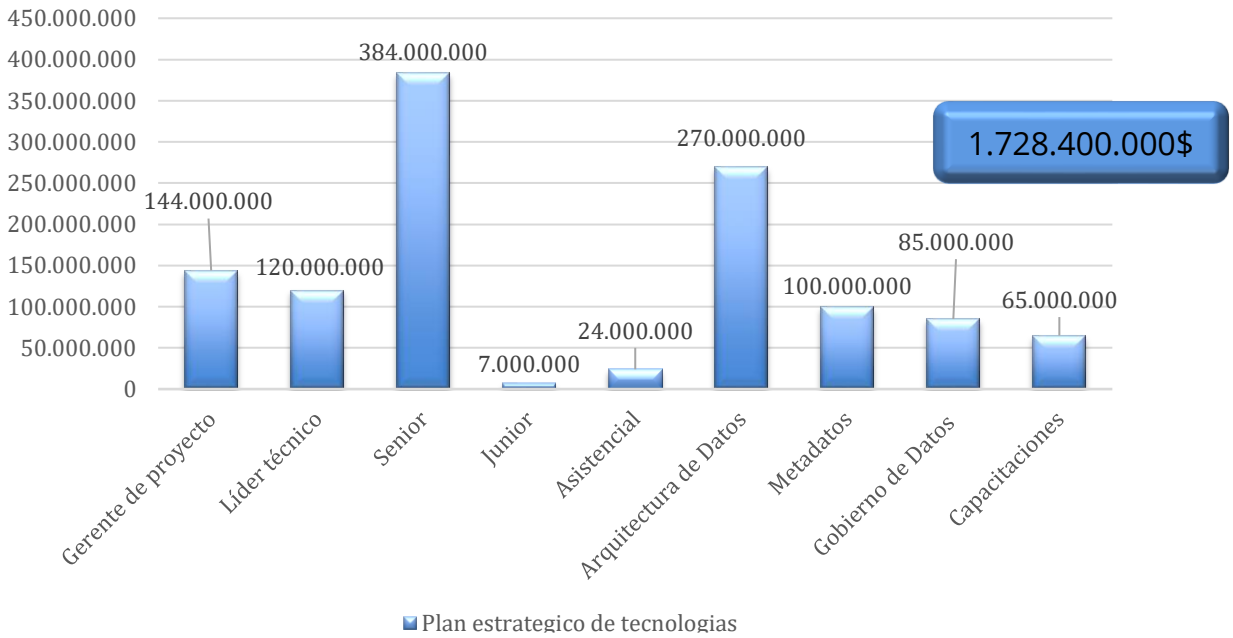
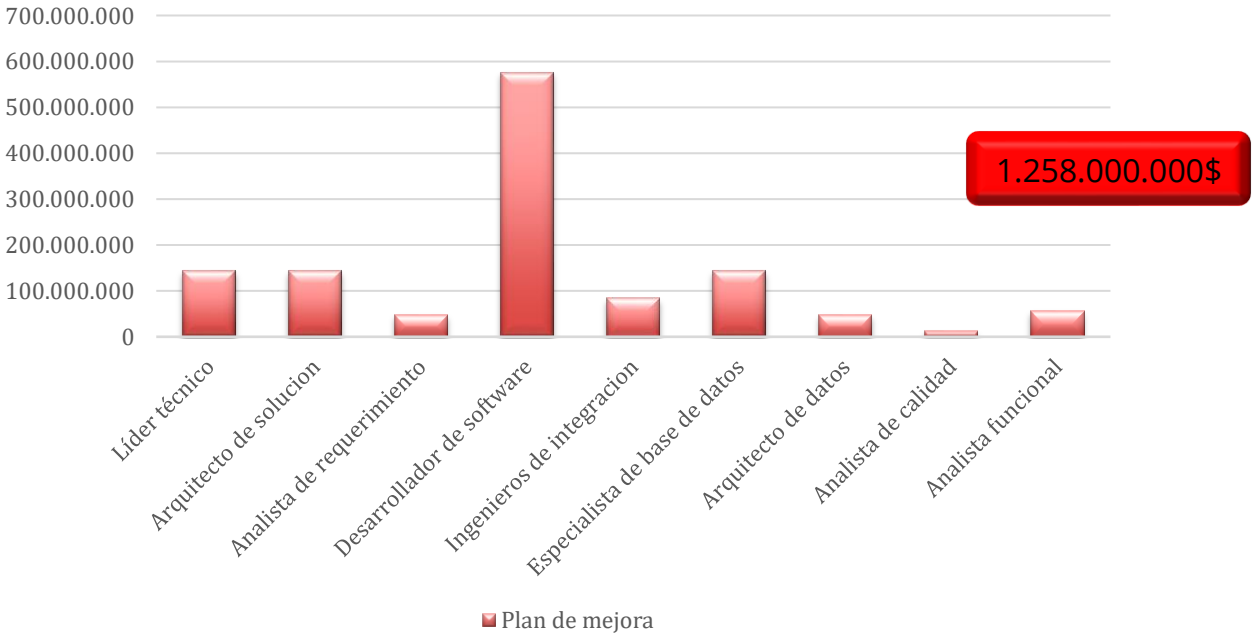


Figura 3

Fortalecimiento de los sistemas de tecnologías

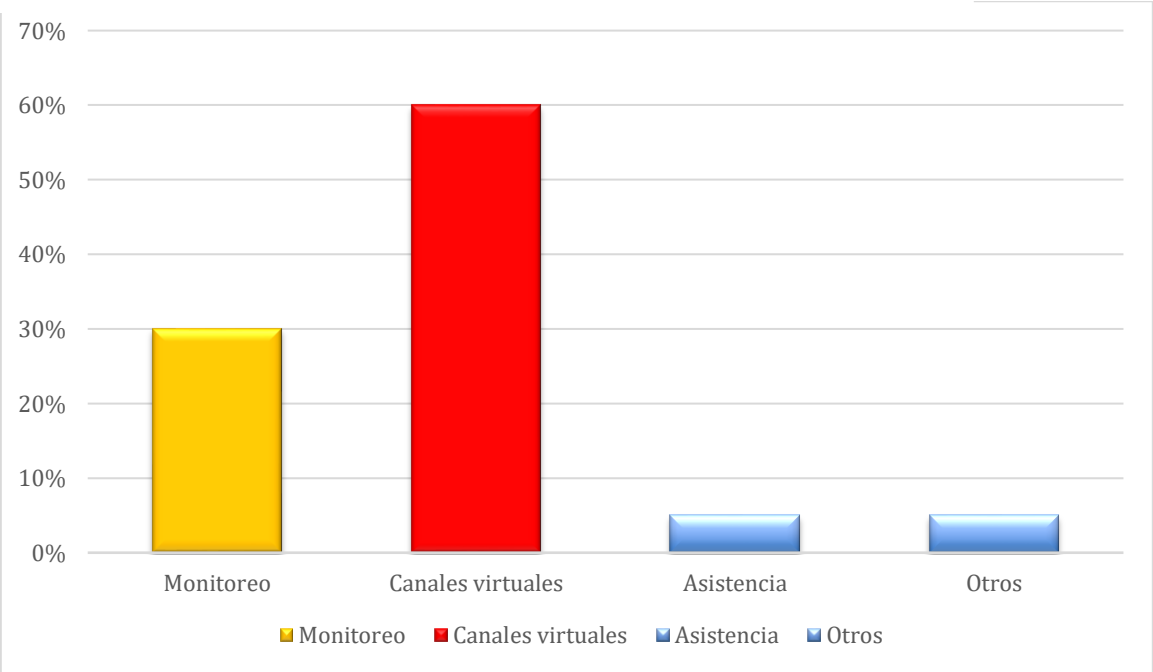


Caso 3: Incidente en el Ministerio de Salud y Protección Social (2023) El grupo cibercriminal Ransomhouse comprometió el datacenter IFX Networks Colombia S.A.S. a través de ataques combinados de phishing y malware, proveedor clave

tecnológico en las aplicaciones misionales del sector salud, lo que provocó la indisponibilidad de las plataformas del ministerio, su impacto en la continuidad de la atención a nivel nacional y el monitoreo de la atención. En esta ocasión se encuentran ausentes los mecanismos de respuesta rápida ante el incidente, así como los costos asociados a las pérdidas. (Figura 4)

Figura 4

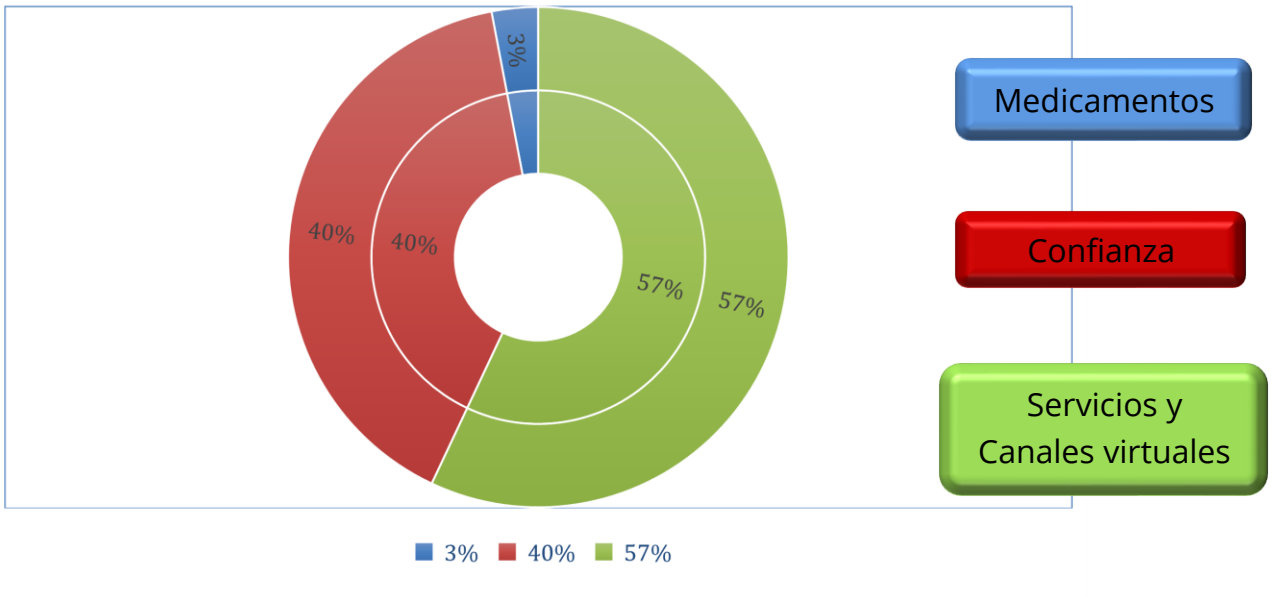
Afectación considerable de la asistencia posterior al conflicto cibernético



Caso 4: Salud Total EPS-S (2024) En el mes de enero de 2024, Salud Total EPS-S reportó haber sido víctima de una ofensiva cibernética externa, la cual generó indisponibilidad de forma parcial de su plataforma tecnológica, afectando a más de 4.8 millones de usuarios; el ataque tuvo como consecuencia la imposibilidad de dar disponibilidad a la información operativa, dificultando la administración de los servicios prestados, impacto en sus usuarios, que ascienden a más de 4,8 millones. (FIGURA 5)

Figura 5

Principales afectaciones externas y consecuencias notorias a la entidad



Impacto Micro y Macroeconómico

Nivel microeconómico (institucional)

Los ciberataques ocasionaron pérdidas operativas muy considerables por la interrupción de servicios esenciales, lo que impactó negativamente en los ingresos de las instituciones. Asimismo, quedaron evidenciados mayores gastos no presupuestarios generados por la restauración de sistemas, compra de tecnología nueva y servicios de consultoría especializada. Adicionalmente, la confianza y relación con los usuarios se deterioraron, afectando la afiliación y retención a largo plazo. Nivel macroeconómico (nacional) A nivel país, los ataques dieron lugar a la desviación de recursos públicos hacia la contingencia por crisis cibernética y la afectación de la asignación presupuestaria original. Además, se identificó una disminución en la productividad del sistema de salud derivada de la afectación de EPS y hospitales con la consecuente pérdida de horas laborales y mayor presión sobre el sistema público. Por otra parte, también se pudo apreciar un creciente y peligroso uso de los sistemas de tecnologías y soluciones extranjeras en el momento de reestablecer sistemas críticos, lo cual dejó en evidencia la vulnerabilidad tecnológica del país

Los casos analizados ponen en evidencia que, desde una perspectiva institucional (es decir, a nivel de las entidades) y, a nivel nacional, estas han evidenciado una clara y significativa afectación negativa. En el plano de la microeconomía, las

entidades afectadas evidenciaron interrupciones operativas y, por lo tanto, pérdidas directas e indirectas, y un deterioro en la confianza y relación con los usuarios. En el plano de la macroeconomía, el redireccionamiento de recursos públicos y el deterioro en la productividad del sistema de salud evidencian costos adicionales por parte del Estado y de los habitantes del país (en este caso, la sociedad civil). Los ataques más prevalentes: Ransomware, Phishing, malware evidentemente han comprometido las infraestructuras críticas, las bases de datos de las historias clínicas, y las plataformas de vigilancia estatal que han evidenciado brechas importantes en ciberseguridad y respuesta institucional. Los resultados ponen de manifiesto la necesidad de robustecer además las capacidades tecnológicas y de gestión institucional dirigidas para asegurar la continuidad y la calidad de los servicios en el sistema general de seguridad social en salud.

Discusión

Los resultados obtenidos en esta investigación ponen de manifiesto la fragilidad persistente del sistema de salud colombiano frente a ciberataques, mostrando, además, una cultura organizacional débil en términos de ciberseguridad. Esta debilidad se evidencia en la ausencia de inversiones sostenidas en nuevas tecnologías, en la escasa capacitación del personal o en unas limitadas estrategias de articulación interinstitucional para gestionas riesgos cibernéticos. Pese a que algunas EPS han establecido planes de contingencia, los mismos se tienden a activar de una forma reactiva, tras un incidente que ya ha tenido lugar, frente a un enfoque de tipo preventivo que recomienda la Organización Mundial de la Salud (OMS, 2022), el cual pone de manifiesto la importancia de contar con medidas preventivas para la mitigación de riesgos antes que se produzcan.

En el contraste, Colombia carece de un plan nacional de ciberseguridad íntegro, articulado y específico para el sector salud, que permita mitigar los altos niveles de riesgo y responder a incidentes de forma colaborativa. Los ataques descritos en este trabajo, en especial los ransomware, phishing o malware, han afectado los sistemas críticos, poniendo en riesgo la no carencia de la información, sino la seguridad y la salud de los pacientes. La pérdida de continuidad de la atención, el quiebre de la supervisión del estado o el deterioro de la reputación institucional son algunas de las consecuencias directas de esta vulnerabilidad.

Finalmente, se hace necesario impulsar una cultura organizacional en el ámbito de ciberseguridad, que contemple la formación constante del recurso humano, la actualización constante de tecnología utilizada, realizar una auditoría de vulnerabilidades contendida en el Plan de Pruebas, implementar planes de respuesta que sean proactivos y coordinados a nivel nacional, y crear un centro nacional de respuesta a incidentes en ciberseguridad como mejora de la capacidad de respuesta del sistema y oportunidad para fomentar el vínculo existente entre la administración pública y privado. Por lo expuesto, la experiencia de Colombia, recogida en los casos revisados, explica perfectamente el ejercicio de reformular las

políticas de ciberseguridad en el sector salud en el sentido de centrarlas en la prevención, en la inversión en tecnología y en la articulación interinstitucional como aspectos importantes en la mejora de la continuidad de las operaciones y la protección de la información de los pacientes y el respeto por sus vidas.

Recomendaciones:

Con base en los hallazgos del actual análisis, se presentan las siguientes sugerencias para incrementar la ciberseguridad en el sistema de salud colombiano y reducir los impactos tanto económicos como operativos de próximos ciberataques: Inversión sostenida en infraestructura y en la gestión de ciberseguridad:

1. Se aconseja la creación de presupuestos permanentes para la prevención de incidentes cibernéticos, tales como la tecnología de última generación, etc. (Gartner, 2024) Cada dólar en prevención puede significar un ahorro de 7 en mitigación y respuesta de crisis.
2. Entrenamiento continuo del capital humano en salud y en tecnología: Se requiere la implementación de programas de capacitación permanente en ciberseguridad para los diversos niveles de los recursos humanos, no solo para los equipos de TI. Esto incluye capacitaciones en buenas prácticas digitales, el reconocimiento de amenazas (como el phishing) y las respuestas a incidentes.
3. Auditorías sobre vulnerabilidades y la gestión de riesgos: Las organizaciones de salud deben llevar a cabo declaraciones periódicas de la seguridad informática, para así dar respuesta a las debilidades que pudieran llegar a existir antes de que éstas sean objeto de aprovechamiento. Dicha auditoría debe ser empleada con equipos de auditoría interna o empresas especializadas con experiencia en el sector de la salud.
4. Actualizar obsolescencias y articular el movimiento hacia sistemas tecnológicos resilientes culturales: Se debe propiciar la progresiva posibilidad de reemplazar tecnologías antiguas, favoreciendo el acceso a la arquitectura de la nube que debe incluir funcionalidades de respaldo automático, redundancia y alta disponibilidad de operación.
5. Creación de un Centro Nacional de Respuesta a Incidentes Cibernéticos que incluiría el CERT en Salud (CERT-Salud): Se propone la creación de este organismo específico y con articulación con el Ministerio de Salud, la Superintendencia Nacional de Salud y la Agencia Nacional Digital para llevar a cabo la respuesta a incidentes, compartir alertas tempranas, generar

protocolos comunes y tejer la cooperación público-privada en materia de ciberseguridad.

La implementación de estas medidas permitirá ir implementando gradualmente un modelo de atención en salud que sea más eficaz, resiliente y dotado para afrontar las cualquier amenaza de tipo digital que surja, manteniendo así la continuidad de los servicios, la protección de los datos e incluso la vida de los pacientes.

Propuesta de Plan Estratégico en Ciberseguridad para el Sector Salud

Para complementar las recomendaciones planteadas, se propone un plan de carácter estratégico, dimensionado en tres ejes que refuercen la resiliencia cibernética de las instituciones del sistema de salud colombiano. Esta propuesta de Plan Estratégico busca orientar la progresiva implementación de acciones concretar y sostenibles en el tiempo.

1. Evaluación Integral de Riesgos. Hay que identificar y gestionar las vulnerabilidades críticas de la infraestructura tecnológica de las instituciones de salud: a) Realizar auditorías internas y externas, incluyendo pruebas de penetración periódicas (pentesting). b) Valorar y actualizar las políticas de acceso a los sistemas, institucionalizando controles de privilegios y autenticación multifactor. c) Analizar y modernizar la infraestructura de hardware y software, priorizando los componentes críticos para la operación clínica y administrativa.
2. Respaldo de Información y Planificadores de Recuperación ante Desastres La capacidad de asegurar continuidad operativa se fundamenta en la capacidad institucional para proteger datos críticos y recuperar actividades de forma rápida ante la existencia de una posible intrusión: Implementarán sistemas, de respaldo seguro, en la que las copias de datos se mantengan fuera de su entorno local y definirán protocolos de recuperación. Mantendrán el alineamiento a esas normas del ámbito nacional e internacional de protección debido a los datos y ciberseguridad. Establecerán relaciones de

proximidad, facilitarán relaciones estratégicas con los proveedores sobre temas de seguridad y recuperación de datos.

3. Controles de Seguridad a priorizar la prevención, sigue siendo la forma más valiosa de enfrentarse a amenazas desde una perspectiva ciberseguridad. Implementarán cifrado de los datos almacenados y en tránsito. Aplicarán segmentación de redes internas para contener las entradas. Desplegarán sistemas de monitoreo en tiempo real y análisis de comportamiento para alertar sobre el comportamiento anómalo

Conclusiones

Los ciberataques que han ocupado la actualidad del sistema de salud colombiano desde 2019 hasta 2024 han puesto de manifiesto las muy importantes implicaciones humanas, operativas y económicas que acarrearían la existencia de una precaria cultura de ciberseguridad, lo que ejemplifican los casos de EPS Sanitas y de la Superintendencia Nacional de Salud, donde los altos costos de la inacción y de la improvisación no son solo financieros, sino que comprometen la continuidad de la atención y la vida de los pacientes.

Se hace un esfuerzo por advertir la urgente necesidad de construcción y puesta en marcha de una política nacional de ciberseguridad de la salud pública, orientada en la prevención, la correcta respuesta y la resiliencia tecnológica, articulando esfuerzos entre EPS, los organismos de control y las autoridades estatales.

La velocidad a la que los ciberdelincuentes crean nuevos métodos hace necesario que las organizaciones mantengan sus infraestructuras tecnológicas al día y que la estrategia avance constantemente.

La implementación de tecnologías avanzadas para mitigar la protección digital, aunadas a la implementación de políticas claras en los esfuerzos de prevención, son claves para tener un bajo nivel de exposición al riesgo.

Como la ciberseguridad es una preocupación mundial, la colaboración interinstitucional —entre EPS, IPS, entidades de gobierno, compañías tecnológicas u organismos internacionales— se hace necesaria para establecer una defensa de ciudad y ayudar a otras organizaciones a planear las mejores acciones para evitar ataques.

El intercambio de información, protocolos, mejores prácticas puede ayudar a la capacidad de respuesta del sector salud y a reducir los efectos derivados de un ataque informático, ya sean económicos, sociales o clínicos.

Finalmente, la transformación digital del sistema de salud no debe romper con la responsabilidad de cuidar sus activos, los cuales son más sensibles, como los datos de los pacientes y la vida misma. La ciberseguridad no debe continuar como un asunto técnico, sino por el contrario se tiene que constituir en un elemento pilar de la gestión en salud pública o privada en Colombia.

Referencias:

Agencia Nacional Digital. (2023). *Estado de la transformación digital en las entidades del sector salud en Colombia*. https://www.agencianacionaldigital.gov.co

ConsultorSalud. (2023). *Ciberataque a EPS Sanitas: afectaciones, pérdidas económicas y respuesta institucional*. https://consultorsalud.com

Heeks, R., & Cuganesan, S. (2020). Resilience, fragility and ICT4D systems: The case of digital health. *Information Systems Journal, 30*(4), 647–678. https://doi.org/10.1111/isj.12270

IBM Security. (2023). *Cost of a data breach report 2023*. IBM Corporation. https://www.ibm.com/reports/data-breach

Ministerio de Salud y Protección Social. (2021). *Informe sobre incidentes de ciberseguridad en la Superintendencia Nacional de Salud*. https://www.minsalud.gov.co

Organización Mundial de la Salud. (2022). *Estrategia mundial sobre salud digital 2020–2025*. https://www.who.int/publications/i/item/9789240020924

Rodríguez, M., & Salazar, L. (2022). Ciberseguridad en el sistema de salud colombiano: un análisis institucional. *Revista Colombiana de Salud Digital, 4*(1), 45–59.

UK National Audit Office. (2018). *Investigation: WannaCry cyber attack and the NHS*. https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/