unicoc
¡EDUCACIÓN...SUPERIOR!

unicoc

COLEGIO ADMINISTRATIVO
Y DE CIENCIAS ECONÓMICAS

CARLOS DAVID CASTAÑEDA MORALES

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

SUSTENTACIÓN

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.

PLANTEAMIENTO DEL PROBLEMA Y JUSTIFICACIÓN

- ¿Cómo afectaron los ciberataques a las entidades de salud y como afecto a la Superintendencia Nacional de Salud y EPS sanitas en términos micro y macro económicos, frente a las medidas de ciberseguridad?

PLANTEAMIENTO DEL PROBLEMA Y JUSTIFICACIÓN

Objetivo General:

- Analizar la afectación de los ciberataques a las entidades de salud y como afecto a la Superintendencia Nacional de Salud y EPS sanitas en términos micro y macro económicos, frente a las medidas de ciberseguridad

Objetivos Específicos:

1. identificar como los ciberataques afectan económicamente y financieramente las entidades principales de salud.
2. describir el impacto económico correctivo, generando recomendaciones para fortalecer la ciberseguridad en el sector salud.
3. evaluar las afectaciones asociados a las intervenciones antero posteriores de EPS sanitas a los hechos.

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.

RESULTADOS

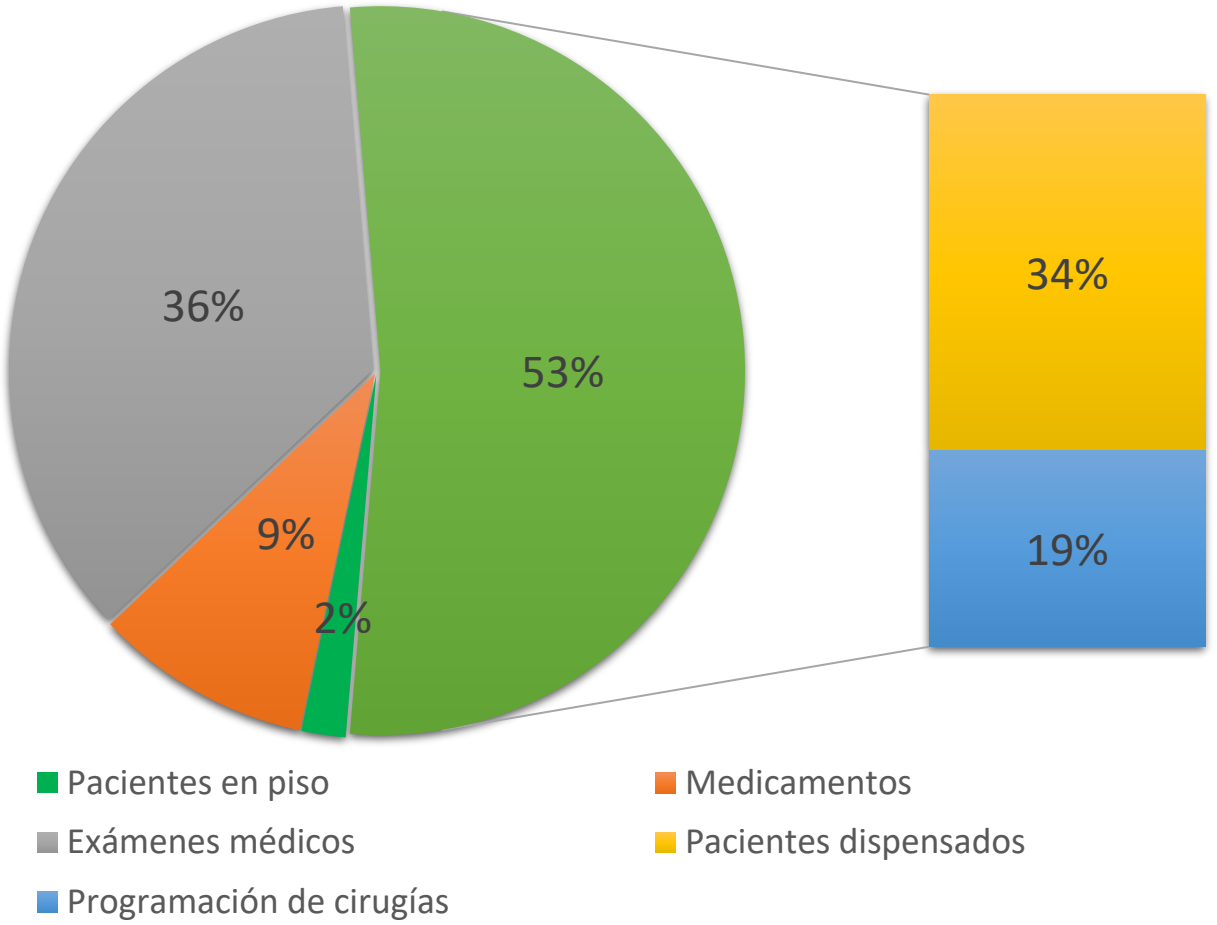
De acuerdo con los objetivos específicos planteados para la presente unidad de trabajo garantizando una adecuada redacción científica a partir de los conocimientos adquiridos, se presentan, a continuación, los resultados del análisis realizado a casos con ciberataques representativos en el sector salud 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

Caso 1: EPS Sanitas (2023)

- Tipo de ataque: Ransomware (White Rabbit)
- Impacto: Paralización de sistemas, imposibilidad de agendar citas o realizar exámenes, pérdida de seguimiento clínico.
- Costo estimado: Hasta USD 1.5 millones directos y pérdidas indirectas por desatención (ConsultorSalud, 2023).
- Reacción institucional: Migración temporal de canales de atención, pérdida de reputación y aumento de quejas de usuarios.

Análisis porcentual de alteraciones por el ciber ataque a EPS sanitas

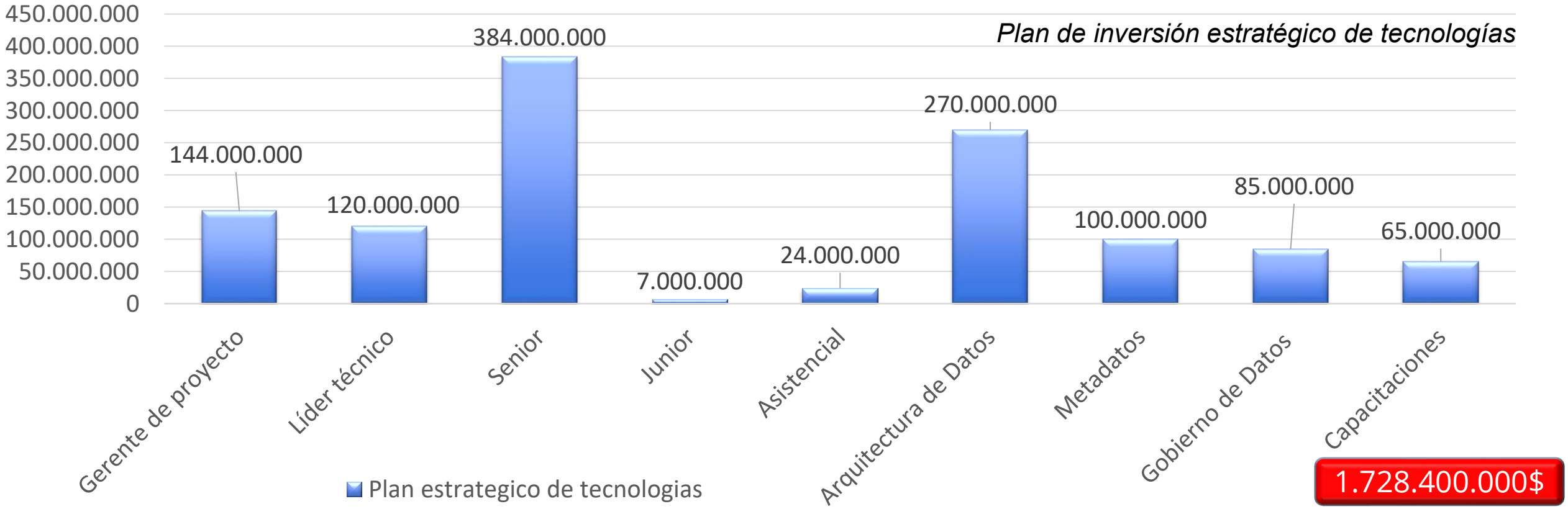


EFECTACION → 293.000 consultas

RESULTADOS

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 (Ministerio de Salud, 2021).

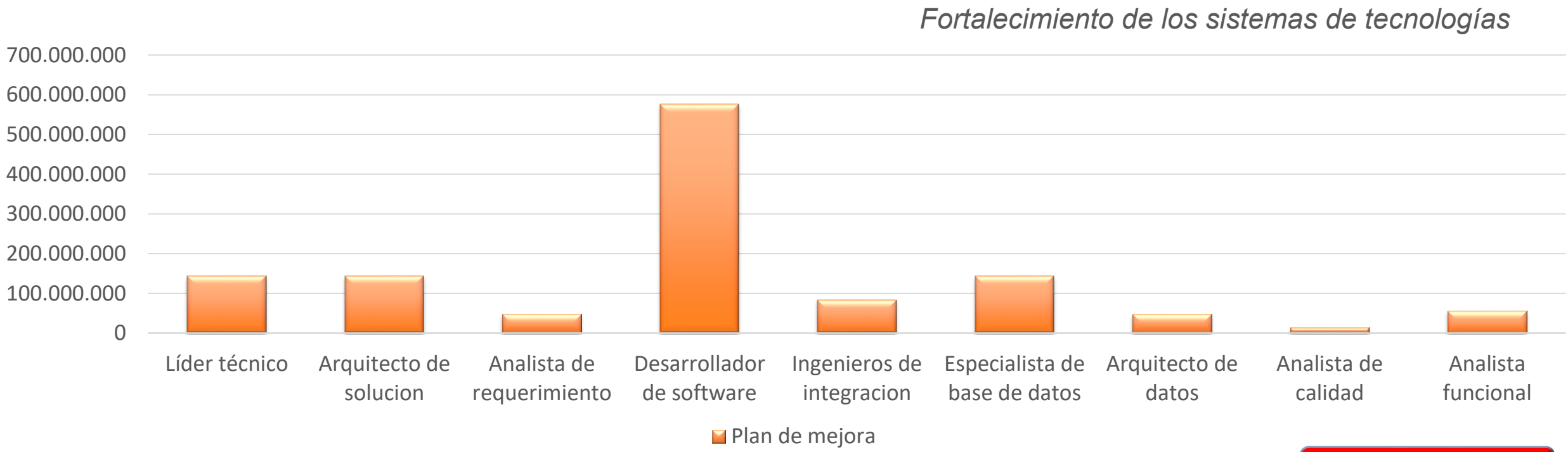


1.728.400.000$

RESULTADOS

Caso 2.

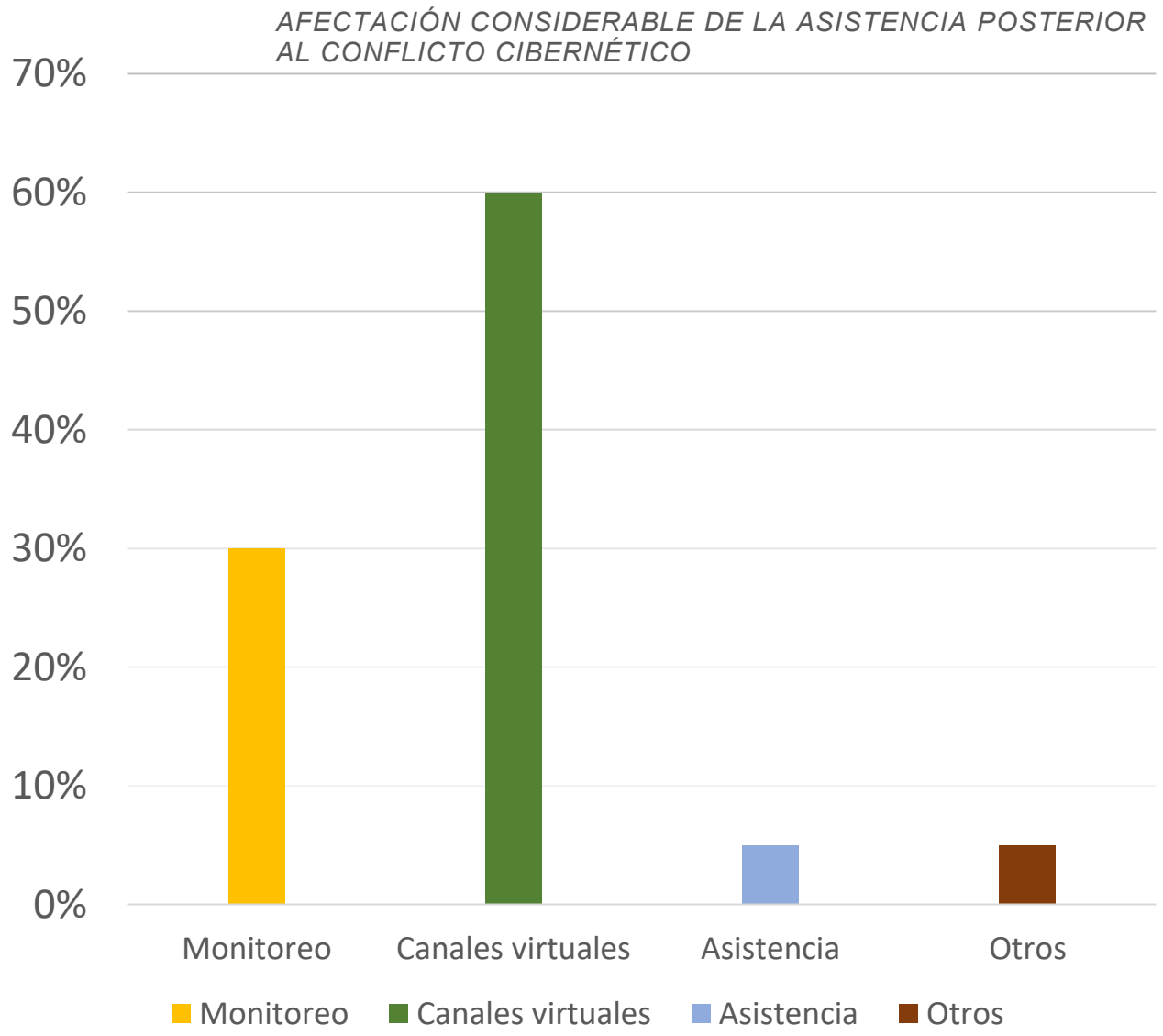
Se destinaron más recursos a fortalecer los sistemas tecnológicos de la entidad. Realizando controles y monitoreos establecidos a la creación de nuevas defensas y actualizaciones tras el ataque incrementado su base económica cerrado brechas de acceso a ciber delincuentes.



1.258.000.000$

Caso 3.

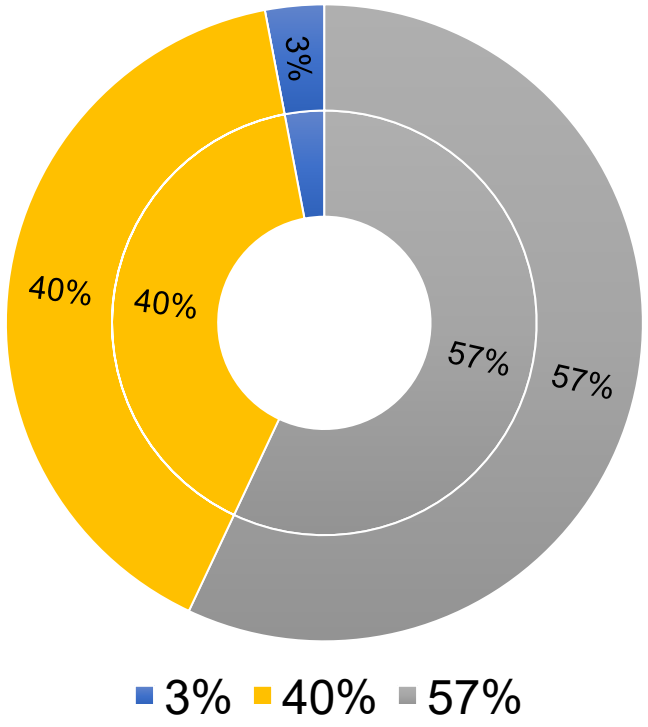
Incidente en el Ministerio de Salud y Protección Social (2023) El grupo cibercriminal Ransomhouse comprometió el datacenter IFX Networks Colombia S.A.S. a través de ataques combinados de phishing y malware, proveedor clave tecnológico en las aplicaciones misionales del sector salud, lo que provocó la indisponibilidad de las plataformas del ministerio, su impacto en la continuidad de la atención a nivel nacional y el monitoreo de la atención.



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.

Principales afectaciones externas y consecuencias notorias a la entidad



PROBLEMAS EN

Medicamentos

Confianza

Servicios y Canales virtuales

Impacto Micro y Macroeconómico

Microeconómico (nivel institucional)

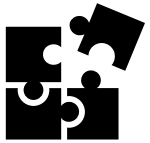
- Pérdidas operativas: Interrupción de servicios esenciales genera disminución en ingresos.
- Gastos no presupuestados: Costos asociados a la restauración de servicios, compra de tecnología emergente y consultoría.
- Reputación y confianza: Afectación en la relación con los usuarios, con impactos a largo plazo en la afiliación y retención.

Macroeconómico (nivel nacional)

- Desviación de recursos: El Estado ha tenido que redireccionar partidas presupuestales para mitigación de crisis cibernéticas.
- Reducción en productividad: La afectación de EPS y hospitales genera pérdida de horas laborales y presión en el sistema público de salud.
- Dependencia tecnológica: Mayor dependencia de soluciones extranjeras para restablecer sistemas críticos.

Impacto Micro y Macroeconómico

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.



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.

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.

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.

Evaluación Integral de Riesgos

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.

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.

Evaluación Integral de Riesgos

Controles de Seguridad a prioridad. 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

PLAN - ESTRATEGICO

1	Evaluación Integral de Riesgos	Identificar vulnerabilidades críticas en la infraestructura tecnológica de estas instituciones	- Realizar auditorías y pruebas de penetración (pentesting) - Evaluar políticas de acceso a sistemas. - Analizar infraestructura de software y hardware.
2	Respaldo y Recuperación ante Desastres	Asegurar la continuidad operativa y proteger datos esenciales de pacientes, afiliados y administrativos	- Mantenerse actualizado sobre normativas de ciberseguridad. - Establecer alianzas con proveedores de seguridad.
3	Controles de Seguridad Proactivos	Fortalecer las defensas para prevenir ciberataques que afecten económica, social y financiera	- Implementar cifrado de datos en reposo y tránsito. - Segmentar redes internas para limitar propagación.

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.

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.

CONCLUSIONES

BIBLIOGRAFIA

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

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