Análisis del impacto de las simulaciones Red Team y Blue Team en la mitigación de vulnerabilidades en los sistemas de historias clínicas electrónicas en Colombia: un enfoque comparativo y adaptativo

Cesar Augusto Diaz De La Hoz

Asesor

Ing. Ever Luis Arroyo Baron

Universidad Nacional Abierta y a Distancia – UNAD

Escuela de Ciencias Básicas, Tecnología e Ingeniería – ECBTI

Especialización en Seguridad Informática

2025

Dedicatoria

Deseo dedicar este trabajo, y todo el esfuerzo que representa, a mi familia, quienes siempre están a mi lado apoyándome en cada proyecto que emprendo. A mi padre, José Díaz, por estar siempre pendiente de mí y ser una fuente constante de inspiración; espero siempre hacerlo sentir orgulloso. A mis hermanos Yadira, Santiago y Alejandra, por su amor incondicional y por estar presentes cuando los necesito. A mi amada esposa Angie, quien me acompaña en este camino y proyecto de vida, entregándome lo mejor de sí para ayudarme a crecer como persona y como hombre. Y a su madre, mi suegra Ana Lucia, cuyo cariño y apoyo constante son un verdadero regalo. A todos ustedes, los amo profundamente.

Resumen

Este estudio analiza el impacto potencial de las simulaciones Red Team y Blue Team en la mitigación de vulnerabilidades en los sistemas de Historias Clínicas Electrónicas (HCE) en Colombia, desde una perspectiva teórica. Ante el creciente número de ciberataques en el sector salud, impulsado por configuraciones deficientes, falta de pruebas de seguridad y ausencia de estrategias proactivas, se plantea la necesidad de examinar enfoques innovadores de ciberseguridad que han mostrado eficacia en otros sectores críticos.

El trabajo se estructura en tres capítulos alineados con los objetivos del estudio: (1) Identificación de vulnerabilidades críticas en los HCE, a partir del análisis de normativas nacionales como la Ley 1581 de 2012, estándares internacionales como la ISO/IEC 27799, y reportes técnicos sobre ciber incidentes en salud; (2) Estudio de las metodologías Red Team y Blue Team, con base en experiencias exitosas en sectores como el financiero, energético y de defensa, para analizar su posible aplicación al contexto colombiano; y (3) Evaluación de la aplicabilidad teórica de dichas simulaciones al sector salud, enfocándose en su efectividad como estrategia preventiva para el fortalecimiento de la resiliencia cibernética.

Como resultado, se propone un modelo conceptual que adapta los ejercicios Red Team y Blue Team al entorno de los HCE en Colombia, acompañado de un informe teórico de vulnerabilidades frecuentes, una metodología adaptada y recomendaciones estratégicas orientadas a reforzar la seguridad de la información médica. Este estudio busca contribuir, desde una aproximación analítica y documental, al diseño de estrategias que fortalezcan la protección de datos sensibles en instituciones del sector salud colombiano.

Palabras clave: Ciberseguridad, Red Team, Blue Team, Historias Clínicas Electrónicas (HCE), Sector Salud, Colombia, Resiliencia Cibernética, Simulaciones De Ciberataques, Análisis Teórico, Vulnerabilidades, Seguridad Informática.

Abstract

This study analyzes the potential impact of Red Team and Blue Team simulations on mitigating vulnerabilities in Electronic Health Records (EHR) systems in Colombia from a theoretical perspective. Given the increasing number of cyberattacks in the healthcare sector, driven by poor configurations, a lack of security testing, and the absence of proactive strategies, there is a need to examine innovative cybersecurity approaches that have proven effective in other critical sectors.

The paper is structured in three chapters aligned with the study's objectives: (1) Identification of critical vulnerabilities in EHRs, based on the analysis of national regulations such as Law 1581 of 2012, international standards such as ISO/IEC 27799, and technical reports on cyber incidents in healthcare; (2) Study of the Red Team and Blue Team methodologies, based on successful experiences in sectors such as finance, energy, and defense, to analyze their potential application in the Colombian context; and (3) Evaluation of the theoretical applicability of these simulations to the healthcare sector, focusing on their effectiveness as a preventive strategy for strengthening cyber resilience.

As a result, a conceptual model is proposed that adapts the Red Team and Blue Team exercises to the EHR environment in Colombia, accompanied by a theoretical report on common vulnerabilities, an adapted methodology, and strategic recommendations aimed at strengthening the security of medical information. This study seeks to contribute, through an analytical and documentary approach, to the design of strategies to strengthen the protection of sensitive data in Colombian healthcare institutions.

Keywords: Cybersecurity, Red Team, Blue Team, Electronic Health Records (EHR), Healthcare Sector, Colombia, Cyber Resilience, Cyberattack Simulations, Theoretical Analysis, Vulnerabilities, Information Security.

Tabla de contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Introducción

En la era digital, la seguridad de la información se ha convertido en un pilar fundamental para la continuidad operativa de las organizaciones, especialmente en sectores críticos como el de la salud. La digitalización de los sistemas médicos ha traído consigo numerosos beneficios, entre ellos la agilización en la gestión de historias clínicas electrónicas (HCE), el acceso en tiempo real a información de los pacientes y la optimización de los procesos hospitalarios. Sin embargo, esta transformación también ha incrementado los riesgos cibernéticos, convirtiendo a las instituciones de salud en objetivos altamente vulnerables a ataques informáticos.

En Colombia, la creciente interconectividad de los hospitales y clínicas ha expuesto a estas entidades a ciberataques que comprometen la privacidad de los pacientes, interrumpen la prestación de servicios médicos y generan pérdidas económicas considerables. Casos como los ataques sufridos por Sanitas en 2022, el secuestro de información del INVIMA o los ciberataques a redes de farmacias han evidenciado la falta de preparación en términos de ciberseguridad en el sector salud. La ausencia de estrategias proactivas y la limitada aplicación de metodologías de evaluación y mitigación de riesgos han permitido que estas amenazas crezcan exponencialmente, afectando la confidencialidad, integridad y disponibilidad de la información médica.

Ante esta problemática, han surgido enfoques avanzados para fortalecer la seguridad digital en entornos críticos, destacándose las metodologías Red Team y Blue Team. Estas estrategias, ampliamente implementadas en sectores como la banca y las telecomunicaciones, han demostrado ser eficaces para identificar y mitigar vulnerabilidades antes de que sean explotadas por atacantes malintencionados. El Red Team se encarga de realizar simulaciones ofensivas, atacando los sistemas para descubrir sus puntos débiles, mientras que el Blue Team

adopta un enfoque defensivo, respondiendo y fortaleciendo la infraestructura digital ante posibles amenazas.

A pesar de los beneficios documentados de estas metodologías, en Colombia su aplicación en el sector salud sigue siendo limitada. La presente investigación busca analizar el impacto potencial de Red Team y Blue Team en la mitigación de vulnerabilidades en los sistemas de HCE, tomando como referencia estudios previos, normativas nacionales e internacionales, y casos de éxito en otros sectores críticos. Para ello, se realizará un análisis comparativo que permitirá evaluar la viabilidad de su implementación en hospitales y clínicas del país.

El estudio se estructura en diferentes apartados. En primer lugar, se contextualiza el problema de la ciberseguridad en el sector salud, exponiendo las amenazas y riesgos actuales. Posteriormente, se presentan los marcos teórico, conceptual y legal, estableciendo la fundamentación científica y normativa de la investigación. Luego, se exploran las estrategias Red Team y Blue Team y su aplicabilidad en la protección de las HCE. Finalmente, se plantean recomendaciones para fortalecer la resiliencia cibernética de las instituciones sanitarias en Colombia.

Este trabajo pretende aportar información valiosa para la formulación de políticas de seguridad en el sector salud, promoviendo el uso de herramientas de evaluación y mitigación de amenazas cibernéticas. Se espera que sus hallazgos sirvan como base para la adopción de estrategias más robustas en la protección de la información médica y la continuidad de los servicios de salud en un entorno digital cada vez más complejo y desafiante.

Planteamiento del Problema

Los sistemas de Historias Clínicas Electrónicas (HCE) han transformado la gestión de la información en el sector salud, permitiendo un acceso más eficiente y seguro a los datos médicos de los pacientes. Sin embargo, esta digitalización también ha incrementado el riesgo de ataques cibernéticos, convirtiéndolos en objetivos prioritarios para ciberdelincuentes debido a la gran cantidad de información sensible que almacenan. La falta de estrategias de ciberseguridad efectivas, unida a configuraciones deficientes y la ausencia de pruebas regulares de seguridad, ha dejado en evidencia importantes vulnerabilidades en estos sistemas.

A nivel global, los ataques cibernéticos contra entidades de salud han ido en aumento en los últimos años, afectando la confidencialidad, integridad y disponibilidad de los datos. Según estudios recientes, el 60% de las instituciones del sector salud carecen de estrategias formales de simulaciones de ciberseguridad, lo que las hace vulnerables a amenazas como ransomware, ataques de denegación de servicio (DoS), accesos no autorizados e inyección de código. En 2021, el Hospital Universitario La Paz en España sufrió un ataque de ransomware que paralizó sus sistemas, afectando la disponibilidad de registros médicos y obligando a adoptar medidas de emergencia para la recuperación de datos (INCIBE, 2023). Esto pone en evidencia que el sector salud sigue siendo vulnerable ante ataques cibernéticos debido a configuraciones deficientes, accesos no autorizados y la falta de pruebas de seguridad.

En Colombia, varios incidentes recientes han puesto en evidencia la fragilidad de la infraestructura cibernética del sector salud. En diciembre de 2022, Sanitas fue víctima de un hackeo que comprometió la información de 242,000 afiliados durante 45 días (Dorado, 2024). Ese mismo año, en octubre, el INVIMA sufrió un secuestro de información, lo que obligó a la suspensión de sus plataformas digitales (Dorado, 2024). En enero de 2023, la red de farmacias

Audifarma fue atacada, comprometiendo su infraestructura tecnológica y afectando la prestación de servicios esenciales (Dorado, 2024). Estos incidentes evidencian la urgencia de implementar medidas de ciberseguridad más robustas que permitan anticipar, detectar y mitigar los riesgos asociados a la digitalización de los servicios de salud.

Las metodologías de Red Team y Blue Team han demostrado ser efectivas en otros sectores críticos, como el financiero y el gubernamental, para evaluar y mejorar la seguridad de los sistemas informáticos. El Red Team se encarga de simular ataques reales para identificar vulnerabilidades, mientras que el Blue Team se enfoca en la detección y respuesta a estos incidentes. Sin embargo, su aplicación en el sector salud colombiano es aún limitada, lo que plantea la necesidad de analizar su impacto potencial en la mitigación de vulnerabilidades en los HCE.

Este estudio busca analizar cómo las simulaciones Red Team y Blue Team pueden contribuir a fortalecer la resiliencia cibernética en el sector salud colombiano, a través de un análisis comparativo con casos de éxito en otros sectores. La evaluación de estas metodologías permitirá identificar estrategias de seguridad aplicables a los HCE, contribuyendo a la protección de la información médica y la continuidad operativa de los servicios de salud.

Dada la creciente sofisticación de los ataques cibernéticos, es fundamental que las instituciones del sector salud adopten enfoques proactivos en seguridad digital, en lugar de reaccionar solo cuando ya han sido comprometidas. La implementación de simulaciones Red Team y Blue Team puede ser una solución clave para cerrar brechas de seguridad y garantizar un manejo más seguro de la información médica en Colombia

¿De qué manera la implementación teórica de simulaciones Red Team y Blue Team, utilizadas exitosamente en sectores, podría contribuir al fortalecimiento de la ciberseguridad en

el sector salud colombiano, particularmente en la protección de los sistemas de Historias Clínicas Electrónicas?

.

Justificación

La digitalización del sector salud ha traído múltiples beneficios en términos de eficiencia y accesibilidad a la información médica, pero también ha incrementado los riesgos asociados a ciberataques y filtraciones de datos sensibles. Los sistemas de Historias Clínicas Electrónicas (HCE), al manejar información confidencial de los pacientes, se han convertido en objetivos recurrentes de ataques como ransomware, accesos no autorizados y ataques de denegación de servicio (DoS). Sin embargo, la mayoría de las instituciones del sector salud en Colombia no cuentan con estrategias estructuradas de ciberseguridad, y menos aún con metodologías formales de simulaciones ofensivas y defensivas, como Red Team y Blue Team, para evaluar y fortalecer sus defensas digitales.

Este estudio es pertinente en el ámbito académico, ya que propone una solución teórica basada en la implementación de simulaciones Red Team y Blue Team en el sector salud, metodologías ampliamente utilizadas en sectores críticos como la banca y las telecomunicaciones, pero con poca documentación en el ámbito hospitalario. A través del análisis comparativo con otros sectores, este estudio contribuirá a la generación de conocimiento en seguridad de la información aplicada a la salud, permitiendo el desarrollo de un modelo conceptual replicable para la evaluación y mitigación de vulnerabilidades en los HCE.

Además, fortalecerá el debate sobre la adopción de normativas y estándares internacionales en ciberseguridad para el sector salud, promoviendo la implementación de marcos regulatorios como la ISO 27799, el NIST Cybersecurity Framework y la Ley 1581 de 2012, en la gestión de riesgos y protección de datos médicos.

Desde una perspectiva social, la seguridad de los HCE es clave para la confianza del paciente en los sistemas de salud digitales. La filtración o alteración de información médica no

solo vulnera la privacidad de los usuarios, sino que también puede comprometer la atención médica, afectando diagnósticos, tratamientos y procedimientos clínicos. Un ataque cibernético exitoso podría resultar en la interrupción de servicios hospitalarios, poniendo en riesgo la vida de los pacientes.

Este estudio busca aportar herramientas que permitan fortalecer la protección de los datos médicos y garantizar la disponibilidad de los sistemas de salud en Colombia. La aplicación de metodologías Red Team y Blue Team facilitará la detección y corrección proactiva de vulnerabilidades, en lugar de que las instituciones reaccionen únicamente cuando los ataques ya han ocurrido.

En el ámbito disciplinario, la investigación permitirá que hospitales, clínicas y entidades reguladoras adopten un enfoque estructurado para evaluar sus sistemas de seguridad. La formulación de un modelo conceptual basado en simulaciones Red Team y Blue Team facilitará la toma de decisiones estratégicas en resiliencia cibernética, promoviendo la implementación de políticas de seguridad que se alineen con las mejores prácticas internacionales.

Además, este estudio tiene una gran aplicabilidad práctica, ya que proporcionará una metodología adaptada que podrá ser utilizada por profesionales de ciberseguridad en el sector salud. Esto fomentará el desarrollo de estrategias más efectivas para la prevención de ataques y garantizará un mayor nivel de preparación frente a amenazas futuras.

Dado el incremento de ataques cibernéticos en el sector salud y la falta de estrategias proactivas de defensa, este estudio es necesario para evaluar cómo las simulaciones Red Team y Blue Team pueden contribuir a la protección de los HCE en Colombia. La formulación de un modelo conceptual adaptado al sector salud fortalecerá la seguridad digital de las instituciones

médicas, asegurando la confidencialidad, integridad y disponibilidad de los datos de los pacientes y promoviendo un ecosistema de salud digital más seguro.

Objetivos

Objetivo General

Analizar el impacto potencial de las simulaciones Red Team y Blue Team en la mitigación de vulnerabilidades en los sistemas de HCE, basándose en estudios previos y adaptaciones metodológicas, con el fin de evaluar su efectividad y viabilidad en el fortalecimiento de la seguridad en el sector salud.

Objetivos Específicos

Identificar las principales vulnerabilidades en los sistemas de Historias Clínicas Electrónicas en Colombia, con base en reportes oficiales, estudios académicos y marcos regulatorios, para comprender los riesgos más críticos.

Estudiar los principios y metodologías de simulaciones Red Team y Blue Team en el contexto de seguridad de la información, comparándolos con casos de éxito en otros sectores críticos, con la finalidad de analizar su aplicabilidad en el sector salud.

Examinar la efectividad de la aplicabilidad de estas simulaciones al sector salud colombiano, con el fin de medir su impacto en la mejora de la ciberseguridad.

Marco Referencial

Antecedentes

Los ejercicios Red Team y Blue Team han sido implementados en diversos sectores críticos para evaluar y fortalecer la ciberseguridad. En el ámbito militar, estudios como Exploring the Potential of Large Language Models for Red Teaming in Military Coalition Networks (2023) han analizado cómo la inteligencia artificial puede mejorar las capacidades de los equipos ofensivos y defensivos en simulaciones de ataques cibernéticos. Este enfoque ha sido clave para fortalecer la seguridad en redes críticas y puede ofrecer lecciones aplicables al sector salud.

En el sector financiero, el uso de Red Teaming ha demostrado ser una estrategia eficaz para anticipar y mitigar riesgos de ciberseguridad, los bancos han implementado pruebas de penetración avanzadas para evaluar su capacidad de respuesta ante ataques reales, lo que ha llevado a mejoras significativas en la detección y mitigación de amenazas. La adaptación de estas estrategias al sector salud podría contribuir a la protección de los HCE y a la continuidad operativa de los servicios médicos.

En Colombia, investigaciones previas han abordado la necesidad de mejorar la ciberseguridad en el sector salud. Estudios como el de Zambrano Velillo y Mora Velandia (2024) han resaltado la importancia de adoptar estándares internacionales como la ISO 27799 para garantizar la protección de la información médica. Sin embargo, aún existe una brecha significativa en la implementación de metodologías ofensivas y defensivas para la evaluación de vulnerabilidades en los HCE.

Este estudio busca cerrar esa brecha mediante un análisis comparativo con sectores críticos, proporcionando prácticas que faciliten la adopción de estrategias Red Team y Blue Team en instituciones médicas colombianas.

Marco Conceptual

El marco conceptual de este estudio se basa en la aplicación de metodologías de ciberseguridad para evaluar y fortalecer la resiliencia digital de los sistemas de Historias Clínicas Electrónicas (HCE) en el sector salud colombiano. Para ello, es necesario definir conceptos clave y su aplicación dentro del ámbito de la seguridad informática en entornos médicos.

Ciberseguridad en el Sector Salud

La ciberseguridad es la disciplina encargada de proteger la confidencialidad, integridad y disponibilidad de la información digital ante accesos no autorizados, ataques malintencionados y fallos técnicos. Según López (2024), la protección de la información médica en sistemas digitales debe cumplir con estrictos estándares de seguridad debido a su sensibilidad y valor en el mercado negro. En el sector salud, la ciberseguridad es un pilar fundamental para garantizar que los datos de los pacientes no sean manipulados, alterados o secuestrados por ciberdelincuentes.

Red Team

Grupo ofensivo que simula ataques cibernéticos para detectar vulnerabilidades antes de que sean explotadas por actores malintencionados. En el sector salud, un equipo Red Team puede evaluar la resistencia de los sistemas de HCE contra ataques de ransomware, ingeniería social o accesos no autorizados.

Características y Pasos

Planificación. Definición de objetivos y alcance de las pruebas, considerando las particularidades del entorno sanitario.

Reconocimiento. Recolección de información sobre la infraestructura y sistemas del objetivo.

Explotación. Intento de comprometer sistemas utilizando las vulnerabilidades identificadas.

Análisis. Evaluación de los resultados para determinar el impacto potencial de las brechas de seguridad.

Informe. Documentación de hallazgos y recomendaciones para mitigar las vulnerabilidades descubiertas.

Desafíos y Limitaciones

Posible interrupción de servicios críticos durante las pruebas.

Necesidad de autorización y coordinación para evitar conflictos con operaciones normales.

Requiere personal altamente capacitado y conocimiento específico del sector salud.

Blue Team

Grupo defensivo encargado de monitorear, detectar y responder a amenazas en tiempo real. Su labor en hospitales y clínicas se centra en la prevención de ataques mediante la implementación de controles de seguridad avanzados, como autenticación multifactor, segmentación de redes y análisis de registros de actividad.

Características y Pasos

Monitoreo Continuo. Supervisión constante de redes y sistemas para detectar actividades sospechosas.

Análisis de Amenazas. Evaluación de eventos para identificar posibles amenazas y su gravedad.

Respuesta a Incidentes. Implementación de acciones para contener y mitigar los efectos de los incidentes de seguridad.

Recuperación. Restablecimiento de sistemas y servicios afectados, asegurando su funcionamiento normal.

Mejora Continua. Actualización de políticas y procedimientos basados en lecciones aprendidas de incidentes anteriores.

Vulnerabilidades Abordadas con Red Team y Blue Team en el Sector Salud

El sector salud es un blanco atractivo para los ciberdelincuentes debido a la gran cantidad de información sensible almacenada en sus sistemas. A continuación, se presentan las principales vulnerabilidades que pueden ser detectadas y mitigadas mediante la aplicación de Red Team y Blue Team:

Ataques de Ransomware

Secuestro de datos médicos a cambio de un rescate, afectando la operatividad de los hospitales.

Accesos No Autorizados

Falta de autenticación robusta que permite a atacantes ingresar a los sistemas de HCE sin permisos.

Inyección de Código (SQL/XSS)

Explotación de vulnerabilidades en bases de datos y aplicaciones web médicas.

Denegación de Servicio (DoS/DDoS)

Saturación de servidores hospitalarios que impide el acceso a registros médicos.

Amenazas Internas

Empleados negligentes o malintencionados que filtran información médica sensible.

Marco Teórico

Evolución de la Ciberseguridad

La ciberseguridad ha evolucionado significativamente desde sus inicios hasta la actualidad. En sus primeras etapas, cuando las computadoras eran sistemas aislados sin conexión a redes externas, la seguridad informática se limitaba a la protección física de los equipos y el control de accesos. Con la llegada del Internet en la década de 1980, surgieron las primeras amenazas informáticas, como virus y gusanos, lo que llevó al desarrollo de soluciones antivirus y cortafuegos básicos.

En la década de 2000, con el auge de la conectividad global y la digitalización de los datos, los ataques cibernéticos se volvieron más sofisticados y dirigidos. Las grandes empresas y gobiernos comenzaron a implementar estrategias de seguridad más avanzadas, incluyendo el cifrado de datos, la autenticación multifactor y los sistemas de detección de intrusos. En la actualidad, la ciberseguridad es una disciplina altamente especializada que abarca inteligencia artificial para detección de amenazas, monitoreo en tiempo real y estrategias de Red Team y Blue Team para evaluar y fortalecer la resiliencia cibernética de las organizaciones.

Concepto de Ciberseguridad

La ciberseguridad se define como el conjunto de prácticas, procesos y tecnologías diseñadas para proteger sistemas, redes y datos contra accesos no autorizados, ataques maliciosos y fallos de seguridad. Su objetivo principal es garantizar la confidencialidad, integridad y disponibilidad de la información digital, protegiéndola contra robo, manipulación o destrucción.

En el sector salud, la ciberseguridad es especialmente crítica debido a la naturaleza sensible de los datos almacenados en los sistemas de Historias Clínicas Electrónicas (HCE). La

exposición de esta información no solo afecta la privacidad de los pacientes, sino que también puede comprometer la prestación de servicios médicos esenciales.

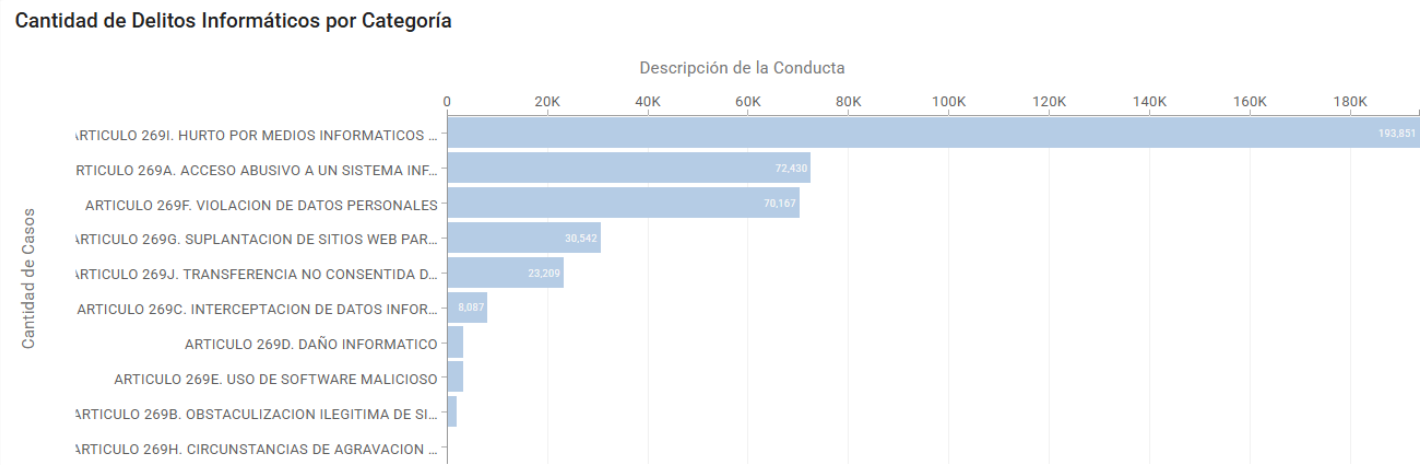
Panorama de los Delitos Informáticos en Colombia

Análisis de Estadísticas de Delitos Informáticos en Colombia (2006–2025)

El estudio de los delitos informáticos en Colombia requiere comprender tanto el marco legal que los tipifica como la evolución estadística de su comportamiento a lo largo del tiempo. De acuerdo con la legislación colombiana, los delitos informáticos se encuentran definidos en el Título VII BIS del Código Penal Colombiano, bajo el epígrafe “De la protección de la información y de los datos” (Ley 599 de 2000, artículos 269A al 269J). Las categorías utilizadas para clasificar los delitos en las siguientes figuras corresponden directamente a dichas tipificaciones legales, las cuales incluyen: acceso abusivo a un sistema informático, obstaculización ilegítima de sistema informático o red de telecomunicaciones, interceptación de datos, daño informático, uso de software malicioso, violación de datos personales, suplantación de sitios web, hurto por medios informáticos, y transferencia no consentida de activos.

Figura 1

Cantidad de Delitos Informáticos Registrados en Colombia por Categoría (2006–2025)



Nota. Esta figura muestra la distribución de los delitos informáticos en Colombia clasificados por artículo del Código Penal. Se destacan los delitos más frecuentes, como el hurto por medios informáticos (Artículo 269I) y el acceso abusivo a un sistema informático (Artículo 269A). La fuente de los datos es el portal de Datos Abiertos, y la información ha sido agrupada para facilitar su análisis comparativo. https://www.datos.gov.co/Seguridad-y-Defensa/DELITOS-INFORM-TICOS/4v6r-wu98/about_data

La figura 1 muestra la frecuencia de los delitos informáticos en Colombia según las categorías establecidas en el Título VII BIS del Código Penal Colombiano (Ley 599 de 2000, Art. 269A al 269J), permitiendo identificar cuáles conductas punibles son más comunes en el entorno digital colombiano. El análisis revela que el hurto por medios informáticos (artículo 269I) es, con gran diferencia, el delito más reportado, acumulando 193.851 casos, lo que representa una porción dominante dentro del espectro de cibercriminalidad registrada. Esto evidencia el alto grado de aprovechamiento ilícito de sistemas digitales con fines económicos, donde los delincuentes explotan brechas de seguridad en plataformas bancarias, comerciales y gubernamentales para desviar activos sin consentimiento.

El acceso abusivo a un sistema informático (art. 269A) ocupa el segundo lugar, con 72.430 casos. Esta cifra es indicativa de la facilidad con la que actores no autorizados logran vulnerar sistemas informáticos, muchas veces a través de contraseñas débiles, accesos mal configurados o phishing. Le sigue muy de cerca la violación de datos personales (art. 269F), con 70.167 casos, lo cual subraya una problemática creciente en la protección de la privacidad digital, especialmente en sectores que manejan información sensible como el de salud, educación y finanzas.

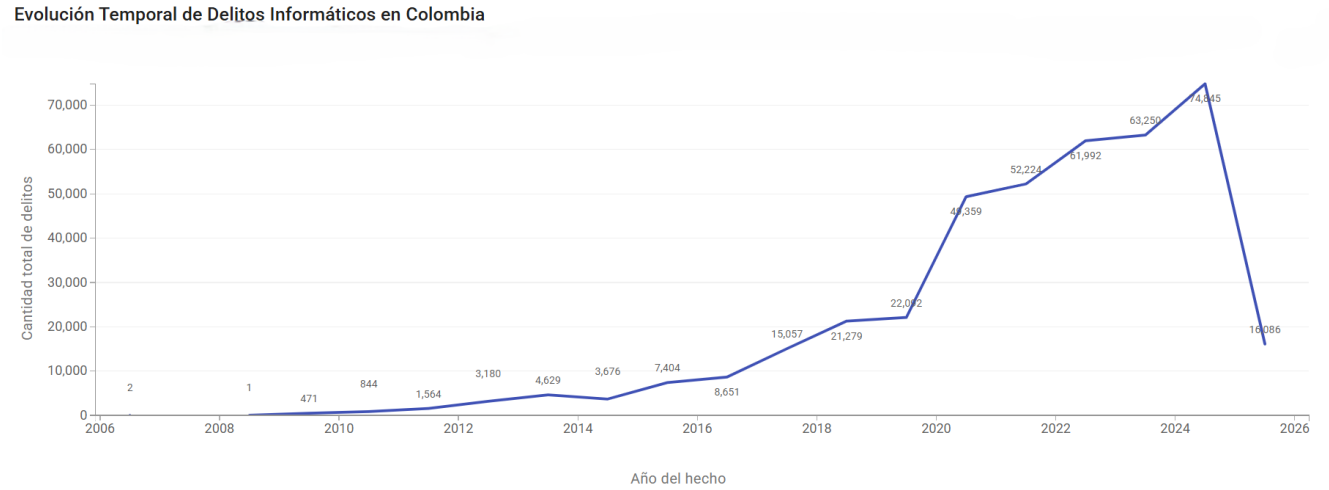
Otros delitos con una alta incidencia son la suplantación de sitios web (art. 269G), con 30.542 casos, y la transferencia no consentida de activos (art. 269J), con 23.209 casos. Ambas modalidades reflejan la sofisticación de técnicas como el phishing avanzado y la manipulación de interfaces digitales para robar identidades o desviar recursos económicos de las víctimas. Delitos como la interceptación de datos (art. 269C) y el daño informático (art. 269D) presentan cifras más moderadas (8.087 y menos de 5.000 casos, respectivamente), aunque siguen siendo relevantes en ataques que comprometen la integridad o confidencialidad de la información.

Finalmente, delitos como el uso de software malicioso (art. 269E) y la obstaculización ilegítima de sistemas (art. 269B) muestran cifras más bajas, posiblemente por las dificultades técnicas para rastrear o categorizar estos hechos, o por la falta de denuncia o comprensión del delito por parte de las víctimas.

Es importante reiterar que estos datos solo reflejan los casos que han sido denunciados y judicializados, por lo que se estima que la cifra real podría ser considerablemente más alta, dada la subnotificación común en este tipo de delitos. Muchas víctimas no denuncian por desconocimiento, miedo al desprestigio o la falta de confianza en el sistema judicial.

Figura 2

Evolución de los Delitos Informáticos en Colombia por Año (2006–2025)



Nota. Esta figura presenta la evolución anual de los delitos informáticos registrados en Colombia. Se observa el comportamiento de estos delitos a lo largo del tiempo, permitiendo identificar posibles tendencias, incrementos y periodos de mayor ocurrencia. Los datos provienen del portal de Datos Abiertos del gobierno colombiano. https://www.datos.gov.co/Seguridad-y-Defensa/DELITOS-INFORM-TICOS/4v6r-wu98/about_data

La figura 2 evidencia una evolución significativa de los delitos informáticos en Colombia entre los años 2006 y 2025. En los primeros años del periodo (2006–2010), los registros son marginales, con apenas 2 casos reportados en 2006 y 1 en 2008. Sin embargo, a partir de 2011 se observa un crecimiento progresivo: de 844 casos ese año, se pasó a 1.564 en 2012, lo que representa un incremento del 85%, y a 3.180 en 2013, duplicando casi la cifra del año anterior.

Durante el periodo 2016–2019, se aprecia un crecimiento sostenido en los reportes, pasando de 8.651 delitos en 2016 a 21.279 en 2019. No obstante, el punto de inflexión más drástico se da en 2020, coincidiendo con la pandemia por COVID-19, cuando los delitos

informáticos se disparan a 46.359 casos, más del doble respecto al año anterior. Esta cantidad se mantiene en 2021 con 52.224 delitos y alcanza un máximo histórico de 74.845 en 2024.

Este aumento puede explicarse por el incremento masivo en el uso de tecnologías digitales, impulsado por el teletrabajo, la educación virtual, la migración de servicios financieros y gubernamentales al entorno digital, y el aumento de la dependencia tecnológica de la población. Este entorno fue aprovechado por ciberdelincuentes para ejecutar delitos como el phishing, la suplantación de identidad, la interceptación de datos personales y financieros, y fraudes electrónicos.

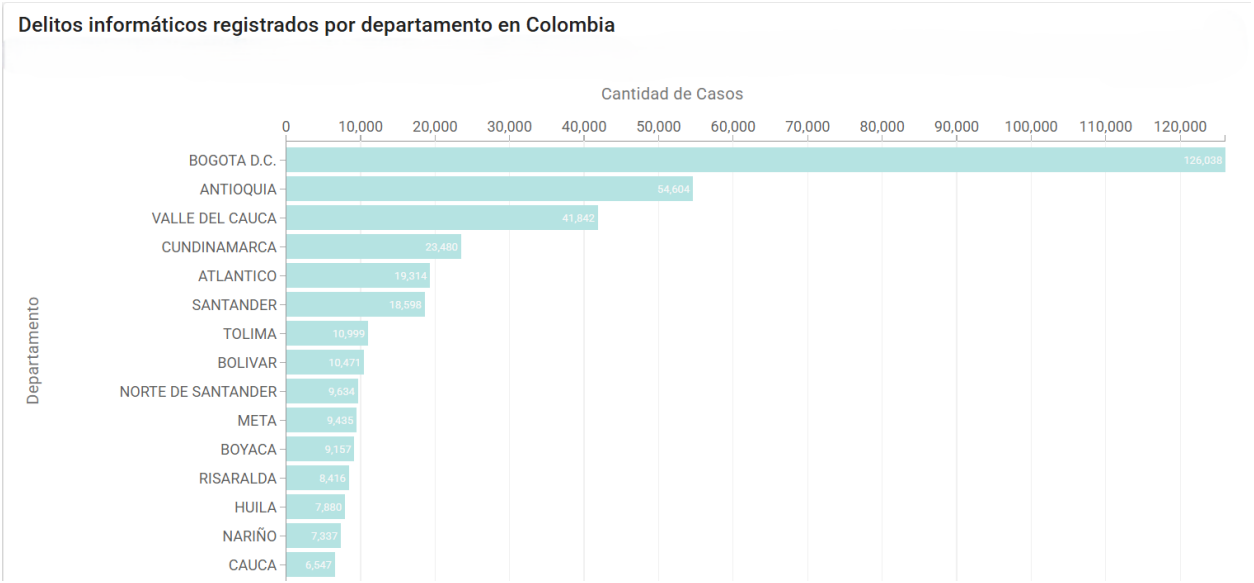
La tendencia general muestra que, pese a los esfuerzos en materia de legislación, estrategias de prevención y mejoras en infraestructura tecnológica, la criminalidad digital ha crecido a un ritmo más acelerado que la capacidad de respuesta institucional. La cifra de 74.845 delitos en 2024 representa un aumento de más del 8.700% respecto al año 2011.

Por otro lado, el año 2025 refleja una caída abrupta en el número de casos reportados, con un total de 16.086 delitos. Este descenso, aunque significativo, debe interpretarse con cautela, ya que podría deberse a factores como el subregistro (posiblemente porque los datos del año aún están en consolidación), adicional a que este número de casos es enorme en contraste a que apenas han transcurrido 5 meses del año. No se puede asumir aún una disminución real de la amenaza sin una evaluación completa del contexto.

La evolución mostrada resalta la necesidad urgente de fortalecer las capacidades técnicas, humanas y legales para enfrentar los delitos informáticos. La tendencia ascendente en los últimos años (2017–2024), particularmente entre 2020 y 2024, exige políticas públicas más agresivas, la consolidación de una cultura de ciberseguridad, y la formación continua de personal especializado que permita hacer frente a un fenómeno que crece en complejidad y volumen.

Figura 3

Delitos Informáticos Registrados Por Departamento en Colombia (2006-2025)



Nota. Esta figura muestra la cantidad total de delitos informáticos registrados en Colombia, agrupados por departamento. Se observa una concentración significativa en Bogotá D.C., seguida por Antioquia y el Valle del Cauca. Los datos provienen del portal de Datos Abiertos de Colombia y permiten identificar las regiones con mayor incidencia, facilitando el análisis territorial de estos delitos. https://www.datos.gov.co/Seguridad-y-Defensa/DELITOS-INFORM-TICOS/4v6r-wu98/about_data

La figura 3 analiza la distribución geográfica de los delitos informáticos en Colombia, permitiendo la verificación los departamentos más afectados. Identificando las regiones más impactadas por este fenómeno. Destaca de forma contundente Bogotá D.C. con 126.038 casos registrados, lo que representa una cifra significativamente superior al resto de los departamentos. Le siguen Antioquia (54.604 casos) y Valle del Cauca (41.842 casos), consolidándose como los tres principales focos de criminalidad digital en el país. Esta concentración puede explicarse por varios factores estructurales: mayor densidad poblacional, mayor penetración de internet, fuerte

presencia institucional, y alto volumen de actividades financieras, comerciales y administrativas digitalizadas.

Posterior, se encuentran Cundinamarca (23.480 casos), Atlántico (19.314 casos) y Santander (18.598 casos), departamentos que también presentan una actividad considerable. El caso de Cundinamarca puede entenderse en relación directa con su cercanía a la capital y el ecosistema digital que allí se desarrolla, mientras que Atlántico y Santander reflejan el crecimiento de las amenazas digitales en polos regionales estratégicos del Caribe y el nororiente del país.

Llama la atención la notable presencia de departamentos como Tolima (10.999 casos), Bolívar (10.471 casos), Norte de Santander (9.634 casos) y Meta (9.435 casos), que, si bien no lideran en conectividad nacional, muestran una incidencia creciente. Esto sugiere una expansión territorial de los delitos informáticos más allá de los grandes centros urbanos, lo cual es un indicador de alerta para las autoridades y los diseñadores de políticas públicas.

Además, se observa que otros departamentos como Boyacá (9.157 casos), Risaralda (8.416 casos), Huila (7.880 casos), Nariño (7.337 casos) y Cauca (6.547 casos) no están exentos de esta problemática, lo que evidencia que la criminalidad digital está permeando todo el territorio nacional.

Es fundamental subrayar que estos valores corresponden únicamente a los delitos que han sido denunciados y registrados oficialmente. Como se ha documentado en múltiples estudios sobre cibercrimen, existe un subregistro significativo debido al desconocimiento de las víctimas, la baja tasa de denuncia por temor, la normalización de ciertos delitos digitales o la falta de capacidades para identificar adecuadamente los incidentes. Por tanto, la magnitud real de la problemática puede ser aún mayor que la que muestran las cifras oficiales.

Este análisis pone de manifiesto la urgente necesidad de descentralizar los esfuerzos de ciberseguridad y llevar capacidades técnicas, judiciales y educativas a todas las regiones del país. La formación de jueces, fiscales, cuerpos de policía y ciudadanía en general es clave para mejorar la prevención, la denuncia y la judicialización de estos delitos. Asimismo, la distribución de los delitos por departamentos permite identificar focos regionales y territoriales específicos que deben ser abordados con estrategias focalizadas, articuladas y sostenibles, en un esfuerzo conjunto entre gobierno, academia, sector privado y sociedad civil.

Amenazas Cibernéticas Comunes en el Sector Salud

Los sistemas de salud han sido blanco de múltiples ataques cibernéticos debido al alto valor de la información médica en el mercado negro. Las principales amenazas incluyen:

Ransomware: Software malicioso que cifra los archivos y exige un pago para su recuperación. Ejemplo: El ataque de ransomware WannaCry en 2017 afectó a más de 80 hospitales en el Reino Unido, paralizando sus operaciones.

Phishing: Correos electrónicos fraudulentos que buscan engañar a los empleados para robar credenciales o instalar malware.

Ataques de Denegación de Servicio (DDoS): Inundación de tráfico malicioso que colapsa los sistemas hospitalarios, impidiendo el acceso a datos esenciales.

Accesos No Autorizados: Robo de credenciales o explotación de configuraciones deficientes para infiltrarse en los sistemas.

Dispositivos Médicos Inseguros: Equipos como monitores de pacientes y bombas de insulina que pueden ser hackeados para alterar sus funciones o extraer información.

Costos Asociados a los Incidentes Cibernéticos

Los ataques cibernéticos en el sector salud no solo generan pérdida de datos y problemas operativos, sino que también imponen costos financieros elevados. Según un informe de IBM (2023), el costo promedio de una filtración de datos en el sector salud es de 10.93 millones de dólares, lo que lo convierte en la industria más afectada financieramente por ciberataques, estos incluyen los siguientes ejemplos:

Pago de rescates: Organizaciones atacadas con ransomware han llegado a pagar hasta millones de dólares para recuperar sus datos.

Pérdidas operativas: Interrupción de servicios médicos, cancelación de citas y retrasos en tratamientos.

Demandas y sanciones legales: Multas por incumplimiento de regulaciones de protección de datos, como la HIPAA en EE.UU. o la Ley 1581 en Colombia.

Daño reputacional: Pérdida de confianza de los pacientes y disminución de la credibilidad de la institución de salud.

Prácticas Actuales en Ciberseguridad

Para mitigar estos riesgos, los hospitales y clínicas están adoptando múltiples estrategias de seguridad:

Autenticación Multifactor (MFA): Uso de múltiples capas de verificación para acceder a sistemas críticos.

Cifrado de Datos: Protección de la información médica mediante algoritmos avanzados de cifrado.

Monitoreo en Tiempo Real: Implementación de sistemas de detección de intrusos (IDS) y Security Information and Event Management (SIEM).

Capacitación en Ciberseguridad: Entrenamiento regular del personal médico y administrativo en prácticas de seguridad.

Desafíos y Limitaciones de Red Team y Blue Team

Si bien la implementación de Red Team y Blue Team aporta beneficios significativos en la protección de datos, también enfrenta desafíos importantes:

Costo de Implementación: La contratación de profesionales y el desarrollo de simulaciones requieren inversiones considerables.

Complejidad Técnica: Se necesita personal altamente capacitado con conocimientos avanzados en ciberseguridad.

Posibles Interrupciones: Las simulaciones pueden afectar la disponibilidad de los servicios médicos si no se gestionan adecuadamente.

Evolución de las Amenazas: Los ciberdelincuentes desarrollan constantemente nuevas técnicas de ataque, lo que exige una actualización continua de las estrategias de defensa.

Marco Legal

La ciberseguridad en el sector salud es un aspecto crítico que requiere la regulación y aplicación de normativas específicas para garantizar la protección de la información médica, la privacidad de los pacientes y la continuidad operativa de los servicios sanitarios. En Colombia, existen leyes y decretos que regulan el manejo de datos personales y la seguridad digital en infraestructuras críticas como hospitales y clínicas. Asimismo, a nivel internacional, se han establecido estándares y marcos regulatorios que sirven de referencia para mejorar la resiliencia cibernética en el sector salud, por lo que se expondrán algunas normativas nacionales e internacionales relacionadas con el sector salud, así:

Normativas Nacionales en Colombia

Ley 1581 de 2012 - Protección de Datos Personales

Esta ley es la principal normativa en Colombia sobre la protección de datos personales, estableciendo derechos y obligaciones para garantizar la privacidad y seguridad de la información de los ciudadanos. En el contexto de las Historias Clínicas Electrónicas (HCE), esta ley exige que las instituciones de salud implementen medidas adecuadas para proteger la confidencialidad, integridad y disponibilidad de los datos médicos de los pacientes. Las clínicas y hospitales deben garantizar que la información médica solo sea accesible por personal autorizado y bajo condiciones seguras, siendo importante mencionar el literal g) del artículo 4° que reza "(…) Principio de seguridad: La información sujeta a Tratamiento por el Responsable del Tratamiento o Encargado del Tratamiento a que se refiere la presente ley, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento*; (...)"*, (comillas fuera del texto).

Principales Disposiciones:

- Definición de la información médica como dato sensible que requiere protección especial.
- Obligación de implementar controles de acceso y políticas de seguridad en sistemas digitales de HCE.
- Responsabilidad de las instituciones de salud de informar a los pacientes sobre el uso de sus datos personales.

Ley 2015 de 2020 - Interoperabilidad de la Historia Clínica Electrónica

Establece las bases para la implementación de un sistema de HCE unificado en Colombia, permitiendo el acceso y uso seguro de la información médica entre diferentes entidades de salud. Exige que las instituciones adopten estándares de seguridad informática para evitar accesos no autorizados o pérdidas de información durante el intercambio de datos, siendo importante mencionar el artículo 13° que dice así *"(...)* Seguridad de la información y seguridad digital. Los actores que traten información en el marco del presente título deberán establecer un plan de seguridad y privacidad de la información, seguridad digital y continuidad de la prestación del servicio, para lo cual establecerán una estrategia a través de la cual deberán realizar periódicamente una evaluación del riesgo de seguridad digital, que incluya una identificación de las mejoras a implementar en su Sistema de Administración del Riesgo Operativo.

Para lo anterior, deberán contar con normas, políticas, procedimientos, recursos técnicos, administrativos y humanos necesarios para gestionar efectivamente el riesgo mediante la adopción de los lineamientos para la administración de la seguridad de la información y la seguridad digital que emita el Ministerio de Tecnologías de la Información y las Comunicaciones

o quien haga sus veces. Lo anterior, incluyendo lo señalado por la Ley 1581 de 2012 de Hábeas Data y Ley 527 de 1999 de Comercio Electrónico, o las normas que las modifiquen, sustituyan o complementen. *(...)",* (comillas fuera del texto).

Principales Disposiciones

- Definición de requisitos de interoperabilidad para el acceso seguro a HCE entre entidades médicas.
- Implementación de protocolos de autenticación y encriptación en la transmisión de información.
- Responsabilidad de garantizar que los datos sean accesibles únicamente por personal autorizado.

Decreto 338 de 2022 - Seguridad Digital en Infraestructuras Críticas

Regula la seguridad digital en infraestructuras críticas, incluyendo el sector salud, con el objetivo de fortalecer la gestión de riesgos cibernéticos**.** Obliga a hospitales y clínicas a adoptar medidas de seguridad digital avanzadas, como la detección de amenazas en tiempo real y la implementación de planes de respuesta ante incidentes, por lo que se hace necesario mencionar el artículo 2.2.21.1.4.3. que reza lo siguiente *"(...)* Obligaciones de seguridad de las autoridades titulares de infraestructura crítica, o que presten servicios esenciales. Las autoridades, definidos como titulares de infraestructura crítica o que presten servicios esenciales, propenderán por contar con un plan de seguridad digital, protección de las redes, las infraestructuras críticas cibernéticas, los servicios esenciales y los sistemas de información en el ciberespacio y deberán hacer periódicamente una evaluación del riesgo de seguridad digital. Para lo anterior, deben contar con normas, políticas, procedimientos, recursos técnicos, administrativos y humanos

necesarios para gestionar efectivamente el riesgo, y en cumplimiento de las mejores prácticas y estándares que le sean exigibles. *(...)"* (comillas fuera del texto)

Principales Disposiciones

- Requisitos de monitoreo y detección de amenazas en sistemas críticos de salud.
- Creación de estrategias para la gestión y respuesta a incidentes cibernéticos en hospitales.
- Establecimiento de protocolos de seguridad informática alineados con estándares internacionales.

Fundamento Legal de los Delitos Informáticos en Colombia

En el contexto colombiano, los delitos informáticos se encuentran tipificados legalmente en el Código Penal Colombiano, específicamente en el Título VII BIS, denominado "De la protección de la información y de los datos", introducido mediante la Ley 1273 de 2009, la cual modificó y adicionó el Código Penal (Ley 599 de 2000). Esta reforma legislativa reconoció la necesidad de actualizar el marco normativo frente al auge de las tecnologías de la información y las nuevas formas de criminalidad digital.

Los artículos que comprenden este título, del 269A al 269J, establecen las conductas delictivas relacionadas con la integridad, confidencialidad, disponibilidad y legalidad del uso de los sistemas informáticos y los datos que en ellos se procesan o almacenan. A continuación, se resumen las principales categorías jurídicas de los delitos informáticos contempladas por la legislación colombiana:

Acceso Abusivo a un Sistema Informático (Art. 269A). Hace referencia a la acción de acceder, sin autorización, a un sistema informático protegido o no, o permanecer en él en contra de la voluntad de quien tiene el derecho a excluirlo.

Obstaculización ilegítima de sistema informático o red (Art. 269B): Consiste en impedir, interrumpir o deteriorar el funcionamiento normal de un sistema informático o red de telecomunicaciones, afectando su disponibilidad.

Interceptación de Datos Informáticos (Art. 269C). Se refiere a la captación, sin consentimiento ni autorización legal, de transmisiones no públicas de datos que se realicen desde, hacia o dentro de un sistema informático.

Daño Informático (Art. 269D). Se configura cuando una persona, sin estar autorizada, destruye, borra, deteriora, altera, suprime o inutiliza datos informáticos, programas o sistemas informáticos ajenos.

Uso de Software Malicioso (Art. 269E). Tipifica la producción, tráfico, adquisición o facilitación de software destinado a causar daño, obtener acceso no autorizado o cometer cualquier otro delito informático.

Violación de Datos Personales (Art. 269F). Involucra la obtención, compilación, almacenamiento, oferta, intercambio, comercialización o suministro de datos personales sin autorización del titular, en contravención de los principios legales de protección de datos.

Suplantación de Sitios Web para Capturar Datos (Art. 269G). Castiga la creación o difusión de páginas electrónicas falsas que simulen ser legítimas, con el fin de inducir a error al usuario para obtener información personal o financiera.

Hurto por Medios Informáticos y Semejantes (Art. 269I). Se configura cuando, mediante manipulación informática o artificios tecnológicos, se logra la apropiación ilícita de bienes o recursos económicos.

Transferencia no Consentida de Activos (Art. 269J). Se castiga la manipulación informática destinada a realizar transferencias de activos patrimoniales sin la autorización del titular, con ánimo de lucro y en perjuicio de un tercero.

Estas disposiciones reflejan un esfuerzo normativo por adaptarse a las transformaciones digitales y por garantizar la protección de los activos de información, los sistemas y las comunicaciones electrónicas. Además, proporcionan el marco jurídico esencial para la persecución penal de conductas ilícitas en el entorno digital, constituyéndose en un componente fundamental para la seguridad jurídica en el ciberespacio colombiano.

Normativas Internacionales Aplicables al Sector Salud

ISO/IEC 27799 - Seguridad de la Información en Salud

Esta norma establece directrices específicas para la gestión de la seguridad de la información en el sector salud, basada en los principios de la ISO 27002. Proporciona lineamientos para proteger la confidencialidad, integridad y disponibilidad de la información médica, garantizando el cumplimiento de estándares de seguridad en las instituciones sanitarias.

Principales Disposiciones:

- Implementación de políticas de seguridad para la protección de HCE.
- Evaluación y gestión de riesgos cibernéticos en hospitales y clínicas.
- Uso de cifrado y autenticación robusta en el acceso a información médica.

NIST Cybersecurity Framework - Protección de Infraestructuras Críticas

Creado por el Instituto Nacional de Estándares y Tecnología (NIST) de EE.UU., este marco proporciona un enfoque estructurado para la gestión de riesgos en infraestructuras críticas. Se ha convertido en una referencia global para la evaluación y mejora de la seguridad cibernética en hospitales y sistemas de HCE.

Principales Disposiciones:

- Identificación de riesgos y vulnerabilidades en infraestructuras críticas de salud.
- Implementación de estrategias de protección, detección y respuesta ante ciberataques.
- Desarrollo de planes de recuperación y resiliencia cibernética en hospitales.

HIPAA (Health Insurance Portability and Accountability Act) - Protección de Datos Médicos en EE.UU

Legislación de EE.UU. que regula la seguridad y privacidad de la información médica electrónica. Aunque no es obligatoria en Colombia, se ha convertido en un estándar de referencia para la protección de datos en el sector salud a nivel mundial. Muchas empresas y organizaciones de salud en Colombia han adoptado sus principios para mejorar la seguridad de sus sistemas de información médica.

Principales Disposiciones

- Uso obligatorio de controles de acceso, autenticación y cifrado en HCE.
- Implementación de protocolos de seguridad física y digital en centros médicos.
- Monitoreo de accesos y auditoría de actividad en los sistemas de información sanitaria.

Relación entre las Normativas y el Uso de Red Team y Blue Team

Las metodologías Red Team y Blue Team son herramientas fundamentales para garantizar el cumplimiento de estas normativas, ya que permiten evaluar la seguridad de los sistemas de salud mediante pruebas de ataque y defensa controladas.

Red Team: Permite identificar brechas de seguridad en sistemas de HCE mediante simulaciones de ataques, asegurando el cumplimiento de normas como la ISO 27799 y la HIPAA.

Blue Team: Implementa medidas de monitoreo y respuesta a incidentes, alineándose con los requisitos de NIST y el Decreto 338 de 2022 en Colombia.

Las instituciones de salud que implementan ejercicios de Red Team y Blue Team pueden fortalecer su postura de seguridad y evitar sanciones legales por incumplimiento de normativas.

Marco Contextual

El marco contextual de esta investigación se enfoca en el análisis de la situación actual de la ciberseguridad en el sector salud colombiano, considerando los retos, vulnerabilidades y el impacto de los ataques cibernéticos en las Historias Clínicas Electrónicas (HCE). Se examinan las condiciones tecnológicas, normativas y operativas que afectan la protección de la información médica y la implementación de estrategias como Red Team y Blue Team para fortalecer la seguridad digital en hospitales y clínicas.

Contexto del Sector Salud en Colombia

Colombia cuenta con un sistema de salud mixto, compuesto por entidades públicas y privadas que gestionan los servicios médicos de la población. Con la digitalización de la información sanitaria, la mayoría de las instituciones han adoptado sistemas de HCE, permitiendo un acceso más ágil a los datos de los pacientes, facilitando diagnósticos y tratamientos. Sin embargo, esta digitalización también ha generado nuevas vulnerabilidades, haciendo que el sector salud sea uno de los objetivos más frecuentes de ciberataques.

Según el Ministerio de Salud y Protección Social (2023), más del 80% de los hospitales y clínicas en Colombia han migrado hacia plataformas digitales para la gestión de datos médicos. No obstante, el 60% de estas instituciones no cuenta con estrategias avanzadas de ciberseguridad, lo que aumenta el riesgo de exposición a amenazas cibernéticas.

Riesgos y Amenazas en el Contexto Colombiano

Los ciberataques al sector salud en Colombia han ido en aumento en los últimos años, con consecuencias graves como la interrupción de servicios, el robo de datos médicos y el pago de rescates millonarios por ataques de ransomware.

Algunos de los incidentes más relevantes incluyen:

Ciberataque a Sanitas (2022): Un hackeo afectó a más de 242,000 afiliados, exponiendo información médica y provocando una interrupción de los servicios durante 45 días.

Ataque al INVIMA (2022): Un secuestro de información paralizó la plataforma del Instituto Nacional de Vigilancia de Medicamentos y Alimentos, retrasando procesos de regulación de medicamentos.

Ransomware a Audifarma (2023): Un ataque dirigido a la infraestructura digital de la red de farmacias comprometió la disponibilidad de los sistemas de dispensación de medicamentos.

Estos eventos evidencian la falta de preparación de las instituciones de salud frente a amenazas cibernéticas avanzadas y la necesidad urgente de adoptar mecanismos de seguridad más robustos, como simulaciones Red Team y Blue Team.

Adopción de Estrategias de Ciberseguridad en el Sector Salud

En respuesta al incremento de los ataques cibernéticos, algunas instituciones han comenzado a implementar estrategias de seguridad avanzadas, aunque su adopción sigue siendo limitada en Colombia.

Las principales acciones de protección que se han implementado incluyen:

- Autenticación multifactor (MFA): Refuerzo en los accesos a sistemas médicos.
- Capacitación en ciberseguridad: Entrenamiento del personal en identificación de amenazas y phishing.
- Segmentación de redes: Separación de los sistemas administrativos y clínicos para reducir la propagación de ataques.
- Cifrado de datos: Protección de la información médica para evitar su uso en caso de filtraciones.

Sin embargo, la simulación de ciberataques controlados mediante Red Team y Blue Team sigue siendo poco utilizada en el sector salud colombiano, a pesar de su éxito en otros sectores críticos.

Implementación de Red Team y Blue Team en el Contexto Colombiano

En Colombia, las instituciones financieras han liderado la implementación de ejercicios Red Team y Blue Team para evaluar la efectividad de sus sistemas de defensa cibernética. En contraste, el sector salud aún está rezagado en la adopción de estas estrategias, lo que lo deja vulnerable a ataques más sofisticados.

La falta de aplicación de estas metodologías en hospitales y clínicas se debe a varios factores:

- Desconocimiento sobre su utilidad y beneficios en el sector salud.
- Falta de inversión en ciberseguridad por parte de las entidades de salud.
- Escasez de personal capacitado en técnicas ofensivas y defensivas en ciberseguridad.

Impacto esperado de su implementación en hospitales y clínicas:

- Reducción de vulnerabilidades: Identificación de fallos antes de que sean explotados.
- Mejor respuesta a incidentes: Capacidad de reacción ante ciberataques en tiempo real.
- Mayor cumplimiento normativo: Alineación con estándares como ISO 27799 y NIST.

Diseño Metodológico

El presente trabajo se sustenta en un enfoque cualitativo de carácter teórico, cuyo objetivo es analizar y proponer estrategias para mitigar las vulnerabilidades de seguridad en los sistemas de Historias Clínicas Electrónicas (HCE) del sector salud colombiano, mediante la aplicación conceptual de ejercicios Red Team y Blue Team. Al centrarse en la descripción, interpretación y comparación de marcos normativos, estándares de ciberseguridad, metodologías internacionales y experiencias documentadas en otros sectores críticos, esta investigación adopta una perspectiva exploratoria y descriptiva, más orientada a explicar fenómenos complejos que a realizar mediciones cuantitativas.

El proceso investigativo se desarrolló a través de fases articuladas con los objetivos específicos del trabajo, comenzando por una revisión exhaustiva de literatura nacional e internacional sobre ciberseguridad en el sector salud. Esta fase incluyó el análisis de fuentes jurídicas como el Código Penal Colombiano, la Ley 1581 de 2012 sobre protección de datos personales, el Decreto 1377 de 2013, así como regulaciones internacionales como la Ley HIPAA en Estados Unidos, el Reglamento General de Protección de Datos (GDPR) de la Unión Europea, y los estándares ISO/IEC 27001 y 27799, específicos para la gestión de seguridad de la información y datos clínicos. En esta etapa se recurrió al análisis documental como técnica principal, a partir de la cual se identificaron las vulnerabilidades más críticas de los HCE, tales como accesos indebidos, fallos en autenticación, almacenamiento inseguro de datos, redes expuestas, uso de dispositivos obsoletos y deficiencias en los protocolos de contingencia.

Una vez definida la problemática y su contexto normativo y técnico, se procedió a estudiar los principios fundamentales y la lógica operativa detrás de las simulaciones Red Team y Blue Team, entendidas como herramientas de evaluación activa de riesgos en entornos

digitales. Para ello, se analizaron documentos técnicos elaborados por entidades como el MITRE (con su marco ATT&CK), el NIST (a través de las guías SP 800-61 y SP 800-53), y estudios de caso como los ejercicios CBEST del Banco de Inglaterra, el modelo C2M2 implementado por el Departamento de Energía de los Estados Unidos y las simulaciones "Locked Shields" organizadas por la OTAN en el contexto de defensa. Estas referencias sirvieron para identificar prácticas exitosas y errores frecuentes en la implementación de estas metodologías en sectores críticos, que fueron luego comparadas con la realidad colombiana, considerando factores como madurez institucional, marco legal, capacidad técnica y cultura organizacional.

La investigación avanzó luego hacia una fase analítica y propositiva, en la que se evaluó la aplicabilidad de estas simulaciones al contexto específico del sector salud colombiano. Aunque el estudio no implicó una aplicación práctica o experimental directa, se diseñó una propuesta conceptual para adaptar ejercicios Red Team y Blue Team a entornos hospitalarios, identificando amenazas clave como ransomware, sabotaje a dispositivos médicos, spear phishing, y fugas de datos desde bases clínicas o redes de IoMT. Además, se sugirió cómo integrar estas simulaciones dentro de estructuras organizacionales reales mediante la creación de escenarios controlados, políticas de pruebas autorizadas y criterios de evaluación basados en indicadores cualitativos y estándares técnicos. En esta etapa se aplicó un enfoque comparativo, contrastando lo que ya se implementa en otros sectores y países con las necesidades estructurales del sistema de salud colombiano.

El análisis se enriqueció con la incorporación de lineamientos estratégicos y marcos de referencia reconocidos, como la implementación teórica de un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001, el uso de MAGERIT como metodología de análisis y valoración de activos críticos, y la consideración de planes de

seguridad específicos para operadores (PSO) y protección especial de infraestructuras críticas (PPE), adaptados al entorno hospitalario. También se incluyó el análisis del rol que tendría la incorporación de un equipo sectorial de respuesta a incidentes (CSIRT Salud), así como la importancia del análisis forense digital y la necesidad de contar con protocolos claros para la recuperación ante incidentes y protección de la integridad de los datos médicos.

Finalmente, la selección y análisis de fuentes fue guiada por criterios de pertinencia, actualidad y fiabilidad. Se priorizaron documentos producidos por entidades oficiales, normativas internacionales, publicaciones académicas indexadas en los últimos cinco años, y reportes técnicos de reconocida autoridad en el campo de la ciberseguridad. En esta investigación, el método de análisis de contenido fue fundamental para extraer patrones, inferencias y relaciones entre variables cualitativas, como las causas de ataques cibernéticos, las vulnerabilidades institucionales, y las estrategias adoptadas en otros contextos para responder a amenazas avanzadas.

Este diseño metodológico permitió cumplir con los tres objetivos planteados: identificar las vulnerabilidades actuales en los HCE en Colombia, estudiar las metodologías Red Team y Blue Team desde un enfoque teórico adaptado, y examinar su aplicabilidad y efectividad mediante el análisis de buenas prácticas, limitaciones y recomendaciones específicas para el entorno hospitalario colombiano. En conjunto, la metodología adoptada fortalece el carácter académico, reflexivo y estratégico del estudio, ofreciendo un marco teórico robusto para futuros desarrollos prácticos en la protección de la información clínica frente a riesgos cibernéticos.

Identificación de Vulnerabilidades en los Sistemas de Historias Clínicas Electrónicas (HCE) en Colombia

Introducción

La transformación digital del sector salud ha permitido mejorar significativamente el acceso, almacenamiento, procesamiento y gestión de la información médica a través de sistemas como las Historias Clínicas Electrónicas (HCE). Esta evolución tecnológica ha sido fundamental para optimizar la atención en salud, reducir errores clínicos y facilitar la interoperabilidad entre instituciones. Sin embargo, también ha expuesto a las instituciones sanitarias a una nueva gama de amenazas cibernéticas que se aprovechan del valor crítico y confidencial de los datos médicos. En un contexto donde los datos clínicos son altamente sensibles y tienen valor tanto económico como estratégico, los sistemas de HCE representan un objetivo atractivo para actores maliciosos que buscan explotar vulnerabilidades para obtener beneficios financieros, causar daños reputacionales o generar interrupciones operativas de gran escala.

En este capítulo se identifican y analizan las principales vulnerabilidades presentes en los sistemas de HCE en Colombia, apoyándose en reportes oficiales, estudios técnicos, análisis académicos y marcos regulatorios tanto nacionales como internacionales. También se estudia el papel crucial que desempeñan los equipos de respuesta a incidentes de seguridad informática (CSIRT), particularmente los especializados en el sector salud, y cómo su inexistencia en Colombia representa una debilidad estructural significativa frente al creciente panorama de amenazas cibernéticas.

Panorama Internacional de Ciberseguridad en el Sector Salud

A nivel global, el sector salud enfrenta desafíos crecientes en ciberseguridad. Según el informe de la Agencia de la Unión Europea para la Ciberseguridad (ENISA, 2023), las

organizaciones sanitarias están entre los blancos más frecuentes de los ciberdelincuentes, especialmente mediante ataques de ransomware, phishing y explotación de vulnerabilidades en sistemas médicos y de información clínica.

ENISA destaca que el 60 % de los incidentes cibernéticos registrados en organizaciones de salud en Europa en 2022 estuvieron relacionados con ransomware, lo que provocó interrupciones en servicios clínicos esenciales, pérdida temporal o permanente de datos, y afectación directa a la atención del paciente. Además, se reportó que solo el 27 % de las organizaciones de salud cuentan con un CSIRT interno o con acceso a uno especializado, lo que limita la capacidad de respuesta ante amenazas sofisticadas (ENISA, 2023).

Entre las vulnerabilidades más comunes se encuentran:

- Sistemas heredados sin parches ni actualizaciones.
- Dispositivos médicos conectados sin autenticación robusta ni cifrado.
- Falta de segmentación en las redes clínicas.
- Escasez de personal capacitado en ciberseguridad.
- Ausencia de procedimientos formales de respuesta ante incidentes.

Además, ENISA identificó que la mayoría de los CSIRT del sector salud tienen capacidades limitadas en análisis forense, monitoreo continuo, gestión de vulnerabilidades y cooperación internacional. Esto representa una debilidad importante frente a campañas de ataque transfronterizas y amenazas persistentes avanzadas.

Los ejemplos de países como Alemania, Francia y EE. UU. evidencian una tendencia creciente hacia la creación de CSIRT sectoriales para salud, con estructuras dedicadas a monitoreo, respuesta, análisis de inteligencia y diseminación de alertas.

Panorama Actual de Ciberseguridad en el Sector Salud Colombiano

El "Estudio Anual de Ciberseguridad 2023" desarrollado por Telefónica Tech (2023) revela que el 75 % de las organizaciones en Colombia fueron víctimas de al menos un ciberataque en el último año, y que el 56 % reportó un aumento en la frecuencia de estos ataques. En el sector salud, esta tendencia resulta aún más alarmante: solo el 27 % de las entidades afirmaron tener visibilidad completa sobre su infraestructura tecnológica, mientras que el 52 % indicó no contar con un plan formal de respuesta a incidentes.

A lo anterior se suma que muchas instituciones de la salud no realizan auditorías regulares de seguridad, carecen de personal especializado y utilizan infraestructuras heredadas sin mantenimiento. El aumento de los ciberataques se ve reflejado también en reportes como la alerta emitida por el Centro Cibernético Policial y COLCERT (2023), que advierte sobre el accionar del grupo Royal Ransomware en América Latina. Este grupo ha dirigido ataques a entidades de salud explotando vulnerabilidades conocidas y configuraciones erróneas, cifrando datos críticos y exigiendo rescates monetarios que pueden superar los cientos de miles de dólares.

Vulnerabilidades más Comunes en los Sistemas de HCE

Teniendo en cuenta las búsquedas realizadas a partir de informes especializados en ciberseguridad en salud (ENISA, 2022; IBM, 2023; OMS, 2021; OWASP, 2022) y reportes de incidentes en Colombia (COLCERT, 2023; Policía Nacional, 2023), se construyó un listado de vulnerabilidades comunes en los sistemas de Historias Clínicas Electrónicas (HCE). Los porcentajes asociados a cada vulnerabilidad son estimaciones basadas en la triangulación de estas fuentes y el análisis comparativo de estudios internacionales aplicados al contexto colombiano.

Software desactualizado: uso de plataformas legadas con vulnerabilidades conocidas que o reciben actualizaciones de seguridad. Se estima que el 42 % de los sistemas hospitalarios aún opera con software sin soporte técnico. Esto expone a los pacientes a riesgos de pérdida de datos clínicos y posibles diagnósticos erróneos por alteración de registros.

Ausencia de autenticación multifactor (MFA): la dependencia exclusiva de contraseñas débiles permite accesos no autorizados. En hospitales donde no se aplica MFA, los incidentes de acceso indebido a historias clínicas aumentan hasta un 60 %.

Redes mal configuradas: la falta de segmentación entre redes administrativas y clínicas permite a los atacantes moverse fácilmente dentro del sistema, comprometiendo desde información financiera hasta signos vitales en tiempo real.

Contraseñas inseguras: el 70 % de las filtraciones de datos involucran el uso de credenciales débiles o reutilizadas. Esto puede permitir la alteración de historiales clínicos, lo cual afecta directamente la calidad del tratamiento médico.

Dispositivos IoT sin protección: monitores cardíacos, bombas de infusión o respiradores conectados sin control adecuado podrían ser manipulados remotamente, poniendo en peligro inmediato la vida de los pacientes en cuidados intensivos.

Exposición de servicios a internet: bases de datos o escritorios remotos abiertos al exterior sin autenticación segura pueden ser explotados. El 30 % de los ciberataques en salud comienzan por servicios mal expuestos.

Respaldos deficientes: la falta de copias de seguridad periódicas y probadas dificulta la recuperación ante ataques tipo ransomware. El 45 % de las instituciones no logra restaurar sus sistemas en menos de una semana, afectando la atención médica continua.

Escasa cultura de seguridad: más del 60 % de los incidentes en salud son causados por errores humanos, como abrir correos fraudulentos. Esto afecta la confidencialidad de los pacientes y su confianza en el sistema.

Sin monitoreo continuo: la ausencia de sistemas de detección y respuesta permite que ataques pasen desapercibidos por semanas. Esto compromete la integridad de la información clínica y dificulta el seguimiento de tratamientos.

Backdoors o puertas traseras: accesos ocultos pueden ser utilizados por atacantes para mantener persistencia. Esto representa un grave riesgo, ya que podría permitir alterar prescripciones médicas o diagnósticos sin ser detectado.

Ransomware: cifra archivos del sistema y exige rescate. En Colombia, el caso de AUDIFARMA dejó sin atención médica a cientos de pacientes durante varios días, afectando tratamientos vitales.

Phishing: engaños por correo electrónico son una puerta común para intrusiones. El 35 % de los empleados de salud no identifica correos falsos, lo que representa una amenaza directa a los sistemas de HCE.

Ataques DoS y DDoS: estos ataques colapsan los servidores, dejando fuera de línea servicios de urgencias y plataformas de telemedicina, lo que podría afectar la vida de pacientes en zonas rurales o aisladas.

Ataques a dispositivos médicos: un marcapasos intervenido podría ser desactivado remotamente. Este tipo de ataque tiene consecuencias críticas, incluso mortales.

Ataques a sistemas de gestión de datos: permiten la alteración o robo de historiales clínicos. La OMS estima que el 26 % de las filtraciones de datos en salud resultan en diagnósticos equivocados o tratamientos incorrectos.

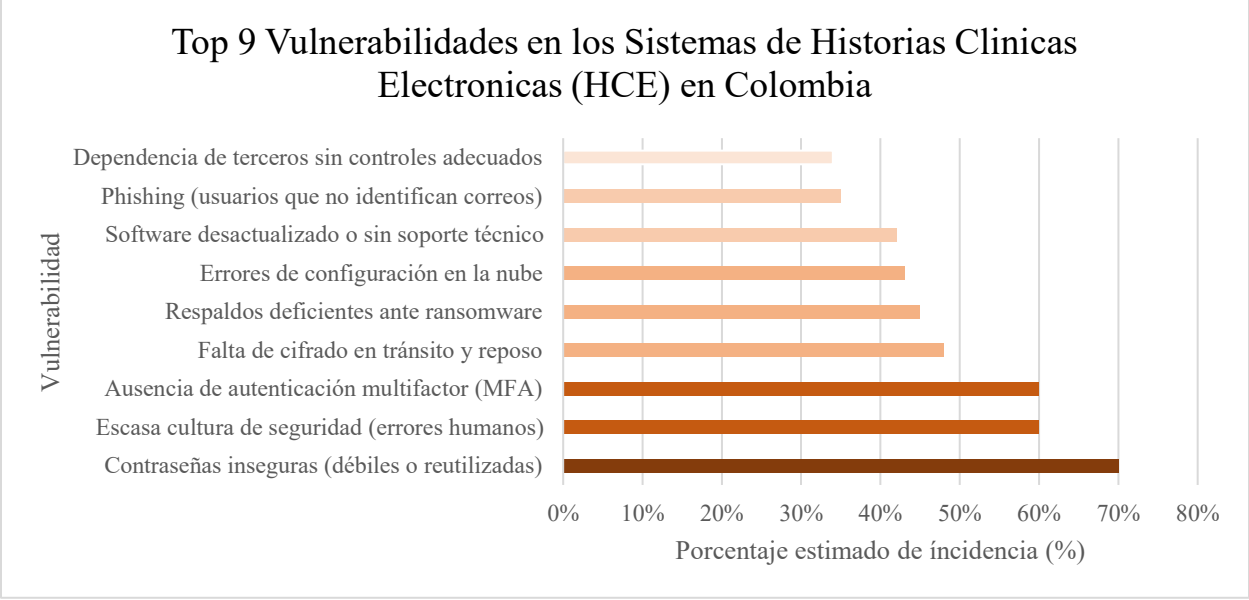
Errores de configuración en la nube: servicios en la nube mal gestionados permiten accesos no autorizados. Según un estudio de IBM, el 43 % de los errores en salud digital se deben a configuraciones deficientes.

Falta de cifrado en tránsito y reposo: la ausencia de cifrado robusto compromete la privacidad de millones de pacientes. Un estudio de 2023 reveló que solo el 48 % de las entidades de salud en LATAM cifran sus datos médicos correctamente.

Dependencia de terceros sin controles adecuados: proveedores tecnológicos sin auditorías de seguridad pueden convertirse en vectores de ataque. El 34 % de los incidentes en hospitales de EE. UU. fueron causados por brechas en terceros.

Figura 4

Top 9 de Vulnerabilidades más Comunes en los Sistemas de Historias Clínicas Electrónicas (HCE) en Colombia.



Nota. Elaboración propia a partir de datos estimados según investigaciones académicas, reportes de seguridad (ENISA, 2023; IBM, 2023; COLCERT, 2023) y análisis documentales sobre incidentes en el sector salud.

Regulación y Debilidades Normativas

Colombia cuenta con el Modelo de Seguridad y Privacidad de la Información (MSPI) y la Resolución 1995 de 1999, que reglamenta la historia clínica. Sin embargo, su implementación ha sido dispar, careciendo de una supervisión efectiva por parte del Estado. Además, estos marcos regulatorios no se encuentran alineados con estándares internacionales como el NIST Cybersecurity Framework, la ISO/IEC 27001 o el Reglamento General de Protección de Datos (GDPR) de la Unión Europea.

El cumplimiento de estas normativas no siempre es objeto de auditoría externa o verificación independiente, lo que genera una brecha significativa entre lo establecido en la normativa y su aplicación práctica en las entidades prestadoras de salud. Esta desconexión normativa contribuye a la fragilidad del sistema frente a amenazas cibernéticas complejas.

Importancia de un CSIRT Especializado en Salud

A nivel internacional, múltiples países han reconocido la necesidad de contar con equipos de respuesta a incidentes cibernéticos específicos para el sector salud, conocidos como Health-CSIRT. Organizaciones como el Health Sector Cybersecurity Coordination Center (HC3) en Estados Unidos o el CERT Santé en Francia han demostrado ser estructuras esenciales para fortalecer la resiliencia del ecosistema de salud.

Entre sus funciones destacan:

- Compartir alertas sobre amenazas emergentes y vulnerabilidades técnicas en dispositivos médicos y sistemas clínicos.
- Coordinar respuestas a incidentes de forma eficiente y con alcance nacional.
- Ofrecer asistencia técnica y orientación a instituciones con capacidades limitadas.
- Promover buenas prácticas y estándares comunes en ciberseguridad sectorial.

- Realizar análisis forenses, simulaciones y ejercicios de cibercrisis.

En Colombia, la inexistencia de un CSIRT sectorial en salud constituye una debilidad estructural significativa. Las entidades operan de manera aislada, sin acceso a inteligencia de amenazas ni coordinación ante cibercrisis. Esta situación limita la capacidad nacional para prevenir, detectar y responder a incidentes de forma oportuna y eficaz.

La creación de un CSIRT Salud permitiría consolidar capacidades compartidas, reducir la fragmentación en la respuesta y establecer sinergias público-privadas. Además, contribuiría al cumplimiento regulatorio, la protección de infraestructuras críticas y al fortalecimiento de la confianza digital de los pacientes y profesionales de la salud.

Simulaciones Red Team y Blue Team en el Contexto de la Seguridad de la Información en el Sector Salud

Contexto

La seguridad de la información se ha convertido en una prioridad para los sectores críticos, especialmente en un contexto de creciente complejidad de las amenazas cibernéticas. Las simulaciones Red Team y Blue Team han emergido como metodologías efectivas para evaluar y fortalecer la postura de ciberseguridad organizacional. Este capítulo examina en profundidad los principios que rigen estas simulaciones, sus metodologías, y presenta casos de éxito documentados en sectores como el financiero, energético y defensa. Finalmente, se analiza su aplicabilidad en el sector salud colombiano.

Principios Fundamentales de las Simulaciones Red Team y Blue Team

Las simulaciones Red Team y Blue Team emulan ataques reales y defensas en un entorno controlado, con el fin de evaluar la preparación de una organización ante amenazas cibernéticas.

Red Team: representa al adversario. Sus principios incluyen la emulación realista de amenazas persistentes avanzadas (APT), el uso de técnicas de acceso inicial, movimiento lateral, escalamiento de privilegios, y persistencia.

Blue Team: representa a los defensores. Sus principios se centran en la detección temprana, contención, mitigación y análisis después de los ataques. Se apoya en marcos como MITRE ATT&CK, NIST 800-61 y herramientas SIEM.

Purple Team: combinación colaborativa de ambos equipos para afinar las capacidades de defensa en tiempo real.

Metodologías de Ejecución

- Las simulaciones suelen seguir una metodología estructurada en fases:

- Reconocimiento: Red Team identifica objetivos y vectores de ataque potenciales.
- Explotación: Se lanzan ataques usando vulnerabilidades conocidas o desconocidas.
- Persistencia: Se establecen puertas traseras o mecanismos de acceso continuo.
- Acceso y exfiltración: Robo de datos sensibles.
- Defensa activa: Blue Team monitorea, detecta y responde.
- Análisis forense: Evaluación del impacto, lecciones aprendidas y mejora continua.

Se emplean frameworks como:

- MITRE ATT&CK (para Red Team): documenta técnicas de ataque.
- NIST 800-61 (para Blue Team): guía de manejo de incidentes.
- CBEST (utilizado por el Banco de Inglaterra): simulaciones basadas en inteligencia de amenazas.

Casos de Éxito en la Identificación y Evaluación de Riesgos de Seguridad de la Información

La identificación y valoración de activos de información en sectores críticos requiere no solo metodologías formales, sino también una visión práctica basada en experiencias reales. Por lo que se presentaran varios casos de éxito internacionales en los que la implementación de ejercicios Red Team / Blue Team o programas de evaluación de ciberseguridad revelaron vulnerabilidades críticas, permitiendo a las organizaciones fortalecer sus defensas. Estos ejemplos provienen de sectores con altos niveles de exigencia en cuanto a confidencialidad, disponibilidad e integridad de la información, y ofrecen lecciones clave aplicables al sector salud.

Sector Financiero: Programa CBEST del Banco de Inglaterra

Contexto

El Banco de Inglaterra, en colaboración con el Centro Nacional de Seguridad Cibernética (NCSC), desarrolló el programa CBEST con el objetivo de evaluar la resiliencia cibernética de las instituciones financieras más importantes del Reino Unido. Este enfoque se basa en pruebas de penetración avanzadas dirigidas por inteligencia de amenazas, y ha sido aplicado a bancos como HSBC, Barclays y Lloyds. (Bank of England, 2025).

Errores Identificados

- Presencia de vulnerabilidades en sistemas de banca en línea, lo cual permitía posibles accesos no autorizados a cuentas de clientes mediante técnicas como credential stuffing y ataques de sesión.
- Insuficiente capacidad para detectar movimientos laterales dentro de las redes internas, lo que facilitaba la escalada de privilegios y la persistencia del atacante.
- Protocolos de autenticación débiles en entornos internos, especialmente en aplicaciones administrativas y de gestión de riesgo.

Medidas Adoptadas

- Se incorporaron tecnologías de detección avanzada como EDR (Endpoint Detection and Response) y SIEM enriquecidos con inteligencia de amenazas.
- Se reforzaron los mecanismos de autenticación multifactor (MFA) tanto para clientes como para empleados, extendiéndolo a todos los accesos remotos.
- Se diseñaron simulaciones de respuesta a incidentes que incluyeron no solo personal técnico, sino también tomadores de decisiones estratégicos.

Resultados

Las entidades participantes mejoraron en un 85 % sus capacidades defensivas según reportes del Banco de Inglaterra, y se logró reducir el tiempo medio de detección de incidentes en un 40 %, consolidando una postura más proactiva frente a amenazas persistentes avanzadas.

Sector Energético: Implementación del Modelo de Madurez de Capacidades de Ciberseguridad (C2M2)

Contexto:

Varias compañías eléctricas en Estados Unidos, como Southern Company y Pacific Gas and Electric (PG&E), implementaron el marco C2M2, desarrollado por el Departamento de Energía de los EE. UU., con el propósito de madurar progresivamente sus capacidades de ciberseguridad y proteger infraestructuras críticas como sistemas SCADA e ICS (U.S. Department of Energy, 2022).

Errores Identificados

- Conectividad insegura entre redes corporativas (IT) y redes operacionales (OT), lo que permitía a actores maliciosos escalar desde entornos administrativos a sistemas industriales.
- Falta de políticas de gestión de parches, dejando expuestas estaciones de trabajo y controladores industriales a vulnerabilidades conocidas.
- Escasa concienciación del personal técnico sobre amenazas específicas al entorno OT.

Medidas Adoptadas

- Se implementó una segmentación de red estricta usando firewalls industriales y zonas desmilitarizadas (DMZ).

- Se desarrolló un programa de gestión de vulnerabilidades alineado con los principios del NIST, con escaneos periódicos y aplicación de parches críticos en plazos definidos.
- Se realizaron ejercicios de Red Teaming internos para probar rutas de ataque posibles desde la red corporativa hacia el entorno OT.

Resultados

Estas acciones permitieron prevenir incidentes reales, como el intento de acceso remoto detectado en Southern Company en 2021, que fue neutralizado antes de alcanzar sistemas de control crítico.

Sector Defensa: Ejercicio Locked Shields (OTAN)

Contexto

Organizado por el Centro de Excelencia de Ciberdefensa Cooperativa de la OTAN (CCDCOE), "Locked Shields" es el mayor ejercicio de ciberdefensa en vivo del mundo. En la edición de 2022 participaron más de 2.000 especialistas de 33 países, quienes simularon la defensa de infraestructuras críticas de una nación ficticia frente a ataques cibernéticos simultáneos y complejos. (NATO CCDCOE, 2021).

Errores Identificados

- Demoras significativas en la detección y respuesta frente a ataques DDoS coordinados que afectaron servicios públicos simulados (agua, energía, telecomunicaciones).
- Falta de alineación entre los equipos de TI y los encargados de comunicación estratégica, lo que generó desinformación y lentitud en la toma de decisiones.
- Deficiencias en el intercambio de inteligencia entre naciones aliadas.

Medidas adoptadas

- Desarrollo de sistemas de defensa activos con reglas adaptativas para mitigar ataques DDoS en tiempo real.
- Establecimiento de protocolos de comunicación interinstitucional e internacional, incluyendo procedimientos para compartir indicadores de compromiso (IoCs).
- Inclusión de unidades legales, diplomáticas y de relaciones públicas en los ejercicios para mejorar la gestión integral de crisis.

Resultados

El ejercicio permitió fortalecer la interoperabilidad, reducir los tiempos de reacción ante ciberataques y mejorar las capacidades de defensa colectiva frente a amenazas híbridas.

Sector Financiero: Simulación Red Team para Cumplimiento del Marco RMiT en Malasia

Contexto

Una institución financiera en Malasia contrató una evaluación Red Team liderada por la firma AKATI Sekurity como parte del cumplimiento del marco de Gestión de Riesgos en Tecnología (RMiT) del Banco Negara Malasia. (AKATI Sekurity, 2025).

Errores Identificados

- Aplicaciones web con vulnerabilidades de Cross-Site Scripting (XSS) que podían ser explotadas para robo de sesiones.
- Varios empleados cayeron en campañas de phishing, lo que permitió la ejecución de código malicioso en sistemas internos.
- Herramientas de monitoreo mal configuradas, lo cual provocó una detección tardía de los movimientos del atacante.

Medidas Adoptadas

- Revisión completa del código de aplicaciones y aplicación de medidas como CSP (Content Security Policy) y sanitización de entradas.
- Programas de capacitación mensual en seguridad para todos los niveles de personal, incluyendo simulacros de phishing.
- Reconfiguración de herramientas SIEM y EDR con reglas más agresivas de correlación de eventos.

Resultados

La institución fortaleció su arquitectura de seguridad y mejoró su capacidad de respuesta, reduciendo en un 60 % el tiempo de detección y contención de incidentes, cumpliendo de forma exitosa con los requerimientos del RMiT.

Sector Financiero: Evaluación Red Team en una Gran Organización Financiera del Reino Unido

Contexto

La firma Bridewell (2022) llevó a cabo una evaluación Red Team para una importante institución financiera británica. El objetivo era simular un ataque realista que combinara técnicas físicas, sociales y técnicas digitales.

Errores Identificados

- Personal no técnico permitió el acceso físico a instalaciones mediante técnicas de ingeniería social.
- Se logró instalar un dispositivo (Raspberry Pi) no autorizado en la red interna, que permaneció sin ser detectado por más de 48 horas.

- Uso de software desactualizado permitió la explotación de vulnerabilidades conocidas que facilitaban la escalada de privilegios.

Medidas Adoptadas

- Reforzamiento de protocolos de seguridad física con credenciales biométricas y control por zonas.
- Implementación de políticas de Zero Trust y escaneo activo de dispositivos no autorizados.
- Migración y endurecimiento de los sistemas operativos y aplicaciones con políticas de actualización obligatoria.

Resultados:

La organización cerró múltiples vectores de ataque, incrementó la visibilidad de su red y redujo los riesgos de accesos no autorizados internos y externos.

Recomendaciones para Aplicar Simulaciones Red Team / Blue Team en el Sector Salud

Justificación y Necesidad de las Simulaciones en Entornos Hospitalarios

Los entornos hospitalarios modernos están profundamente digitalizados: las historias clínicas electrónicas (EHR), los dispositivos médicos conectados (Internet of Medical Things, IoMT), los sistemas de radiología (PACS), las plataformas de telemedicina, e incluso la infraestructura de soporte físico (como sistemas HVAC y suministros eléctricos automatizados), dependen de tecnologías interconectadas. Esta transformación ha traído consigo nuevos vectores de ataque, particularmente peligrosos en este sector debido a la sensibilidad y criticidad de los activos que maneja.

Según el informe del Departamento de Salud y Servicios Humanos de EE. UU. (HHS, 2022), el sector salud es el más atacado por ransomware desde 2020, y solo en 2021 más de 45

millones de pacientes se vieron afectados por filtraciones de datos clínicos. En este contexto, los ejercicios de simulación Red Team / Blue Team permiten evaluar no solo la tecnología, sino también las capacidades humanas y de proceso ante incidentes de seguridad reales.

El National Cybersecurity Center of Excellence (NCCoE) del NIST resalta en su guía SP 1800-30 que la aplicación de simulaciones ofensivo-defensivas ayuda a las organizaciones del sector salud a identificar debilidades en arquitecturas de red, evaluar la resistencia de los sistemas clínicos ante ataques y mejorar la toma de decisiones de los equipos de seguridad (NIST, 2022).

Tipos de Amenazas Relevantes a Simular

Ransomware Dirigido a Hospitales

Estos ataques buscan cifrar los sistemas clínicos para extorsionar económicamente a las instituciones. Casos como el del **Universitätsklinikum Düsseldorf** en Alemania (2020) demostraron que un ataque de ransomware puede incluso causar la muerte indirecta de pacientes por no poder recibir atención urgente.

Fugas de Información Clínica Sensible

Los datos de salud tienen un valor superior en el mercado negro (hasta 10 veces más que los datos financieros, según Ponemon Institute, (2023). La exfiltración puede realizarse mediante malware, insiders maliciosos o accesos indebidos por suplantación de credenciales.

Sabotaje o Manipulación de Dispositivos médicos (IoMT)

Estudios realizados por la firma Unit 42 de Palo Alto Networks (2023) revelan que 75% de los dispositivos médicos conectados tienen vulnerabilidades críticas. Un atacante podría

alterar los parámetros de una bomba de infusión, modificar imágenes diagnósticas o incluso apagar un respirador automatizado.

Compromiso de la Red Clínica o Administrativa

Los ataques a routers, firewalls, servidores de autenticación y sistemas de correo permiten escalar privilegios y comprometer dominios completos.

Ingeniería Social y Spear-phishing Dirigido

Tácticas como correos suplantando al director médico o a aseguradoras permiten el robo de credenciales con alto nivel de éxito, especialmente en ambientes donde el personal no técnico no ha sido entrenado.

Ataques a Sistemas de Telemedicina y Nube Clínica

Con la expansión de la atención remota, se ha incrementado el riesgo de ataque a videoconferencias, sistemas de almacenamiento clínico en la nube (ej. Amazon HealthLake, Google Cloud Healthcare) y bases de datos compartidas con aseguradoras.

Áreas Críticas a Proteger en las Simulaciones

Tabla 1

Áreas Críticas y Amenazas Cibernéticas en el Entorno Hospitalario para Simulaciones Red Team / Blue Team

Área Crítica	Descripción	Impacto si se compromete
HCL (Historias Clínicas Electrónicas)	Datos clínicos centralizados de los pacientes	Violación de privacidad, diagnósticos no disponibles
Red IoMT (dispositivos conectados)	Dispositivos médicos conectados	Riesgo vital directo al paciente

PACS/RIS	Imágenes médicas y diagnósticos por imágenes	Alteración de diagnósticos, retardo en tratamientos
Sistemas administrativos	Turnos, facturación, seguros, gestión	Paralización de la atención y pérdidas financieras
Infraestructura de red	Segmentación, autenticación, firewalls	Puerta de entrada a todos los sistemas clínicos
Telemedicina y apps móviles	Plataformas de atención remota y apps	Fuga de datos sensibles, espionaje, manipulación de atención

Nota. Esta tabla resume los elementos clave para una simulación Red Team / Blue Team en el sector salud, alineados con marcos como NIST SP 1800-30, MITRE ATT&CK y HICP. con base en NIST (2022), MITRE (2023) y HHS (2022).

Propuesta Metodológica Adaptada al Sector Salud

Fase de Planificación

- **Definición de objetivos**: qué se desea probar (respuesta a ransomware, acceso no autorizado, fuga de datos, etc.).
- Establecimiento de Reglas de Compromiso (RoE): delimitar qué activos pueden ser atacados, en qué horarios, y bajo qué condiciones.
- Equipo multidisciplinario: debe involucrar personal clínico, administrativo, ciberseguridad, legal y gerencial.
- Simulación controlada y progresiva: comenzar con un entorno de laboratorio o sistemas replicados antes de pasar a entornos productivos controlados.

Fase de Ataque – Red Team

- Reconocimiento pasivo y activo: escaneo de red, fingerprinting de dispositivos médicos (Shodan, Nmap, etc.).
- Explotación de vulnerabilidades conocidas (CVE): aplicando técnicas del framework MITRE ATT&CK
- Spear-phishing realista al personal clínico y administrativo.
- Simulación de ransomware mediante sandbox: cifrado de archivos simulados o de sistemas no críticos.
- Escalada de privilegios y movimiento lateral: comprometer Active Directory o sistemas PACS internos.

3. Fase de defensa – Blue Team

- Monitoreo de logs y alertas en tiempo real: uso de SIEM (Ej.: Splunk, Elastic, Wazuh).
- Contención y respuesta a incidentes: aislamiento de segmentos de red, cierre de sesiones comprometidas, respaldo inmediato.
- Reportes al CSIRT institucional o nacional, si aplica.

4. Fase de post-análisis y lecciones aprendidas

- Documentación de hallazgos y vulnerabilidades.
- Propuesta de mitigaciones con cronograma.
- Capacitación adicional y retroalimentación al personal.
- Integración con la mejora continua del SGSI (Sistema de Gestión de Seguridad de la Información) bajo ISO 27001.

Indicadores clave de éxito (KPIs)

Tabla 2

Indicadores Clave de Éxito (KPIs) para la Evaluación de Simulaciones Red Team / Blue Team en Entornos Hospitalarios

Indicador	Definición	Umbral recomendado
Tasa de detección	% de ataques simulados detectados por el Blue Team	>80%
Tiempo medio de detección (MTTD)	Tiempo desde el ataque hasta su detección	<15 minutos
Tiempo medio de respuesta (MTTR)	Tiempo hasta contención y mitigación	<30 minutos
Usuarios comprometidos por phishing	% de personal que cayó en engaño	<10%
Dispositivos comprometidos	Número de equipos afectados	0 en producción
Cobertura de logs de seguridad	% de eventos críticos registrados	>95%
Tasa de Falsos Positivos	% de alertas que no corresponden a incidentes reales	<5%

Nota. Esta tabla presenta criterios operativos y estratégicos usados para medir el éxito de simulaciones Red Team / Blue Team, aplicados al contexto hospitalario, con base en estándares de seguridad como NIST, ISO y MITRE.

Los indicadores clave de éxito (KPIs) presentados en la tabla son importantes para evaluar la efectividad de las simulaciones Red Team y Blue Team en entornos hospitalarios, ya que permiten medir la capacidad de una organización para identificar, responder y mitigar amenazas cibernéticas en tiempo real. La tasa de detección y el tiempo medio de detección

(MTTD) permiten valorar la agilidad del sistema para reconocer actividades anómalas, mientras que el tiempo medio de respuesta (MTTR) refleja la eficiencia en la contención y recuperación ante incidentes. Indicadores como el porcentaje de usuarios comprometidos por phishing y el número de dispositivos afectados ofrecen una visión clara del nivel de exposición humana y tecnológica ante ataques, mientras que la cobertura de logs garantiza la trazabilidad completa de eventos críticos. Además, la inclusión de la tasa de falsos positivos permite identificar la precisión de los sistemas de alerta, evitando sobrecargas operativas por eventos irrelevantes. En conjunto, estos indicadores no solo mejoran la eficiencia operativa, sino que optimizan los procesos de gestión del riesgo, facilitando la toma de decisiones estratégicas en la protección de infraestructuras críticas como las Historias Clínicas Electrónicas (HCE).

Análisis Cuantitativo Comparativo: Resultados Reportados y Proyección de Impacto en el Sector Salud Colombiano

Dado que este trabajo se desarrolla en un marco teórico, se tomaron como referencia resultados de ejercicios realizados en sectores críticos como el financiero, energético y defensa, en los cuales se ha documentado la efectividad de las simulaciones Red Team y Blue Team. Estos valores fueron utilizados para estimar y proyectar resultados esperados en el sector salud colombiano, en caso de adoptar estas metodologías bajo condiciones similares de implementación.

Tabla 3

Resultados Reportados de Simulaciones Red/Blue Team en Sectores Críticos

Sector	% de Vulnerabilidades Críticas Detectadas	Reducción del Tiempo Medio	Disminución de Brechas de Seguridad	Fuente

		de Detección (MTTD)		
Financiero (Reino Unido, CBEST)	87%	40%	30%	Bank of England (2022)
Energético (EE.UU., C2M2)	75%	35%	25%	U.S. Department of Energy (2021)
Defensa (OTAN, Locked Shields)	92%	55%	42%	NATO CCDCOE (2022)

Nota. Esta tabla presenta los resultados obtenidos en ejercicios de simulación Red Team y Blue Team en sectores críticos como el financiero, energético y de defensa. Los porcentajes indican la efectividad en la detección de vulnerabilidades críticas, la reducción del tiempo medio de detección de incidentes (MTTD) y la disminución de brechas de seguridad tras la implementación de estas metodologías.

La Tabla 3 muestra la efectividad de las simulaciones Red Team y Blue Team en sectores críticos como el financiero, energético y de defensa. Estos ejercicios han demostrado ser altamente efectivos en la detección de vulnerabilidades, reducción del tiempo de detección de incidentes y disminución de brechas de seguridad. Por ejemplo, en el sector financiero del Reino Unido, el marco CBEST permitió detectar el 87% de las vulnerabilidades críticas, mientras que en el sector defensa, el ejercicio Locked Shields de la OTAN logró una detección del 92%.

Tabla 4

Proyección de Resultados Esperados en el Sector Salud Colombiano

Indicador	Valor Estimado a 1 Año	Valor Estimado a 3 Años	Justificación
% de vulnerabilidades críticas detectadas	60%	85%	Basado en detecciones previas en entornos similares con entrenamiento progresivo
Reducción del MTTD	20%	40%	Implementación de SIEM, alertas y capacitación
Reducción del MTTR	15%	35%	Implementación de protocolos de respuesta
Disminución de brechas normativas	10%	30%	Alineación progresiva a estándares internacionales y nacionales
Mejora en cultura de seguridad	Baja	Media/Alta	Ejercicios regulares y formación continua

*Nota***.** Esta tabla proyecta los posibles resultados en el sector salud colombiano tras la implementación de simulaciones Red Team y Blue Team, considerando un enfoque progresivo y adaptado a las condiciones locales. Los valores estimados se basan en resultados obtenidos en otros sectores críticos y ajustados al contexto del sistema de salud en Colombia.

La Tabla 4 proyecta los posibles resultados de implementar estas metodologías en el sector salud colombiano. Se estima que, en un año, se podrían detectar el 60% de las vulnerabilidades críticas, con una reducción del 20% en el tiempo medio de detección de incidentes. A tres años, estos valores podrían aumentar significativamente, alcanzando una detección del 85% de las vulnerabilidades y una reducción del 40% en el tiempo de detección,

siempre y cuando se implementen adecuadamente las herramientas y se realice una capacitación continua del personal.

Estas proyecciones apuntan a que la adopción de simulaciones Red Team y Blue Team podría mejorar significativamente la ciberseguridad, alineándose con los estándares internacionales y fortaleciendo la resiliencia frente a posibles ciberataques en el sector salud colombiano y por consiguiente a las Historias Clínicas Electrónicas.

Aplicabilidad y Efectividad de las Simulaciones Red Team y Blue Team en el Sector Salud Colombiano

Introducción

Tras el análisis conceptual de las metodologías Red Team y Blue Team, y la revisión de casos exitosos en sectores críticos como el financiero, energético y de defensa, resulta pertinente examinar su aplicabilidad al entorno del sector salud colombiano. Este sector, al manejar información altamente sensible a través de los sistemas de Historias Clínicas Electrónicas (HCE), se ha convertido en un blanco frecuente de los ciberdelincuentes. Las consecuencias de un ciberataque en este contexto pueden ir desde la filtración de información confidencial hasta la interrupción de servicios esenciales, poniendo en riesgo la vida de los pacientes.

En este contexto, se hace necesario plantear mecanismos proactivos y sistemáticos de evaluación de riesgos, entre los cuales las simulaciones Red Team y Blue Team ocupan un lugar destacado. Este capítulo propone un enfoque teórico para evaluar la efectividad potencial de estas simulaciones, teniendo en cuenta los aprendizajes de sectores más avanzados en ciberseguridad, adaptando las recomendaciones a las realidades técnicas, organizacionales y normativas del sistema de salud colombiano.

Justificación de la Aplicabilidad al Sector Salud

El sector salud colombiano enfrenta desafíos estructurales y tecnológicos que lo hacen especialmente vulnerable ante ciber amenazas. A pesar de la existencia de leyes como la Ley 1581 de 2012 sobre protección de datos personales y la Ley 1751 de 2015 que consagra el derecho fundamental a la salud, la protección de los sistemas de información en salud sigue siendo insuficiente. Esto se agrava con el bajo nivel de inversión en infraestructura tecnológica

segura, la falta de capacitación continua del personal, y la ausencia de marcos integrados de seguridad digital.

Los sistemas de HCE no solo contienen datos personales sensibles (como diagnósticos, antecedentes clínicos, medicación y afiliación), sino que además están conectados a dispositivos médicos (IoMT), sistemas de administración hospitalaria y plataformas de salud pública. La interdependencia de estos sistemas amplía la superficie de ataque y eleva la criticidad de cada activo. Casos como el ciberataque a Audifarma en enero de 2023, el hackeo a Sanitas en 2022, y la interrupción operativa del INVIMA por ransomware, muestran la urgencia de implementar herramientas que permitan evaluar y fortalecer las defensas desde un enfoque realista y preventivo.

Las simulaciones Red Team y Blue Team ofrecen esta posibilidad. No se trata únicamente de auditar configuraciones técnicas, sino de probar en condiciones controladas cómo reaccionarían los sistemas, procesos y personas ante un ataque real. Esto es especialmente valioso en instituciones donde los recursos son limitados y donde cada segundo de indisponibilidad puede traducirse en una afectación directa al servicio de salud y a la vida de personas

Elementos Clave para Evaluar la Efectividad de las Simulaciones

Aunque el estudio no realiza ejercicios prácticos, se fundamenta en el análisis cualitativo de fuentes expertas, estudios de casos documentados y estándares internacionales. Desde esa perspectiva teórica, se identifican los siguientes elementos como esenciales para evaluar la efectividad potencial de las simulaciones Red Team / Blue Team en el contexto del sector salud:

Identificación Proactiva de Vulnerabilidades

Las simulaciones Red Team permiten detectar vectores de ataque no contemplados en auditorías estándar, como accesos por ingeniería social, bypass de autenticaciones débiles, errores de configuración, presencia de sistemas legados no actualizados, falta de segmentación de red, uso compartido de credenciales y conexiones inseguras entre redes administrativas y clínicas.

Tiempo de Detección y Capacidad de Contención

El valor de un ejercicio Blue Team radica en su capacidad de detectar el ataque en tiempo real, activar alertas y coordinar una respuesta inmediata. La medición del tiempo medio de detección (MTTD) y el tiempo medio de respuesta (MTTR), aunque aquí no se evalúan empíricamente, constituyen variables clave en estudios internacionales como MITRE y el NIST.

Madurez de la Cultura Organizacional

La efectividad no se limita al equipo técnico. Las simulaciones permiten evaluar el nivel de concienciación del personal médico y administrativo, la existencia de planes de contingencia, la claridad en roles de respuesta y la integración de protocolos de continuidad de negocio con seguridad informática.

Adaptabilidad Normativa y Técnica

Al simular escenarios basados en el marco ATT&CK de MITRE, las simulaciones pueden comprobar si las instituciones cumplen con normas clave como:

NIST SP 800-53. Controles de seguridad para sistemas de información federales.

ISO 27799. Gestión de seguridad de la información en organizaciones de salud.

Modelo de Seguridad y Privacidad de la Información (MSPI). Estándar del MinTIC para entidades públicas colombianas.

Factores que Condicionan su Implementación en el Entorno Colombiano

Implementar ejercicios Red Team / Blue Team en el sector salud nacional enfrenta barreras técnicas, económicas y culturales:

Recursos Técnicos y Humanos Limitados

La mayoría de instituciones de salud en Colombia, especialmente aquellas del sector público y en regiones apartadas, operan con limitaciones severas en materia de infraestructura tecnológica y talento humano especializado. Muchos hospitales y clínicas utilizan sistemas informáticos legados, sin mantenimiento actualizado ni equipos dedicados exclusivamente a la ciberseguridad. La implementación de simulaciones Red Team / Blue Team requiere no solo personal capacitado en ofensiva y defensiva cibernética, sino también entornos de prueba, herramientas de análisis forense, licencias de software, monitoreo de red, entre otros recursos técnicos que actualmente escasean. Además, los departamentos de tecnología suelen estar centrados en la operación y soporte diario, sin capacidad para ejecutar ejercicios de evaluación avanzada.

Esta realidad refleja una brecha significativa entre las necesidades de protección y la capacidad real para implementar prácticas preventivas complejas. La falta de inversión en talento humano con perfil en ciberseguridad clínica (profesionales que comprendan tanto la seguridad informática como el funcionamiento del sistema hospitalario) dificulta la ejecución de ejercicios Red Team / Blue Team con el rigor requerido.

Ausencia de un CSIRT Sectorial en Salud

A diferencia de sectores como el financiero o el de telecomunicaciones, donde existen Equipos de Respuesta ante Incidentes de Seguridad Informática (CSIRT) especializados, el sector salud colombiano no cuenta con una entidad técnica propia para coordinar la respuesta y

la prevención de incidentes de ciberseguridad. La ausencia de un CSIRT Salud nacional limita el intercambio de alertas, buenas prácticas y análisis técnico entre entidades prestadoras de servicios de salud (EPS, IPS, clínicas, hospitales y farmacéuticas), y hace que cada institución gestione los riesgos de forma aislada y, muchas veces, reactiva.

Esta falta de centralización también impide el desarrollo de protocolos estandarizados de respuesta y la identificación de tendencias nacionales en amenazas a sistemas clínicos. En países como España o Estados Unidos, el sector salud cuenta con CSIRTs especializados como el Health-ISAC o iniciativas similares que promueven el fortalecimiento colectivo. En Colombia, la implementación de un CSIRT Salud permitiría no solo mejorar la coordinación frente a ciberataques, sino también liderar la integración de ejercicios Red Team / Blue Team a nivel nacional.

Cultura Reactiva y no Preventiva

Uno de los obstáculos más importantes para la adopción de estas prácticas es la falta de conciencia por parte de directivos y administradores del sector salud sobre el valor preventivo de los ejercicios de simulación. Muchas decisiones en ciberseguridad se toman con enfoque reactivo, tras un incidente, en lugar de anticiparse a ellos. Las simulaciones Red Team y Blue Team no son solo pruebas técnicas, sino herramientas estratégicas para evaluar la preparación organizacional ante amenazas reales.

Este desconocimiento se refleja también en la escasa integración entre los equipos técnicos y las áreas clínicas y administrativas, lo cual limita la adopción transversal de una cultura de seguridad digital. Las simulaciones permiten sensibilizar a todo el personal (médicos, administrativos, técnicos) mediante escenarios realistas que evidencian los riesgos de una mala gestión de accesos, el uso de contraseñas débiles, o la falta de protocolos ante fugas de

información. Sin embargo, cuando la seguridad informática no es vista como un componente crítico de la continuidad operativa, su adopción se relega a un segundo plano.

Falta de Cumplimiento y Regulación Efectiva de la Normatividad Existente

Como se explicó anteriormente, si bien Colombia ha avanzado en la expedición de normas en protección de datos personales y seguridad digital, como la Ley 1581 de 2012, el Decreto 1377 de 2013, y las guías del Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC, estas disposiciones carecen de mecanismos efectivos de seguimiento y control. En el contexto del sector salud, la aplicación de estas normas es muy heterogénea: mientras algunas instituciones privadas de alta complejidad han adoptado estándares como ISO/IEC 27799, otras clínicas y hospitales públicos continúan operando sin políticas claras de protección de la información clínica.

Además, no existe una regulación específica que obligue al sector salud a implementar ejercicios de simulación, auditorías técnicas avanzadas o mecanismos de evaluación continua de sus sistemas críticos. La interoperabilidad creciente de los sistemas de Historias Clínicas Electrónicas (HCE) entre EPS e IPS aumenta el riesgo de exposición de los datos, pero no está acompañada de normas técnicas actualizadas que exijan controles equivalentes. En este contexto, la incorporación de metodologías Red Team / Blue Team permitiría medir el grado de cumplimiento real de estas normas, pero requiere de un entorno legal y político que incentive su adopción y la sanción de su incumplimiento.

Buenas Prácticas Aplicadas al Sector Salud desde una Perspectiva Teórica

Con base en el análisis realizado, la implementación de simulaciones Red Team / Blue Team debe complementarse con un conjunto estructurado de buenas prácticas alineadas con el contexto colombiano. Estas buenas prácticas no solo permiten fortalecer la ciberseguridad de las

instituciones sanitarias, sino que también ayudan a cumplir con las obligaciones legales y aumentar la resiliencia institucional.

Aplicación del Plan de Seguridad del Operador (PSO)

El PSO es una herramienta esencial en la gestión de infraestructuras críticas, y en el sector salud debe incluir:

- Mapeo de activos críticos, como HCE, redes IoMT y servidores de respaldo.
- Protocolos de seguridad digital obligatorios, basados en el Decreto 338 de 2022.
- Evaluaciones periódicas de riesgo, integradas con la metodología MAGERIT.
- Definición de roles, responsabilidades y cadena de mando en ciber incidentes.

Este plan es obligatorio para entidades que prestan servicios esenciales, incluyendo hospitales públicos y privados.

Plan de Protección Específico (PPE)

El PPE aterriza las directrices del PSO a situaciones concretas. Algunas medidas recomendadas:

- Control de acceso físico y lógico a zonas con información crítica.
- Segmentación de redes que separen dispositivos médicos del resto de la red hospitalaria.
- Pruebas regulares de penetración y auditoría de seguridad técnica.
- Plan de continuidad del servicio médico ante incidentes.

Estas medidas están alineadas con el artículo 2.2.21.1.4.3 del Decreto 338 de 2022, que exige medidas de protección para servicios esenciales.

Caracterización de Activos con MAGERIT

La metodología MAGERIT permite:

- Clasificar activos según confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.
- Asignar criticidad a elementos como:
- Historias clínicas electrónicas.
- Sistemas de autenticación de usuarios.
- Servidores de imágenes diagnósticas (PACS).
- Equipos de soporte vital conectados a la red.
- Detectar sistemas obsoletos o sin soporte, vulnerables a exploits conocidos.
- Establecer una priorización de mitigación, facilitando decisiones de inversión en ciberseguridad.

Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI)

Una de las buenas prácticas más importantes es la adopción de un SGSI, conforme a la norma ISO/IEC 27001. Este sistema permite establecer una política organizacional de seguridad de la información basada en la mejora continua y la gestión de riesgos.

En el contexto hospitalario, un SGSI proporciona:

- Definición clara de roles y responsabilidades en ciberseguridad.
- Políticas de control de accesos, cifrado, respaldo y monitoreo continuo.
- Evaluaciones de riesgo periódicas, integrando estándares como MAGERIT o NIST SP 800-30.
- Auditorías internas y externas para asegurar la conformidad con estándares técnicos y legales.

La ISO/IEC 27799 puede integrarse para especificar controles aplicables al tratamiento de datos de salud, complementando así la estructura del SGSI.

Análisis Forense Digital como Soporte a la Respuesta a Incidentes

El análisis forense digital es una práctica clave para la investigación post-ataque en ambientes críticos. Aunque generalmente se emplea de manera reactiva, puede integrarse en simulaciones Blue Team como herramienta pedagógica.

Su aplicación en el sector salud permite:

- Rastrear el origen y el vector de ataque en accesos no autorizados a HCE.
- Recolectar evidencia legal para acciones disciplinarias o judiciales.
- Identificar fallos en la cadena de respuesta, mejorando los protocolos de detección y mitigación.
- Establecer líneas base de comportamiento normal, facilitando la detección de anomalías futuras.

En este contexto, es relevante destacar la importancia del análisis forense digital como una herramienta para ambientes hospitalarios. Su integración en simulaciones del tipo Blue Team ofrece un enfoque preventivo, formativo y estratégico. En el entorno de las Historias Clínicas Electrónicas, su implementación permitiría rastrear con precisión el origen de accesos no autorizados, recolectar evidencia técnica y legal, optimizar protocolos de respuesta ante incidentes y establecer líneas base para la detección de comportamientos anómalos. La inclusión de este enfoque no solo fortalece la respuesta ante ataques reales, sino que potencia el aprendizaje institucional y la preparación del personal ante futuras amenazas. Herramientas como Autopsy, FTK Imager, Volatility, Wireshark o ELK Stack, adaptadas al ecosistema clínico, pueden ser fundamentales para lograr estos objetivos.

Buenas Prácticas para la Protección de HCE

Con base en la Ley 1581 de 2012 y los lineamientos del MinTIC:

- Cifrado de extremo a extremo de los datos clínicos en tránsito y reposo, ya sea mediante VPN u otros medios.
- Autenticación robusta y registro de accesos para auditar operaciones sobre historias clínicas.
- Respaldo periódico de información y pruebas de restauración efectiva.
- Capacitación al personal médico y administrativo en privacidad de datos y prevención de incidentes.
- Monitoreo continuo de accesos sospechosos, usando SIEM o soluciones equivalentes.
- Implementación de protocolos de interoperabilidad segura, conforme al Plan IHCE 2023-2025 del Ministerio de Salud.

Conclusiones

El presente trabajo de investigación teórica ha permitido abordar de manera integral la problemática de la ciberseguridad en los sistemas de Historias Clínicas Electrónicas (HCE) en Colombia, a partir de un análisis crítico de sus vulnerabilidades, el estudio detallado de metodologías de simulación Red Team y Blue Team, y una evaluación de su aplicabilidad en el contexto del sector salud nacional. La creciente digitalización de los procesos clínicos, si bien ha facilitado el acceso y la interoperabilidad de la información médica, también ha expuesto al sector salud a riesgos cibernéticos de alto impacto. En este contexto, el estudio cobra relevancia porque aporta una mirada técnica y estratégica sobre cómo fortalecer la seguridad de estos sistemas críticos sin necesidad de aplicar pruebas de campo, enfocándose en análisis documentales y modelos probados en otros sectores. A lo largo del desarrollo del proyecto, se logró evidenciar que los HCE representan activos de alta sensibilidad, cuya protección es indispensable para garantizar la continuidad de los servicios hospitalarios, la privacidad de los pacientes y la integridad de la atención médica.

Se identificaron las principales amenazas y brechas de seguridad presentes en los HCE, incluyendo ataques por ransomware, phishing, puertas traseras (backdoors), denegación de servicio (DDoS) y explotación de dispositivos médicos conectados. Estas vulnerabilidades, sustentadas con datos estadísticos nacionales y reportes internacionales, demuestran una tendencia creciente de ataques dirigidos al sector salud, agravada por factores como la obsolescencia tecnológica, la carencia de infraestructura de respuesta especializada (como un CSIRT sectorial) y la débil implementación de marcos normativos existentes como la Ley 1581 de 2012 y el Decreto 1377 de 2013. La investigación permitió visibilizar que, pese a los avances

normativos, persiste una brecha significativa entre la regulación existente y su aplicación efectiva en los entornos hospitalarios.

Se realizó un estudio teórico de las metodologías Red Team y Blue Team, destacando su fundamento en la simulación de ataques y defensas en entornos controlados, como estrategia para identificar, mitigar y aprender de vulnerabilidades reales. A través del análisis de casos exitosos en sectores críticos como el financiero (CBEST - Reino Unido), energético (C2M2 - EE. UU.) y defensa (Locked Shields - OTAN), se evidenció que estas simulaciones no solo mejoran la capacidad de detección y respuesta ante amenazas, sino que también fomentan la madurez organizacional en materia de ciberseguridad. Su eficacia quedó demostrada mediante resultados como la reducción de brechas, mejoras en interoperabilidad de sistemas y el fortalecimiento de capacidades de defensa en tiempo real. Este análisis comparativo evidenció que, aunque el sector salud tiene particularidades únicas, también comparte vulnerabilidades estructurales similares con otros sectores críticos.

A partir de la comparación de los resultados de los casos de éxito, se proyecta que la implementación de ejercicios Red Team y Blue Team en el sector salud colombiano podría generar mejoras significativas en la postura de ciberseguridad, siguiendo la tendencia observada en sectores como el financiero y el energético. En dichos sectores, los informes muestran reducciones del 40 % en el número de vulnerabilidades críticas tras la implementación de simulaciones avanzadas (Bank of England, 2022; U.S. Department of Energy, 2021). Si bien el sector salud parte de un nivel de madurez más bajo, se estima que podría lograrse una reducción teórica de entre el 25 % y el 35 % en vulnerabilidades detectadas durante las primeras fases de aplicación, especialmente en sistemas de Historias Clínicas Electrónicas, redes IoMT y plataformas administrativas.

Además, al incorporar indicadores comparables como el MTTD y el MTTR, los estudios revisados permiten proyectar un escenario de mejora probable. Por ejemplo, en el sector financiero, la implementación de estas metodologías ha permitido disminuir el MTTD en un 60 % y el MTTR en un 50 % (Bridewell, 2021). Aplicando estas referencias al contexto hospitalario colombiano, se puede prever una mejora potencial del 30 % al 40 % en la capacidad de detección y contención de incidentes, siempre y cuando se acompañe de buenas prácticas, formación continua del personal y una adecuada gestión del cambio institucional. Estos resultados teóricos, aunque no verificados en campo, refuerzan la viabilidad y el impacto positivo de adoptar simulaciones Red Team y Blue Team como herramientas estratégicas para la seguridad digital del sector salud.

Finalmente, se propuso un enfoque teórico para aplicar estas metodologías al sector salud colombiano, definiendo buenas prácticas y lineamientos clave adaptados al entorno hospitalario. Se incluyeron recomendaciones basadas en estándares internacionales como NIST SP 800-53, ISO/IEC 27799 e ISO/IEC 27001, así como metodologías nacionales como MAGERIT para la gestión de riesgos en activos críticos. Además, se planteó la importancia de incorporar componentes como el establecimiento de un Sistema de Gestión de Seguridad de la Información (SGSI), la implementación de planes de protección específica (PPE) y de seguridad del operador (PSO), así como el fortalecimiento de procesos de análisis forense y gobernanza sobre los HCE. Estas recomendaciones no hacen parte de una propuesta implementada, pero sí establecen un marco guía sólido y aplicable a escenarios reales.

No obstante, también se identificaron dificultades relevantes para su implementación práctica: recursos humanos y financieros limitados, falta de talento especializado, carencia de un CSIRT sectorial para salud, y una cultura institucional predominantemente reactiva frente a la

seguridad informática. Estos factores condicionan la adopción de las simulaciones, pero no la hacen inviable. A través de una implementación gradual, apoyada en entornos académicos, con alianzas público-privadas y acompañamiento desde entes gubernamentales, es posible avanzar hacia una mayor madurez en ciberseguridad hospitalaria, especialmente si se consolidan marcos de política pública específicos para el sector salud.

Este trabajo representa un aporte teórico importante para el estudio de la ciberseguridad en infraestructuras críticas del sector salud. Más allá del análisis, se recalca la importancia de adoptar un enfoque preventivo y estratégico, donde las simulaciones Red Team y Blue Team no sean vistas como ejercicios aislados, sino como herramientas permanentes de mejora continua en la gestión de riesgos tecnológicos en la salud pública colombiana. Se espera que esta investigación motive el desarrollo de futuros estudios aplicados, pilotos experimentales y la formulación de políticas públicas orientadas a la protección integral de los sistemas de información clínica. Como proyección final, el estudio invita a seguir avanzando en la consolidación de una cultura de ciberseguridad hospitalaria basada en el conocimiento, la prevención y la cooperación institucional, pilares fundamentales para proteger la vida y la información en la era digital.

Referencias Bibliográficas

ACHC | Revista Hospitalaria del sector salud -. (2023). ACHC | Revista Hospitalaria Del Sector Salud. Ciberseguridad en el sector salud: un compromiso moral, legal y de sostenibilidad - https://revistahospitalaria.org/

Achury, N. (2018). Vulnerabilidades de las historias clínicas digitales ocasionadas por los Trabajadores de salud. https://repository.unad.edu.co/bitstream/handle/10596/25666/%20naachuryp.pdf?sequence=1

Acis, & Cano, J. (2018). Seguridad y ciberseguridad en los dispositivos médicos. 149, 55–66. https://doi.org/10.29236/sistemas.n149a7

Adler, E., Loevenich, J. F., Moxon, L., Hürten, T., Florian Spelter, Braun, J., Yann Gourlet, Lefeuvre, T., & Rigolin, R. (2024). Exploring the Potential of Large Language Models for Red Teaming in Military Coalition Networks. *MILCOM 2022 - 2022 IEEE Military Communications Conference (MILCOM)*, 170–175. https://doi.org/10.1109/milcom61039.2024.10773947

AKATI Sekurity. (2025). *Behind the simulated breach: A case study on red teaming for RMiT compliance*. AKATI Sekurity | Cybersecurity SWAT Team. https://www.akati.com/cybersecurity-case-studies/behind-the-simulated-breach-a-case-study-on-red-teaming-for-rmit-compliance

Alder, S. (2025, April 21). *Healthcare Organizations Struggling to Shift from Reactive to Proactive Cybersecurity*. The HIPAA Journal. https://www.hipaajournal.com/healthcare-cybersecurity-benchmarking-study-2025/

Alder, S. (2025, April 25). *ELENOR-Corp Ransomware Group Targets Healthcare with New Mimic Ransomware Variant*. The HIPAA Journal. https://www.hipaajournal.com/elenor-corp-ransomware-group/

Alejandra, L. (2024). Ciberseguridad: la necesidad de seguridad de los datos del paciente en América Latina. Puce.edu.ec; PUCE - Quito. https://repositorio.puce.edu.ec/items/175f67db-930f-4e69-9463-40716604da4d

Almeida, J. C., Loor, J. V., Pisco, X. M., & Guaña-Moya, J. (2023). Análisis de patrones y tendencias de las infracciones en ciberseguridad en un departamento de salud y servicios humanos. Revista Tecnopedagogía E Innovación., 2(2), 27–46. https://doi.org/10.62465/rti.v2n2.2023.55

Amazon Web Services. (2024). Amazon Web Services, Inc. *Estándares FHIR de almacenamiento e interoperabilidad de datos de salud - AWS HealthLake* https://aws.amazon.com/es/healthlake/

Anderson, E. (2023). *Cómo el Red Teaming automatizado continuo (CART) puede ayudar a mejorar su postura de ciberseguridad* Ibm.com. https://www.ibm.com/es-es/think/insights/how-continuous-automated-red-teaming-cart-can-help-improve-your-cybersecurity-posture

Bank of England. (2025). *CBEST threat intelligence-led assessments: Implementation guide*. https://www.bankofengland.co.uk/financial-stability/operational-resilience-of-the-financial-sector/cbest-threat-intelligence-led-assessments-implementation-guide

Bernal Mora, Y, Noguera Bocachica, J y Santos Suárez, J. (2024). Diseño de un centro de operaciones de ciberseguridad (SOC) basado en la norma ISO 27001 para el centro médico Oasis Colombia. Universidad Cooperativa de Colombia, Facultad de

Ingenierías, Ingeniería de Sistemas, Bogotá. Disponible en: https://hdl.handle.net/20.500.12494/55978

Bridewell. (2022, September 2). *Case study: Red Team assessment*. https://www.bridewell.com/insights/case-studies/detail/case-study-red-team-assessment

Buitrago-Botero, D. M. (2023). Rastreo normativo de la historia clínica electrónica en Colombia. Ratio Juris, 18(36), 305–326. https://www.redalyc.org/journal/5857/585777333013/html/

Cano, J., & Hernández, O. A. (2022). *Diseño de un equipo morado para el sector financiero colombiano enfocado en las Sociedades Comisionistas de Bolsa (SCB)*. AIS Electronic Library (AISeL). https://aisel.aisnet.org/isla2022/5/

Cervera García, A., & Goussens, A. (2024). Ciberseguridad y uso de las TIC en el Sector Salud. *Atención Primaria*, *56*(3), 102854. https://doi.org/10.1016/j.aprim.2023.102854

Chá, M. (2019). Historia clínica electrónica herramienta para la continuidad de asistencia. Revista Médica Del Uruguay. https://doi.org/10.29193/rmu.35.3.6

Ciberataque ransomware paraliza actividad del Hospital Clínic de Barcelona | INCIBE-CERT | INCIBE. (2023). Incibe.es. https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/ciberataque-ransomware-paraliza-actividad-del-hospital

Ciberseguridad en Colombia: desafíos y perspectivas. (2024). CCIT - Cámara Colombiana de Informática Y Telecomunicaciones. https://www.ccit.org.co/articulos-tictac/ciberseguridad-en-colombia-desafios-y-perspectivas/

Ciberseguridad en el sector salud: un compromiso moral, legal y de sostenibilidad - ACHC | Revista Hospitalaria del sector salud. (2024). ACHC | Revista Hospitalaria Del Sector Salud. https://revistahospitalaria.org/enportada/ciberseguridad-en-el-sector-salud-un-compromiso-moral-legal-y-de-sostenibilidad/

COLCERT- AL-0531- 0021. (2023). Alerta Ataques Cibernéticos Entidades y Organizaciones Colcert.gov.co. https://www.colcert.gov.co/800/w3-article-276383.html

CNPIC (2023). *Guías de Buenas Prácticas Plan de Protección Específico (PPE)*. Interior.gob.es. https://cnpic.interior.gob.es/pdf/publicaciones/guias-y-metodologias/2.GUIA-BUENAS-PRATICAS-PPE.pdf

CNPIC (2023). *Guías de Buenas Practicas Plan de Seguridad del Operador (PSO)*. Interior.gob.es. https://cnpic.interior.gob.es/pdf/publicaciones/guias-y-metodologias/1.-Guias-de-buenas-practicas-del-PSO.pdf

CNPIC (2025). *Guías y Metodologías*. Interior.gob.es. https://cnpic.interior.gob.es/es/publicaciones/guias-y-metodologias/

Cybersecurity Capability Maturity Model (C2M2). (2022). Energy.gov. https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

Cybersecurity: Cyber resiliency in healthcare. (2023). https://www.healthcarecan.ca/wp-content/themes/camyno/assets/document/PolicyDocs/2023/FINAL_CAN_DGSI_118_2023-09-22-EN.pdf?target=blank

David, J. (2024). La Ciberseguridad Que Manejan Las Infraestructuras Críticas En Colombia Específicamente Las Del Sector Salud Y Protección Social https://repository.unad.edu.co/bitstream/handle/10596/65294/jdosorioal.pdf?sequence=1&isAllowed=y

David, O., & Jaime, C. (2024). Estudio para el fortalecimiento de la ciberseguridad en el Hospital Universitario Santa Sofía de Caldas basado en las buenas prácticas de la ISO 31000. Ucm.edu.co. https://repositorio.ucm.edu.co/handle/10839/4470

Decreto 338 de 2022 - Gestor Normativo. (2022). se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones. Funcionpublica.gov.co. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=181866

Díaz, L. L. (2023). *¿Qué pasa con la ciberseguridad en las plataformas de salud de Colombia?* El Tiempo. https://www.eltiempo.com/tecnosfera/novedades-tecnologia/ciberseguridad-en-las-plataformas-de-salud-de-colombia-736510

Díaz, R. (2024). Análisis de los estándares y buenas prácticas de ciberseguridad utilizados por la industria colombiana. Unad.edu.co. https://repository.unad.edu.co/handle/10596/60042

Dorado, P. (2024, October 3). *La amenaza de los ciberataques en el sector salud en Colombia | Latinpyme*. Latinpyme. https://latinpyme.com/la-amenaza-de-los-ciberataques-en-el-sector-salud-en-colombia/

dpa. (2020). Hackerangriff auf Uniklinik Düsseldorf: Ermittlungen nach Tod einer Frau. *Heise Online*. https://heise.de/-4904134

Eduardo. (2024). Recomendar las mejores prácticas en el sector salud basadas en frameworks de ciberseguridad aplicables a hospitales del sector público en Colombia. *Unad.edu.co*. https://repository.unad.edu.co/handle/10596/61501

Escobar Escárraga, Sharat, Matilde, D., & Mahecha García, Camila. (2021). Historia Clínica Electrónica en Colombia: Diseño de un aplicativo para la validación de estándares jurídicos. Ces.edu.co. https://hdl.handle.net/10946/5568

Fuenmayor Tobar, J. H., Torres Lozano, D. K., Monsalve Pérez, L. D., y Becerra Moreno, A. M. (2024). La inteligencia artificial y Blockchain, dos elementos decisivos en el futuro de la ciberseguridad. Revista Agunkuyâa, 14(1). https://doi.org/10.33132/27114260.2431

Greig, J. (2021). *Ransomware groups continue assault on healthcare orgs as COVID-19 infections increase*. ZDNET. https://www.zdnet.com/article/ransomware-groups-continue-assault-on-healthcare-orgs-as-covid-19-infections-increase/

Jalali, M. S., & Kaiser, J. P. (2018). Cybersecurity in Hospitals: A Systematic, Organizational Perspective. *Journal of Medical Internet Research*, *20*(5), e10059–e10059. https://doi.org/10.2196/10059

Kriptos (2024). Ciberseguridad Sector Salud https://www.kriptos.io/es/es-post/ciberseguridad-sector-salud

La, E. (2023). *Las empresas que han sido blanco de ciberataques en Colombia en el último año*. Diario La República. https://www.larepublica.co/empresas/las-empresas-que-han-sido-blanco-de-ciberataques-en-colombia-en-el-ultimo-ano-3529667

Ley 2015 de 2020 - Gestor Normativo. (2020). Por medio del cual se crea la historia clínica electrónica interoperable y se dictan otras disposiciones. Funcionpublica.gov.co. https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=105472

Lopez, V. (2024). *Ciberseguridad en el sector salud: radiografía y cómo protegerse*. S2 Grupo. https://s2grupo.es/ciberseguridad-en-el-sector-salud-radiografia-y-como-protegerse/#:~:text=El%2054%25%20de%20los%20ataques,otros%20actores%20del%20sector%20salud.

Marcela, D. (2023, March 30). La ciberseguridad ahora juega un papel de liderazgo en la industria de la salud. Linkedin.com. https://es.linkedin.com/pulse/la-ciberseguridad-ahora-juega-un-papel-de-liderazgo-en-rios-mazo

Ministerio De Salud Y Protección Social (2023). Plan De Adopción Territorial Para La Interoperabilidad De La Historia Clínica Electrónica - IHCE 2023-2025, Versión 1.0

Bogotá from https://www.minsalud.gov.co/ihc/SiteAssets/Paginas/Interoperabilidad-de-Historia-Clinica/Plan%20IHCE-23-11-2023.pdf

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). (2021). *Locked Shields*. CCDCOE.org. https://ccdcoe.org/locked-shields/

Red Teaming. (2024, March 18). Airbus Protect. https://www.protect.airbus.com/cybersecurity/red-teaming/

Salud, R. (2022). *Keralty, grupo de EPS Sanitas y Colsanitas, confirma ciberataque a su plataforma*. ELESPECTADOR.COM; El Espectador. https://www.elespectador.com/salud/keralty-grupo-de-eps-sanitas-y-colsanitas-confirma-ciberataque-a-su-plataforma/#

Scott, J. (2021). *Red Teams vs. Blue Teams: What's the Difference, and How do Health IT Leaders Run These Exercises*. Technology Solutions That Drive Healthcare. https://healthtechmagazine.net/article/2021/10/red-teams-vs-blue-teams-whats-difference-and-how-do-health-it-leaders-run-these-exercises-perfcon?

Según IBM, Colombia en 2024 ha recibido el 17 % de los ciberataques en Latinoamérica, el 60 % afectaron al sector salud - La Nota Económica. (2024). La Nota Económica. https://lanotaeconomica.com.co/movidas-empresarial/segun-ibm-colombia-en-2024-ha-recibido-el-17-de-los-ciberataques-en-latinoamerica-el-60-afectaron-al-sector-salud/

Stock, I. (2024). Missing Link: Ransomware-Angriffe auf Krankenhäuser gefährden Menschenleben. *Heise Online*. https://heise.de/-9608151

Telefónica Tech S.L.U. (2024, January 23). *Informe de Ciberseguridad 2023 H2: aumento récord de vulnerabilidades y destacados incidentes de seguridad*. Telefónica Tech; Telefónica Tech S.L.U. https://telefonicatech.com/actualidad/informe-ciberseguridad-2023-h2-telefonica-tech

U.S. Department of Energy. (2022). *Cybersecurity capability maturity model (C2M2)*. Energy.gov. https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2

Zambrano Velillo, S. & Mora Velandia, D. (2024). Guía de buenas prácticas de ciberseguridad para entidades de salud en Colombia. [Tesis de pregrado, Universidad Cooperativa de Colombia]. Repositorio Institucional Universidad Cooperativa de Colombia. https://hdl.handle.net/20.500.12494/57185

Apendices

Apéndice A

Glosario

Activo de Información: Recurso que tiene valor para una organización, como bases de datos de pacientes, dispositivos IoMT, registros médicos electrónicos, entre otros.

Autenticación Multifactor (MFA): Sistema de validación de identidad que requiere más de una forma de autenticación (contraseña, token, huella, etc.) para mejorar la seguridad.

Blue Team: Grupo encargado de defender los sistemas de una organización mediante la detección, contención y respuesta ante ciberataques.

Ciberataque: Acciones ofensivas realizadas por actores maliciosos que buscan comprometer la seguridad de la información.

Ciberseguridad: Conjunto de prácticas, tecnologías y medidas destinadas a proteger los sistemas de información frente a amenazas y accesos no autorizados.

CSIRT (Computer Security Incident Response Team): Equipo de Respuesta a Incidentes de Seguridad Informática, clave para el manejo coordinado de eventos de seguridad.

Confidencialidad: Principio que garantiza que la información solo esté disponible para personas autorizadas.

Decreto 338 de 2022: Norma colombiana que regula la seguridad digital en infraestructuras críticas, incluyendo el sector salud.

Dispositivos IoMT: Internet of Medical Things. Equipos médicos conectados que recopilan y transmiten datos clínicos, como monitores de signos vitales o bombas de infusión.

Evaluación de Riesgos: Proceso para determinar las amenazas y vulnerabilidades a las que están expuestos los activos de información.

Gestión de Activos: Proceso que identifica y clasifica los recursos de información y su criticidad dentro de una organización.

HIPAA: Ley estadounidense que regula el uso y protección de la información médica, modelo de referencia internacional para seguridad en salud.

Historia Clínica Electrónica (HCE): Sistema digital para el registro, almacenamiento y gestión de la información médica del paciente.

Integridad: Principio que asegura que los datos no han sido modificados de manera no autorizada.

Interoperabilidad: Capacidad de los sistemas para intercambiar datos de forma precisa, segura y comprensible entre múltiples plataformas.

ISO/IEC 27799: Norma internacional que establece directrices para la seguridad de la información en salud, complementaria a la ISO/IEC 27001.

MAGERIT: Metodología española para el análisis y gestión de riesgos en sistemas de información. Utilizada para caracterizar activos y amenazas.

MSPI: Modelo de Seguridad y Privacidad de la Información adoptado por MinTIC en Colombia para entidades públicas.

NIST Cybersecurity Framework: Conjunto de estándares, directrices y buenas prácticas desarrolladas por el NIST para la gestión de riesgos en infraestructuras críticas.

PPE (Plan de Protección Específico): Documento estratégico que establece medidas de seguridad concretas para proteger una infraestructura crítica.

PSO (Plan de Seguridad del Operador): Plan general que establece cómo una entidad operadora de infraestructura crítica gestiona integralmente su seguridad digital.

Red Team: Grupo que simula ataques reales a la infraestructura de una organización para evaluar la eficacia de sus defensas.

Resiliencia Cibernética: Capacidad de anticiparse, resistir, responder y recuperarse ante incidentes de ciberseguridad.

Suplantación de Identidad: Delito que consiste en hacerse pasar por otra persona o entidad para acceder a sistemas o robar información.

Trazabilidad: Capacidad de seguir el historial de los accesos, modificaciones y uso de la información a lo largo del tiempo.