POLÍTICAS DE SEGURIDAD EN LA INFRAESTRUCTURA TECNOLÓGICA DE INSTITUCIONES DE SALUD MEDIANTE UN APPLIANCE FORTINET 80E: ESTUDIO DE CASO HOSPITAL BÁSICO JIPIJAPA

SECURITY POLICIES IN THE TECHNOLOGICAL INFRASTRUCTURE OF HEALTH INSTITUTIONS THROUGH A FORTINET 80E APPLIANCE: JIPIJAPA BASIC HOSPITAL CASE STUDY

Oscar Stalin Baque Pinargote [1*]

[1] Máster en Telecomunicaciones, Ingeniero en Sistemas, Docente de la Carrera Tecnologías de la Información, Facultad de Ciencias Técnicas, Grupo de Investigación Sistemas Inteligentes y Ciberfísicos, Universidad Estatal del Sur de Manabí. Ecuador. ORCID: https://orcid.org/0000-0003-1954-211X. Correo: oscar.baque@unesum.edu.ec

José Arturo Asanza Chóez [2]

[2] Master Universitario en Dirección Comercial y Marketing, Licenciado en Contabilidad y finanzas, Docente de la Carrera Administración de Empresas, Universidad Estatal del Sur de Manabí, Jipijapa, Ecuador. ORCID: https://orcid.org/0009-0005-0259-349X. Correo: arturo.asanza@unesum.edu.ec

Christian Dionisio Chiquito Manrique [3]

[3] Magister en Tecnologías de la Información y la Comunicación, Ingeniero en Computación y Redes, GAD – Jipijapa. Ecuador. ORCID: https://orcid.org/0009-0004-0601-2253. Correo: chiquito-christian6286@unesum.edu.ec

Christian Ruperto Caicedo Plúa [4]

[4] Doctor en Gestión de la Tecnología y la Innovación PhD, Magister en Gerencia Educativa, Ingeniero en Computación y Redes, Coordinador del Grupo de Investigación Sistemas Inteligentes y Ciberfísicos, Docente Titular de la Carrera de Tecnologías de la Información, Becario Senescyt, Docente Investigador Senescyt, Facultad de Ciencias Técnicas, Universidad Estatal del Sur de Manabí. Ecuador. ORCID: https://orcid.org/0000-0001-7351-8642. Correo: christian.caicedo@unesum.edu.ec

*** Autor para correspondencia:** christian.caicedo@unesum.edu.ec

Resumen

La presente investigación tiene como objetivo la implementación de políticas de seguridad informática para proteger los activos tecnológicos y reducir riesgos en la infraestructura tecnológica del Hospital Básico Jipijapa en la provincia de Manabí, a través de la identificación del estado del arte sobre políticas de seguridad informática en activos tecnológicos, la determinación las vulnerabilidades existentes y el diseño de políticas de seguridad informática para proteger los activos tecnológicos en organizaciones públicas. La metodología utilizada se enmarco desde el paradigma interpretativo, de enfoque cualitativo, tipo de investigación estudio de caso, los métodos escogidos fueron: bibliográfico, inductivo, análisis y síntesis, de alcance descriptivo, la técnica fue la entrevista a través de un cuestionario estructurado además de utilizar herramientas tecnológicas para el escaneo de la red de datos en periodos de tiempo. Los resultados develan la necesidad de la implementación de políticas de seguridad a través de la tecnología *appliance Fortinet 80e* en la infraestructura tecnológica del Hospital Básico Jipijapa y adherir políticas de seguridad propuestas en esta investigación, el presente modelo puede ser utilizado en otros entornos por otros hospitales y organizaciones médicas para mejorar sus estrategias de seguridad cibernética y proteger la información confidencial de los pacientes, este trabajo aporta al proyecto de investigación Institucional: "Factores que determinan la aceptación de tecnologías de ciudades inteligentes aplicado a estudiantes con un alto nivel de educación y al grupo de investigación: Grupo de Investigación Sistemas Inteligentes y Ciberfísicos – UNESUM".

Palabras clave: políticas de seguridad; infraestructura tecnológica; appliance Fortinet 80e.

Abstract

The objective of this research is the implementation of computer security policies to protect technological assets and reduce risks in the technological infrastructure of the Jipijapa Basic Hospital in the province of Manabí, through the identification of the state of the art on computer security policies in technological assets, determining existing vulnerabilities and designing computer security policies to protect technological assets in public organizations. The methodology used was framed from the interpretive paradigm, with a qualitative approach, type of case study research, the methods chosen were: bibliographic, inductive, analysis and synthesis, descriptive in scope, the technique was the interview through a structured questionnaire to use technological tools to scan the data network over time periods. The results reveal the need to implement security policies through the Fortinet 80e appliance technology in the technological infrastructure of the Jipijapa Basic Hospital and adhere to security policies proposed in this research. This model can be used in other environments by other hospitals and medical organizations to improve their cybersecurity strategies and protect confidential patient information, this work contributes to the Institutional research project: "Factors that determine the acceptance of smart city technologies applied to students with a high level of education and to the research group: Intelligent and Cyberphysical Systems Research Group – UNESUM."

Keywords: *security politics; Technological infrastructure; Fortinet 80e appliance*

Fecha de recibido: 07/01/2024
Fecha de aceptado: 09/03/2024
Fecha de publicado: 12/03/2024

Introducción

La ciberseguridad, también conocida como seguridad informática, se focaliza en salvaguardar la integridad y confidencialidad de la información, particularmente durante su procesamiento. Su enfoque central es prevenir la manipulación no autorizada de datos y procesos, asegurando que tanto individuos como equipos tecnológicos y datos permanezcan resguardados frente a posibles daños y amenazas originadas por terceros.

Esta disciplina se erige como un pilar esencial en la era digital, donde la información se convierte en un activo crítico y su protección es fundamental para preservar la confianza y el funcionamiento eficiente de sistemas, tanto a nivel individual como organizacional. La ciberseguridad, por tanto, no solo responde a la necesidad de evitar intrusiones no autorizadas, sino que también aborda el desafío constante de anticiparse y contrarrestar las cada vez más sofisticadas tácticas empleadas por actores malintencionados (1).

Al resguardar la integridad de los datos y la privacidad de los usuarios, la ciberseguridad no solo contribuye a mantener la confiabilidad de los sistemas informáticos, sino que también juega un papel crucial en la protección de la identidad digital y la mitigación de riesgos financieros asociados con posibles violaciones de seguridad (2). En última instancia, su propósito principal radica en garantizar un entorno digital seguro, donde la información fluya de manera confiable y las interacciones digitales se lleven a cabo sin comprometer la seguridad de los involucrados.

Para alcanzar con éxito este propósito, resulta imperativo garantizar la seguridad integral de la infraestructura informática, abordando tanto los aspectos internos como externos. La reducción de vulnerabilidades es esencial, y en este contexto, las políticas de seguridad desempeñan un papel central en la estrategia de seguridad informática (3). Implementadas de manera apropiada en el hardware y software pertinentes, estas políticas proporcionan un control meticuloso sobre las operaciones de la red, manteniéndonos alerta y preparados ante posibles vectores de ataque.

La importancia de la seguridad informática se manifiesta de manera destacada en la prevención y mitigación de riesgos (4). La seguridad interna se refiere a la salvaguarda contra amenazas que pueden surgir desde dentro de la propia red, como accesos no autorizados o mal uso de recursos (5). Por otro lado, la seguridad externa se enfoca en blindar la infraestructura contra amenazas externas, como ataques cibernéticos provenientes de fuentes externas.

Las políticas de seguridad, al ser el núcleo esencial de esta defensa, deben ser meticulosamente diseñadas y aplicadas en los componentes críticos de hardware y software. Este enfoque proactivo no solo busca reaccionar ante incidentes, sino prevenirlos en primer lugar (6). La aplicación adecuada de estas políticas ofrece un monitoreo continuo, alertas tempranas y una respuesta rápida ante cualquier indicio de actividad sospechosa. La disciplina en el ámbito informático encargada de resguardar la privacidad de datos en los sistemas se ha consolidado como una esfera esencial para el funcionamiento y éxito empresarial. En la era digital actual, donde la información constituye un activo crítico, la protección de datos no solo se erige como una obligación legal, sino que se convierte en un imperativo estratégico para la integridad y confianza de las operaciones empresariales.

La creciente interconexión de sistemas y la omnipresencia de datos digitales han acentuado la necesidad de una gestión y protección proactiva de la privacidad (7). En este contexto, esta disciplina no solo responde al

cumplimiento normativo, sino que también se erige como una salvaguarda contra posibles riesgos reputacionales y financieros asociados con brechas de seguridad y violaciones de privacidad. La importancia de esta disciplina radica en su capacidad para preservar la confidencialidad, integridad y disponibilidad de la información (8). Al implementar prácticas y tecnologías de protección de datos, las empresas no solo cumplen con regulaciones vigentes, sino que también fortalecen la confianza de los clientes y demás partes interesadas (9).

Así, esta disciplina se posiciona como un elemento crucial para asegurar la continuidad y sostenibilidad de las operaciones empresariales en un entorno digital dinámico y desafiante. En la contemporaneidad, la seguridad de las redes de comunicación de datos constituye uno de los desafíos primordiales en cualquier empresa. Al igual que en la seguridad física, reconocemos que no existe una garantía absoluta de protección del 100% para la infraestructura informática; siempre existe una potencial vulnerabilidad que requiere atención diligente (10). Surge, por tanto, la imperiosa necesidad de desarrollar prácticas que no solo reduzcan el riesgo latente, sino que también minimicen el impacto que podría derivarse de amenazas potenciales.

La comprensión de que la seguridad informática no puede ser una certeza absoluta nos impulsa a adoptar un enfoque proactivo (11). En lugar de buscar una protección infalible, nos centramos en estrategias que disminuyan la probabilidad de incidentes y, al mismo tiempo, atenúen su alcance en caso de que se materialicen. Este planteamiento reconoce la dinámica cambiante de las amenazas cibernéticas y la necesidad de una respuesta ágil y eficaz. La implementación de prácticas de seguridad robustas se convierte así en un componente crítico de la estrategia empresarial (12). Desde la segmentación de redes hasta la autenticación multifactorial, se busca crear capas de defensa que, en conjunto, fortalezcan la resiliencia de la infraestructura (13). Además, la concientización y capacitación continua del personal se erigen como elementos esenciales para fortalecer la primera línea de defensa contra posibles amenazas.

La seguridad informática abarca un conjunto integral de tecnologías, procesos y políticas diseñadas para resguardar redes, tráfico de datos y activos accesibles por red contra amenazas como ciberataques, accesos no autorizados y pérdida de datos (14). Esta salvaguarda es esencial para todas las organizaciones, desde pequeñas empresas hasta las corporaciones más extensas y proveedores de servicios en diversos sectores, dado el constante aumento en la superficie de ataque.

En un entorno digital cada vez más complejo, la seguridad informática se erige como el baluarte fundamental para proteger activos críticos y la infraestructura misma (11). La necesidad de esta defensa se torna aún más imperiosa a medida que las amenazas cibernéticas evolucionan y se diversifican (Ruperto et al., 2016). Desde intrusiones maliciosas hasta intentos de acceso no autorizado, las organizaciones se enfrentan a un panorama de riesgos en constante crecimiento, destacando así la vital importancia de la seguridad de red. Cada organización, independientemente de su tamaño o industria, se convierte en un potencial blanco de amenazas digitales (15)La implementación de medidas de seguridad, como firewalls, sistemas de detección de intrusiones y protocolos de cifrado, se vuelve esencial para mitigar riesgos y garantizar la integridad y confidencialidad de los datos (15). La seguridad de red no solo busca prevenir ataques, sino también proporcionar un entorno en el que las operaciones puedan llevarse a cabo con confianza y eficiencia.

Las instituciones de salud gestionan una infraestructura tecnológica vital que se ve continuamente amenazada por ciberdelincuentes que emplean diversas técnicas, tales como el malware (virus, troyanos, gusanos,

ransomware, *spyware*), *phishing* (suplantación de identidad), *man in the middle* (hombre en el medio), ataques de denegación de servicios (DDoS), Inyecciones SQL, entre otros. Este escenario coloca al limitado personal de tecnologías en una constante lucha por mantener la estabilidad de la red y la funcionalidad de los servicios, desviando su atención de tareas igualmente esenciales, como actualizaciones y mejoras en las plataformas.

La sofisticación de los ataques cibernéticos contra instituciones de salud ha aumentado significativamente, generando una presión constante sobre los profesionales de tecnologías. La diversidad de amenazas, desde el robo de datos hasta la interrupción de servicios críticos, implica que el personal de tecnologías debe dedicar considerables esfuerzos a la detección, mitigación y respuesta a estos incidentes(16). Esta realidad no solo afecta la seguridad de la información, sino que también impide una gestión eficiente del tiempo y recursos, lo que resulta en la postergación de actualizaciones y mejoras esenciales.

La saturación del personal de tecnologías no solo compromete la seguridad de los datos y la infraestructura, sino que también impacta negativamente en la capacidad de la institución de salud para evolucionar tecnológicamente. La necesidad urgente de fortalecer las defensas cibernéticas se vuelve evidente, permitiendo así que el personal pueda dedicar más tiempo y recursos a iniciativas de mejora y actualización que contribuyen directamente a la calidad y eficacia de los servicios de salud.

Dada la imperante necesidad expuesta, resulta esencial implementar un *appliance* que, mediante políticas adecuadas, automatice la mitigación de la mayoría de los ataques, contribuyendo así a mejorar significativamente los tiempos de respuesta de los sistemas en la infraestructura tecnológica (17). La seguridad de esta infraestructura emerge como un tema crítico para cualquier organización que gestione datos sensibles, y en el caso específico de instituciones de salud, se vuelve fundamental garantizar la protección de la información de los pacientes, la privacidad y confidencialidad de los datos médicos, así como la seguridad de los registros financieros.

La elección del *appliance Fortinet 80e* se revela como una medida estratégica, ya que ofrece una amplia gama de funcionalidades de seguridad, incluyendo firewall de próxima generación, antivirus, protección contra intrusiones, filtrado de contenido, VPN y gestión unificada de amenazas, entre otras. Este dispositivo se presenta como una solución integral capaz de abordar diversas capas de seguridad, proporcionando una defensa robusta contra una variedad de amenazas cibernéticas. La implementación de un *appliance* de esta envergadura no solo representa un paso hacia una mayor seguridad, sino que también ofrece la ventaja de una respuesta más rápida y automatizada ante posibles ataques (18). Al incorporar políticas de seguridad apropiadas, se establece una línea de defensa proactiva que no solo protege la integridad de los datos, sino que también reduce la carga operativa del personal de tecnologías, permitiéndoles enfocarse en iniciativas estratégicas y mejoras continuas en la infraestructura.

La adopción de este *appliance* representa una oportunidad significativa para que los hospitales fortalezcan su postura de seguridad en la infraestructura tecnológica. Al implementar esta solución, se logra una mejora sustancial en la seguridad, disminuyendo el riesgo inherente de pérdida de datos y mitigando la posibilidad de sufrir ataques cibernéticos (19). Esta medida no solo resguarda la integridad de la información sensible, sino que también actúa como una salvaguarda efectiva para garantizar el cumplimiento de regulaciones y normativas de privacidad y seguridad de la información médica, como la HIPAA.

La necesidad de proteger la información médica en hospitales es imperativa, dada la sensibilidad y confidencialidad de los datos que manejan. La implementación de este *appliance* se convierte, por lo tanto, en un paso crucial para elevar los estándares de seguridad, no solo en respuesta a las crecientes amenazas cibernéticas, sino también para cumplir con normativas estrictas que rigen la privacidad y seguridad de la información en el ámbito de la salud. Además de proporcionar una defensa activa contra posibles riesgos, la adopción de este *appliance* facilita el alineamiento con regulaciones como la HIPAA, que establece estándares rigurosos para la protección de la información médica. Al hacerlo, no solo se refuerza la seguridad interna del hospital, sino que también se construye una base sólida para la confianza de los pacientes y se demuestra un compromiso firme con la integridad y confidencialidad de sus datos médicos.

En este contexto, el objetivo primordial de la investigación es evaluar la factibilidad y los beneficios asociados con la integración del *appliance Fortinet 80e* en la infraestructura tecnológica de instituciones de salud, con el fin de asegurar la protección integral de datos y fortalecer la seguridad en general (20). La iniciativa se enfoca en analizar detalladamente cómo esta solución específica puede contribuir de manera efectiva a salvaguardar la integridad y confidencialidad de la información en entornos críticos como el sector de la salud. La elección de Fortinet 80e se sustenta en su versatilidad y funcionalidades integrales, las cuales se postulan como elementos clave para proporcionar una defensa robusta contra las amenazas cibernéticas que afectan a las instituciones de salud. La investigación busca, por tanto, no solo determinar la viabilidad técnica de la implementación, sino también identificar los beneficios tangibles que esta solución podría aportar a la seguridad general de la infraestructura tecnológica.

Además, la evaluación se orienta hacia la comprensión de cómo el appliance puede contribuir a cumplir con los estándares y regulaciones específicos del sector de la salud, garantizando así que la implementación no solo sea técnica y operativamente viable, sino también normativamente compatible. La investigación busca proporcionar una base sólida de datos y análisis que respalden la toma de decisiones informadas respecto a la adopción de esta solución en entornos de atención médica.
La presente investigación de enfoque mixto presenta dos resultados fundamentales. Realiza una revisión de la literatura científica para enmarcar el estado del arte actual, y propone una solución a la problemática objeto de estudio a parir de un estudio de caso en el Hospital Básico Jipijapa.

Materiales y métodos

La presente investigación nace del paradigma interpretativo, de enfoque cualitativo (21), el cual denota tres preguntas importantes para el desarrollo de un proyecto de investigación: ¿Qué? ¿Cómo? y ¿Con qué? Desde lo ontológico, epistemológico y metodológico.

Dentro de la presente investigación se plantea la unidad de análisis 1: Pregunta Ontológica: denotando el estado del arte sobre políticas de seguridad informática para proteger activos tecnológicos y REDUCIR riesgos a través de la metodología de (22). Preguntas: ¿Cuál es el marco teórico que sustenta el tema objeto de estudio?; ¿Cómo diagnosticar el estado actual de servicios que se transmiten en la infraestructura informática del Hospital Básico Jipijapa?; ¿Qué políticas de seguridad informática en la infraestructura tecnológica diseñar para el Hospital Básico Jipijapa mediante un APPLIANCE FORTINET 80E? Se tererminaron las unidades de análisis 2 y3:

- Unidad de análisis 2: preguntas epistemológicas denotando la relación y adquisición de datos a través de la entrevista y del instrumento cuestionario estructurado para extraer características y elementos relevantes sobre vulnerabilidades existentes que ponen en riesgo los activos tecnológicos del Hospital Básico Jipijapa, ¿Cómo la implementación de políticas de seguridad informática protegerá los activos tecnológicos y reducirá los riesgos en el Hospital Básico Jipijapa en la provincia de Manabí, Ecuador?; ¿Qué metodologías se han aplicado para generar políticas de seguridad informática en infraestructuras tecnológicas?
- Unidad de análisis 3: pregunta metodológica: desde el paradigma positivista, enfoque interpretativo, esta unidad se relaciona con el diseño de políticas de seguridad informática adecuadas y específicas para proteger los activos tecnológicos del Hospital Básico Jipijapa en la provincia de Manabí, Ecuador. ¿Qué tipo de metodología, procedimientos y métodos son los más empleados para el análisis de datos? El diseño de la investigación fue a través de un estudio de caso (23).

La aplicación de diferentes métodos investigativos, como el análisis-síntesis, histórico-lógico y revisión bibliográfica, enriquecieron y fortalecieron el presente proyecto de investigación. A continuación, se describe cómo se utilizaron estos métodos:

- Análisis-Síntesis:
  a) Realizar un análisis detallado de la infraestructura tecnológica actual del Hospital Básico Jipijapa para identificar vulnerabilidades y riesgos de seguridad.
  b) Examinar las prácticas actuales de seguridad informática y evaluar su eficacia.
  c) Analizar las regulaciones y normativas locales e internacionales relacionadas con la seguridad de la información en el ámbito de la salud.
  d) Sintetizar los hallazgos del análisis para identificar patrones, tendencias y áreas críticas que requieran atención en la implementación de políticas de seguridad.
  e) Desarrollar propuestas y recomendaciones sintetizadas para mejorar la seguridad informática en la infraestructura del hospital.
- Histórico-Lógico:
  a) Investigar la evolución histórica de la seguridad informática en entornos hospitalarios, examinando casos de estudio y lecciones aprendidas de implementaciones anteriores.
  b) Analizar incidentes de seguridad pasados en hospitales para comprender las amenazas y vulnerabilidades específicas que pueden haber surgido en el pasado.
  c) Aplicar un enfoque lógico para diseñar un marco de políticas de seguridad informática adaptado a las necesidades específicas del Hospital Básico Jipijapa.
  d) Establecer conexiones lógicas entre los elementos del marco de políticas, asegurando coherencia y eficacia en la aplicación.
- Revisión Bibliográfica:
  a) Examinar estudios académicos y artículos científicos relacionados con la seguridad informática en entornos hospitalarios y la implementación de políticas de seguridad en la atención médica.
  b) Revisar las mejores prácticas y estándares de seguridad informática aplicables al sector de la salud.
  c) Consultar manuales técnicos y documentos de proveedores de soluciones de seguridad informática para comprender las características específicas del hardware y software propuestos.

Explorar literatura técnica que describa la implementación exitosa de políticas de seguridad en hospitales similares.

Protocolo de revisión de la literatura

Se siguió la metodología propuesta por (18), a través de los siguientes pasos:

- **Paso 1: Definir el alcance de la investigación**

La presente revisión sistemática de la literatura científica sobre la implementación de políticas de seguridad informática en la infraestructura tecnológica brinda una visión integral, fundamentada y actualizada sobre el tema. Ayuda a identificar el estado actual del conocimiento, evaluar la calidad de la evidencia, identificar brechas y lagunas, y proporcionar información relevante para la toma de decisiones. Esto puede ser especialmente útil para informar estrategias de implementación de políticas de seguridad informática más efectivas y adaptadas a contextos específicos, como el Hospital Básico Jipijapa de la provincia de Manabí, Ecuador, en este caso particular. En esta etapa, debes estableció claramente el tema de tu investigación y delimitar el alcance de tu Estado del Arte, definiendo las palabras clave: políticas de seguridad informática e infraestructura tecnológica, además de las bases de datos utilizadas: Scopus, Scholar y Dialnet, dentro de los criterios de calidad: artículo científico, tesis de postgrado, que el articulo tenga citas, que el resumen contenta la siguiente estructura (problema, objetivos, metodología, resultados y conclusiones) lo que permitió identificar los estudios relevantes en la literatura científica.

- **Paso 2: Búsqueda y selección de estudios**

Se realizó una búsqueda exhaustiva en bases de datos académicas, revistas científicas, conferencias y otros recursos relevantes para tu área de investigación. Utilizó las palabras clave ciberseguridad e infraestructura tecnológica y criterios de búsqueda para filtrar y seleccionar los estudios más pertinentes. Excluye aquellos que no cumplan con tus criterios de inclusión (alto número de citas, información enmarcada en los últimos 3 años, que el resumen contenga problema, objetivos, metodología, resultados y conclusiones en 250 palabras). Se procedió a buscar información en la base de datos Scopus denotando 919 artículos científicos en formato CSV y RIS.

Las herramientas tecnológicas utilizadas fueron: Citespace y Vosviwer (24) permitiendo denotar un análisis de conglomerados observando relaciones y la evolución sistemática de la Ciencia, a continuación, se detallan características importantes.

- **Paso 3: Evaluación de la calidad de los estudios**

Una vez que hayas seleccionado los estudios relevantes, es importante evaluar su calidad y validez. Examina la metodología utilizada, el tamaño de la muestra, la rigurosidad de los análisis y cualquier sesgo potencial en los resultados.

- **Paso 4: Extracción y organización de datos**

Se procedió la extraer los datos relevantes de cada estudio seleccionado elementos como: problema, objetivos, las metodologías, los resultados principales y las conclusiones.

- **Paso 5: Análisis y síntesis de los resultados**

Se analizó los datos obtenidos de la base de datos Scopus s extraídos de los estudios seleccionados y busca patrones, tendencias o discrepancias en los resultados. Se identificaron las principales conclusiones y hallazgos de los estudios revisados.

Se realiza un análisis crítico de los estudios y muestra cómo se relacionan entre sí. En el estado del arte se realiza un análisis de la bibliografía sobre la implementación de políticas de seguridad en la infraestructura tecnológica de un hospital mediante un *appliance Fortinet* 80e. Se examinan los resultados de investigaciones recientes sobre el uso de este dispositivo en hospitales expresados en artículos científicos.

Además, se revisarán los trabajos relacionados con la implementación de políticas de seguridad en la infraestructura tecnológica de un hospital utilizando otros dispositivos similares, como Cisco ASA y Check Point, con el fin de comparar los resultados y determinar la eficacia del appliance Fortinet 80e en esta área. En los últimos años, ha habido una serie de investigaciones sobre Fortinet 80e y sus capacidades de seguridad. Aquí se presenta un resumen de algunas de las publicaciones más relevantes de los últimos 3 años que constituyen el estado del arte.

Consideraciones éticas

Todos los participantes fueron informados del contexto de la investigación antes de contestar el cuestionario para obtener su consentimiento. Se garantizó la confidencialidad y el anonimato de los datos recopilados. La investigación se llevó a cabo de acuerdo con los principios éticos y las pautas establecidas por nuestra institución académica.

Resultados y discusión

Uno de los principales resultados de la investigación, fue la revisión de la literatura realizada. En la figura 1, se muestra 919 artículos que forman parte de la unidad de análisis de documentos por año, denotando interés significativo desde el año 2002 con un nivel de crecimiento importante llegando hasta el pico más alto en el 2020 y en el 2023 se tiene una base de creciente de 18 documentos relacionados con políticas de seguridad informática en organizaciones.

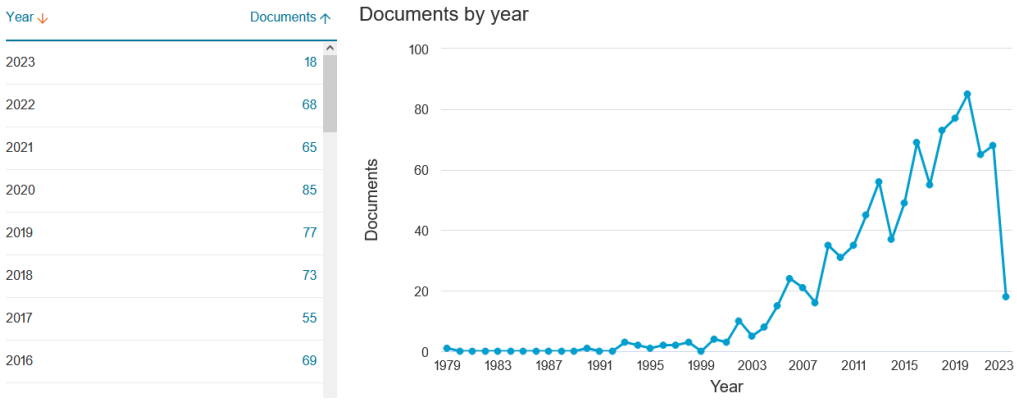

Figura 1. Documentos por año identificados en la base datos Scopus hasta el año 2023.
Fuente: Adaptado de la base de datos Scopus, 2023.

En la Figura 2, muestra que Estados Unidos con 269 artículos científicos es el que más se destaca en la publicación de resultados de investigación seguido por Reino Unido, Malasia, China, entre otros. Dentro de los países de América del Sur se tiene a Brasil con 18 documentos de alto impacto, Perú con 5 documentos, Colombia con 3 documentos y Ecuador con 3 documentos, criterios que forman parte importante para entender el desarrollo sistemático que ha tenido mencionado fenómeno de estudio.

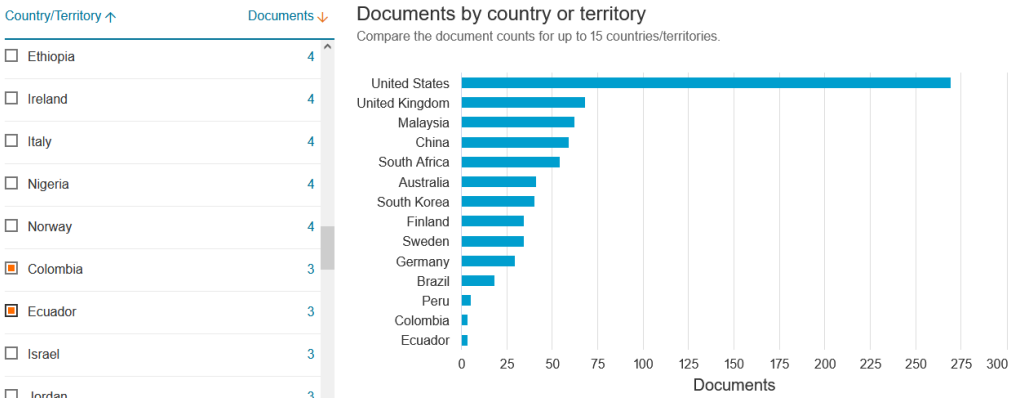

Figura 2. Países donde más interés se tiene sobre Políticas de seguridad informática.
Fuente: Adaptado de la base de datos Scopus, 2023.

En la Figura 3, se puede observar que se encontraron 729 artículos científicos desde el área de las Ciencias de la Computación, 255 artículos desde las Ciencias Sociales, desde las ingenierías 200 artículos, denotando gran interés desde el enfoque técnico – científico en miras a fortalecer políticas de seguridad informática en entornos organizacionales.

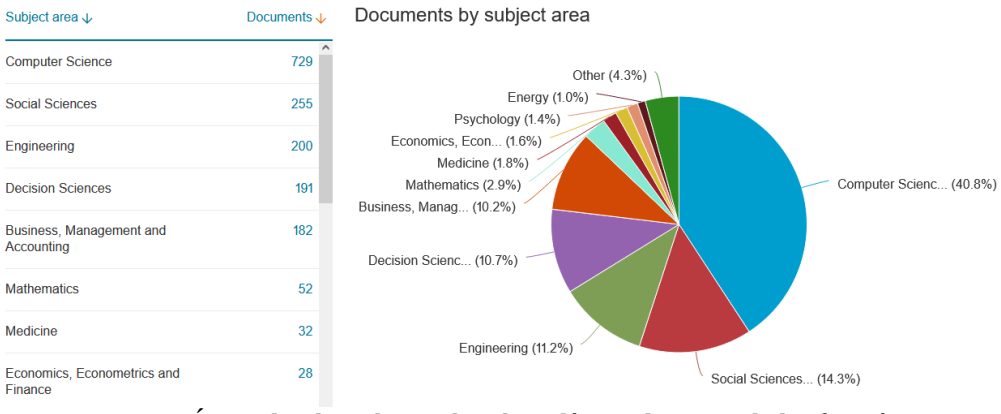

Figura 1. Áreas donde se han aplicado políticas de seguridad informática.
Fuente: Adaptado de la base de datos Scopus, 2023

La Figura 4, denota las revistas científicas que publican con mayor relevancia los resultados sobre políticas de seguridad informática en las organizaciones señalando las siguientes: *Computers and Security*, *Information and Computer Security*; IFIP *Advances in Information and Communication Technology*; Journal Of Computer Information Systems e *Information And Management*.

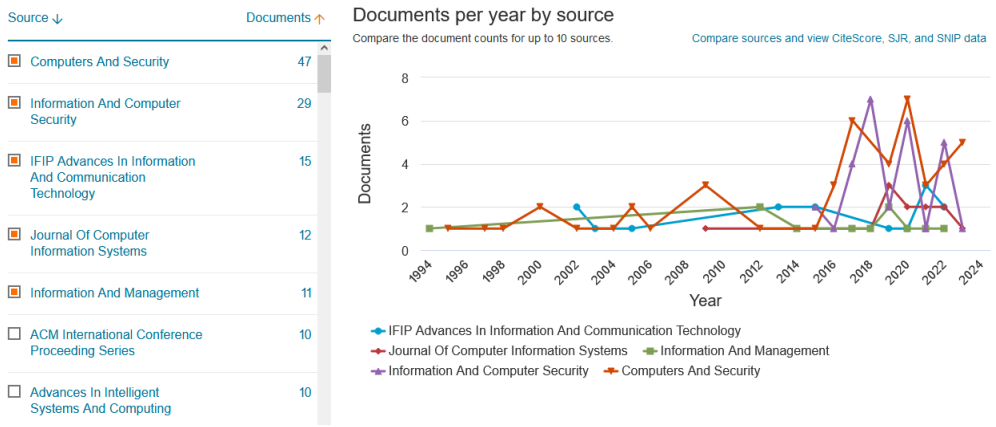

Figura 2. Revistas científicas donde con mayor realce se publica sobre políticas de seguridad informática.
Fuente: Adaptado de la base de datos Scopus, 2023.

A continuación, se realizó un análisis de conglomerados de palabras claves de la base de datos Scopus, denotando en la Figura 5, la importancia de las palabras claves utilizadas en la investigación.

Keyword	Occurrences	Total link strength
security of data	584	4394
information security policies	533	4087
security systems	454	3576
information security	259	1825
information security policy	199	1397
information systems	160	1331
security policy	113	915
behavioral research	99	908
personnel	103	868
information use	92	786
information management	91	752
compliance	76	659
information security managements	66	606
public policy	66	558
industrial management	57	551
surveys	54	506

Figura 3. Coocurrencias de palabras claves y relaciones.
Fuente: Adaptado de la base de datos Scopus, 2023

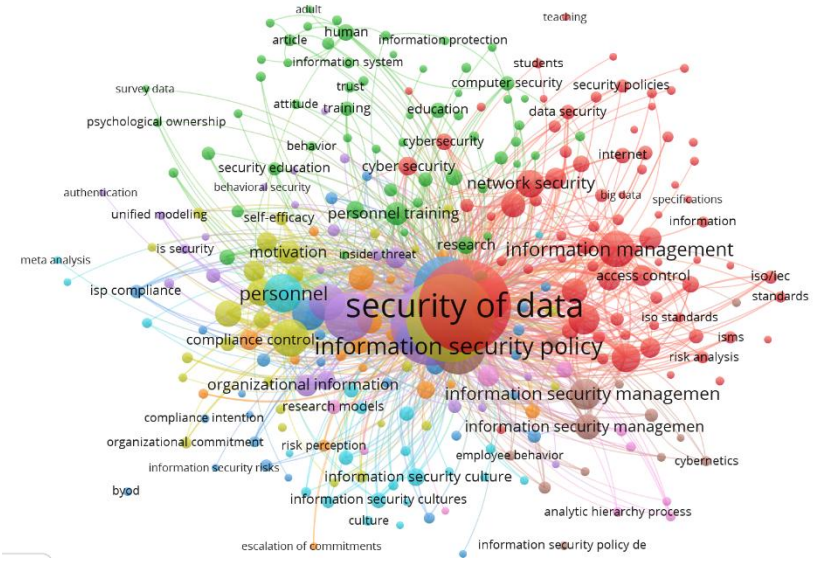

Figura 4. Análisis de conglomerados de palabras claves con datos de Scopus, 2023.
Fuente: Adaptado de la base de datos Scopus, 2023.

En la Figura 6, se denota una red de conglomerados explicando las relaciones significativas entre las palabras más utilizadas en las investigaciones encontradas en la base de datos Scopus, de igual manera la Figura 7, identifica elementos importantes sobre la temática investigada (ciberseguridad, seguridad de los datos, seguridad en la red).

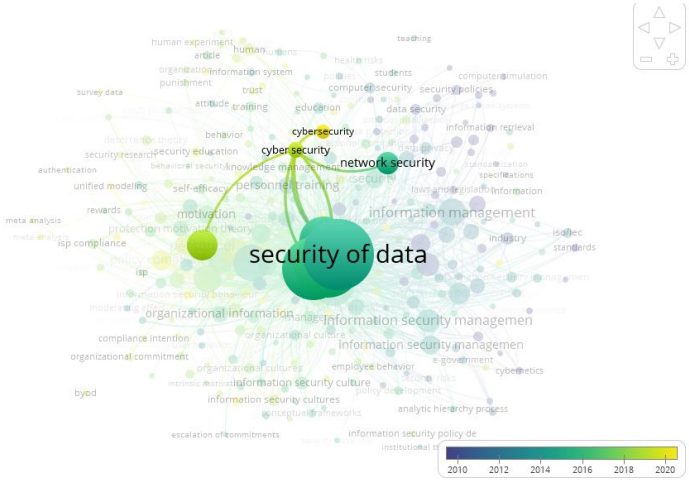

Figura 5. Identificación de elementos sobre la temática investigada.
Fuente: Adaptado de la base de datos Scopus, 2023.

La tabla 1 muestra los elementos y características de los artículos científicos recuperados con la implementación del protocolo de revisión definidos.

Tabla 1. Elementos y características de los artículos científicos identificados.

Artículo	Cantidad pertinente de citas	Fuentes actualizadas	Metodología utilizada	Consistencia y coherencia	Objetividad y ausencia de sesgos	Relevante para la investigación
(25)	X	X	X	X	X	X
(26)	X	X	X	X	X	X
(27)	X	X	X	X	X	X
(28)	X	X	X	X	X	X
(29)						
(30)	X	X	X	X	X	X
(31)	X	X	X	X	X	X

Fuente: Adaptado de la base al proceso de análisis de los artículos científicos

Para los autores (25) analizaron el ransomware y como estos afectan y se propagan a través de redes afectando los activos de información de la organización, como registros médicos electrónicos, servidores de bases de datos, servidores de archivos, servidores de aplicaciones, servidores web, controladores de dominio y otros dispositivos conectados, incluyendo dispositivos de IoT y SCADA (Supervisión, Control y Adquisición de Datos). Esta investigación se basó en controles técnicos y administrativos, estándares de seguridad, procedimientos, pautas y mejores prácticas siguiendo marcos de seguridad como ISO 27001, HIPAA y NIST. El objetivo principal fue mitigar los ataques de ransomware y proteger la organización de sus efectos perjudiciales.

Por otra parte, los temas de ciberseguridad son relevantes ya que resulta importante establecer políticas de seguridad de la información y ponerlas en práctica, los autores (26) desarrollaron una simulación de un posible ataque a los sistemas SCADA utilizados en el ámbito financiero identificando vulnerabilidades del sistema. Los autores (27) reconocieron que el eslabón más débil en una organización es la seguridad de la información, identificaron antecedentes para el cumplimiento de los empleados aplicando políticas de seguridad de la información (ISP) de una organización. Se llevó a cabo una entrevista entre usuarios de computadoras de organizaciones, estableciendo una política de seguridad de la información. Un novedoso modelo de múltiples teorías se deriva de la teoría de la acción razonada, la teoría de la evaluación cognitiva y Hanoo, y ese modelo se presenta para evaluar los datos recopilados a través de la entrevista. Los resultados muestran que la intención de cumplir de un empleado está influenciada por la actitud, los programas de concientización sobre seguridad y las recompensas. La intención de cumplir, a su vez, influye en el cumplimiento real del ISP.

Los autores (18) argumenta que las investigaciones actuales se enfocan en analizar cómo los mecanismos de influencia externa, como la disuasión, inciden en el cumplimiento de la política de seguridad de la información (ISPC) en las organizaciones. Este artículo aborda la formación de la ISPC desde una perspectiva de motivación autónoma, basada en las teorías del intercambio social y de la autodeterminación. Se llevó a cabo una entrevista con 261 empleados, y se aplicó un análisis de regresión jerárquica para verificar las hipótesis planteadas. Los hallazgos señalan lo siguiente: en primer lugar, la satisfacción laboral y la responsabilidad personal tienen un impacto positivo en la ISPC. En segundo lugar, la satisfacción laboral percibida por los empleados se relaciona positivamente con la responsabilidad personal, y la severidad de la disuasión actúa como un moderador negativo en esta conexión. Por último, la responsabilidad personal media la relación entre la satisfacción laboral y la ISPC. Este estudio sugiere que el respaldo organizacional debería enfocarse en

fomentar la autodeterminación percibida de los empleados, manteniendo la disuasión a un nivel moderado para adaptarse a la estrategia de seguridad de la organización y al entorno de seguridad de la información.

Los autores (32) investigan el papel desempeñado por las contribuciones basadas en la literatura en el desarrollo práctico de políticas de seguridad de la información (ISP). Se realiza una revisión de la literatura para identificar las entradas comúnmente utilizadas en la teoría para el desarrollo de ISP. Luego, empleando un enfoque interpretativo a través de la teoría institucional, se examina la influencia de las aportaciones basadas en la literatura en la práctica del desarrollo de ISP. Este estudio se apoya en entrevistas semiestructuradas con altos funcionarios y gerentes de seguridad de la información con experiencia en el sector público sueco. A partir de la revisión de la literatura, se identifican 10 insumos clave para el desarrollo de ISP. Los resultados de las entrevistas indican que estos insumos desempeñan un papel más amplio que el de simples herramientas racionales, ya que factores como el contexto organizacional, las presiones institucionales y la búsqueda de legitimidad juegan un papel crucial en el desarrollo efectivo de las políticas de seguridad de la información.

Los autores (17) determinaron que la gestión de la Seguridad de la Información, destinada a resguardar los activos de información de una organización, constituye una actividad de suma importancia en el ámbito organizacional. La observancia por parte de los empleados de la Política de Seguridad de la Información ha captado la atención de los investigadores, quienes han propuesto prácticas vinculadas al respaldo de la Alta Dirección, la elaboración de la Política de Seguridad de la Información y la comunicación. Este artículo presenta las prácticas identificadas a partir de una revisión de la literatura científica en relación con el cumplimiento de la Política de Seguridad de la Información. La implementación de estas prácticas identificadas contribuye al acatamiento efectivo de la Política de Seguridad de la Información.

Así mismo los autores (28) investigan los determinantes de una percepción positiva de la cultura de seguridad de la información (ISC) y cómo esta afecta la intención de cumplimiento (INT) de la Política de Seguridad de la Información (ISP) en profesionales de TI y no TI en universidades públicas de Malasia. Se emplea un modelo de ecuación estructural de mínimos cuadrados parciales con PLS MGA para evaluar los modelos estructurales y de medición, comparando los resultados entre ambos grupos. Los hallazgos revelan que todos los factores contribuyen de manera significativa a la ISC en ambos grupos, con dos de siete factores que muestran diferencias significativas. Aunque ambos grupos comparten los mismos factores de ISC, se observa una diferencia significativa entre profesionales de TI y no TI en cuanto a la percepción de la necesidad del compromiso de la alta dirección y el conocimiento de seguridad de la información para implementar una ISC positiva. Además, existe una disparidad significativa entre estos dos grupos en cuanto a la influencia de la ISC en la INT de cumplimiento de ISP. La ISC tiene una menor influencia en la INT para profesionales no TI en comparación con los profesionales de TI dentro de la misma ISC. Este estudio también propone soluciones integrales de ciberseguridad para fortalecer la cultura de seguridad de la información y el cumplimiento de los empleados en relación con la Política de Seguridad de la Información.

Los autores (31) presentan el desarrollo de un cuestionario validado destinado a evaluar el comportamiento de seguridad de la información. El artículo tiene como objetivo proporcionar información sobre el proceso de validación del cuestionario y los resultados de un estudio cuantitativo basado en datos recopilados a través de entrevistas cuantitativas en universidades africanas del Sur (N = 263). La metodología aplicada, que incluyó un análisis factorial exploratorio, resultó en la identificación de 11 factores. Los valores del alfa de Cronbach

para estos 11 factores superaron todo el umbral de 0.7, indicando así que el cuestionario posee validez y confiabilidad. Los resultados del análisis de correlación revelan una relación estadísticamente significativa entre los factores de competencia y los factores de autonomía. Asimismo, se observa una relación parcialmente significativa entre la autonomía y los factores de relación, así como entre la competencia y los factores de relación. De igual manera es importante realizar análisis exhaustivos sobre la administración de la seguridad de la información en el ámbito de la salud. De igual manera la identificación de desafíos en términos de privacidad y seguridad y la importancia de la gestión de riesgos, la implementación de políticas y procedimientos, la capacitación del personal y la participación del paciente.

Los autores (33) examinaron las leyes y normativas vigentes vinculadas a la salvaguardia de la privacidad y confidencialidad de los datos de los pacientes en el ámbito sanitario. Se resaltó la imperiosa necesidad de acatar dichas regulaciones y de ofrecer una protección adecuada para asegurar la privacidad y confidencialidad de la información de los pacientes. Denotando la importancia de generar un marco integral para la seguridad de la información en el sector de la salud (17), el marco debe cubrir las áreas clave de la gestión de riesgos, la seguridad de la tecnología de la información, la gestión de la seguridad y la gestión de incidentes. Así mismo, los autores (34) identificaron las amenazas y riesgos asociados a la ciberseguridad, enfatizando la vital importancia de fomentar la conciencia de seguridad y proporcionar capacitación al personal como medida para MITIGAR estos riesgos.

Se subraya la importancia crítica de salvaguardar la información en entornos hospitalarios, tomando en cuenta los elementos clave que guían la investigación en este ámbito. Asimismo, se ha llevado a cabo una exhaustiva revisión de la literatura académica y técnica actual, centrándose en el uso del APPLIANCE FORTINET 80E en hospitales y comparándolo con dispositivos similares. Este análisis posibilita una evaluación más precisa y comprensión de las ventajas y características distintivas del Fortinet 80E en el contexto de la seguridad de la información en el entorno hospitalario.

La teoría del Sistema Integrado de Gestión de la Seguridad de la Información y los Elementos Generales de una Política de Seguridad Informática, son teorías fundamentadas en estándares como ISO/IEC 17799 (2000), y proporcionan un sólido marco conceptual para comprender y abordar la crucial necesidad de asegurar la confidencialidad, integridad y disponibilidad de los datos en los sistemas de información.

La inclusión de estas teorías no solo robustece la investigación, sino que también aporta un enfoque estructurado respaldado por estándares internacionalmente reconocidos en la gestión de la seguridad de la información, especialmente en entornos hospitalarios. Este enfoque estructurado no solo contribuye a la coherencia metodológica, sino que también garantiza una aplicación eficiente y efectiva de medidas de seguridad en el ámbito hospitalario.

Estudio de caso Hospital Básico de Jipijapa

Se realizó un análisis exhaustivo del Hospital Básico de Jipijapa, ubicado en la provincia de Manabí, Ecuador. Se examinó detalladamente los aspectos clave vinculados a la infraestructura tecnológica y la seguridad de datos actualmente implementadas en el hospital. El propósito fundamental de este diagnóstico fue obtener una visión integral de la situación presente, con el fin de identificar tanto las fortalezas existentes como las áreas susceptibles de mejora, especialmente en lo que respecta a la tecnología y seguridad de la información para la gestión eficaz de datos y la prestación de servicios médicos de calidad. Mediante este enfoque, se

buscó establecer una base sólida que facilitó la formulación de recomendaciones y soluciones destinadas a impulsar la modernización y optimización tecnológica en el Hospital Básico de Jipijapa.

En el Hospital Básico Jipijapa, se encuentra el área de Tecnologías Informáticas y Comunicaciones, la cual opera con un data center que alberga cuatro equipos servidores. Estos servidores desempeñan un papel fundamental al proporcionar las diversas herramientas tecnológicas utilizadas en todos los departamentos de esta unidad de salud. Sin embargo, es crucial señalar que estos servidores han superado su vida útil y carecen de vigencia tecnológica, lo que se refleja en su alto consumo de energía eléctrica, la ocupación significativa de espacio físico y la demanda extensa de horas de servicio por parte del único personal técnico disponible. Esta situación plantea un desafío significativo para la eficiencia operativa y la continuidad del servicio, subrayando la necesidad apremiante de abordar la obsolescencia tecnológica y mejorar la infraestructura informática en el hospital (35).

Se presentan desafíos significativos en cuanto a la seguridad de la información debido a los actuales ataques que enfrenta la red de datos, agravados por la falta de recursos para mejorar el Data Center y adquirir equipos que refuercen la seguridad y protección de la información. Esta carencia pone en riesgo la disponibilidad de los productos tecnológicos esenciales que la institución necesita para ofrecer servicios de calidad y llevar a cabo sus actividades en pos del bienestar social de la comunidad a la que atiende esta unidad de salud.

El diagnóstico de esta problemática se llevó a cabo en dos fases. En primer lugar, se identificaron los desafíos existentes relacionados con la seguridad de la información y la infraestructura tecnológica. A continuación, se abordará de manera integral la necesidad de fortalecer la ciberseguridad y mejorar los recursos tecnológicos, reconociendo la importancia crítica de estas medidas para mantener la calidad y disponibilidad de los servicios ofrecidos por la institución de salud:

1. Escaneo de la red y ataques controlados para la detección de vulnerabilidades a través del enfoque cualitativo de (36).
2. Entrevista con un cuestionario de preguntas estructuradas aplicada a 50 participantes que trabaja en el Hospital básico de Jipijapa, con el objeto de percibir los factores que afectan la seguridad de datos dentro de infraestructura tecnológica de la Institución.

Los resultados obtenidos se pueden observar en 2 momentos:

a) Primer momento: Escaneo de la red de datos del Hospital Básico Jipijapa.

Durante un periodo de dos semanas, se llevaron a cabo ataques controlados e inocuos, así como procesos de escaneo de red y paquetes, con el objetivo de identificar posibles vulnerabilidades en cada sistema. Esta estrategia se implementó considerando que las infraestructuras de tecnologías de la información presentan necesidades y soluciones de ciberseguridad específicas. En el análisis realizado, se abordaron los vectores de ataque más comunes, entre ellos "phishing", malware, fuerza bruta, inyección SQL, "cross-site scripting" y denegación de servicios. La información detallada al respecto se presenta en la Tabla 2. Este enfoque se diseñó para adaptarse a las particularidades de cada sistema, permitiendo una evaluación exhaustiva de las amenazas y la posterior implementación de medidas de seguridad personalizadas.

Tabla 2. Ataques a la red del hospital básico de Jipijapa.

Tipo de ataque	Cantidad de ataques
Ataques de Pishing	47
Ataques de Malware	32
Ataques de Fuerza Bruta	17
Ataques de Inyección SQL	67
Ataques de Cross-Site Scripting XSS	23
Ataques de Denegación de Servicios	217
Total	**403**

Realizado por: Los investigadores

En la Tabla 2, se destaca que el tipo de ataque más recurrente en la red de datos es la "Denegación de Servicios", con un total de 217 incidentes registrados. Este hallazgo sugiere que los atacantes intentaron saturar el sistema objetivo mediante un gran volumen de solicitudes, lo que culminó en una interrupción o inaccesibilidad del servicio para los usuarios legítimos. Este patrón revela la importancia de implementar medidas específicas para mitigar y prevenir este tipo de ataques, asegurando así la continuidad y disponibilidad de los servicios en la red, mejorando resultados de los autores (37).

En la segunda posición, se encuentran los ataques de "Inyección SQL", con un total de 67 incidentes registrados. Este tipo de ataques tiene como objetivo principal explotar las vulnerabilidades presentes en las consultas de bases de datos, con la finalidad de obtener acceso no autorizado o extraer información confidencial de manera ilícita. La relevancia de este hallazgo subraya la necesidad de reforzar la seguridad en las consultas de bases de datos, implementando medidas efectivas para prevenir y contrarrestar posibles amenazas de inyección SQL en el sistema.

En la tercera posición, se identifican los ataques de "Phishing" con un total de 47 casos. El "phishing" representa una modalidad de ataque en la que los ciberdelincuentes buscan engañar a los usuarios con el objetivo de obtener información confidencial, como contraseñas, datos bancarios o información personal. Estos ataques suelen desplegarse a través de correos electrónicos, mensajes de texto o llamadas telefónicas fraudulentas. La frecuencia de estos incidentes subraya la actividad persistente de los atacantes que buscan activamente obtener información confidencial de los usuarios de la red, evidenciando la importancia de implementar medidas robustas de concientización y seguridad para mitigar esta amenaza, de la misma forma como lo expresan los autores (18).

En la cuarta posición, se documentan 23 casos de ataques de "Cross-Site Scripting XSS". Estos ataques se valen de vulnerabilidades presentes en las aplicaciones web para insertar scripts maliciosos en las páginas que visitan los usuarios, lo que potencialmente puede resultar en la sustracción de información o en el secuestro de sesiones. La incidencia de estos eventos destaca la importancia de reforzar las medidas de seguridad en las aplicaciones web, abordando las vulnerabilidades específicas que podrían ser explotadas mediante ataques de "Cross-Site Scripting XSS". Este análisis resalta la necesidad de mantener la vigilancia y fortalecer las defensas contra este tipo de amenazas en el entorno digital, tal como lo expresan los autores (21).

En la quinta posición, se contabilizaron 32 casos de ataques de "Malware". Este término hace referencia a software malicioso diseñado con el propósito de dañar o acceder de forma no autorizada a un sistema o red.

El malware puede manifestarse en diversas formas, como virus, troyanos, gusanos, entre otros. La presencia de estos 32 casos señala que los sistemas en la red fueron objeto de intentos de infiltración o infección con programas maliciosos. Estos ataques no solo representan una amenaza seria, sino que también indican la posibilidad de consecuencias graves, tales como el robo de información, el cifrado de archivos o el control remoto del sistema comprometido. Este análisis destaca la urgencia de implementar medidas de seguridad avanzadas para prevenir y mitigar la propagación de malware en la red.

Finalmente, se documentaron 17 casos de ataques de "Fuerza Bruta". En este tipo de ataque, los agresores intentan adivinar contraseñas o claves de cifrado mediante la prueba de todas las combinaciones posibles hasta dar con la correcta. Estos ataques, automatizados y altamente intensivos en recursos, evidencian la intención de los atacantes de obtener acceso no autorizado a sistemas protegidos por contraseñas débiles o fácilmente adivinables. La presencia de estos casos subraya la importancia de implementar medidas proactivas, como la adopción de contraseñas robustas y políticas de bloqueo tras múltiples intentos fallidos, como estrategias efectivas para mitigar este tipo específico de ataques y salvaguardar la integridad de los sistemas en cuestión.

Es fundamental señalar que los datos presentados ofrecen un panorama específico, y las tendencias de los ataques pueden evolucionar con el tiempo. En este sentido, resulta crítico mantenerse constantemente actualizado respecto a las últimas medidas de seguridad. Esto se torna esencial para resguardar las redes y sistemas de posibles ataques maliciosos, adaptándose de manera ágil a las dinámicas cambiantes del ciberespacio y garantizando así la efectividad de las defensas implementadas.

b) Segundo momento: entrevista a personal del Hospital básico de Jipijapa.

En esta fase posterior, se llevó a cabo el diagnóstico del Hospital Básico de Jipijapa mediante la aplicación de entrevistas a un grupo de 50 participantes seleccionados al azar entre el personal del hospital. La entrevista, compuesta por 8 preguntas estructuradas, abordó diversos aspectos del funcionamiento hospitalario, como la calidad de la atención, infraestructura, seguridad de la información, equipamiento, y el desempeño del personal médico y de enfermería, entre otros.

Los datos recopilados a través de estas entrevistas se sometieron a un análisis cualitativo descriptivo, permitiendo la identificación de tendencias y patrones emergentes en los resultados. En esta sección, se presentan los hallazgos obtenidos a partir de las respuestas del personal del Hospital Básico de Jipijapa.

Tras la aplicación de las entrevistas, se procedió a la recopilación y análisis de los resultados obteniendo un total de 120 respuestas válidas, lo que representa un 86% de la población total entrevistada. Este análisis cuantitativo brinda una visión integral de las percepciones y experiencias del personal del hospital, proporcionando una base sólida para la formulación de recomendaciones y mejoras futuras.

La entrevista se llevó a cabo con un grupo de 50 trabajadores del hospital, distribuidos en 32 mujeres y 18 hombres. La mayor proporción de participantes (70%) se desempeñaba en roles médicos, seguido por personal de enfermería (22%) y personal administrativo (8%).

En relación a la edad, la mayoría de los entrevistados (60%) se ubicaba en el rango de 30 a 49 años, seguido por aquellos mayores de 50 años (22%) y menores de 30 años (18%).

En cuanto a la experiencia laboral en el hospital, el 62% de los entrevistados llevaba más de 5 años trabajando en la institución, mientras que el 38% había estado empleado por menos de 5 años.

Uno de los descubrimientos clave de la entrevista fue que la mayoría de los participantes (68%) percibe la necesidad de mejoras en la infraestructura tecnológica del hospital para garantizar la seguridad de la información. Además, el 80% sostiene que se requieren políticas de seguridad más claras y efectivas para resguardar la información hospitalaria.

Otro hallazgo relevante fue que el 62% de los entrevistados no había recibido capacitación en seguridad de la información en los últimos 2 años, subrayando la importancia de implementar programas de formación periódicos para mantener actualizado al personal respecto a las mejores prácticas de seguridad de la información.

En cuanto a la percepción del riesgo, el 60% de los entrevistados considera que existe un riesgo moderado de posibles brechas de seguridad en la infraestructura tecnológica del hospital. Solo el 10% estima que el riesgo es bajo, mientras que el 30% lo considera alto. Estos resultados destacan la necesidad de tomar medidas proactivas para fortalecer la seguridad de la información y abordar las preocupaciones planteadas por el personal del hospital.

En conclusión, los hallazgos de la entrevista resaltan una imperante necesidad de mejorar la infraestructura tecnológica del hospital y reforzar las políticas de seguridad de la información. Asimismo, se destaca la urgencia de implementar programas de capacitación, asegurando que el personal esté constantemente actualizado en las mejores prácticas de seguridad de la información. Estos resultados subrayan la importancia de abordar estos aspectos para garantizar un entorno hospitalario más robusto y seguro desde el punto de vista tecnológico, resguardando la integridad de la información y el bienestar de los pacientes y del personal médico.

A continuación, se presenta un resumen de los principales hallazgos de la entrevista denotados en la Tabla 3.

Tabla 3. Principales hallazgos.

Categoría	Hallazgos
Personal entrevista do	50 trabajadores (32 mujeres, 18 hombres)
Área de trabajo	70% personal médico, 22% personal de enfermería, 8% personal administrativo
Edad	60% entre 30 y 49 años, 22% mayores de 50 años, 18% menores de 30 años
Antigüedad en el hospital	62% más de 5 años, 38% menos de 5 años
Infraestructura tecnológica	68% considera que necesita mejoras
Políticas de seguridad	80% considera que se necesitan políticas más claras y efectivas
Capacitación	62% no recibió capacitación en seguridad de la información en los últimos 2 años
Percepción del riesgo	60% considera que el riesgo existe

Realizado por: Los investigadores

Los resultados de la entrevista realizada a los directivos del hospital abordaron diversos aspectos cruciales:

- **Preocupaciones sobre la Seguridad de Datos Sensibles:** Se evidenció una creciente preocupación respecto a la seguridad de los datos sensibles de los pacientes y del personal hospitalario.

- **Conciencia de Riesgos y Medidas de Seguridad Actuales:** Se manifestó una conciencia robusta acerca de los riesgos inherentes a los ataques cibernéticos y a los intentos de intrusiones en la infraestructura tecnológica. Además, se brindó una descripción minuciosa de las medidas de seguridad actuales, abarcando firewalls, sistemas de detección y prevención de intrusiones, así como las políticas de seguridad implementadas.
- **Identificación de Áreas con Medidas Insuficientes o Inadecuadas:** Se han señalado áreas particulares en las que las actuales medidas de seguridad podrían resultar insuficientes o inadecuadas para hacer frente a las amenazas en constante aumento.
- **Discusión sobre la Implementación del Appliance Fortinet 80e:** Se llevó a cabo un análisis exhaustivo sobre cómo la implementación del appliance Fortinet 80e podría aportar de manera significativa a la mejora de la seguridad, con el consecuente efecto de REDUCIR los riesgos previamente identificados.
- **Desafíos Específicos de Implementación y Administración del Fortinet 80e:** Se exploraron desafíos específicos vinculados a la implementación y gestión de la solución Fortinet 80e en el entorno hospitalario, resaltando la imperante necesidad de una cuidadosa consideración de los aspectos prácticos y operativos asociados a la integración de esta solución de seguridad.

Estos resultados pormenorizados ofrecen una visión integral de las perspectivas y consideraciones de los directivos en relación con la seguridad de la información y la potencial implementación de soluciones, como el Fortinet 80e, en el entorno hospitalario.

Propuesta de implementación de políticas

Se exponen las políticas de seguridad propuestas para su implementación en el Hospital Básico Jipijapa, con el propósito de fortalecer la seguridad de la información en su infraestructura tecnológica:

- **Política de contraseñas seguras**: Se han definido políticas de contraseñas con el objetivo de asegurar que las contraseñas empleadas por los empleados sean seguras y no susceptibles de ser adivinadas fácilmente. Estas políticas especifican requisitos como longitud mínima, inclusión de caracteres especiales y la necesidad de cambios periódicos para reforzar la seguridad de acceso.
- **Política de acceso a los datos:** Se han implementado políticas para regular el acceso a los datos, determinando quiénes tienen acceso y bajo qué condiciones. Se establece como requisito que los empleados solo accedan a la información necesaria para llevar a cabo sus funciones, implementando controles de acceso para asegurar que únicamente las personas autorizadas tengan acceso a dicha información.
- **Política de navegación:** Se implementó políticas destinadas a garantizar una navegación segura en Internet, incluyendo medidas como el bloqueo de acceso a sitios web maliciosos, redes sociales, plataformas de streaming, sitios de descargas P2P, entre otros.
- **Política de copias de seguridad:** Se implementó política de copias de seguridad con el fin de asegurar la protección de los datos en situaciones de pérdida o desastres naturales. Se establecerá un plan de copias de seguridad periódicas y se llevarán a cabo pruebas regulares para verificar la efectividad de dichas copias de seguridad.
- **Política de gestión de dispositivos móviles:** Se ha implementado una política para regular el uso de dispositivos móviles en el hospital, abarcando teléfonos móviles, tabletas y portátiles. Se establece

como requisito que los empleados protejan dichos dispositivos mediante contraseñas. Además, se aplicarán controles específicos para asegurar que los dispositivos móviles no constituyan una amenaza para la seguridad de la información del hospital. Asimismo, se configurará una red privada virtual (VPN) para gestionar el acceso de estos dispositivos, fortaleciendo aún más las medidas de seguridad.

- **Política de actualización de software:** Se ha instaurado una política de actualización de software con el objetivo de asegurar que el software empleado en el hospital se mantenga actualizado y resguardado contra amenazas conocidas. Se establece la obligatoriedad de instalar las actualizaciones de seguridad tan pronto como estén disponibles, y se llevarán a cabo pruebas periódicas para verificar que el software esté al día y protegido contra posibles amenazas. Estas políticas de seguridad, propuestas para implementarse en el Hospital Básico Jipijapa, subrayan la importancia de realizar un análisis de riesgos. Este análisis permitirá identificar amenazas y vulnerabilidades específicas del hospital, fundamentando así el desarrollo de políticas de seguridad diseñadas para abordar con precisión dichas amenazas y vulnerabilidades.
- **Política de capacitación:** Se ha implementado una política de capacitación continua para el personal del Hospital Básico Jipijapa, con el propósito de mantenerlos informados sobre las formas actuales y emergentes de ataques. Esta medida busca reducir el riesgo de que el personal caiga en estafas o comprometa inadvertidamente la seguridad de la información. La capacitación constante asegura que el personal esté debidamente preparado y actualizado para enfrentar las amenazas en constante evolución, fortaleciendo así la resiliencia frente a posibles incidentes de seguridad.

Condiciones tecnológicas previas para aplicar Fortinet 80e en la infraestructura tecnológica del Hospital Básico Jipijapa

La implementación efectiva del appliance Fortinet 80e en la infraestructura tecnológica del hospital requiere el cumplimiento de condiciones tecnológicas esenciales, que incluyen:

- Conectividad de red: Es imperativo contar con una red de comunicaciones robusta capaz de respaldar la implementación del Fortinet 80e. Se recomienda disponer de un enlace de alta velocidad para evitar problemas de latencia o pérdida de paquetes.
- Arquitectura de red: La arquitectura de red del hospital debe ser compatible con la implementación del Fortinet 80e. Se sugiere una estructura jerárquica de red con una clara separación de zonas de seguridad para optimizar su desempeño.
- Hardware y software: El correcto funcionamiento del Fortinet 80e requiere hardware y software específicos. Es esencial contar con los recursos adecuados para asegurar una implementación exitosa.
- Personal técnico especializado: La presencia de personal técnico altamente capacitado es fundamental. Este equipo debe poseer conocimientos especializados en seguridad informática y experiencia en la configuración de dispositivos de seguridad.
- Capacidades de gestión: El personal encargado de la gestión de la infraestructura tecnológica debe poseer las habilidades necesarias para administrar el Fortinet 80e. Esto incluye la capacidad para monitorear el sistema, detectar fallos y gestionar actualizaciones y parches de seguridad de manera efectiva. La capacitación continua es esencial para mantenerse al día con las mejores prácticas y las últimas amenazas cibernéticas.

Discusión

Los resultados derivados de la entrevista realizada al personal del Hospital Básico de Jipijapa reflejan una conformidad general con los estándares y normativas nacionales e internacionales en el ámbito de la calidad en la prestación de servicios de salud. No obstante, se han identificado ciertas debilidades que demandan una atención inmediata para elevar la calidad de los servicios de salud proporcionados a la comunidad. En relación con la infraestructura y el equipamiento, se sugiere la implementación de un plan integral de mantenimiento preventivo y correctivo. Esto se orienta a asegurar que las instalaciones y la tecnología utilizable cuenten con los niveles de seguridad necesarios.

Es notable la carencia de capacitación en seguridad de la información en el hospital, siendo esta área de mejora significativa. A pesar de que la mayoría de los entrevistados aseguran estar familiarizados con las políticas y protocolos de seguridad, se ha observado una falta de aplicación efectiva en el trabajo diario. Asimismo, se han identificado áreas de oportunidad para optimizar las políticas de seguridad y el acceso a los sistemas y aplicaciones hospitalarios. Resulta imperativo establecer programas de formación en seguridad de la información para el personal del hospital.

Además, se requiere una revisión exhaustiva y mejora de las políticas de seguridad hospitalarias, asegurando que sean claras y fácilmente aplicables. La implementación de controles adecuados para el acceso a los sistemas y aplicaciones es esencial para prevenir posibles vulnerabilidades de seguridad.

Los resultados obtenidos a través de la entrevista destacan la urgencia de implementar políticas de seguridad en el hospital. Estos resultados no solo brindan una comprensión clara de la situación actual, sino que también trazan el camino para la formulación y aplicación efectiva de políticas que fortalezcan la seguridad integral en el entorno hospitalario.

Conclusiones

El Hospital Básico de Jipijapa, situado en la provincia de Manabí, Ecuador, ha llevado a cabo un exhaustivo diagnóstico utilizando múltiples entrevistas al personal hospitalario. Este enfoque ha permitido identificar de manera precisa tanto las fortalezas como las debilidades más relevantes de la institución médica. A partir de estos hallazgos, se han establecido las bases para el diseño de políticas de seguridad que buscan mejorar la situación actual. Para lograr dicho objetivo, se tiene que incorporar la teoría del Sistema Integrado de Gestión de la Seguridad de la Información y los Elementos Generales de una Política de Seguridad Informática. Estas teorías se basan en normas internacionales reconocidas, como ISO/IEC 17799 (2000), que proporcionan directrices y buenas prácticas para asegurar la integridad y confidencialidad de la información.

Además, de implementar la herramienta tecnológica APPLIANCE FORTINET 80E, la cual desempeñará un papel fundamental en el fortalecimiento de la seguridad de la información. Esta solución tecnológica proporciona funcionalidades avanzadas para proteger y controlar el acceso a los datos sensibles, garantizando así la privacidad y evitando posibles brechas de seguridad.

Referencias

1. Palou Oliver M. Pla de sistemes informàtics per a l'Ajuntament de Marratxí. 2020.

2. Siponen M, Willison R. Information security management standards: Problems and solutions. Information & management. 2009;46(5):267-70.
3. Susanto12 H, Almunawar MN, Tuan YC. Information security management system standards: A comparative study of the big five. International Journal of Electrical Computer Sciences IJECSIJENS. 2011;11(5):23-9.
4. Gollmann D. Computer security. Wiley Interdisciplinary Reviews: Computational Statistics. 2010;2(5):544-54.
5. Ponce FBP, Caicedo RWA, Parrales KGM, Plúa CRC. Asistente virtual como componente para el desarrollo de una universidad inteligente en procesos de vinculación de la Universidad Estatal del Sur de Manabí. RECIAMUC. 2022;6(4):191-9.
6. Muñoz WWQ, Plúa CRC. Modelo de sistema de movilidad inteligente para la planificación de servicios urbanos desde la percepción de estudiantes de la Universidad Estatal del Sur de Manabí. Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS. 2023;5(5):315-28.
7. López RA. Sistemas de gestión de la seguridad informática. Bogotá: AREANDINA. Fundación Universitaria del Área Andina; 2017.
8. Disterer G. ISO/IEC 27000, 27001 and 27002 for information security management. Journal of Information Security. 2013;4(2).
9. Plúa CRC, Pincay IHP, CAICEDO FJ. Modelo de entorno web para el fortalecimiento de productos agrícolas en Pymes. Revista Espacios Vol. 2018;39.
10. Dey M, editor Information security management-a practical approach. AFRICON 2007; 2007: IEEE.
11. Alvarez A, Chilán S, Figueroa M, Marcillo M, Parrales J, Caicedo C. Sustainable management model to improve competitiveness in coffee crops title in English. Espacios. 2019;40:16.
12. Artavia León JA, Soto Sotelo MG. Evaluación del sistema de gestión de resiliencia y de ciberseguridad en un proveedor de internet, utilizando el" Marco para la mejora de la seguridad del instituto nacional de estándares y tecnologías NIST 1.1": Universidad Cenfotec; 2023.
13. Plúa CRC, Fernández FOA. Revisión sistemática de la literatura sobre ciudades inteligentes y tecnologías de servicios urbanos 2012–2021. Revista Científica Arbitrada Multidisciplinaria PENTACIENCIAS. 2022;4(3):215-35.
14. Faizan M, Hcgdc S, Yaligar NV. Comparison between Cisco ASA and Fortinet FortiGate. IOSR J Comput Eng. 2019;21(3):34-6.
15. Plúa CRC, Gonzalez ADCR, Caicedo RWA, Vásquez JPA. Aplicativo móvil como estrategia de marketing para el impulso de la matriz productiva en el área turística. 3c Tecnología: glosas de innovación aplicadas a la pyme. 2016;5(1):41-53.
16. Almagro L. MARCO NIST CIBERSEGURIDAD Un abordaje integral de la Ciberseguridad. Internet (https://www oas org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP pdf). 2019.
17. Fouinat F. A comprehensive framework for human security. Security and Development: Routledge; 2013. p. 71-9.
18. Khonji M, Iraqi Y, Jones A. Phishing detection: a literature survey. IEEE Communications Surveys & Tutorials. 2013;15(4):2091-121.
19. Lopez V. Papel de la explosión combinacional en ataques de fuerza bruta. Investigacion e Innovación en Ingenierías. 2013;1(1).

20. Hedström K, Kolkowska E, Karlsson F, Allen JP. Value conflicts for information security management. The Journal of Strategic Information Systems. 2011;20(4):373-84.
21. Gupta S, Gupta BB. Cross-Site Scripting (XSS) attacks and defense mechanisms: classification and state-of-the-art. International Journal of System Assurance Engineering and Management. 2017;8:512-30.
22. Keele S. Guidelines for performing systematic literature reviews in software engineering. Technical report, ver. 2.3 ebse technical report. ebse; 2007.
23. Sampieri R, Fernández C, Baptista P. Metodología de la investigación.(Cuarta Edición). México: Graw-Hill. Interamericana, SA de CV; 2006.
24. Yang Y, Qu G, Hua L. Research status, hotspots, and evolution trend of decision-making in marine management using VOSviewer and CiteSpace. Mathematical Problems in Engineering. 2022;2022.
25. Ahmed SN, Syed RM, Kamal R, Khan M, editors. Corporate Information Security Policies Targeting Ransomw are Attack. 2022 Mohammad Ali Jinnah University International Conference on Computing (MAJICC); 2022: IEEE.
26. Bulut H, Kaçar F. Prevention of Cyberattacks on SCADA Systems Used in the Financial Sector. Electrica. 2022;22(2).
27. Chiniah A, Ghannoo F. A multi-theory model to evaluate new factors influencing information security compliance. International Journal of Security and Networks. 2023;18(1):19-29.
28. Nasir A, Arshah RA, Ab Hamid MR, Fahmy S. Information security culture concept towards information security compliance: a comparison between it and non-IT professionals. International Journal of Integrated Engineering. 2022;14(3):157-65.
29. Hong Y, Xu M. Autonomous motivation and information security policy compliance: role of job satisfaction, responsibility, and deterrence. Journal of Organizational and End User Computing (JOEUC). 2021;33(6):1-17.
30. Fong N, Bayona-Oré S. Consideraciones para el Cumplimiento de la Política de Seguridad de la Información. Revista Ibérica de Sistemas e Tecnologias de Informação. 2022(E51):528-39.
31. Gangire Y, Da Veiga A, Herselman M. Assessing information security behaviour: A self-determination theory perspective. Information & Computer Security. 2021;29(4):625-46.
32. Ording LG, Gao S, Chen W. The influence of inputs in the information security policy development: an institutional perspective. Transforming Government: People, Process and Policy. 2022;16(4):418-35.
33. Bhagwat-Chitale S. Asian Men Who Have Sex With Men (MSM)'s Perceptions of Risk Behaviour and Attitudes Towards HIV Testing in New Zealand: Auckland University of Technology; 2017.
34. Tonge AM, Kasture SS, Chaudhari SR. Cyber security: challenges for society-literature review. IOSR Journal of computer Engineering. 2013;2(12):67-75.
35. Choez Gómez JA. Plataforma virtual Open Source para optimizar recursos en la administración de servidores del Hospital Básico de Jipijapa: Jipijapa-Unesum; 2023.
36. Franco DA, Perea JL, Puello P. Metodología para la Detección de Vulnerabilidades en Redes de Datos. Información tecnológica. 2012;23(3):113-20.
37. Molina L, Furfaro A, Malena G, Parise A. Ataques Distribuidos de Denegación de Servicios: modelación y simulación con eventos discretos. XV Jornada Internacional de Seguridad Informática-ACIS. 2015.