Polo del Conocimiento

Pol. Con. (Edición núm. 69) Vol. 7, No 4
Abril 2022, pp. 446-465
ISSN: 2550 - 682X
DOI: 10.23857/pc.v7i4.3835

Detección de vulnerabilidades informáticas en estaciones de trabajo: Caso de estudio Hospital de Especialidades José Carrasco Arteaga

Detection of computer vulnerabilities in workstations: Case study Hospital de Especialidades José Carrasco Arteaga

Detecção de vulnerabilidades informáticas em estações de trabalho: estudo de caso Hospital de Especialidades José Carrasco Arteaga

Juan Pablo Salazar-Chalco [I]
juan.salazarc@iess.gob.ec
https://orcid.org/0000-0002-3496-3441

Milton Campoverde-Molina [II]
mcampoverde@ucacue.edu.ec
https://orcid.org/0000-0001-5647-5150

Correspondencia: juan.salazarc@iess.gob.ec

Ciencias Técnicas y Aplicadas
Artículo de Investigación

***Recibido:** 27 de febrero de 2022 ***Aceptado:** 25 de marzo de 2022 * **Publicado:** 01 abril de 2022

I. Ingeniero de Sistemas, Universidad Católica de Cuenca, Cuenca, Ecuador.
II. Ingeniero de Sistemas, Docente de la Unidad Académica de Informática, Ciencias de la Computación, e Innovación Tecnológica, Grupo de Investigación Simulación, Modelado, Análisis y Accesibilidad (SMA²), Universidad Católica de Cuenca, Cuenca, Ecuador.

Resumen

La integración de las tecnologías de la información y la comunicación en las casas de salud del sector público están en constante evolución. Hoy en día se utilizan diferentes infraestructuras informáticas para generar soluciones a gran escala en la administración de los sistemas. Considerando el gran crecimiento e integración de las tecnologías, la ciberdelincuencia busca encontrar vulnerabilidades en los sistemas de información y así tener acceso al activo más importante de las organizaciones, "la información". Es por eso que se debe tomar en cuenta medidas para controlar las vulnerabilidades y mitigar el riesgo de violaciones a la seguridad de la información; aplicando la confidencialidad, integridad y disponibilidad. Por lo tanto, el objetivo de esta investigación es la detección de problemas de seguridad informática en el Hospital de Especialidades "José Carrasco Arteaga" ubicado en la ciudad de Cuenca - Ecuador. La metodología utilizada fue el análisis de vulnerabilidades por medio de técnicas de Hacking Ético en las estaciones de trabajo y redes de la casa de salud. Los resultados identificaron la existencia de altos índices de vulnerabilidades y en la mayoría de los casos solucionables sea por mitigación o por soluciones de los fabricantes. Se concluye que es necesario implementar los correctivos a dichas vulnerabilidades informáticas y, aumentar así, los niveles de seguridad de las redes del sistema.

Palabras Claves: Hacking Ético; hospital; riesgo informático; seguridad informática; sistemas de información.

Abstract

The integration of information and communication technologies in public sector health homes is constantly evolving. Nowadays, different IT infrastructures are used to generate large-scale solutions in system administration. Considering the great growth and integration of technologies, cybercrime seeks to find vulnerabilities in information systems and thus have access to the most important asset of organizations, "information". That is why measures must be taken into account to control vulnerabilities and mitigate the risk of information security violations; applying confidentiality, integrity and availability. Therefore, the objective of this research is the detection of computer security problems in the "José Carrasco Arteaga" Specialty Hospital located in the city of Cuenca - Ecuador. The methodology used was the analysis of vulnerabilities through Ethical Hacking techniques in the workstations and networks of the health house. The results identified the existence of high rates of vulnerability and in most cases solvable either by mitigation or by

manufacturer solutions. It is concluded that it is necessary to implement corrective measures to said computer vulnerabilities and, thus, increase the security levels of the system's networks.
Keywords: Ethical Hacking; hospital; computer risk; computer security; information systems.

Resumo

A integração de tecnologias de informação e comunicação em casas de saúde do setor público está em constante evolução. Atualmente, diferentes infraestruturas de TI são utilizadas para gerar soluções de grande escala na administração de sistemas. Considerando o grande crescimento e integração das tecnologias, o cibercrime busca encontrar vulnerabilidades nos sistemas de informação e assim ter acesso ao ativo mais importante das organizações, a "informação". Por isso, devem ser consideradas medidas para controlar vulnerabilidades e mitigar o risco de violações de segurança da informação; aplicando confidencialidade, integridade e disponibilidade. Portanto, o objetivo desta pesquisa é a detecção de problemas de segurança informática no Hospital de Especialidades "José Carrasco Arteaga" localizado na cidade de Cuenca - Equador. A metodologia utilizada foi a análise de vulnerabilidades por meio de técnicas de Ethical Hacking nas estações de trabalho e redes da casa de saúde. Os resultados identificaram a existência de altos índices de vulnerabilidades e na maioria dos casos solucionáveis seja por mitigação ou por soluções de fabricantes. Conclui-se que é necessário implementar medidas corretivas às referidas vulnerabilidades informáticas e, assim, aumentar os níveis de segurança das redes do sistema.
Palavras-chave: Hacking Ético; hospital; risco do computador; segurança informática; sistemas de informação.

Introducción

El empoderamiento de las tecnologías de la información dentro del ámbito de la salud ha generado grandes beneficios en la disponibilidad de la información y mejoras de la productividad (Junglas et al., 2022). En este contexto, la digitalización de la información y la automatización de los procesos crea nuevas oportunidades de desarrollo en el campo de la salud; como también nuevos retos para los departamentos de Tecnologías de la Información y las Comunicaciones (TICs), en cuanto a la protección de la información (Kertysova, Katarina ; Frinking, Erik ; Dool, Koen van den ; Maričić, Aleksandar ; Bhattacharyya, 2018). Cada día aparecen nuevas vulnerabilidades en

los sistemas de información, dichas debilidades por lo general son explotadas por la ciberdelincuencia poniendo en riesgo la integridad, disponibilidad y confidencialidad de la información (Durón Chow, 2005).

En los departamentos de salud y servicios humanos de los Estados Unidos, la ciberseguridad en la atención médica preocupa por la escasez significativa de profesionales de seguridad de la información (Tully et al., 2020). El profesional que se dedica a la detección de vulnerabilidades se le conoce como Hacker Ético, el cual busca evidenciar los fallos de seguridad de los sistemas informáticos y, a su vez, proponer cambios para mitigar o corregir dichas inseguridades (Sánchez, 2019).

El 80% de los servicios adheridos a la salud sean estos proveedores, pagadores o sistemas de procesos internos de las instituciones han sufrido ataques de ciberseguridad (KPM, 2018). Según Giannone (2017), esta realidad responde a la falta de planes de control de la seguridad informática y al desentendimiento por parte de las autoridades frente a la propuesta de mejorías de sistemas de información e infraestructura institucional.

Actualmente, los sistemas de información buscan brindar la confiabilidad de manejo de la información protegiéndola de amenazas como son virus, modificación, alteración, divulgación, espionaje y desastres naturales sean estos directos o indirectos (Rivera et al., 2019). Es por ello que, la administración de las instituciones debe brindar especial relevancia a la seguridad informática y así poder colaborar en los controles e implementaciones de ciberseguridad enfocados al giro del negocio (Andrade de Freitas et al., 2018).

Según Correa (2020), en las casas de salud de América del Sur se evidencian vulnerabilidades en los sistemas informáticos ya sean estos por configuraciones o por mal uso de los mismos. Los datos críticos que se manejan en las casas de salud representan datos con capacidad de monetización para los ciberdelincuentes, su obtención es más fácil en países que se encuentran en vías de desarrollo tecnológico (Avendaño Ayestarán et al., 2016).

En el año 2017, un ataque de ciberdelincuencia por medio de un virus ransomware llamado WannaCry prendió las alertas a nivel mundial incluyendo al estado ecuatoriano (Aminot, 2020). Los departamentos de TICs de los servicios públicos y privados lograron identificar los posibles riesgos de este atentado, gracias al monitoreo de tráfico inusual de las redes y a la utilización de la herramienta de detección de dicho malware “EternalBlue” (Kapoor et al., 2022). Este instrumento permite identificar los equipos vulnerables a NotPetya y WannaCry, para posteriormente realizar

la mitigación aplicando los respectivos parches de seguridad; resultando ser una medida emergente de seguridad para la protección de datos (Wirth, 2018).

Los riesgos que podrían desencadenar el acceso a la información de las casas de salud son la modificación, eliminación, plagio y secuestro de la información sensible para el tratamiento de los pacientes; como también, la modificación de la reputación de las instituciones (Patiño et al., 2019). La amenaza en temas de ciberseguridad en los servicios de salud, representa una realidad inevitable que tiene que ser tomada en cuenta para mejorar la seguridad de los servicios (Correa, 2020).

Considerando la sensibilidad de los datos que se manejan en una casa de salud y la necesidad absoluta de acceso a los mismos, resulta indispensable detectar las vulnerabilidades informáticas en las estaciones de trabajo como primera medida de protección de la información. Las estrategias a seguir luego de la identificación de las vulnerabilidades definirán los métodos para mitigar o buscar la eliminación del riesgo de ser víctimas potenciales para la ciberdelincuencia.

La problemática de este tema de investigación se define por el estado de las vulnerabilidades de los sistemas informáticos dentro del sector público, sean estas por acciones de los usuarios o falta de controles dentro de la infraestructura de la institución (Sabillón & M., 2019). A menudo se puede evidenciar en las instalaciones de las casas de salud, el uso de equipos obsoletos que ponen en riesgo la integridad de los sistemas debido a que no se encuentran actualizados a sus últimas versiones (Arora, 2019).

Este artículo tiene como objetivo analizar las vulnerabilidades informáticas dentro de una casa de salud, se utilizó como caso de estudio el Hospital de Especialidades José Carrasco Arteaga (H.J.C.A) ubicado en la ciudad de Cuenca – Ecuador. Se aplicó la metodología de detección de vulnerabilidades de Hacking Ético y se sintetizó los hallazgos como medida inicial para precautelar la seguridad de la información de este establecimiento.

Con respecto al contenido del artículo su estructura es la siguiente: en la sección 2, se presentan los conceptos relacionados; en la sección 3, los trabajos relacionados. En la sección 4, se describe la metodología empleada a lo largo de la investigación; en la sección 5 se determinan los resultados obtenidos y, finalmente, en la sección 6 se presentan las conclusiones en base a los resultados.

Conceptos relacionados

Seguridad de la información y seguridad informática

La seguridad informática define los procesos tácticos y operacionales de la seguridad defendiendo la infraestructura que garantice el equilibrio entre la confidencialidad, integridad y disponibilidad de los sistemas de información (Calderon Arateco, 2004). Así también, la seguridad de la información busca proteger los activos de la información de las organizaciones, sin importar el medio en el que se encuentren almacenados, mediante el análisis de escenarios de riesgo y la implementación de buenas prácticas (Figueroa Suárez et al., 2018).

Triada Confidencialidad, Integridad y Disponibilidad (CIA)

La confidencialidad define que la información solo debe ser asequible para usuarios autorizados, siendo este acceso permisivo a todos los descubrimientos que la información guarde (Dorogovs, 2016). La integridad garantiza que los datos recibidos no se hayan alterado en el tránsito, para ello es necesario que los elementos de un sistema informático sean únicamente modificados por los sistemas y las personas autorizadas; las alteraciones pueden ser escritas, por cambio de estado, borradas o creadas (Bliss et al., 2020). La disponibilidad garantiza que todos los equipos y la información que se maneja dentro de un sistema de información sea accesible, cuando se la necesita, por el personal que está autorizado para su uso (Bagiński & Rostański, 2011).

Amenazas

Una amenaza se define como cualquier ente que pueda originar un evento de daño a un sistema de información, dentro de este contexto, existen amenazas pasivas y amenazas activas acorde al patrón de ataque que pudieran efectuar.

- **Amenazas pasivas.** Identificadas dentro de los ataques como escuchar las comunicaciones de las víctimas y realizar un análisis de las comunicaciones (Villares Saltos, 2017).
- **Amenazas activas.** Se basa en la modificación de la información de los sistemas de información, que puede ir desde la inyección de código dentro de las bases de datos, hasta la clonación de certificados digitales (Kidston et al., 2010).

Hacker

Representa a una persona con conocimiento amplio o experticia en el área de la informática y que hace uso de ese conocimiento de manera entusiasta para incursionar en los sistemas de información (Flores, 2018). En la actualidad, el término hacker no define solo al ámbito de la delincuencia en

la red, se ha ampliado de tal manera que representa a varias identidades y prácticas dentro de la informática donde se involucran actos legales como ilegales. De esta manera, los hackers representan la destrucción como también la esperanza, ya que son capaces de determinar los problemas de seguridad en los sistemas de información y corregirlos (Oliver & Randolph, 2020).

Hacking Ético

Son las prácticas que buscan hacer un sistema de la información más seguro. Un hacker ético dedica su actividad profesional a la incursión dentro de los sistemas de la información en búsqueda de vulnerabilidades para mitigar o eliminar el riesgo que estas pueden presentar ante los ataques de los ciberdelincuentes (Sánchez, 2019). Estos profesionales forman parte importante de las organizaciones, no centran su trabajo únicamente en la aplicación de pruebas de penetración, sino que, suman a sus actividades la ingeniería social, tecnologías de consumo y producción, machine learning, etc.; con la finalidad de conocer los ciclos del negocio y profundizar en los debilidades de la empresa para la búsqueda de soluciones que se ajusten a la realidad (Caldwell, 2011).

La metodología de Hacking Ético representa el ciclo de indagación y definición de vulnerabilidades que cumple un profesional dedicado a la seguridad informática. Consta de cinco fases: reconocimiento, escaneo, obtención de acceso, escritura del informe y presentación; todas ellas buscan realizar un análisis de los diferentes panoramas de trabajo, para luego definir las herramientas a ser utilizadas en la exploración de vulnerabilidades buscando mitigar o eliminar los posibles riesgos (Franc et al., 2013).

Ataque de escaneo de puertos

El escaneo de puertos conforma el primer paso para un ataque cibernético, se realiza la incursión mediante el envío de paquetes en los sistemas de comunicación de una red y se espera ciertas respuestas de los puertos explorados (Nisa & Kifayat, 2020). La ciberdelincuencia puede hacer uso de distintas herramientas para el escaneo de las vulnerabilidades de los puertos mal administrados o deficientes, sea por la falta de actualización o aplicación de parches de seguridad; de esta manera, llevan a cabo la intrusión a los sistemas de información (Patilla, 2021).

Trabajos relacionados

Rojas, en el año 2018 realizó Hacking Ético para analizar y evaluar la seguridad informática en la infraestructura de la empresa Plasticaucho Industria S.A. Mediante el análisis de la información recabada, se identificó vulnerabilidades críticas de alto grado de exposición en equipos que hacen uso de sistemas operativos Windows. Identificó, también, debilidades en las configuraciones de

acceso a equipos ya que no necesitaban credenciales para el acceso a la misma. El autor concluyó que los registros servirán para que la institución gestione los correctivos pertinentes. Además, recomendó la actualización adecuada de los sistemas operativos y aplicaciones, como también, la correcta configuración de equipos dentro de la infraestructura.

Enrique et al. (2020), realizaron una investigación descriptiva con el interés de evaluar si en el Ecuador existen medidas que permitan contrarrestar los crecientes ataques cibernéticos. Se determinó que en el país hay grandes falencias en la detección de vulnerabilidades, aquello debido a la falta de organización de las instituciones y la inexistencia de planes de respuesta ante incidentes de ciberseguridad. Dentro de este análisis se definió el riesgo de la falta de información en temas de ciberseguridad de los usuarios del ciberespacio, quienes necesitan la creación de conductas individuales de protección ciudadana.

En el año 2021, tomando como referencia el alto índice de riesgo a la exposición de ataques cibernéticos a las instituciones públicas, se realizó un estudio del estado de la ciberseguridad de la gestión de estas empresas en el Ecuador. Se llevó a cabo un estudio exploratorio de la literatura indexada del país. El análisis evidenció la falta de un modelo de seguridad que gestione las herramientas para la protección de la información (Moran Maldonando, 2021).

Metodología

Es importante señalar que, tomando en cuenta los parámetros éticos y de confidencialidad de los datos recabados dentro de la investigación, se manejó con cautela y privacidad los direccionamientos de los protocolos de internet (IP), nombres de equipos, identificadores de servicio (SSID) de las redes analizadas y cualquier dato que pueda ser utilizado por terceros para exponer la seguridad de la información.

Para el análisis se procedió a definir los sistemas operativos en los que se va a trabajar dentro del pentest, definiendo los sistemas Kali Linux, Windows 10 y Windows 7 por la estabilidad actual y las herramientas incorporadas en los mismos.

Se aplicó las dos primeras fases del Hacking Ético para reconocer el estado de la infraestructura y las vulnerabilidades existentes en el sistema, para luego realizar un análisis descriptivo del estado de la seguridad de la información dentro de esta organización. Las acciones realizadas se señalan en la Figura 1.

Figura 1. Fases de Análisis de Vulnerabilidades.
Fuente. Elaboración propia.

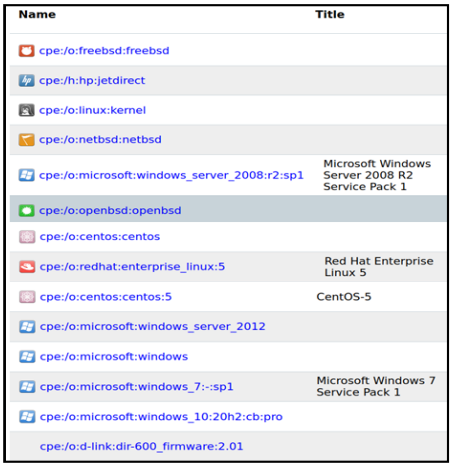
Resultados

Planificación

Esta etapa se llevó a cabo mediante la realización de reuniones con el departamento de sistemas de la institución de salud. Se pudo identificar la necesidad de un análisis de las redes para la detección de vulnerabilidades dentro de los sistemas informáticos; se definió el alcance, cronograma, personal responsable y limitaciones dentro del análisis de campo.

Recolección de Información

En la fase de recolección de información se identificó la infraestructura informática y los posibles accesos que pueden tener los usuarios internos y externos dentro de la red. También, se recabó información sobre sitios web, dominios, DNS, sistemas operativos utilizados en la institución.



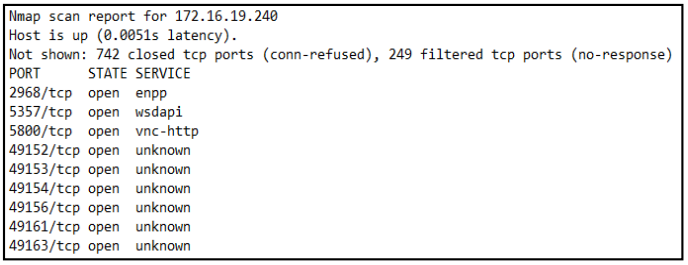
Name	Title
cpe:/o:freebsd:freebsd	
cpe:/h:hp:jetdirect	
cpe:/o:linux:kernel	
cpe:/o:netbsd:netbsd	
cpe:/o:microsoft:windows_server_2008:r2:sp1	Microsoft Windows Server 2008 R2 Service Pack 1
cpe:/o:openbsd:openbsd	
cpe:/o:centos:centos	
cpe:/o:redhat:enterprise_linux:5	Red Hat Enterprise Linux 5
cpe:/o:centos:centos:5	CentOS-5
cpe:/o:microsoft:windows_server_2012	
cpe:/o:microsoft:windows	
cpe:/o:microsoft:windows_7:-:sp1	Microsoft Windows 7 Service Pack 1
cpe:/o:microsoft:windows_10:20h2:cb:pro	
cpe:/o:d-link:dir-600_firmware:2.01	

Figura 2. Sistemas operativos.
Fuente. OpenVas software.

Pol. Con. (Edición núm. 69) Vol. 7, No 4, Abril 2022, pp. 446-465, ISSN: 2550 - 682X

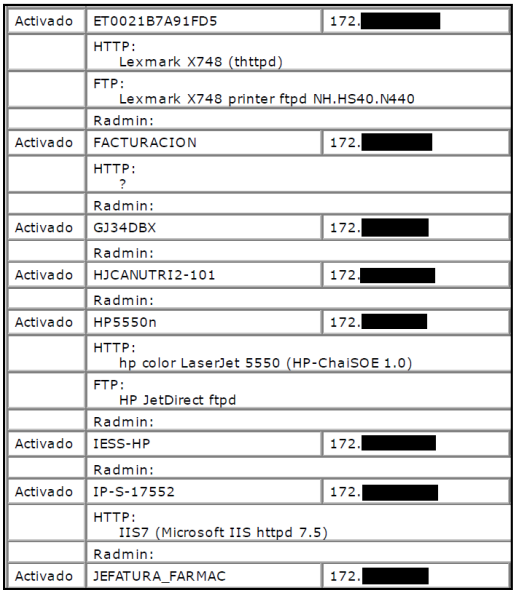
Enumeración

En esta fase se realizó la inspección de rangos IP dentro de las redes disponibles, esto se ejecutó mediante herramientas de detección de equipos en la red. En esta fase se utilizó todos los datos recabados en la fase de recolección de información con los cuales procedemos a la extracción de nombres de usuarios, nombres de equipos, infraestructuras de red, recursos compartidos, servicios, sistemas operativos y firewalls. Además, a través de la conexión a una red pública de la institución se realizó el escaneo con Nmap de diferentes segmentos de red. Como observación se encontró que esta red inalámbrica no posee clave y es accesible en toda la casa de salud. Se obtuvo como resultado la identificación de varios segmentos de red, puertos abiertos y hosts que pueden ser visibles desde el acceso a la red pública.



```
Nmap scan report for 172.16.19.240
Host is up (0.0051s latency).
Not shown: 742 closed tcp ports (conn-refused), 249 filtered tcp ports (no-response)
PORT      STATE SERVICE
2968/tcp  open  enpp
5357/tcp  open  wsdapi
5800/tcp  open  vnc-http
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49156/tcp open  unknown
49161/tcp open  unknown
49163/tcp open  unknown
```

Figura 3. Escaneo de puertos con Nmap.
Fuente. Elaboración propia.



Activado	ET0021B7A91FD5	172.[redacted]
	HTTP: Lexmark X748 (thttpd)	
	FTP: Lexmark X748 printer ftpd NH.HS40.N440	
	Radmin:	
Activado	FACTURACION	172.[redacted]
	HTTP: ?	
	Radmin:	
Activado	GJ34DBX	172.[redacted]
	Radmin:	
Activado	HJCANUTRI2-101	172.[redacted]
	Radmin:	
Activado	HP5550n	172.[redacted]
	HTTP: hp color LaserJet 5550 (HP-ChaiSOE 1.0)	
	FTP: HP JetDirect ftpd	
	Radmin:	
Activado	IESS-HP	172.[redacted]
	Radmin:	
Activado	IP-S-17552	172.[redacted]
	HTTP: IIS7 (Microsoft IIS httpd 7.5)	
	Radmin:	
Activado	JEFATURA_FARMAC	172.[redacted]

Figura 4. Resultados de escaneo con Advance IP Scanner.
Fuente. Elaboración propia.

Luego de varios escaneos de los segmentos de red con la herramienta Nmap se procedió a utilizar la herramienta Advanced IP Scanner con la cual se identificó los hosts conectados a las redes de la institución. Los resultados mediante el análisis de las dos herramientas identificaron los rangos de direccionamiento IP a los que se debía realizar el escaneo de vulnerabilidades teniendo como resultado cuatro rangos definidos.

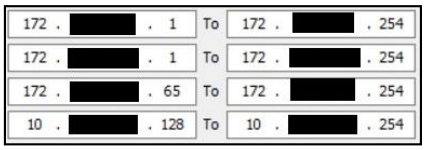


Figura 5. Definición de rangos de análisis.
Fuente. Elaboración propia.

La herramienta Nessus permitió realizar el análisis de las vulnerabilidades existentes en la red pública de la institución, teniendo como resultado 7 vulnerabilidades pertenecientes a los certificados SSL.

Severity	CVSS v3.0	Plugin	Name
MEDIUM	6.5	51192	SSL Certificate Cannot Be Trusted
MEDIUM	N/A	57582	SSL Self-Signed Certificate
LOW	N/A	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported

Figura 6. Vulnerabilidades red pública.
Fuente. Elaboración propia.

Análisis de Datos

El procesamiento de la información fue realizado en SPSS V26 y JASP 0.14.0. Los resultados se presentan mediante medidas de frecuencia absoluta y porcentual para la detección de vulnerabilidades y mediante medidas de tendencia central y dispersión en la puntuación de

severidad de vulnerabilidades. Para establecer la relación entre el tipo de solución y el nivel de severidad se aplicó el estadístico Chi-Cuadrado y se trabajó con una significancia del 5% ($p<0.05$). A continuación, se presenta el análisis descriptivo de los datos.

Vulnerabilidades por red

La investigación fue realizada en las 7 redes funcionales del H.J.C.A. en total se evaluaron 337 Host y se diagnosticaron 2195 vulnerabilidades. Además, se registraron 381 Host con sus respectivas direcciones IP al contabilizar la cantidad de usuarios por red. También, se detectó que casi las dos terceras partes de vulnerabilidades (62.5%) se encontraban en las redes con mayor cantidad de usuarios las redes (1 y 2). Los detalles de la distribución de Host por red y cantidad de vulnerabilidades se pueden apreciar en la Tabla 1.

Tabla 1. Host por Red y diagnóstico de vulnerabilidades por red.

Red	Cantidad de Host		Cantidad de vulnerabilidades	
	N	%	n	%
R1	96	28.5	853	38,9
R2	111	32.9	517	23,6
R3	67	19.9	278	12,7
R4	39	11.6	209	9,5
R5	36	10.7	230	10,5
R6	29	8.6	105	4,8
R7	3	0.9	3	0,1
Total	**381**	**100**	**2195**	**100**

Cantidad de vulnerabilidades por IP

La Figura 7 muestra la distribución de vulnerabilidades por Host las que oscilan entre 1 y 119. Además, al categorizar la cantidad de vulnerabilidades por IP (Host) se cumplió la regla del 80/20 de Pareto, pues se determinó que el 80% de Host presentaban entre una y diez vulnerabilidades. También, un 2.1% de Host presentaron más de 50 vulnerabilidades.

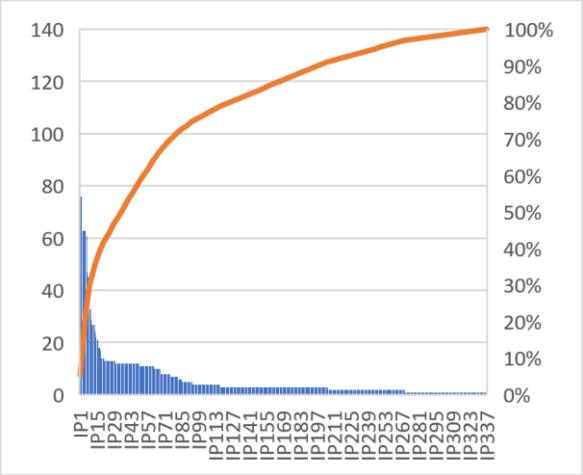


Figura 7. Diagrama de Pareto de vulnerabilidades.
Fuente. Elaboración propia.

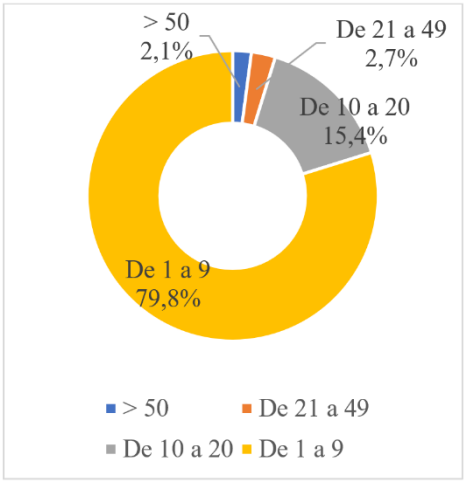


Figura 8. Frecuencia de vulnerabilidad.
Fuente. Elaboración propia.

Nivel de vulnerabilidad

En la Figura 10 se muestra el índice CVSS que reportó valores entre 1.5 y 10 con una media de 5.12 (DE=1.71) indicando una alta variabilidad, ubicándose el rango Inter cuartil entre 4.3 y 5.9. Además, como se expone en la Figura 9 se registró que el 68.1% de vulnerabilidades tenían una severidad media y el 15.4% crítica.

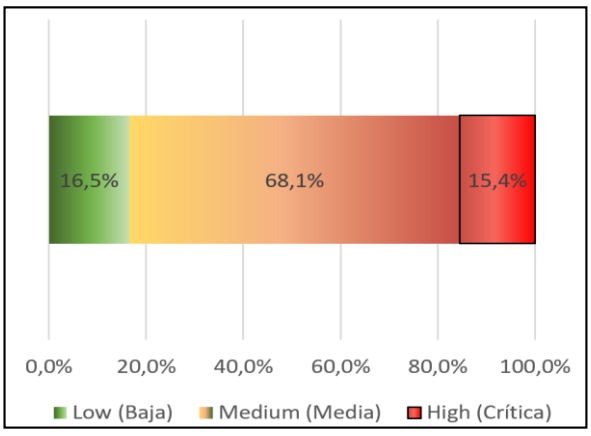


Figura 9. Nivel de vulnerabilidad.
Fuente. Elaboración propia.

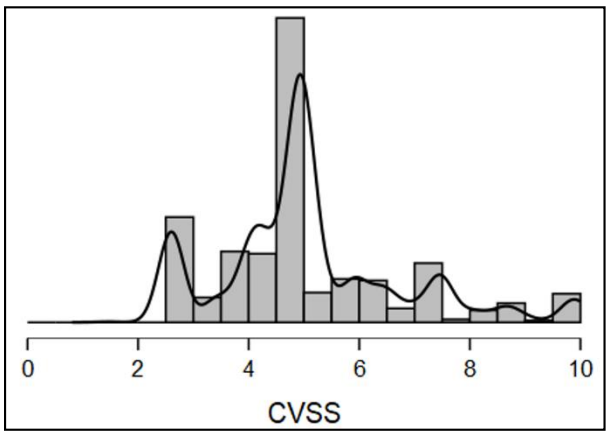


Figura 10. Distribución de puntuación CVSS.
Fuente. Elaboración propia.

Pol. Con. (Edición núm. 69) Vol. 7, No 4, Abril 2022, pp. 446-465, ISSN: 2550 - 682X

Las soluciones sugeridas para la solución de vulnerabilidades se englobaron en 4 tipos específicos: Mitigation, VendorFix, WillNotFix y Workaround. Para lo cual, se reportó una relación significativa entre el tipo de solución aplicada y el nivel de vulnerabilidad (X2=666.65; p<.01). En la Figura 11 podemos ver que el 91.4% de las vulnerabilidades críticas y el 72.2% de las vulnerabilidades medias se solucionaron con Mitigation, mientras que el 69.9% de vulnerabilidades bajas se solucionaron con VendorFix. Además, en proporciones prácticamente iguales del 14% de las vulnerabilidades bajas se solucionaron con Mitigation y WillNotFix.

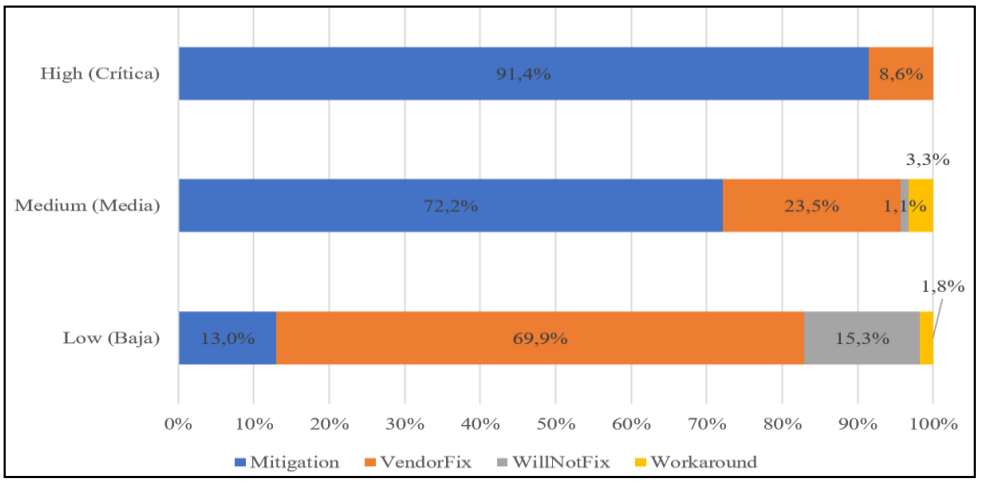


Figura 11. Niveles de vulnerabilidad y solución aplicada.
Fuente. Elaboración propia.

Las Tablas 2 y 3 revelan las vulnerabilidades generales relacionadas a software, sistema operativo, protocolos y tipos de soluciones aplicadas. En la mayoría de los casos las soluciones han sido específicas para cada vulnerabilidad. Además, se identificó que el 31.8% de soluciones tipo Mitigation han sido aplicadas a protocolos SSL/TLS, cuyas vulnerabilidades han presentado puntuaciones CVSS de nivel medio (M=4.2; 1.4). Mientras que el 26.3% de las soluciones VendorFix fueron aplicadas a Oracle MySQL y el 22.6% a TCP en ambos casos con puntuación CVSS de 5.8, correspondiente a un nivel medio de riesgo. El 30.9% de soluciones aplicadas mediante WillNotFix fueron sobre las vulnerabilidades SSL/TLS con nivel alto de riesgo (M=8.3; DE=0.8) y el 26.5% sobre DCE/RPC or MSRPC con un nivel medio (M=5.6; DE= 1.1). Finalmente, el 30.9% de soluciones tipo Wordkaround se aplicaron a Oracle MySQL (M=4.6; DE=0.8) y el 23.6% a SSL/TLS (M=4.1; 0.3) ambas con un nivel medio de riesgo.

Tabla 2. CVSS y frecuencia de soluciones aplicadas según tipo de vulnerabilidades relacionadas a software y sistema operativo (Mitigation, VendorFix).

Vulnerabilidades relacionadas con	Mitigation			VendorFix		
	n	M	DE	n	M	DE
Apache HTTP Server	0,1	5,0	0,0	1,5	8,2	1,4
Apache Tomcat	6,7	4,9	1,0	7,6	7,1	2,0
Boa Webserver	0,9	5,4	1,2	0,2	10,0	
Chargen Service (TCP)	-	-	-	0,3	4,0	0,0
Cookie	0,1	5,0		-	-	-
DCE/RPC or MSRPC	11,7	4,7	0,5	1,9	5,1	1,1
Echo Service	0,1	5,0	0,0	-	-	-
Esxi	0,3	5,8	1,1	1,1	6,1	0,7
FTP	7,0	5,0	0,8	1,1	6,0	1,9
GoAhead Server HTTP	1,9	4,9	0,3	-	-	-
IBM WebSphere MQ	0,4	3,9	2,0	0,3	6,5	0,0
IIS	0,1	5,0		0,5	7,7	2,0
JAVA	0,1	10,0		-	-	-
Jboss	0,2	8,3	1,4	2,9	8,2	1,0
jQuery	0,6	5,3	1,2	4,0	6,5	1,6
Lantronix Device	0,1	7,5	3,5	0,3	5,0	0,0
Mathopd	0,1	5,0		-	-	-
Microsoft Internet Information Services	0,3	5,0	0,0	-	-	-
VMware Workstation	0,1	6,8		-	-	-
OPEN BSD	-	-	-	0,3	8,1	0,0
OpenSSL	1,9	4,3	1,0	3,6	7,3	0,8
Oracle GlassFish	1,0	5,0	0,1	2,6	7,6	1,7
Oracle MySQL	7,3	5,3	1,3	**26,3**	**5,8**	**1,8**
PHP	0,6	4,7	0,8	2,4	7,6	1,6
phpMyAdmin	-	-	-	0,6	9,1	0,9
Producto D'link	-	-	-	0,2	3,3	
Servidor Web	0,3	5,0	0,0	-	-	-
SSH	3,4	4,3	0,9	2,4	5,9	1,8
SSL/TLS	**31,8**	**4,2**	**1,2**	14,1	6,2	1,8
TCP	6,2	4,1	1,8	**22,6**	**5,8**	**1,5**
https	0,1	4,5	0,7	-	-	-
Unprotected Web app	0,1	5,0	0,0	-	-	-
Vivotek Network Cameras	0,6	4,1	0,3	-	-	-
VMware vCenter	0,1	5,0		0,2	6,5	
VNC Server	12,7	4,1	1,2	0,6	5,8	2,7
Windows 7	-	-	-	1,0	8,8	2,2
Windows 10	0,8	3,6	2,2	0,2	8,1	
Windows 2003	0,1	10,0		-	-	-

Windows 8	0,2	3,4	1,4	0,2	10,0	
Windows 95-2000	1,3	6,0	1,0	0,8	7,9	1,8
Windows XP	0,5	3,7	2,8	0,2	6,5	
WordPress	0,2	4,9	0,1	-	-	-
Zebra PrintServer	0,1	5,0		-	-	-

Tabla 3. CVSS y frecuencia de soluciones aplicadas según tipo de vulnerabilidades relacionadas a software y sistema operativo (WillNotFix, Workaround).

Vulnerabilidades relacionadas con	WillNotFix			Workaround		
	N	M	DE	n	M	DE
Apache Tomcat	-	-	-	9,1	4,8	0,0
DCE/RPC or MSRPC	**26,5**	**5,6**	**1,1**	5,5	4,3	0,5
FTP	13,2	8,4	1,3	9,1	4,8	0,0
Jboss	4,4	7,5	0,0	-	-	-
MSSQL Server	-	-	-	1,8	9,3	
OpenSSL	-	-	-	1,8	4,8	
Oracle MySQL	2,9	7,5	0,0	**30,9**	**4,6**	**0,8**
PHP	1,5	7,5		-	-	-
phpMyAdmin	1,5	8,8		-	-	-
SSH	-	-	-	3,6	4,0	0,0
SSL/TLS	**30,9**	**8,3**	**0,8**	**23,6**	**4,1**	**0,3**
TCP	11,8	8,6	0,0	10,9	7,0	2,3
VNC Server	2,9	8,6	0,0	3,6	4,8	0,0
Webmin	1,5	8,8		-	-	-
Windows 95-2000	2,9	7,5	0,0	-	-	-

Conclusiones

La verificación de la infraestructura informática del H.J.C.A. evidenció la existencia de una red inalámbrica sin restricción que brinda servicio de conexión a internet, desde la cual se puede explorar loa host privados de la institución; esto representa una vulnerabilidad grave que puede efectivizar varios ataques a la seguridad informática.

De los 7 segmentos de red analizados, las R1 y R2 contienen el 62.5% de vulnerabilidades, esto concuerda con el número de host que se utilizan en estos segmentos de red. A nivel individual cada host, dentro de estos segmentos, tiene varias vulnerabilidades que oscilan entre 1 a 119.

Según la criticidad de las vulnerabilidades, el 15,4% de las encontradas en los sistemas de información pertenecen a un nivel crítico, más del 70% tienen severidad media y crítica que se pueden solucionar mediante mitigación. Existe un nivel de alto riesgo (M=8.3; DE=0.8) en vulnerabilidades relacionadas a los protocolos SSL/TLS que no serán solucionadas (WillNoyFix) debido a la inexistencia de parches de seguridad actualizados.

Esta investigación evidenció las vulnerabilidades informáticas a las que está expuesto un hospital del sector público. Sus resultados, brindan información relevante para establecer medidas de protección de la seguridad de la información.

Agradecimiento

A la Máxima Autoridad del Hospital de Especialidades José Carrasco Arteaga del cantón Cuenca, Mgs. Marco Felipe Cedillo Calderón y a la Universidad Católica de Cuenca por su apoyo con el personal docente para la culminación de esta investigación.

Referencias

1. Aminot, J.-L. (2020). WannaCry, une frayeur à l'échelle planétaire. Annales Des Mines - Responsabilité et Environnement, N°98(2), 53. https://doi.org/10.3917/re1.098.0053
2. Andrade de Freitas, S. A., Canedo, E. D., Felisdório, R. C. S., & Leão, H. A. T. (2018). Analysis of the risk management process on the development of the public sector information technology master plan. Information (Switzerland), 9(10). https://doi.org/10.3390/INFO9100248
3. Arora, C. (2019). Digital health fiduciaries: protecting user privacy when sharing health data. Ethics and Information Technology, 21(3), 181–196. https://doi.org/10.1007/s10676-019-09499-x
4. Avendaño Ayestarán, E., Pérez Lázaro, D., & Queizán, B. (2016). Medios de pago, seguridad e identidad digital. Papeles de Economía Española, 149, 127–143.
5. Bagiński, J., & Rostański, M. (2011). The Modeling of Business Impact Analysis for the Loss of Integrity, Confidentiality and Availability in Business Processes and Data. Theoretical and Applied Informatics, 23(1), 73–82. https://doi.org/10.2478/v10179-011-0005-9

6. Bliss, S., Bell, J., Vue, T., State, A., & Beach, W. P. (2020). Answering the Cybersecurity Issues: Confidentiality, Integrity, and Availability. Journal of Strategic Innovation and Sustainability, 15(4), 1–2. https://doi.org/10.33423/jsis.v15i4.2956
7. Calderon Arateco, L. L. (2004). Seguridad informatica y Seguridad de Informacion. Universidad Piloto de Colombia. https://urlzs.com/fneMj
8. Caldwell, T. (2011). Ethical hackers: Putting on the white hat. Network Security, 2011(7), 10–13. https://doi.org/10.1016/S1353-4858(11)70075-7
9. Correa, J. (2020). MANUAL DE BUENAS PRÁCTICAS EN SEGURIDAD DE LA JUAN JOSÉ CORREA SÁNCHEZ Trabajo de grado para optar al título de Ingeniero Biomédico Javier Enrique Camacho Cogollo Ingeniero Biomédico MsC . Gestión de Innovación Tecnológica INGENIERÍA BIOMÉDICA. 1–174. https://urlzs.com/b4t4L
10. Dorogovs, P. (2016). E-Service Security Challenges : Availability , Integrity , Confidentiality. 4(1), 68–78. https://urlzs.com/pjT9Y
11. Durón Chow, J. Ñ. (2005). Los ataques de la informática y la protección de datos personales en Nicaragua. Encuentro, 71, 30–53. https://doi.org/10.5377/encuentro.v0i71.4224
12. Enrique, J., Chang, A., Juan, T., & Aguirre, B. (2020). Análisis De Ataques Cibernéticos Hacia El Ecuador. Revista Científica Aristas, 2(1), 18–27. https://urlzs.com/UqJHE
13. Figueroa Suárez, J. A., Rodríguez-Andrade, R. F., Bone-Obando, C. C., & Saltos-Gómez, J. A. (2018). La seguridad informática y la seguridad de la información. Polo Del Conocimiento, 2(12), 145. https://doi.org/10.23857/pc.v2i12.420
14. Flores, Q. C. A. (2018). Tipos De Hackers. 16–18. https://n9.cl/0a84c2
15. Franc, I., Grubor, G., & Njegus, A. (2013). METALURGIA INTERNATIONAL vol . XVIII Special Issue no . 4 (2013) 345. XVIII(4), 344–352.
16. Giannone, A. (2017). Investigación en Progreso: Método de Inclusión de Hacking Ético en el Proceso de Testing de Software. Revista Latinoamericana de Ingenieria de Software, 4(6), 252. https://doi.org/10.18294/relais.2016.252-254
17. Junglas, I., Goel, L., Rehm, S.-V., & Ives, B. (2022). On the benefits of consumer IT in the workplace—An IT empowerment perspective. International Journal of Information Management, 64, 102478. https://doi.org/10.1016/j.ijinfomgt.2022.102478

18. Kapoor, A., Gupta, A., Gupta, R., Tanwar, S., Sharma, G., & Davidson, I. E. (2022). Ransomware detection, avoidance, and mitigation scheme: A review and future directions. Sustainability (Switzerland), 14(1), 1–25. https://doi.org/10.3390/su14010008
19. Kertysova, Katarina ; Frinking, Erik ; Dool, Koen van den ; Maričić, Aleksandar ; Bhattacharyya, K. (2018). Cybersecurity : Ensuring awareness and resilience of the private sector across Europe in face of mounting cyber risks.
20. Kidston, D., Li, L., Tang, H., & Mason, P. (2010). Mitigating security threats in tactical networks. … Communication and Networks, …, 1–14. https://n9.cl/1e835
21. KPMG. (2018). HEALTH CARE AND CYBER SECURITY: Increasing Threats Require Increased Capabilities. Kpmg.Com.
22. Moran Maldonando, N. M. (2021). Estado de la ciberseguridad en las empresas del sector público del Ecuador: una revisión sistemática. Universidad Politécnica Salesiana, Guayaquil, Ecuador, 1–17. https://n9.cl/gwnhsb
23. Nisa, M. U., & Kifayat, K. (2020). Detection of Slow Port Scanning Attacks. 1st Annual International Conference on Cyber Warfare and Security, ICCWS 2020 - Proceedings. https://doi.org/10.1109/ICCWS48432.2020.9292389
24. Oliver, D. J., & Randolph, A. B. (2020). Hacker Definitions in Information Systems Research. Journal of Computer Information Systems, 00(00), 1–13. https://doi.org/10.1080/08874417.2020.1833379
25. Patilla, H. J. (2021). Snort Open Source como detección de intrusos para la seguridad de la infraestructura de red. 15(3), 55–73.
26. Patiño, S., Caicedo, A., & Guaña, E. R. (2019). Modelo de evaluación del dominio control de acceso de la norma ISO 27002 aplicado al proceso de gestión de bases de datos. RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao, 2019(E22), 230–241.
27. Rivera, J. ., Herrera, V. ., Naranjo, X. ., & Narváez, C. (2019). Gestión de Riesgos de TIC en hospitales públicos. RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao, 05, 280–292. https://n9.cl/mjtcd
28. Rojas, A. (2018). Repositorio Universidad Técnica de Ambato: Hacking ético para analizar y evaluar la seguridad informática en la infraestructura de la Empresa Plasticaucho Industrial S.A. https://n9.cl/qzzzy

29. Sabillón, R., & M., J. J. C. (2019). Auditorías en Ciberseguridad: Un modelo de aplicación general para empresas y naciones. RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, 32, 33–48. https://doi.org/10.17013/risti.32.33-48
30. Sánchez, A. (2019). Hacking ético: impacto en la sociedad. Especialización En Seguridad Informática. Universidad Piloto de Colombia. https://urlzs.com/aXWY4
31. Tully, J., Selzer, J., Phillips, J. P., O'Connor, P., & Dameff, C. (2020). Healthcare Challenges in the Era of Cybersecurity. Health Security, 18(3), 228–231. https://doi.org/10.1089/hs.2019.0123
32. Villares Saltos, C. A. (2017). Estrategia De Hacking Ético Y Los Niveles De Seguridad En La Intranet De La Cooperativa De Ahorro Y Crédito 13 De Abril Ltda De La Ciudad De "Ventanas." Tesis Postgrado, 549, 134. https://n9.cl/96vfj
33. Wirth, A. (2018). To patch, or not to patch, that is the question. Biomedical Instrumentation and Technology, 52(4), 318–321. https://doi.org/10.2345/0899-8205-52.4.318