**UNIVERSIDAD TÉCNICA DEL NORTE**

**FACULTAD DE POSGRADO**

**MAESTRÍA EN COMPUTACIÓN CON MENCIÓN EN SEGURIDAD INFORMÁTICA**

**TRABAJO DE INTEGRACIÓN CURRICULAR**

**TEMA:**

# ARQUITECTURA DE SEGURIDAD PARA LA CONTINUIDAD DE SERVICIOS WEB DE CONSULTA EXTERNA DEL HOSPITAL BÁSICO "RAÚL MALDONADO MEJIA" DEL CANTON CAYAMBE

Trabajo de Titulación previo a la obtención del Título de Magíster en Computación con mención en Seguridad Informática

**Línea de investigación:** Ciberseguridad (seguridad cibernética)


**AUTOR:**

SEGUNDO FRANKLIN LARA CARTAGENA

**DIRECTOR:**

MSC. VICENTE ALEXANDER GUEVARA VEGA


**Ibarra – Ecuador**

**2025**

# CERTIFICACIÓN DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Ibarra, 18 de diciembre de 2025

MSc. Vicente Alexander Guevara Vega

**DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR**

**CERTIFICA:**

Haber revisado el presente informe final del trabajo de Integración Curricular, mismo que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en constancia, autorizo su presentación para los fines legales pertinentes.

Firmado electrónicamente por:
**VICENTE ALEXANDER GUEVARA VEGA**
Validar únicamente con FirmaEC

MSc. Vicente Alexander Guevara Vega

c.c.: 1002334827

**DEDICATORIA**

En memoria de mis padres…

## AGRADECIMIENTOS

A mi querida Universidad Técnica del Norte y a sus maestros, quien a lo largo de mi formación académica me han dado la oportunidad de crecer a nivel personal y profesional.

# UNIVERSIDAD TÉCNICA DEL NORTE

## BIBLIOTECA UNIVERSITARIA

### AUTORIZACIÓN DE USO Y PUBLICACIÓN

### A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

## 1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

| **DATOS DE CONTACTO** | | | |
|---|---|---|---|
| **CÉDULA DE IDENTIDAD:** | 1714632575 | | |
| **APELLIDOS Y NOMBRES:** | LARA CARTAGENA SEGUNDO FRANKLIN | | |
| **DIRECCIÓN:** | CAYAMBE, OLMEDO N5-45 Y PICHINCHA | | |
| **EMAIL:** | franklynlara@hotmail.com | | |
| **TELÉFONO FIJO:** | | **TELÉFON OMÓVIL:** | 0992232324 |
| **DATOS DE LA OBRA** | | | |
| TÍTULO: | ARQUITECTURA DE SEGURIDAD PARA LA CONTINUIDAD DE SERVICIOS WEB DE CONSULTA EXTERNA DEL HOSPITAL BÁSICO “RAÚL MALDONADO MEJIA” DEL CANTON CAYAMBE | | |
| **AUTOR (ES):** | SEGUNDO FRANKLIN LARA CARTAGENA | | |
| **FECHA: DD/MM/AAAA** | 31/05/2023 | | |
| SOLO PARA TRABAJOS DE GRADO | | | |
| **PROGRAMA:** | ☐ **PREGRADO** ☒ **POSGRADO** | | |
| **TITULO POR EL QUE OPTA:** | Magíster en Computación con mención en Seguridad Informática | | |
| **ASESOR /DIRECTOR:** | Msc. Vicente Alexander Guevara Vega | | |

**2. CONSTANCIAS**

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 18 días del mes de diciembre de 2025.

**EL AUTOR:**


(Firma)……

Nombre: Segundo Franklin Lara Cartagena

**Tabla de Contenido**

INDICE DE TABLAS ..... xii

INDICE DE FIGURAS ..... xiv

RESUMEN ..... xvii

ABSTRACT ..... xviii

1 CAPITULO I: EL PROBLEMA ..... 1

1.1 Problema de investigación ..... 1

1.1. Interrogantes de la investigación ..... 3

1.1.1 Objetivo general ..... 4

1.1.1. Objetivos específicos ..... 4

1.2 Justificación ..... 5

2 CAPITULO II: MARCO REFERENCIAL ..... 7

2.1 Antecedentes ..... 7

2.2 Marco teórico ..... 9

2.2.1 Proceso de Revisión de la Literatura (LR) ..... 10

2.2.2 Metodología de la revisión sistemática ..... 10

2.2.3 Identificación de Literatura Relevante ..... 11

2.2.4 Estrategias de Búsqueda ..... 12

2.2.5 Criterios de Inclusión y Exclusión ..... 12

2.2.6 Análisis y Selección ..... 12

2.2.7 Síntesis de la Literatura ..... 12

2.2.8 Unidad de análisis ..... 13

2.2.9 Cadena de búsqueda ..... 14

2.2.10 Búsqueda de documentos ..... 14

2.2.11 Procedimiento y Resultados ..... 15

2.2.12 Evaluación y Síntesis ..... 15

2.2.13 Selección de artículos ..... 15

2.2.14 Extracción de datos relevantes ..... 20

2.2.15 Matriz de conceptos ..... 20

2.3 Marco Conceptual ..... 21

2.3.1 Componentes de un servicio web ..... 21

2.3.2 Hardware ..... 22

2.3.3 Servicios en la nube ..... 23

2.3.4 Software ..... 24

2.3.4.1 Clasificación del software de aplicación ..... 25

2.3.5 Aplicaciones web ..... 26

2.3.6 Tipos de aplicaciones web ..... 27

2.3.7 Servidores Web ..... 28

2.3.8 Comunicaciones ..... 29

2.3.8.1 Protocolo HTTP y HTTPS ..... 29

2.3.9 Certificados SSL/TLS ..... 30

2.3.10 Métricas Web ..... 31

2.3.10.1 Funcionalidad ..... 31

2.3.10.2 Usabilidad ..... 31

2.3.10.3 Seguridad..... 31

2.3.11 Arquitectura de software y su clasificación ..... 32

2.3.12 Arquitectura de software enfocada a la ciberseguridad ..... 33

2.3.13 Seguridad en servicios web basados en software libre ..... 34

2.3.14 Lenguajes de Modelado ..... 35

2.3.15 ArchiMate Core Framework ..... 36

2.3.16 Seguridad Informática y Seguridad de la información ..... 36

2.3.17 Normativa y Estándares de Seguridad de la Información..... 37

2.3.18 Riesgos ..... 38

2.3.19 Riesgos en ataques informáticos..... 39

2.3.20 Ataques informáticos ..... 39

2.3.21 Ataques comunes a servicios web ..... 40

2.3.22 Análisis y Gestión de Riesgos ..... 41

2.3.23 Análisis de riesgos informáticos y ciberseguridad ..... 41

2.3.24 Metodologías para el Análisis y gestión de riesgos de la Información..... 42

2.3.25 Metodología MAGERIT v.3 ..... 43

2.3.26 Resiliencia Digital..... 43

2.3.27 Continuidad de servicios ..... 43

2.3.28 La continuidad de servicios web ..... 44

2.3.29 ISO/IEC 27031:2011 ..... 45

2.3.30 Indicadores clave de la Norma ISO 27031..... 45

2.4 Marco legal ..... 46
3 CAPITULO III MARCO METODOLÓGICO ..... 49
3.1 Descripción del área de estudio ..... 49
3.2 Diseño metodológico de la evaluación ..... 51
3.3 Enfoque y tipo de investigación ..... 53
3.4 Procedimiento de investigación ..... 55
3.4.1 Fase 1 Análisis de Riesgos ..... 55
3.4.2 Fase 2 Métricas del servicio web de consulta externa ..... 55
3.4.3 Fase 3 Prueba de concepto servicio web seguro, modelado arquitectónico ... 56
3.4.4 Fase 4 Evaluación de cumplimiento de la norma ISO NTE INEN-ISO/IEC 27031 ..... 56
3.5 Consideraciones bioéticas ..... 57
4 CAPITULO IV RESULTADOS Y DISCUSIÓN ..... 58
4.1 Resultados ..... 58
4.1.1 Metodología MAGERIT v.3 ..... 58
4.1.2 Métricas del servicio web de consulta externa ..... 68
4.1.3 Prueba de concepto ..... 74
4.1.4 Evaluación de cumplimiento ..... 82
4.1.4.1 Caracterización de la muestra ..... 82
4.1.4.2 Impactos por activo en C–I–D ..... 89
4.1.4.3 BIA y parámetros RTO/RPO ..... 90
4.1.5 Principales temas abordados ..... 94

4.1.5.1 Prácticas de ciberseguridad ..... 95

4.1.5.2 Normativas y estándares aplicados en el sector salud ..... 95

4.1.6 Análisis de la funcionalidad ..... 95

4.1.6.1 Desempeño del sistema ..... 95

4.1.6.2 Fiabilidad y disponibilidad ..... 96

4.1.1. Evaluación de la usabilidad ..... 96

4.1.6.3 Facilidad de uso ..... 97

4.1.7 Seguridad de los servicios web ..... 97

4.1.7.1 Detección de Intrusiones ..... 97

4.2 Discusión ..... 98

4.2.1 Comparación con estudios previos ..... 98

4.2.1.1 Consistencia de los resultados ..... 99

4.2.1.2 Innovaciones y avances recientes ..... 101

4.2.2 Implicaciones prácticas ..... 103

4.2.2.1 Mejora de la funcionalidad ..... 103

4.2.2.2 Optimización de la usabilidad ..... 105

4.2.2.3 Fortalecimiento de la seguridad ..... 105

4.2.3 Limitaciones de la revisión ..... 106

4.2.3.1 Limitaciones metodológicas ..... 106

4.2.3.2 Áreas no abordadas ..... 106

4.2.4 Recomendaciones para futuras investigaciones ..... 107

4.2.4.1 Nuevas líneas de investigación ..... 107

CONCLUSIONES Y RECOMENDACIONES ..... 108

Conclusiones ..... 108

Recomendaciones ..... 109

Referencias ..... 110

5 ANEXOS ..... 115

## INDICE DE TABLAS

Tabla 1. *Centros de salud de primer nivel de atención* ..... 2

Tabla 2. *Principales ciberamenazas en Ecuador* ..... 9

Tabla 3. *Cadena de búsqueda* ..... 14

Tabla 4. *Búsqueda de documentos* ..... 15

Tabla 5. *Fases selección artículos* ..... 16

Tabla 6. *Artículos seleccionados* ..... 16

Tabla 7. *Alcance del diseño y unidad de análisis* ..... 51

Tabla 8. *Población y muestra* ..... 52

Tabla 9. *Ítems por dimensión* ..... 52

Tabla 11. *Enfoque y diseño* ..... 53

Tabla 12. *Alcance y muestra* ..... 54

Tabla 13. *Técnicas e instrumentos* ..... 54

Tabla 14. *Escalas de probabilidad* ..... 60

Tabla 15. *Escalas de impacto* ..... 60

Tabla 16. *Matriz de Riesgos* ..... 60

Tabla 17. *Vulnerabilidades y salvaguardas activos de información* ..... 65

Tabla 18. *Páginas o recursos más usados del sitio logs Apache* ..... 70

Tabla 19. *Registro de datos para análisis de rendimiento App Consulta Externa* ..... 72

Tabla 20. *Resumen de análisis de rendimiento App Consulta Externa* ..... 72

Tabla 21. *Análisis con https://tools.pingdom.com* ..... 72

Tabla 22. *Análisis de funciones con herramienta para desarrolladores* ..... 73

Tabla 23. *Pregunta 1* ..... 82

Tabla 24. *Pregunta 2* ..... 83

Tabla 25. *Pregunta 3* ..... 84

Tabla 26. *Pregunta 4* ..... 85

Tabla 27. *Pregunta 5* ..... 86

Tabla 28. *Pregunta 6* ..... 87

Tabla 29. *Pregunta 7* ..... 88

Tabla 30. *Impactos en la disponibilidad, integridad y confidencialidad* ..... 89

Tabla 31. *Análisis de procesos críticos y prioridad de recuperación* ..... 90

Tabla 32. *Citas agendadas por especialidad año 2024* ..... 91

Tabla 33. *Promedio de citas agendadas año 2024* ..... 91

Tabla 34. *Citas confirmadas por especialidad año 2024* ..... 92

Tabla 35. *Promedio de citas confirmadas año 2024* ..... 92

Tabla 36. *Análisis de Impacto al Negocio (BIA) – Consulta Externa* ..... 92

Tabla 37. *Análisis de impacto RTO y RPO en citas y atención médica* ..... 93

Tabla 38. *Análisis de requisitos* ..... 93

Tabla 39. *Resultados de temas abordados* ..... 95

## INDICE DE FIGURAS

Figura 1. *Árbol de Problemas*..... 3

Figura 2. *Triada de la seguridad* ..... 6

Figura 3. *ENISA principales amenazas 2024* ..... 8

Figura 4. *Metodología de la Revisión Sistémica*..... 11

Figura 5. *Identificación de literatura relevante*..... 13

Figura 6. *Preguntas de Investigación*..... 14

Figura 7. *Componentes de servicio web*..... 22

Figura 8. *Componentes de hardware para servicio web*..... 23

Figura 9. *Servicios en la nube*..... 23

Figura 10. *Clasificación de software de sistema y aplicación* ..... 25

Figura 11. *Beneficios de las aplicaciones web* ..... 26

Figura 12. *Tipos de aplicaciones web* ..... 27

Figura 13. *Servidores web más usados* ..... 28

Figura 14. *Protocolo http vs https*..... 30

Figura 15. *Métricas web: funcionalidad, usabilidad, seguridad*..... 32

Figura 16. *Arquitectura de software* ..... 33

Figura 17. *Arquitectura de seguridad* ..... 34

Figura 18. *Componentes principales de seguridad en servicios web* ..... 35

Figura 19. *Lenguaje UML* ..... 36

Figura 20. *Diferencias entre seguridad informática y de la información*..... 37

Figura 21. *ISO/IEC 27001*..... 38

Figura 22. *Gestión de Riesgos de la información*..... 38

Figura 23. *Vulnerabilidades más comunes en aplicaciones web*..... 40

Figura 24. *Gestión de Riesgos y continuidad de negocio*..... 41

Figura 25. *Continuidad de servicios* ..... 44

Figura 26. *TIC para la continuidad del negocio* ..... 45

Figura 27. *Tiempo de recuperación objetivo (RTO) y punto de recuperación objetivo (RPO)* ..... 46

Figura 28. *Ubicación del HBRMM* ..... 49

Figura 29. *Unidades de salud cantones Cayambe y Pedro Moncayo - Pichincha* ..... 50

Figura 30. *Infraestructura de red HBRMM – Consulta Externa* ..... 51

Figura 31. *Fases de investigación* ..... 55

Figura 32. *Arquitectura de seguridad propuesta* ..... 56

Figura 33. *Activos de información Consulta Externa HBRMM* ..... 58

Figura 34. *Proyecto de análisis de riesgos con PILAR - Servicio de Consulta Externa HBRMM* ..... 59

Figura 35. *PILAR – valoración de los activos* ..... 59

Figura 36. *Mapa de Calor de Riesgos MAGERIT v3* ..... 62

Figura 37. *Nmap – escaneo de puertos y vulnerabilidades* ..... 63

Figura 38. *Nmap – puertos abiertos* ..... 63

Figura 41. *Nikto – vulnerabilidades* ..... 64

Figura 42. *Hostedscan – informe de Vulnerabilidades* ..... 64

Figura 43. *Resumen de vulnerabilidades por herramienta de escaneo* ..... 65

Figura 44. *Salvaguardias servicio web Consulta Externa* ..... 67

Figura 45. *Cultura Organizacional HBRMM* ..... 68

Figura 46. *Infraestructura tecnológica servicio web de Consulta Externa* ..... 68

Figura 47. *Objetivo estratégico relación servicio web de Consulta Externa* ..... 69

Figura 48. *Funcionalidad de App web de Consulta Externa* ..... 69

Figura 49. *Resumen mensual de estadísticas y tráfico de servicio web Apache* ..... 70

Figura 50. *Análisis con herramienta integrada en el navegador Google Chrome* ..... 73

Figura 51. *Capa de Tecnología – Infraestructura y software* ..... 75

Figura 52. *Servicio de Consulta Externa - Capas de negocio, aplicación y tecnología*..... 76

Figura 53. *Arquitectura de seguridad desplegada en https://hospitalbasicocayambe.online/* ..... 77

Figura 54. *Geolocalización de IP pública servidor VPS Miami* ..... 78

Figura 55. *Página inicial aplicación web de Consulta Externa desplegada* ..... 78

Figura 56. *Informe SSL de hospitalbasicocayambe.online* ..... 79

Figura 57. *Generación de claves privada y pública para acceso vía SSH* ..... 79

Figura 58. *Servicio Fail2ban en ejecución*..... 79

Figura 59. *UFW reglas activas de firewall* ..... 80

Figura 60. *Web Aplication Firewall (WAF) en ejecución*..... 80

Figura 61. *Aplication Firewall (WAF) resultado test con payload OWASP CRS 3.2.0* ..... 80

Figura 62. *Respuesta Cabeceras HTTP de seguridad* ..... 81

Figura 63. *Servicio de Snort activo y en ejecución*..... 81

Figura 64. *Snort IDS analizando tráfico* ..... 81

Figura 65. *Pregunta 1*..... 83

Figura 66. *Pregunta 2*..... 84

Figura 67. *Pregunta 3*..... 85

Figura 68. *Pregunta 4*..... 86

Figura 69. *Pregunta 5*..... 87

Figura 70. *Pregunta 6* ..... 87

Figura 71. *Pregunta 7* ..... 88

Figura 72. *Definiciones NTE INEN-ISO/IEC 27031 / ISO/IEC 27031*..... 93

UNIVERSIDAD TÉCNICA
DEL NORTE FACULTAD DE POSGRADO

PROGRAMA DE MAESTRÍA COMPUTACIÓN
CON MENCIÓN EN SEGURIDAD INFORMÁTICA

# ARQUITECTURA DE SEGURIDAD PARA LA CONTINUIDAD DE SERVICIOS WEB DE CONSULTA EXTERNA DEL HOSPITAL BÁSICO "RAÚL MALDONADO MEJIA" DEL CANTON CAYAMBE

**Autor:** Segundo Franklin Lara Cartagena

**Tutor:** Msc. Alexander Guevara Vega

**Año:** 2025

## RESUMEN

El objetivo del proyecto es diseñar una arquitectura de seguridad para la continuidad de servicios web de consulta externa del Hospital Básico "Raúl Maldonado Mejía" HBRMM del cantón Cayambe. La investigación se desarrolló en cuatro fases: inicia con el análisis de riesgos usando la herramienta PILAR para la recolección de datos para identificar los activos críticos de información. Mediante la aplicación de la metodología MAGERIT v.3 y el uso software para la ejecución de pruebas de penetración como Nmap, Nikto y Hostedscan se determinaron amenazas, vulnerabilidades, riesgos y se plantearon salvaguardas orientadas a mejorar la confidencialidad, integridad y disponibilidad de la información (CID). En la Fase 2 se identificaron métricas que permitieron evaluar aspectos de rendimiento, funcionalidad, usabilidad y seguridad de la aplicación web de gestión de citas y agendamiento del HBRMM, se analizaron logs de servicios con Webalizer, mediciones con Pingdom y utilitarios de navegador. En la Fase 3 se desarrolló una prueba de concepto, desplegando en un VPS con varias herramientas de seguridad basadas en software libre (entre ellas UFW, WAF, Snort, Logwatch), con el fin de implementar una arquitectura de web server segura y modelada en ArchiMate Core Framework. Finalmente, en la Fase 4 se realiza la evaluación de cumplimiento de la norma NTE INEN-ISO/IEC 27031, considerando impactos en la CID, procesos críticos, análisis de impacto del negocio (BIA) y parámetros RTO/RPO. Como conclusión, se determina que la aplicación de la metodología MAGERIT v.3 permite gestionar de manera adecuada los riesgos de seguridad, mientras que ArchiMate facilita una representación clara y entendible de la arquitectura propuesta. Asimismo, las métricas de rendimiento, funcionalidad, usabilidad y seguridad permiten plantear mejoras en el sistema de gestión de citas y agendamiento. En conjunto, este modelo contribuye con la continuidad de las operaciones, siendo replicable y sostenible para otras instituciones de salud.

**Palabras clave**: arquitectura seguridad, riesgos Magerit, continuidad, INEN-ISO/IEC 27031

UNIVERSIDAD TÉCNICA
DEL NORTE FACULTAD DE POSGRADO

PROGRAMA DE MAESTRÍA COMPUTACIÓN
CON MENCIÓN EN SEGURIDAD INFORMÁTICA

# ARQUITECTURA DE SEGURIDAD PARA LA CONTINUIDAD DE SERVICIOS WEB DE CONSULTA EXTERNA DEL HOSPITAL BÁSICO "RAÚL MALDONADO MEJIA" DEL CANTON CAYAMBE

**Autor:** Segundo Franklin Lara Cartagena

**Tutor:** Msc. Alexander Guevara Vega

**Año:** 2025

## ABSTRACT

The objective of the project is to design a security architecture for the continuity of outpatient web services at the Raúl Maldonado Mejía Basic Hospital (HBRMM) of Cayambe. The research was carried out in four phases: it began with a risk analysis using the PILAR tool to collect data and identify critical information assets. Through the application of the MAGERIT v.3 methodology and the use of software for penetration testing such as Nmap, Nikto, and Hostedscan, threats, vulnerabilities, and risks were identified, and safeguards were proposed to improve the confidentiality, integrity, and availability of information (CIA). In Phase 2, metrics were identified to evaluate aspects of performance, functionality, usability, and security of the HBRMM appointment management and scheduling web application. Service logs were analyzed with Webalizer, measurements with Pingdom, and browser utilities. In Phase 3, a proof of concept was developed, deploying a VPS with several free software-based security tools (including UFW, WAF, Snort, and Logwatch) in order to implement a secure web server architecture modeled on the ArchiMate Core Framework. Finally, in Phase 4, compliance with the NTE INEN-ISO/IEC 27031 standard is evaluated, considering impacts on the CID, critical processes, business impact analysis (BIA), and RTO/RPO parameters. In conclusion, it has been determined that the application of the MAGERIT v.3 methodology allows for the adequate management of security risks, while ArchiMate facilitates a clear and understandable representation of the proposed architecture. Likewise, the performance, functionality, usability, and security metrics allow for improvements to be made to the appointment and scheduling management system. Overall, this model contributes to the continuity of operations, being replicable and sustainable for other healthcare institutions.

**Keywords**: security architecture, Magerit risks, continuity, INEN-ISO/IEC 27031

# 1 CAPITULO I: EL PROBLEMA

## 1.1 Problema de investigación

La informática hoy en día está integrada completamente a nuestras actividades cotidianas: visitamos sitios web, revisamos el correo electrónico, descargamos infinidad de archivos y documentos, y accedemos a diferentes redes con total naturalidad, sin mayor preocupación por los riesgos de seguridad que pueden existir. Estas acciones, que ya se vuelven mecánicas, puedan suponer una amenaza significativa para la seguridad digital, tanto a nivel personal como empresarial (Cremer et al., 2022).

De acuerdo con Zaid & Garai (2024) “La ciberseguridad es la práctica de defender las computadoras, los servidores, los dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica”. Esta definición resalta la importancia de proteger tanto el hardware como el software, elementos fundamentales en cualquier tipo de dispositivo electrónico.

El acceso remoto a servidores que alojan servicios web, correo electrónico y bases de datos son los elementos imprescindibles a proteger, ya que, si un atacante encuentra y explota alguna vulnerabilidad en ellos, podría ocasionar la indisponibilidad de recursos tecnológicos críticos o fundamentales en las organizaciones.

Trabajar en red y acceder a servicios web de manera remota representa un gran avance; sin embargo, también puede suponer un riesgo si alguien logra infiltrarse en aplicaciones o sistemas de uso exclusivo de las organizaciones. Desde un dispositivo externo con acceso a internet, un atacante o curioso podría acceder sin autorización y comprometer la información de pacientes en el caso de instituciones de salud.

De manera más específica en instituciones prestadoras de servicios de salud, un problema de seguridad informática puede exponer datos de la organización, así como in formación de pacientes y usuarios, lo que podría traer consecuencias legales.

La indisponibilidad de servicios web en el área de consulta externa de un hospital público genera inconformidad en los pacientes, afecta la imagen y valores institucionales, y aumenta los tiempos de espera en el agendamiento de citas y atención médica.

La falta de atención médica en fechas y horarios planificados genera pérdidas económicas para los pacientes del sector urbano y rural, ya que muchos de ellos son referidos desde distintas parroquias y acuden a citas médicas programadas. La indisponibilidad del servicio web de consulta externa provoca que dichos pacientes sean atendidos en fechas posteriores, lo que, en algunos casos puede ocasionar mayor deterioro de su salud (European Union Agency for Cybersecurity., 2024).

El Ministerio de Salud Pública de Ecuador (MSP), en los cantones de Cayambe y Pedro Moncayo, provincia de Pichincha, mantiene centros de salud que ofrecen servicios considerados de primer nivel o de atención básica. Sin embargo, pacientes con problemas de salud más complejos requieren atención de segundo nivel o de especialidad, lo que genera referencias al Hospital Básico “Raúl Maldonado Mejía” (HBRMM) de la ciudad Cayambe.

En la Tabla 1, se detallan los centros de salud de primer nivel de los cantones Cayambe y Pedro Moncayo que proporcionan atención primaria en salud.

**Tabla 1.**

*Centros de salud de primer nivel de atención*

| No. | Código SGI [a] | Cantón | Unidad Operativa |
|---|---|---|---|
| 1 | 1707 | Cayambe | Ascázubi |
| 2 | 1694 | Cayambe | Cangahua |
| 3 | 1695 | Cayambe | Espiga de Oro |
| 4 | 1692 | Cayambe | Ayora |
| 5 | 2723 | Cayambe | Cayambe |
| 6 | 3446 | Cayambe | Juan Montalvo |
| 7 | 1693 | Cayambe | Olmedo |
| 8 | 1697 | Cayambe | Pesillo |
| 9 | 1696 | Cayambe | Otón |
| 10 | 1698 | Cayambe | Cuzubamba |
| 11 | 1703 | Pedro Moncayo | La Esperanza |
| 12 | 1700 | Pedro Moncayo | Malchinguí |
| 13 | 1699 | Pedro Moncayo | Tabacundo |
| 14 | 1701 | Pedro Moncayo | Tocachi |
| 15 | 1702 | Pedro Moncayo | Tupigachi |

*Nota*. Unidades operativas del MSP, provincia de Pichincha Código Único de Establecimiento Sistema de Gestión Integral

Este proyecto busca diseñar una Arquitectura de Seguridad para garantizar la continuidad de servicios web de consulta externa del HBRMM del cantón Cayambe, basado en la Metodología de Análisis y Gestión de Riesgos con Magerit v.3 y Archimate Core Framework como lenguaje de modelado arquitectónico, utilizando software libre.

En la siguiente figura podemos encontrar el árbol de problemas donde se detallan las causas y efectos de la indisponibilidad de servicios web en el servicio de consulta externa del hospital básico.

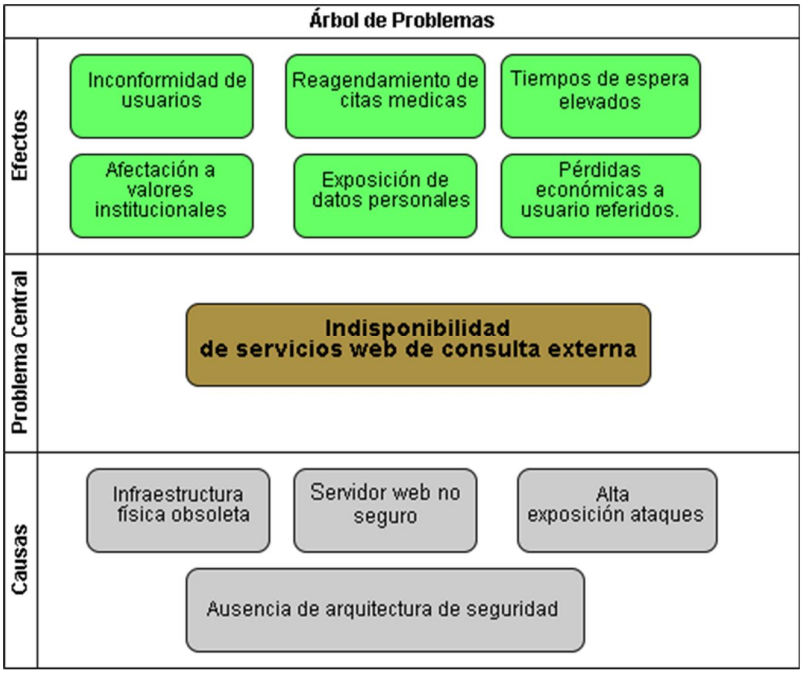



**Figura 1.** *Árbol de Problemas*

*Nota. Causas y efectos de la indisponibilidad de servicios web en consulta externa HBRMM.*

### 1.1. Interrogantes de la investigación

En este contexto se plantea las siguientes interrogantes de investigación:

¿El diseño de una arquitectura de seguridad para los servicios web del HBRMM permitirá salvaguardar de mejor manera la información de los pacientes en el servicio de consulta externa?

¿Una adecuada gestión de riesgos permitirá mejorar la continuidad de los servicios web de consulta externa de la institución?

¿Realizar una prueba de concepto desplegando de manera aislada servicios web seguros para el servicio de consulta externa, permitirá mejorar los niveles de confidencialidad, integridad y disponibilidad de la información?

### *1.1.1 Objetivo general*

Diseñar una arquitectura de seguridad para la continuidad de servicios web de consulta externa del Hospital Básico “Raúl Maldonado Mejía” del cantón Cayambe, basado en la metodología de análisis y gestión de riesgos con MAGERIT v.3 y ArchiMate Core Framework como lenguaje de modelado arquitectónico.

### *1.1.1. Objetivos específicos*

- Diagnosticar los riesgos a servicios web aplicando la metodología MAGERIT v.3, para determinar las amenazas y vulnerabilidades que impacten de manera potencial a la disponibilidad de los servicios web de consulta externa.
- Identificar las métricas relacionadas con los servicios web de consulta externa.
- Desarrollar una prueba de concepto mediante el despliegue de servicios web con una arquitectura de seguridad basado en ArchiMate Core Framework y soluciones basadas software libre.
- Evaluar el cumplimiento de la continuidad de servicios web de consulta externa, mediante la norma NTE INEN-ISO/IEC 27031.

## 1.2 Justificación

Garantizar una vida sana y promover el bienestar de todos a todas las edades, es parte de la Agenda 2030 y los Objetivos de Desarrollo Sostenible Una oportunidad para América Latina y el Caribe, para lograr el desarrollo sostenible es fundamental garantizar una vida saludable, promover el bienestar para todos a cualquier edad, en donde el acceso a los sistemas de salud juega un papel muy importante en temas de prevención y tratamiento de enfermedades (Martin, s. f.).

La meta 3.8 del Objetivo 3 de Salud y Bienestar menciona que se pretende "Lograr la cobertura sanitaria universal, incluida la protección contra los riesgos financieros, el acceso a servicios de salud esenciales de calidad y el acceso a medicamentos y vacunas inocuos, eficaces, asequibles y de calidad para todos" (World Health Statistics, 2024).

El Plan de Creación de OPORTUNIDADES 2021-2025, en su objetivo número 5 busca proteger a las familias, garantizar sus derechos y servicios además de, garantizar el derecho a la salud integral, gratuita y de calidad, concibiendo a la salud como un derecho humano y abordado los vínculos entre los sectores urbanos y rurales, enfatizando la atención a grupos vulnerables (*PLAN-NACIONAL-DE-DESARROLLO-2021-2025*, 2025.).

La política 10.1 del objetivo 10 del plan antes mencionado, pretende “Fortalecer al Estado para mantener la confidencialidad, integridad y disponibilidad de la información frente amenazas provenientes del ciberespacio y proteger su infraestructura critica” (*Ficha metodológica de definición de metas del plan nacional de desarrollo, 2024*). La meta para el año 2025 es incrementar el índice de ciberseguridad global de 26,3 a 51,3 mejorando de esta manera la capacidad del país para responder amenazas cibernéticas.

Las organizaciones e instituciones públicas deben formar parte de la transformación tecnológica con el uso de las TIC. Esta transformación no necesariamente debe estar ligada al uso de sistemas de información, almacenamiento y procesamiento de datos, sino también, a una arquitectura de seguridad que garantice que dichos sistemas de cumplan con los principios de confidencialidad, integridad y disponibilidad (Rodríguez, 2021).

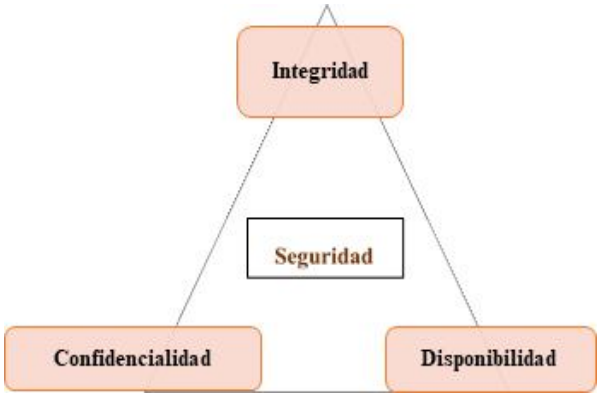



**Figura 2.** *Triada de la seguridad*

*Nota: Diseño propio a partir del concepto de la triada de seguridad*

La falta de implementación de herramientas de seguridad informática en los servicios web del HBRMM, impide garantizar la continuidad de los sistemas de información relacionados con el área de consulta externa como prestador de atenciones de salud de segundo nivel.

La justificación de esta propuesta pretende que el diseño de una arquitectura de seguridad para el servicio web de consulta externa del HBRMM, de la ciudad de Cayambe, basada en la metodología de análisis y gestión de riesgos con MAGERIT v.3 y ArchiMate Core Framework como lenguaje de modelado, se constituya en una herramienta que permita priorizar controles generales aplicables a los activos de información relacionados, buscando definir lineamientos para el acceso y manejo seguro del sitio web para la gestión de citas médicas del área de consulta externa; estableciendo controles técnicos a implementarse, evaluando su impacto en la mejora de la seguridad, minimizando la interrupción de los servicios web, y mitigando riesgos asociados a la seguridad y la falta de disponibilidad (Technology, 2024).

Finalmente, la línea de investigación de la UTN a la que aporte a esta propuesta tiene relación a la numero 10. Desarrollo, estudio de software y seguridad cibernética, de manera específica a la aplicación de seguridad en software.

# 2 CAPITULO II: MARCO REFERENCIAL

En la actualidad, la seguridad es un punto inflexible tanto en lo personal y peor en lo informático y se ha transformado en un pilar primordial para garantizar la continuidad de los servicios web, en el sector de la salud tiene un eje transcendental para garantizar el respaldo de información sensible. La progresiva dependencia de las tecnologías de la información y la comunicación para la ayuda de servicios de salud ha enviado un mensaje claro para que se desarrolle arquitecturas confiables, seguras y robustas. La finalidad de estas arquitecturas es proteger contra ataques cibernéticos, y garantizar la prolongación de los servicios básicos ante cualquier ataque. Este capítulo revisa los antecedentes importantes para establecer por qué el desarrollo de una arquitectura de seguridad orientada a garantizar de manera ininterrumpida todos los servicios web del HBRMM de la ciudad de Cayambe.

## 2.1 Antecedentes

Se conoce de salud y de seguridad en software; casi nada se desconoce un 75%, garantizar los sistemas de salud ha sido considerado muy relativo ya que, según estudios e investigaciones, no han podido garantizar el respaldo, continuidad y el acoplamiento de los servicios en línea en el área de salud de todo el ecuador. En esta época, se ha visto como los avances tecnológicos de estrategia y de aplicaciones web para afrontar los desafíos de seguridad específicos del sector de la salud (Admass et al., 2024).

Con este proyecto se pretende brindar una arquitectura de seguridad que se enmarque en algo específico relacionado con el entorno de la salud, garantizando y asegurando la disponibilidad de los servicios en línea. Esta arquitectura va a integrar prácticas de gestión de riesgos, como la metodología MAGERIT, y marcos de diseño arquitectónico, como ArchiMate, para ofrecer un diseño holístico y estructurado que facilita la verificación, evaluación y tratamiento de riesgos en los sistemas de información.

MAGERIT como metodología, considera las normas ISO/IEC 27001 y la ISO/IEC 27002 mismas que proporcionan guías para la implementación de sistemas de gestión de seguridad de la información (SGSI), todo esto respaldado con controles de seguridad, que pueden ser modificados a las necesidades específicas de las organizaciones de salud, promoviendo así la confidencialidad, integridad y disponibilidad de los datos (*ISO/IEC 27032:2023 - ISO/IEC 27032:2023*, s. f.).

De acuerdo con la consultora Haseeb-ur-rehman et al., (2023) la norma ISO/IEC 27031 busca asegurar la continuidad de las operaciones de una organización en un entorno tecnológico, minimizando el impacto de incidentes y desastres, y fortaleciendo tanto la resiliencia como capacidad de recuperación.

La adaptación de la continuidad de los servicios web en el sector salud a los estándares internacionales de seguridad de la información permitiría mitigar los riesgos asociados a ciberataques y otros incidentes que comprometan la disponibilidad e integridad de los servicios.

Para el año 2024, la Agencia de la Unión Europea para la Ciberseguridad (ENISA) identificó siete amenazas principales para la ciberseguridad (2024, p. 9), las cuales se presentan en la figura 3. Una de las más relevantes es aquella que afecta a la disponibilidad de la información.


**Figura 3.** *ENISA principales amenazas 2024*

*Nota: Tomado de (Agencia de la Unión Europea para la Ciberseguridad, 2024). CC-BY*

De acuerdo con la página de Gobierno Electrónico del Ecuador, las principales ciberamenazas que afectan al país y que pueden comprometer la continuidad de servicios web en instituciones y organizaciones a nivel nacional, se detallan en la Tabla 2.

**Tabla 2.**

*Principales ciberamenazas en Ecuador*

| No. | Amenaza |
|---|---|
| 1 | Suplantación de identidad |
| 2 | Correo no deseado |
| 3 | Software malicioso |
| 4 | Fuga de información |
| 5 | Amenaza interna |
| 6 | Manipulación física/daño/robo/pérdida |
| 7 | Robo de identidad |
| 8 | *Ataques de aplicaciones web |
| 9 | Programa de secuestro de datos |
| 10 | Negación de servicio |
| 11 | *Ataques basados en la web |
| 12 | Violación de datos |
| 13 | Redes de bots |
| 14 | Minería de criptomonedas maliciosa |
| 15 | Espionaje cibernético |

*Nota: Tomado de Gobierno Electrónico de Ecuador (s. f.) *Asociadas a servicios web*

Estos antecedentes sugieren el desarrollo de una arquitectura de seguridad robusta para servicios web, requiere un enfoque integrador que combine prácticas apropiadas de gestión de riesgos, herramientas de control de seguridad reconocidas y un marco adecuado de modelado arquitectónico. La ejecución de estas tácticas permitirá al HBRMM del cantón Cayambe optimizar la seguridad y la continuidad de sus servicios web en línea del área de consulta externa, observando metodologías y normas internacionales, que respondan positivamente a los crecientes ataques cibernéticos en el sector de la salud.

## 2.2 Marco teórico

Dentro de lo que es el marco teórico, vamos a dar a conocer investigaciones realizadas en base a estudios previos y teorías fundamentadas que cuadren con la realidad y que brinden la arquitectura de seguridad recomendada para la continuidad de los servicios web en el ámbito de la salud. Se comenzó con un meticuloso proceso de selección para la revisión de los problemas reales, asegurando incluir investigaciones actuales y relevantes que proporcionen

una base sólida y actualizada para nuestro estudio. Este proceso nos permitirá identificar, recolectar evidenciar, sintetizar los aportes teóricos y empíricos que son eficaces para abordar tanto el problema de investigación como los objetivos que van a ser planteados.

### *2.2.1 Proceso de Revisión de la Literatura (LR)*

Consiste en proporcionar y dar a atender con apreciación profunda y estructurada sobre el estado actual del conocimiento en un área específica de estudio. La revisión sistemática de la literatura permitirá iniciar correctamente y es crucial en la investigación correcta, Este proceso implica la selección minuciosa de estudios relevantes, permitiendo a los investigadores resumir resultados existentes, identificar vacíos en la literatura, y establecer nuevas direcciones para la investigaciones presentes y futuras.

### *2.2.2 Metodología de la revisión sistemática*

Es una adaptación para observar pros y contras de la literatura, este estudio sigue una serie de pasos estratégicos, diseñados para garantizar una cobertura absoluta y objetiva del cuerpo de conocimiento existente sobre la arquitectura de seguridad para la continuidad de los servicios web en línea en el contexto de la salud. Basándonos en las investigaciones hechos por expertos en el campo (Page et al., 2021a).

#### *Definición de criterios de inclusión y exclusión*

Se establece con parámetros claros para mencionar estudios e investigaciones publicados en los últimos años, asegurando la relevancia y actualidad de la información. Se dio prioridad a trabajos peer-reviewed que abordan directamente la seguridad informática, la arquitectura de seguridad, y la continuidad de servicios web en el sector salud.

#### *Búsqueda en bases de datos académicas*

Se utilizó bases de datos reconocidas como PubMed, IEEE Xplore, Scopus y Google Scholar, empleando una combinación de palabras clave relacionadas con nuestra área de estudio (Rethlefsen et al., 2021).

#### *Selección y evaluación de estudios*

Cada estudio identificado fue evaluado en función de su título, resumen y relevancia para los objetivos de la investigación. Se empleó el modelo PRISMA como guía para garantizar una selección sistemática y transparente de la literatura (Page et al., 2021b).

***Análisis y síntesis de la literatura***

Los estudios seleccionados fueron sometidos a un análisis detallado, destacando hallazgos clave, metodologías empleadas y conclusiones relevantes. Este enfoque nos permitió identificar tendencias comunes, así como divergencias en la investigación existente.

***Identificación de lagunas en la literatura***

El análisis crítico de los estudios contribuyó a identificar áreas insuficientemente exploradas y preguntas de investigación no resueltas, guiando el enfoque de nuestra investigación hacia contribuciones significativas al cuerpo de conocimiento existente.

Este riguroso proceso de revisión de la literatura no solo subraya la importancia de utilizar técnicas sistemáticas y bases de datos académicas adecuadas, (Svarre & Russell-Rose, 2025) sino que también resalta la necesidad de fortalecer la capacitación metodológica y el desarrollo de habilidades en la búsqueda y evaluación de literatura académica relevante.

En la figura 4 se detallan los pasos seguidos para la revisión sistémica de la literatura.

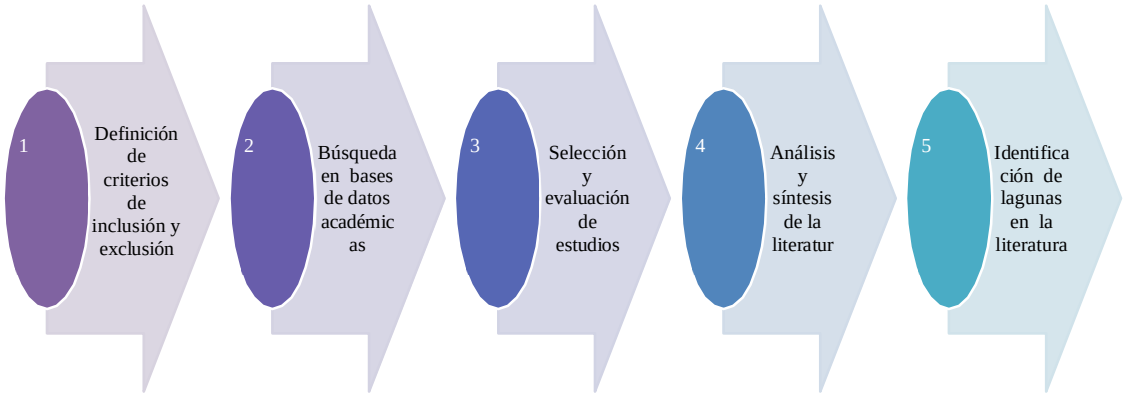



**Figura 4.** *Metodología de la Revisión Sistémica*

*Nota: Adaptado de la revisión sistemática de literatura (Mera Macías et al., 2020)*

### *2.2.3 Identificación de Literatura Relevante*

La identificación de literatura relevante es un paso esencial en el proceso de revisión de la literatura, donde el objetivo es recopilar estudios previos que proporcionen una base sólida para el análisis y desarrollo del tema de investigación. Este proceso implica una serie de estrategias meticulosas para garantizar que se capturen todas las contribuciones significativas relacionadas con la arquitectura de seguridad para la continuidad de los servicios web en el sector de la salud.

### *2.2.4 Estrategias de Búsqueda*

La estrategia de búsqueda se diseñó para abarcar una amplia gama de bases de datos académicas y científicas, incluyendo PubMed, IEEE Xplore, Scopus, y Google Scholar. Se utilizaron combinaciones de palabras clave específicas como "arquitectura de seguridad", "continuidad de servicios web", "servicios de salud en línea", y "normativas de seguridad informática en salud". Esta búsqueda se limitó casi en su mayoría a trabajos publicados en los últimos cinco años para asegurar la relevancia y actualidad de la información.

### *2.2.5 Criterios de Inclusión y Exclusión*

Se establecieron criterios de inclusión y exclusión claros para filtrar la literatura.

Se incluyeron estudios que:

- Estuvieran publicados en revistas académicas peer-reviewed.
- Abordaran directamente los temas de arquitectura de seguridad, continuidad de servicios web y su aplicación en el contexto de la salud.
- Presentaran metodologías claras y resultados verificables.
- Se excluyeron los estudios que:
- No estuvieran relacionados directamente con el ámbito de la seguridad informática en servicios de salud.
- Fueran publicaciones no académicas como blogs, opiniones, y notas de prensa.

### *2.2.6 Análisis y Selección*

Cada fuente identificada fue sometida a un análisis preliminar basado en su título y resumen para determinar su relevancia. Los trabajos seleccionados en esta fase inicial fueron luego examinados en detalle, evaluando su metodología, resultados, y contribuciones al campo de estudio. Este enfoque permitió consolidar una colección de fuentes pertinentes que apoyan y enriquecen el marco teórico de nuestra investigación.

### *2.2.7 Síntesis de la Literatura*

La síntesis de la literatura relevante identificada se centró en extraer y comparar los hallazgos clave, las teorías aplicadas, y las conclusiones de cada estudio. Esta síntesis proporciona una visión comprensiva de los avances actuales en la arquitectura de seguridad para servicios web en la salud, destacando tanto logros como desafíos pendientes.

Este meticuloso proceso de identificación y análisis de la literatura relevante no solo subraya la profundidad y alcance de la investigación actual en el campo, sino que también establece un sólido punto de partida para nuestro estudio

En la figura 5 podemos apreciar los pasos realizados para la identificación de la literatura relevante.

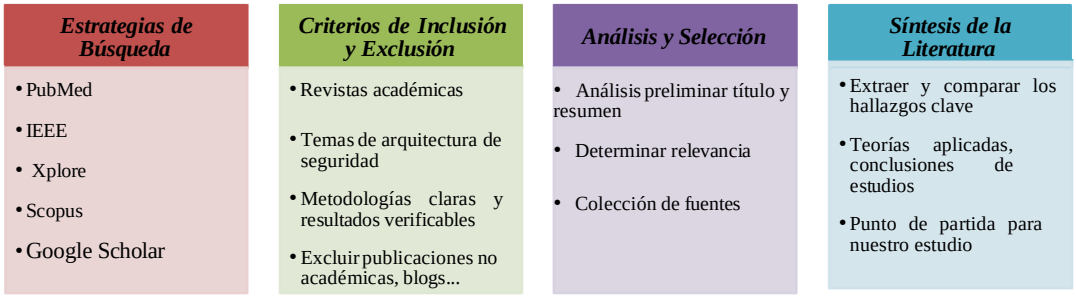



**Figura 5.** *Identificación de literatura relevante*

### *2.2.8 Unidad de análisis*

La unidad de análisis se enfoca en examinar las arquitecturas de seguridad de la información implementadas en los sitios web, con particularidad en las organizaciones de salud y su impacto. Se evaluará si estas arquitecturas cumplen con las normativas y estándares actuales de seguridad de la información, poniendo énfasis en su capacidad para proteger datos sensibles y asegurar la continuidad de los servicios.

De la unidad de análisis planteada, se desprenden las siguientes preguntas de investigación que se muestra a continuación.

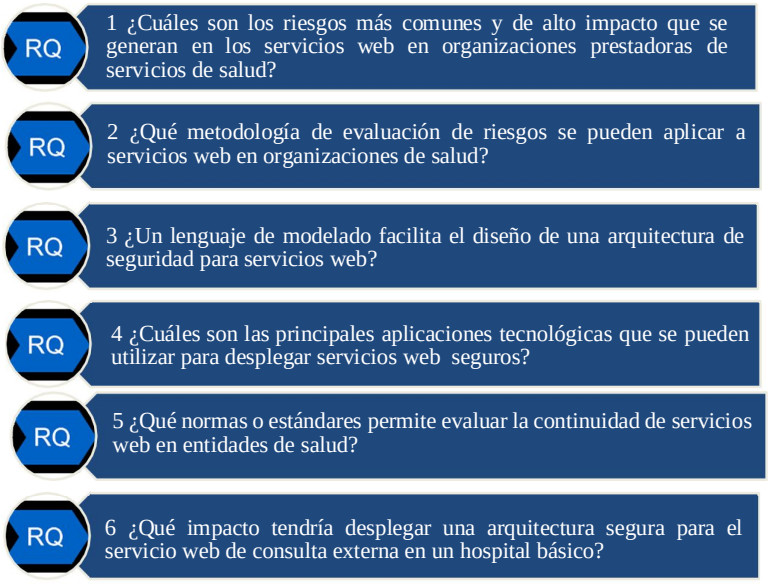


**Figura 6.** *Preguntas de Investigación*

*Nota: Elaboración propia*

### *2.2.9 Cadena de búsqueda*

En la investigación de arquitecturas de seguridad para la continuidad de servicios web en salud, la cadena de búsqueda es vital para capturar la literatura más pertinente y actual. Se estableció una estrategia de búsqueda exhaustiva en múltiples bases de datos académicas, orientada a encontrar estudios que abordan las arquitecturas de seguridad, los estándares de protección de datos y las mejores prácticas en el contexto de los servicios web de atención de salud, misma que se representa en la siguiente tabla.

**Tabla 3.**

*Cadena de búsqueda*

| Criterio | Scopus | PubMed | Google Scholar |
|---|---|---|---|
| **Cadena de búsqueda** | "seguridad de la información" AND ("salud electrónica" OR "estándares de seguridad") | ("protección de datos en salud" AND "infraestructura de seguridad en salud") OR "regulaciones de salud" | ("arquitectura de seguridad en servicios de salud" AND "protocolos de cifrado") AND "cumplimiento normativo en salud" |
| **SUBTOTAL** | 130 | 115 | 265 |
| **TOTAL 510** | | | |

*Nota. Obtenido de Scopus, PubMed, Google Scholar*

La búsqueda se centró en su mayoría en documentos publicados en los últimos cinco años para garantizar la relevancia y actualidad de la información. Los términos de búsqueda se seleccionaron cuidadosamente para abarcar tanto aspectos técnicos como normativos de la seguridad en el ámbito sanitario. Esta metodología asegura una cobertura integral de la literatura disponible.

### *2.2.10 Búsqueda de documentos*

En la investigación de arquitecturas de seguridad para servicios web de salud, se ejecutó una búsqueda documental siguiendo un protocolo sistemático para identificar fuentes pertinentes y de alta calidad. Este proceso se llevó a cabo en reconocidas bases de datos académicas y se documentó cuidadosamente para garantizar la trazabilidad y la replicabilidad de los resultados.

### *2.2.11 Procedimiento y Resultados*

Se efectuó una búsqueda detallada con palabras clave específicas relacionadas con la seguridad de la información y los servicios web en el ámbito de la salud, utilizando las siguientes bases de datos.

**Tabla 4.**

*Búsqueda de documentos*

| Base de Datos | Criterio de Búsqueda | Número de Documentos Iniciales | Documentos después de Filtro Temporal | Documentos Seleccionados |
|---|---|---|---|---|
| **Google Scholar** | "arquitectura de seguridad en servicios de salud" | 500 | 320 | 150 |
| **Redalyc** | "seguridad de datos y salud electrónica" | 200 | 120 | 60 |
| **Scopus** | "estándares de seguridad en servicios web de salud" | 300 | 180 | 90 |

*Nota. Se considera un total documentos seleccionados: 300*

Se aplicaron filtros de selección para limitar los resultados a publicaciones de los últimos cinco años, con el objetivo de concentrarse en la evolución reciente y las tendencias actuales en el dominio de la seguridad en servicios de salud. Los documentos fueron evaluados en base a su relevancia, rigor metodológico y contribución al tema de investigación.

### *2.2.12 Evaluación y Síntesis*

La evaluación de los documentos seleccionados permitió sintetizar la información más relevante, destacando los desarrollos en el diseño e implementación de arquitecturas de seguridad, así como las normativas que rigen la protección de datos en entornos de salud electrónica. Esta síntesis informa directamente al desarrollo del marco teórico y las metodologías propuestas en este estudio.

La búsqueda de documentos es una etapa fundamental en la investigación que asegura una base de conocimiento sólida y actualizada para abordar las preguntas de investigación planteadas y cumple con las prácticas recomendadas en la investigación académica.

### *2.2.13 Selección de artículos*

Para la selección de artículos se siguió un proceso estructurado en tres fases:

En la primera fase, se aplicaron criterios de inclusión y exclusión para filtrar la literatura inicialmente identificada. Se consideraron documentos que contenían términos clave relacionados con la arquitectura de seguridad en servicios web de atención de salud, protocolos de seguridad, normativas relevantes y estudios publicados.

La segunda fase consistió en seleccionar artículos con base en su relevancia para el problema y su aporte previsto al estudio, tras revisar títulos con resúmenes con palabras clave para ordenarlos según pertinencia hacia el marco teórico con las preguntas de investigación mediante un registro sistemático de inclusión con prioridad para fuentes con cobertura conceptual suficiente verificable. En la etapa final se efectuó una lectura crítica de texto completo con énfasis en metodología con análisis de resultados con recomendaciones, se priorizaron trabajos que profundizan en el diseño con implementación de arquitecturas de seguridad en entornos de atención en salud y la figura 5 ilustra el flujo seguido desde el cribado inicial hasta la síntesis integradora con criterios de calidad utilizados.

**Tabla 5.**

*Fases selección artículos*

| Base de Datos | Fase I | Fase II | Fase III |
|---|---|---|---|
| Redalyc | 80 | 20 | 7 |
| Scopus | 120 | 22 | 7 |
| Google Scholar | 100 | 30 | 14 |
| Total | 300 | 72 | 23 |

*Nota. Obtenido de (Redalyc), (Scopus) y (Google Scholar)*

**Tabla 6.**

*Artículos seleccionados*

| Código | Título | Autor(es) | Información relevante |
|---|---|---|---|
| **A1** | Metodología para detectar riesgos en seguridad informática en la universidad autónoma de Zacatecas basada en pruebas de penetración | Pedro Morales González, Sodel Vázquez Reyes, Santiago Villagrana Barraza, Perla Elizondo, C. H. C. Ramírez, A. González (2022) | Vulnerabilidades en la Universidad Autónoma de Zacatecas identificadas mediante pruebas de penetración. |

| | | | |
|---|---|---|---|
| **A2** | Pruebas de penetración para la seguridad informática al servidor web del laboratorio de ciberseguridad en la Universidad Politécnica Estatal del Carchi, 2021 | Álvaro Steebe Castillo Enríquez, Jairo Vladimir Hidalgo Guijarro, Carlitos Alberto Guano Cárdenas (2022) | Diagnóstico de vulnerabilidades en servidores web y su impacto en la seguridad. |
| **A3** | Estructuración de un sistema de información geoespacial para el análisis de datos de seguridad alimentaria, intervenciones nutricionales y de salud humana en Panamá | Kevin González Ortega, Eliecer Aguilar, Ana Gabriela Aizprúa, E. Cedeño, Javier E. Sanchez-Galan (2023) | Uso de información geoespacial para el análisis de seguridad alimentaria y salud en Panamá. |
| **A4** | Ética y seguridad informática en el sector de la salud pública en el siglo XXI | E. Bernita, Carolina Paladines Zapata, Cecil H. Flores Balseca (2017) | Aspectos éticos y de seguridad informática en la salud pública. |
| **A5** | Proceso de control de la gestión de Seguridad y Medio Ambiente mediante la aplicación de un sistema web | Nadia Violeta Alonzo Gomero, Daniel Lovera Dávila (2022) | Implementación de un sistema de gestión de seguridad y salud en el trabajo vía web. |
| **A6** | Desarrollo de un aplicativo web para la administración de las historias clínicas de salud ocupacional DE Mobile System E. U. | Gregorio Andres Velasquez Moreno, Jose James Parra Duran (2020) | Creación de un aplicativo web para la gestión de historias clínicas en salud ocupacional. |
| **A7** | Descripción de la implantación y grado de desarrollo de tecnología de comunicación e informática de los equipos de Atención Primaria en los servicios autonómicos de salud en España | Laura Carbajo Martín, Remedios Martín Álvarez, María Pilar Astier Peña, R. Rotaeche del Campo, Jorge Navarro Pérez, Ignacio Párraga Martínez (2021) | Evaluación de la tecnología de comunicación e informática en Atención Primaria en España. |
| **A8** | Sistema de gestión de seguridad y salud ocupacional para las aulas y laboratorios de la Facultad de Ingeniería y Arquitectura de la Universidad de El Salvador basado en la norma OHSAS 18001 | Heraldo Yaider Espinoza, Emilio Alexander Hernández Bernal, Rocío Aminta Huezo Delgado (2016) | Implementación de un sistema de gestión de seguridad y salud ocupacional en la Universidad de El Salvador. |
| **A9** | Estrategia informática con arquitectura MVC y Responsive Web Design en la gestión de datos de los pacientes del hospital maternidad Babahoyo en el área de estadística | E. León, Á. Rafael (2016) | Aplicación de MVC y diseño web responsivo en la gestión de datos de pacientes. |

| | | | |
|---|---|---|---|
| **A10** | Análisis de técnicas de Machine Learning aplicadas a la ciberseguridad informática para mejorar la detección de intrusiones y comportamientos anómalos en la Web | William Ruiz Martínez (2021) | Uso de Machine Learning en la mejora de la detección de intrusiones y comportamientos anómalos en la web. |
| **A11** | Plan de seguridad informática del departamento de tecnologías de la información y comunicación de la Universidad Técnica de Babahoyo para mejorar la gestión en la confidencialidad e integridad de la información | Mejía Viteri, José Teodoro (2015) | Importancia de la seguridad informática en la gestión de la confidencialidad e integridad de la información universitaria. |
| **A12** | Desarrollo de un esquema de seguridad y un firewall de borde para el sistema web de una empresa de salud | Cueva Delgado, H. Eduardo (2015) | Implementación de medidas de seguridad avanzadas para proteger la información de una empresa de medicina pre-pagada. |
| **A13** | Prototipo de Sistema de Información Web Aplicando Desarrollo Guiado por Pruebas del Sistema de Gestión de la Seguridad y Salud en el Trabajo en Empresas de Producción: Caso de Estudio Munkys SAS | D. M. Vega (2018) | Desarrollo de un prototipo web para la gestión de la seguridad y salud en el trabajo, aplicando TDD. |

| | | | |
|---|---|---|---|
| **A14** | Auditoría informática a la parte física y lógica de la red de datos en la empresa solidaria de salud Emssanar E.S.S. sedes corporativa Pasto y sedes alto Putumayo | Diego Acosta, Heider Quetama (2015) | Evaluación de la seguridad en la red de datos de Emssanar E.S.S. para identificar falencias. |
| **A15** | Síndrome de burnout en los profesionales de salud: revisión sistemática | Geannella Carolina Ávila Agreda, Andrés Alexis Ramírez Coronel, Isabel Cristina Mesa Cano, Karina de Lourdes Serrano Paredes (2021) | Impacto del agotamiento profesional en el sector salud y su relación con la calidad del servicio. |
| **A16** | Auditoría informática de la seguridad de la red física y lógica para el departamento de gestión informática y sistemas de la dirección provincial de salud de Pichincha (DPSP) | S. Calle, Emilly Jeanett Guanotuña Lascano (2010) | Implementación de medidas de seguridad en la gestión informática de la salud pública. |
| **A17** | Aplicación de los árboles de decisión en la identificación de sitios web fraudulentos | Christian Layme Fernández, José Manuel Suri Canaza, David Jose Peña Ugarte, Jhon Yoset Luna Quispe (2022) | Uso de Machine Learning para mejorar la seguridad informática en la web. |
| **A18** | Prevención de riesgos laborales: Seguridad y salud en la construcción | José Manuel Ros Gilabert, Lucía Blanco Bartolomé (2019) | Estrategias y prácticas para mejorar la seguridad y salud en el sector de la construcción. |
| **A19** | Reingeniería de sistema web para pacientes del hospital Naval Guayaquil utilizando arquitectura de cuatro capas, con sistema de autenticación único, e implementación de servidor web de aplicaciones | C. Arce, Cristhian Fabián (2016) | Mejora de los servicios de atención en el Hospital Naval Guayaquil mediante la reingeniería de sus sistemas web. |
| **A20** | Desarrollo de un esquema de seguridad y un firewall de borde para el sistema web de una empresa de salud | Cueva Delgado, H. Eduardo (2015) | Implementación de medidas de seguridad avanzadas para proteger la información de una empresa de salud. |
| **A21** | Prototipo de Sistema de Información Web Aplicando Desarrollo Guiado por Pruebas del Sistema de Gestión de la Seguridad y Salud en el Trabajo en Empresas de Producción: Caso de Estudio Munkys SAS | D. M. Vega (2018) | Desarrollo de un prototipo web para la gestión de la seguridad y salud en el trabajo, aplicando TDD. |

| | | | |
|---|---|---|---|
| **A22** | Plan institucional de adecuación a los estándares de calidad: acreditación basada en el modelo centrado en el estudiante de carreras de ingeniería e informática | Cristina Liliam Greiner, María Viviana Godoy Guglielmone (2023) | Estrategias para la adecuación de planes de estudio a estándares de calidad en ingeniería e informática. |
| **A23** | Auditoría informática a la parte física y lógica de la red de datos en la empresa solidaria de salud Emssanar E.S.S. sedes corporativa Pasto y sedes alto Putumayo | Diego Acosta, Heider Quetama (2015) | Evaluación de la seguridad en la red de datos de Emssanar E.S.S. para identificar falencias. |

*Nota. Descripción y análisis a partir de las fuentes de Redalyc, Scopus y Google Scholar*

### *2.2.14 Extracción de datos relevantes*

Tras la selección de artículos, se procedió a la extracción de datos relevantes para construir una base de conocimiento especializado en arquitecturas de seguridad para servicios web de atención de salud. Esta información se organizó en una matriz de conceptos para ilustrar cómo cada artículo contribuye a los diferentes temas relacionados con la seguridad informática en la salud.

### *2.2.15 Matriz de conceptos*

La matriz categoriza los conceptos clave relacionados con la seguridad en servicios web de atención de salud extraídos de los artículos seleccionados:

| Código | Seguridad en Servicios Web | Protocolos de Seguridad | Normativas Relevantes | Impacto de la Seguridad Informática | Metodologías de Implementación | Evaluación y Análisis de Resultados |
|---|---|---|---|---|---|---|
| **A1** | X | | | X | | |
| **A2** | X | X | | | | X |
| **A3** | | X | | | X | |
| **A4** | | | X | | | X |
| **A5** | X | | X | | X | |
| **A6** | X | | | X | | |
| **A7** | X | X | | | X | |
| **A8** | X | | | | | |
| **A9** | | X | | | | X |
| **A10** | X | | | X | | |
| **A11** | | X | | | X | |

| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **A12** | | | | | X | | | | | | X | |
| **A13** | X | | | | | | | | X | | | |
| **A14** | X | | | | | | X | | | | | |
| **A15** | | | | X | X | | | | | | | |
| **A16** | X | | | | | | | | X | | | |
| **A17** | | | | X | | | X | | | | | |
| **A18** | X | | | | | | | | | | X | |
| **A19** | | | X | | X | | | | X | | | |
| **A20** | X | | | | | | X | | | | | |
| **A21** | | | X | | | | | | X | | | |
| **A22** | X | | | | X | | | | | | | |
| **A23** | | | | | | | X | | | X | | X |

*Nota. Conceptos clave en artículos seleccionados*

Esta tabla proporciona una visión panorámica de la contribución de cada artículo a los temas centrales del proyecto de investigación. Cada 'X' marca la presencia de información relevante en ese artículo relacionada con el concepto en cuestión. La tabla está diseñada para facilitar la comparación y el análisis transversal de la información extraída y es fundamental para la síntesis de conocimiento en el desarrollo del marco teórico.

## 2.3 Marco Conceptual

El marco conceptual de una arquitectura de seguridad para servicios web de consulta externa en el contexto de la salud es una estructura comprensiva que integra los principios, las técnicas y las políticas necesarias para proteger los datos y la infraestructura. Este marco no solo abarca las tecnologías utilizadas sino también las prácticas de diseño y los estándares que aseguran que los servicios web sean robustos contra amenazas y vulnerabilidades.

### *2.3.1 Componentes de un servicio web*

Una organización que desee mantener en funcionamiento un servicio web tradicional requiere de varios componentes asociados al hardware, software y comunicaciones a fin de mantener su funcionamiento apropiado, en la figura 7 podemos sintetizar esos requerimientos básicos:

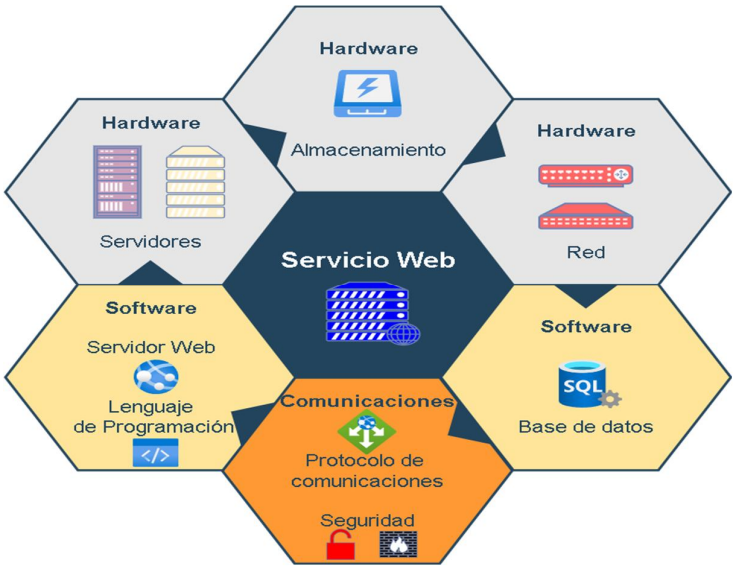



**Figura 7.** *Componentes de servicio web*

*Nota: Elaboración propia*

### *2.3.2 Hardware*

Un servicio web requiere de servidores para alojar y ejecutar aplicaciones accesibles a usuarios de forma remota, estos equipos deben ser lo suficientemente potentes para soportar las peticiones de usuarios clientes y el tráfico esperado, además de poseer la suficiente capacidad de almacenamiento para los datos recopilados (Romero, 2024).

A nivel de red se necesita de dispositivos que permita que los servidores tengan acceso a la Internet y otros componentes de infraestructura como son: Data Center, cableado estructurado, enrutadores, switches, entre otros.

En la siguiente figura se resume algunas características en cuanto a hardware que se debe considerar:

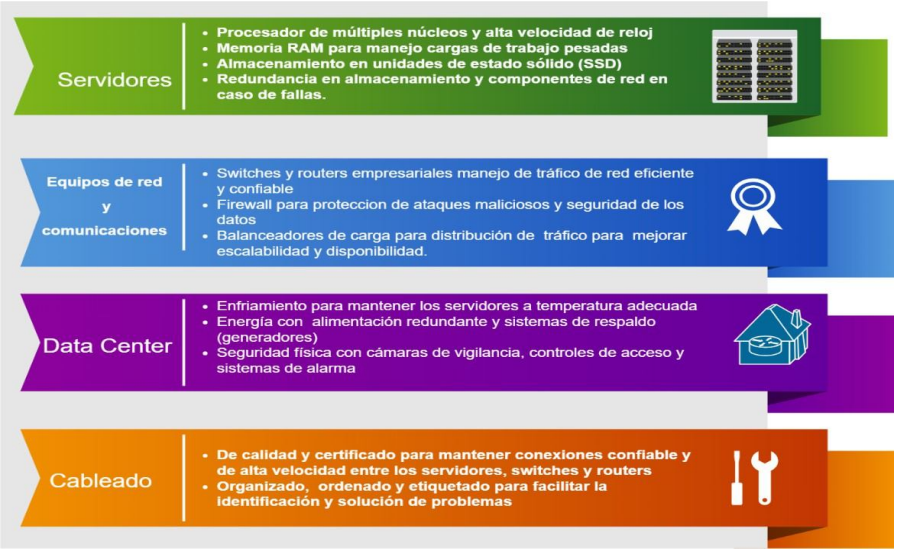



**Figura 8.** *Componentes de hardware para servicio web*

*Nota: Diseño basado en Guía de hardware de servidor: Arquitectura, productos y gestión (Moore, 2024)*

### *2.3.3 Servicios en la nube*

En la actualidad los servicios en la nube o computación en la nube, ofrecen recursos informáticos que permiten omitir el uso de equipos físicos locales, organizaciones y personas pueden acceder a servidores, almacenamiento, bases de datos, redes, software, análisis de datos y demás, a través de proveedores de estos servicios.

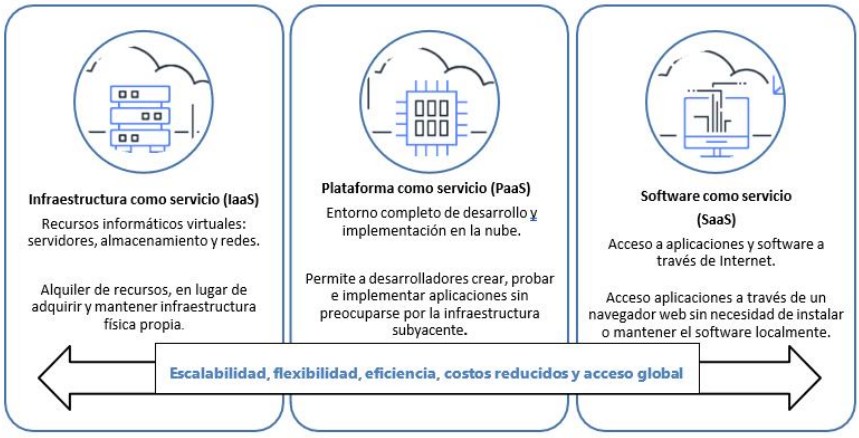



**Figura 9.** *Servicios en la nube*

*Nota. Diseño basado en informática en la nube. Ventajas y Beneficios (Amazon Web Services, Inc., s. f.)*

Los servicios en la nube han transformado radicalmente la forma en que las organizaciones, incluidas las del sector salud, almacenan, acceden y gestionan sus datos.

Relativiti ( 2023) destacan cómo la implementación de un sistema de gestión de seguridad y salud en el trabajo vía web puede beneficiarse enormemente de la infraestructura y flexibilidad que ofrecen los servicios en la nube. Esta adaptabilidad se traduce en una mayor eficiencia en la gestión de riesgos y en la implementación de medidas preventivas, esenciales en el ámbito de la salud.

Por otro lado, Nagua & Andrés (2020) ilustra la importancia de los servicios en la nube para el desarrollo de prototipos de sistemas de información web, especialmente en el contexto de la gestión de la seguridad y salud en el trabajo

Los servicios en la nube aportan escalabilidad con elasticidad con eficiencia de costos para la gestión de aplicaciones de salud pues permiten ajustar recursos según la demanda con provisión rápida de cómputo y almacenamiento con integración de equipos a distancia todo dentro de marcos de seguridad con cumplimiento normativo que sostienen trazabilidad de accesos con cifrado en tránsito con resguardo de copias. Su adopción habilita una administración más dinámica de recursos con respuesta oportuna ante incidencias de seguridad y eventos operativos, mejora la continuidad del servicio con calidad constante en redes hospitalarias mediante planes de contingencia probados con recuperación ante desastres que preservan la confidencialidad de datos clínicos sensibles mediante controles de acceso con monitoreo continuo que reducen riesgos mientras fortalecen la experiencia del paciente.

### *2.3.4 Software*

En su definición más básica el diccionario de la lengua española define al software como “el conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora” (RAE- ASALE, s. f.) ampliando esa definición podemos agregar que si estos están diseñados con la finalidad de facilitar tareas específicas o ayudan a resolver necesidades concretas se consideran como software de aplicación.

Los softwares de aplicación sostienen la prestación de consulta externa en salud, como muestra Ortega 2023 al destacar una metodología para identificar riesgos de seguridad informática con análisis de vulnerabilidades en entornos universitarios que puede extrapolarse a clínicas y hospitales donde la protección de datos de pacientes con continuidad operativa requiere procesos de evaluación integrados desde el diseño inicial. En la misma línea, González 2022 subraya el valor de las pruebas de penetración para resguardar la integridad de servidores web en arquitecturas clínicas, con detección de fallas que previene brechas de datos mientras incorporar estas pruebas junto con otras técnicas de evaluación durante el desarrollo produce

aplicaciones más seguras que reducen incidentes de seguridad e incrementan la confianza del usuario.

Se puede resumir que las pruebas de penetración y la evaluación de riesgos no son solo pasos aislados sino partes integrales de un proceso continuo de mejora de la seguridad, lo que refleja la naturaleza dinámica de la ciberseguridad y la necesidad de adaptarse a nuevas amenazas y vulnerabilidades.

#### 2.3.4.1 Clasificación del software de aplicación

Clasificar el software resulta clave para definir capas de seguridad en servicios web de salud porque orienta qué controles aplicar en cada módulo y qué niveles de disponibilidad exigir con base en riesgos priorizados, Soto 2024 aporta un aplicativo para historias clínicas de salud ocupacional que subraya categorías con requerimientos altos de confidencialidad con continuidad operativa bajo respaldo controlado. González Ortega et al. 2023 estudian sistemas geoespaciales aplicados a seguridad alimentaria con salud y muestran que la clasificación debe considerar función junto con capacidad para manejar datos complejos y sensibles, así el software que trata datos personales de salud requiere resguardos criptográficos con control de acceso más registro de actividad más pruebas de penetración superiores a los de aplicaciones generales.

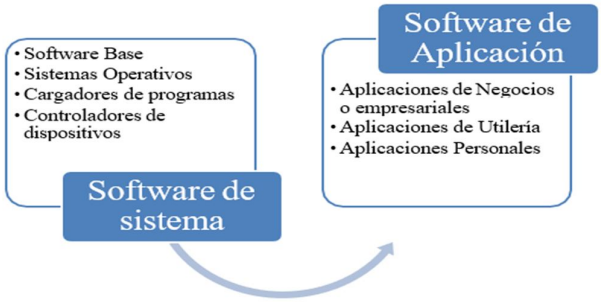



**Figura 10.** *Clasificación de software de sistema y aplicación*

*Nota: Diseño basado en Olarte Gervacio, L*

Como conclusión de los referidos autores sobre el tema, se destaca que en el contexto de la atención de salud, donde el manejo de información sensible es la norma, una clasificación precisa es un paso fundamental para garantizar la protección de los datos y la confianza de los usuarios en los servicios de salud proporcionados.

### *2.3.5 Aplicaciones web*

Una aplicación web es un tipo de software que se ejecuta en los navegadores web, donde las organizaciones necesitan intercambiar información y proporcionar servicios de forma remota, estas van desde sitios de comercio electrónico, mensajería instantánea, redes sociales, gestión documental, banca en línea, software hospitalario, entre otras, que permiten acceder a funcionalidades complejas sin la necesidad de instalar o configurar un software en equipos de escritorio o dispositivos móviles.

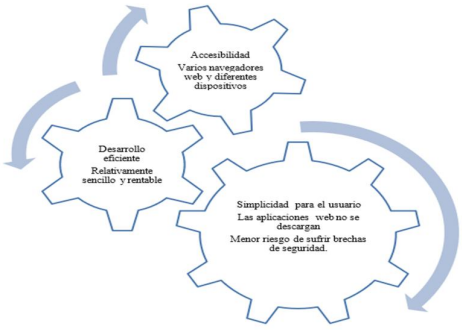



**Figura 11.** *Beneficios de las aplicaciones web*

*Nota: Diseño basado AWS Web-application*

Las aplicaciones web en el sector salud constituyen una herramienta fundamental para la prestación eficiente y accesible de servicios médicos, (Castillo Enríquez, 2021), enfatizan la necesidad de adoptar arquitecturas web flexibles y adaptativas como MVC (Model-View-Controller) y diseños web responsivos para la gestión de datos de los pacientes. Esto no solo mejora la experiencia del usuario, sino que también asegura que la información crítica sea presentada y gestionada de manera efectiva y segura en diversos dispositivos, un factor cada vez más relevante en la era del acceso móvil, la correcta implementación de aplicaciones web debe seguir una serie de protocolos de seguridad rigurosos y adaptarse a las necesidades cambiantes de los profesionales y pacientes.

Se concluye que, las aplicaciones web en el contexto de la salud deben ser diseñadas y auditadas con un enfoque multidimensional que abarque tanto la usabilidad como la seguridad, la implementación de arquitecturas y diseños flexibles, junto con auditorías informáticas regulares, es esencial para asegurar la integridad, la confidencialidad y la disponibilidad de la información de salud en la prestación de servicios médicos.

### *2.3.6 Tipos de aplicaciones web*

A continuación, se presentan los tipos de aplicaciones web:

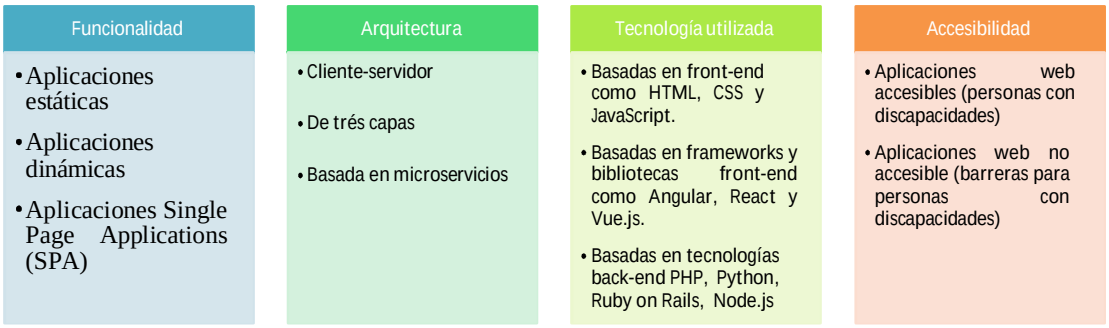



**Figura 12.** *Tipos de aplicaciones web*

*Nota: Diseño basado en explicación de aplicaciones web (Amazon Web Services Inc., s. f.)*

En la era digital actual, las aplicaciones web desempeñan un papel muy importante en el acceso a servicios y la gestión de información, especialmente en el ámbito de la salud. Velasquez Moreno & Parra Duran, (2020) explora cómo las técnicas de Machine Learning se aplican en la ciberseguridad para mejorar la detección de intrusiones y comportamientos anómalos en la web, destacando la importancia de las aplicaciones web dinámicas y su capacidad para aprender y adaptarse a nuevas amenazas. Esta adaptabilidad es esencial para las aplicaciones que manejan datos sensibles, como los relacionados con la salud.

Los árboles de decisión aplicados a la detección de sitios fraudulentos muestran la diversidad funcional del desarrollo web orientado a seguridad en salud, pues integran ingestión de señales con evaluación automatizada para reconocer patrones maliciosos y bloquear vectores de ataque con rapidez con registros de entrenamiento auditables más umbrales de decisión ajustados a indicadores de riesgo del sector. De ese marco emergen dos familias de aplicaciones clave para ecosistemas clínicos seguros y eficientes: dinámicas que interactúan con el usuario mediante adaptación de interfaz, junto con analíticas que procesan volúmenes extensos para extraer patrones con alertas tempranas que sostienen continuidad operativa con resguardo de datos clínicos sensibles bajo gobernanza clara de roles con métricas de desempeño más planes de continuidad probados.

Esta revisión resalta que la evolución y diversificación de las aplicaciones web en la atención de la salud requieren un enfoque de seguridad informática robusto y adaptable. La integración de técnicas avanzadas de Machine Learning y análisis de datos en estas aplicaciones no solo mejora la seguridad, sino que también potencia la eficiencia y efectividad de los servicios de salud digitales.

### *2.3.7 Servidores Web*

El uso de servidores web bajo software libre ocupa un alto porcentaje de participación en el mercado, en la encuesta de julio de 2024 de netcraft.com podemos observar 12.891.416 computadoras se encuentran orientadas a la web, en donde Apache mantiene una importante participación.

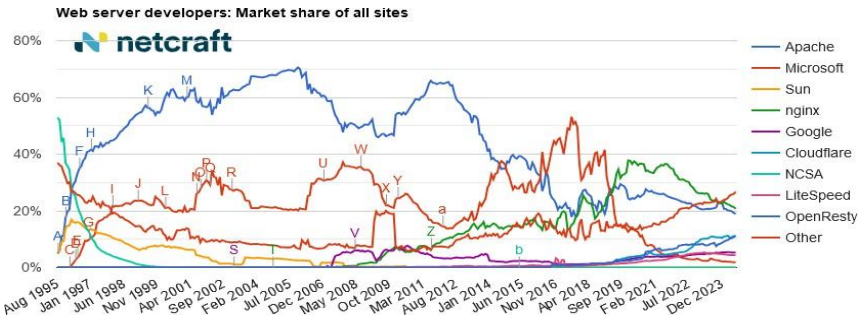



**Figura 13.** *Servidores web más usados*

*Nota: Tomado de encuesta sobre servidores web Julio de 2024 (Netcraft, 2024)*

La importancia de los servidores web en la arquitectura de seguridad para servicios de consulta externa en el sector salud es indiscutible. Carreño Arce, (2016) subraya cómo el desarrollo de un esquema de seguridad y un firewall de borde para el sistema web de una empresa de salud no solo mejora la protección de la información sensible, sino que también fortalece la infraestructura contra ataques externos. Esta medida es esencial en un entorno donde la integridad y la disponibilidad de los datos de salud son críticas para la operación continua de los servicios de salud.

España León (2016) muestran, a partir de un sistema de gestión de seguridad y salud ocupacional implementado en la Universidad de El Salvador, que un servidor web puede administrar datos junto con protocolos de protección dentro de una institución educativa con prácticas transferibles al sector salud que fortalecen la prevención de riesgos mediante reglas claras de acceso con registros auditables con procesos trazables. En la consulta externa el servidor web opera como punto de conexión entre usuarios y servicios con manejo seguro de solicitudes, por ello la configuración correcta con protección perimetral con endurecimiento del servidor resulta esencial para resguardar datos clínicos mediante firewalls con detección de intrusiones con protocolos cifrados bajo políticas de mínimo acceso con monitoreo continuo que mantienen cumplimiento con disponibilidad.

Esta revisión de la literatura permite establecer que los servidores web son una componente crítica en la arquitectura de seguridad de los servicios de salud en línea. La correcta

configuración y protección de estos servidores asegura la integridad, confidencialidad y disponibilidad de los datos de salud, facilitando la prestación segura y eficiente de servicios de consulta externa. Los estudios de Carreño Arce, (2016) y España León (2016) ilustran la importancia de una infraestructura web robusta y segura, resaltando la necesidad de adoptar enfoques proactivos y bien informados en la seguridad de los servidores web.

### *2.3.8 Comunicaciones*

#### 2.3.8.1 Protocolo HTTP y HTTPS

Sustituir el Protocolo de Transferencia de Hipertexto por su versión cifrada HTTPS constituye un avance clave para resguardar la comunicación en aplicaciones web críticas del sector salud, porque cifra el canal entre cliente y servidor con validación de identidad mediante certificados que reducen la exposición a ataques de intermediario con aumento de fiabilidad de los intercambios clínicos según la evaluación tecnológica reportada por Vega 2018 en Atención Primaria. El uso de HTTPS protege datos sensibles como historias clínicas frente a interceptación o manipulación por terceros no autorizados, ya que combina integridad del mensaje con confidencialidad extremo a extremo mediante suites criptográficas con control de claves que habilitan auditoría de accesos con registros fiables para sostener cumplimiento normativo en entornos distribuidos de consulta externa y telemedicina.

Arce y Fabián (2016) muestran a partir de la implementación de protocolos en el Hospital Naval Guayaquil que la reestructuración del sistema web con adopción de HTTPS mejora la prestación de atención al habilitar un canal cifrado que resguarda datos clínicos frente a interceptación con integridad con control de claves con disponibilidad en consultas externas con trazabilidad de accesos. Esa evidencia respalda que fortalecer la configuración del servidor con firewalls con detección de intrusiones con protocolos seguros incrementa la confianza en los servicios en línea de la institución con efectos sobre bienestar del paciente al reducir riesgos de exposición de información sensible, por lo cual el uso de HTTPS se asume como medida central en la gobernanza de seguridad aplicada a plataformas clínicas.

El protocolo HTTPS basado en SSL/TLS cifra la comunicación entre cliente y servidor con verificación de autenticidad del sitio, lo cual resulta vital para impedir ataques de intermediario junto a fraudes de suplantación en entornos de salud electrónica porque protege credenciales clínicas con formularios de acceso con transferencias de archivos sensibles bajo control criptográfico que dificulta la manipulación del tráfico así bloquea lecturas no autorizadas. Los hallazgos descritos por Carreño Arce (2016) sobre su aplicación en salud

muestran que una infraestructura web con certificados válidos con configuración robusta con monitoreo eleva la confianza del usuario, por ello la adopción de HTTPS en aplicaciones clínicas es un paso crítico para resguardar información del paciente y preservar la confidencialidad con la integridad de los datos bajo procedimientos auditables.

La siguiente figura muestra las diferencias entre las diferencias entre HTTP y HTTPS

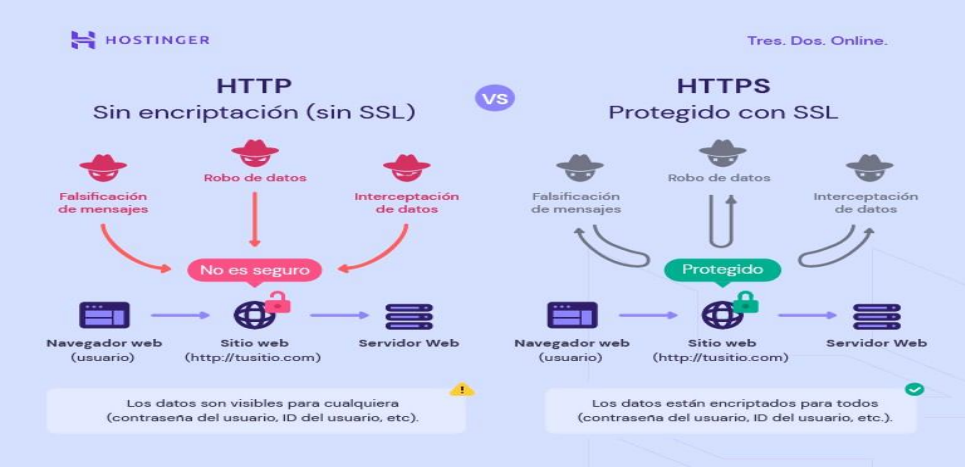



**Figura 14.** *Protocolo http vs https*

*Nota: Diferencias entre protocolo http y https, tomado de Hostinger (J, 2025)*

### *2.3.9 Certificados SSL/TLS*

La implementación de certificados SSL/TLS es fundamental en el aseguramiento de la seguridad en aplicaciones web, especialmente en el dominio de la salud donde la privacidad y la protección de datos son críticas. (Sheffer et al., 2022)destacan la relevancia de estos certificados en la auditoría informática realizada a la red de datos de Emssanar E.S.S., enfatizando cómo el uso de SSL/TLS mejora significativamente la seguridad de la información al cifrar la comunicación entre el cliente y el servidor. Esto no solo previene la interceptación y lectura de los datos transmitidos por entidades no autorizadas, sino que también asegura la autenticidad de la fuente de la información, un aspecto crucial en la transmisión de datos sensibles de salud.

La adopción de SSL/TLS en los servidores web es un estándar de seguridad reconocido que protege la transferencia de información confidencial, incluyendo detalles financieros y registros médicos de los pacientes. La encriptación que proporciona SSL/TLS es vital para cumplir con regulaciones de protección de datos como HIPAA y GDPR, las cuales imponen estrictos requisitos de seguridad para el manejo de información personal y de salud.

Se concluye en base a esta revisión que los certificados SSL/TLS es un componente

importante en la seguridad y eficacia de las aplicaciones web en el sector de la salud. La implementación adecuada de SSL/TLS garantiza la seguridad de la comunicación.

### *2.3.10 Métricas Web*

Las métricas web son cruciales para evaluar y mejorar la eficiencia, usabilidad y seguridad de los servicios web en el sector salud. Estas métricas permiten identificar áreas de mejora, optimizar la funcionalidad y garantizar la protección de los datos sensibles de los pacientes.

#### 2.3.10.1 Funcionalidad

La funcionalidad en los servicios web se refiere a la capacidad de un sitio web para cumplir con sus objetivos y proporcionar las características y servicios esperados. En el contexto de la salud, esto incluye la disponibilidad y el correcto funcionamiento de sistemas para la gestión de historias clínicas electrónicas, la programación de citas y la comunicación entre pacientes y profesionales de la salud.

Un estudio de Ștefan et al., (2024) destaca la importancia de las métricas de funcionalidad, como la tasa de éxito de las transacciones y la capacidad de respuesta del sistema, para asegurar que los servicios web cumplan con las expectativas de los usuarios y mantengan la eficiencia operativa

#### 2.3.10.2 Usabilidad

La usabilidad mide la facilidad con la que los usuarios pueden navegar y utilizar un sitio web. En el ámbito sanitario, es esencial que las plataformas sean intuitivas y accesibles para personas de diversas edades y habilidades técnicas. Las métricas de usabilidad incluyen la tasa de error del usuario, el tiempo necesario para completar tareas específicas y la satisfacción del usuario.

Según un estudio de Ștefan et al., (2024), la usabilidad es fundamental para mejorar la experiencia del paciente y aumentar la adopción de tecnologías de salud digital. Las evaluaciones de usabilidad ayudan a identificar barreras y a diseñar interfaces más amigables.

#### 2.3.10.3 Seguridad

La seguridad es una preocupación primordial en los servicios web de salud debido a la naturaleza sensible de los datos tratados. Las métricas de seguridad se centran en la capacidad de un sistema para proteger la información contra accesos no autorizados y ataques cibernéticos. Esto incluye la implementación de sistemas de detección de intrusiones, cifrado

de datos y medidas de autenticación robustas.

Un artículo de Tea et al., (2024) describe cómo los sistemas de detección de intrusiones (IDS) son vitales para identificar y mitigar amenazas en el entorno de la salud inteligente. La combinación de algoritmos de aprendizaje automático, como Random Forest y algoritmos genéticos, ha demostrado mejorar significativamente la detección y reducir las tasas de falsos positivos.

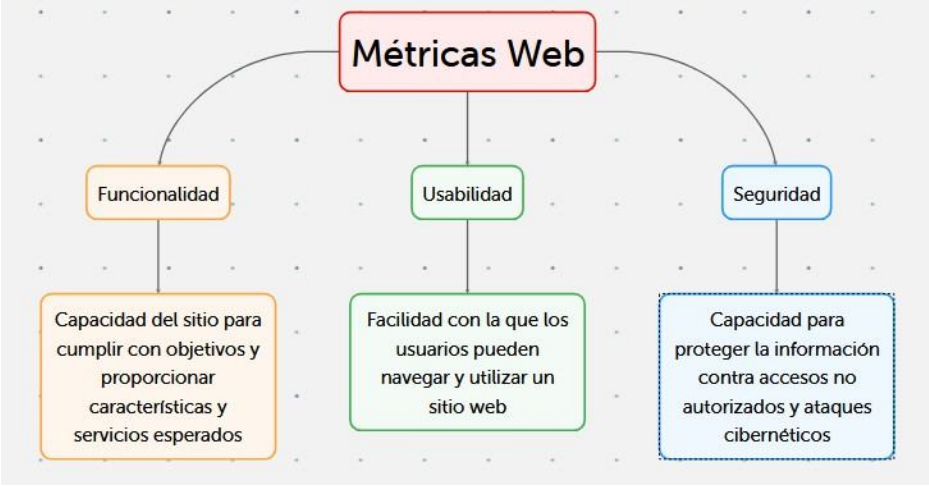



**Figura 15.** *Métricas web: funcionalidad, usabilidad, seguridad*

*Nota: Diseño propio*

### *2.3.11 Arquitectura de software y su clasificación*

La arquitectura de software juega un papel fundamental en el desarrollo de sistemas informáticos robustos y eficientes, proporcionando el marco para diseñar soluciones que satisfagan los requisitos específicos de cada proyecto. Christy et al., (2024) destacan la importancia de comprender y aplicar adecuadamente la arquitectura de software y su clasificación para mejorar la gestión de la seguridad y la integridad de la información en entornos de salud. La clasificación de la arquitectura de software en modelos como monolíticos, basados en microservicios, u orientados a servicios, entre otros, permite a los desarrolladores elegir el enfoque más adecuado para cada aplicación, teniendo en cuenta factores como la escalabilidad, la mantenibilidad y la seguridad.


**Figura 16.** *Arquitectura de software*

*Nota: Diseño propio*

En el sector de la salud, donde la fiabilidad y la protección de los datos son críticos, seleccionar la arquitectura de software adecuada es esencial para construir sistemas que no solo sean seguros y confiables, sino también capaces de adaptarse a las cambiantes necesidades y regulaciones del ámbito sanitario. Al-Sarayreh et al., (2024) enfatiza la relevancia de implementar planes de seguridad informática que se alineen con la arquitectura elegida, para la confidencialidad e integridad de la información de los pacientes.

La elección de una arquitectura de software adecuada y su clasificación son fundamentales para el éxito de cualquier sistema de información, especialmente en el sector de la salud. La comprensión profunda de las opciones disponibles permite a los desarrolladores diseñar sistemas que no solo cumplen con los requisitos funcionales, también abordan eficazmente los desafíos de seguridad.

### *2.3.12 Arquitectura de software enfocada a la ciberseguridad*

La integración de consideraciones de ciberseguridad desde las primeras etapas del diseño de la arquitectura de software es crucial para desarrollar aplicaciones web y sistemas de información seguros. Al-Sarayreh et al., (2024) examinan cómo la adopción de una arquitectura de software enfocada en la ciberseguridad puede mitigar los riesgos asociados a ataques informáticos en el sector de la construcción, un enfoque igualmente aplicable al ámbito de la salud. Esta perspectiva de diseño implica la incorporación de controles de seguridad, como la autenticación, la autorización, el cifrado de datos y la protección contra inyecciones de código, directamente en la arquitectura del sistema.

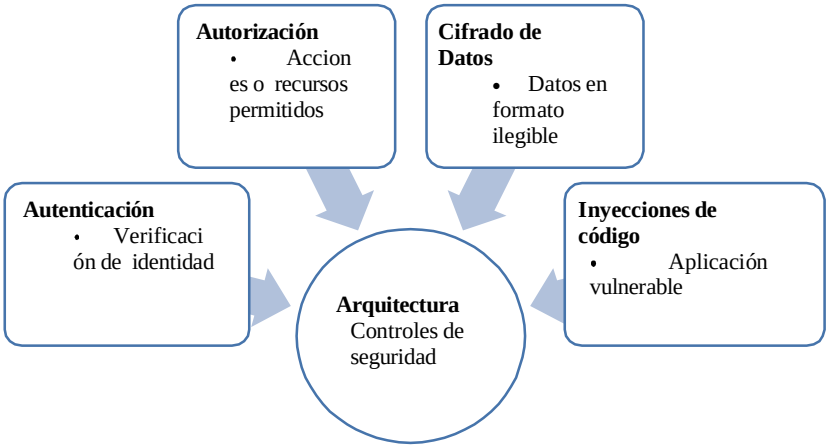



**Figura 17.** *Arquitectura de seguridad*

*Nota: Diseño propio*

La adopción de estas prácticas no solo ayuda a proteger los sistemas de posibles amenazas externas, sino que también asegura que la gestión de la seguridad sea una consideración integral en el desarrollo del software, y no simplemente una capa adicional añadida posteriormente. En el contexto de la salud, donde la seguridad de los datos del paciente es primordial, una arquitectura de software enfocada en la ciberseguridad es esencial para prevenir brechas de datos, garantizar la confidencialidad de la información y mantener la confianza de los usuarios en los servicios de salud digitales.

Integrar la ciberseguridad como un elemento fundamental de la arquitectura de software desde el inicio del proceso de desarrollo garantiza la creación de sistemas más seguros y resilientes. Esta aproximación es crítica en el sector de la salud, donde la protección de los datos del paciente y la continuidad de los servicios son de máxima importancia.

### *2.3.13 Seguridad en servicios web basados en software libre*

La seguridad en servicios web basados en software libre es un área de interés creciente debido a la amplia adopción de soluciones de código abierto en el desarrollo de aplicaciones web, especialmente en el sector de la salud donde la protección de datos es crítica. (Sparx, 2022) discuten las ventajas de utilizar software libre para el desarrollo de servicios web, destacando su transparencia, flexibilidad y la posibilidad de auditoría de seguridad por parte de la comunidad. Sin embargo, también subrayan la importancia de implementar prácticas de seguridad robustas, dado que el acceso abierto al código fuente podría potencialmente facilitar la identificación de vulnerabilidades por parte de actores maliciosos.

Algunas de las prácticas recomendadas para asegurar servicios web basados en software

libre incluyen la actualización regular del software para aplicar parches de seguridad, la configuración cuidadosa de los servicios para minimizar la superficie de ataque y pruebas de penetración para identificar y remediar vulnerabilidades. Además, es esencial la contribución a la comunidad del software libre, participando en la detección y corrección de problemas de seguridad, lo que a su vez beneficia a todos los usuarios del software.


**Figura 18.** *Componentes principales de seguridad en servicios web*

*Nota: Diseño propio*

La adopción de software libre en el desarrollo de servicios web en el ámbito de la salud ofrece la oportunidad de construir sistemas más seguros y personalizados, siempre y cuando se mantengan prácticas de gestión de seguridad informática rigurosas.

### *2.3.14 Lenguajes de Modelado*

En el contexto de la arquitectura de software enfocada a la ciberseguridad, los lenguajes de modelado como UML (Unified Modeling Language) o SysML (Systems Modeling Language) juegan un papel crucial. Fuentes et al., (2024) examinan cómo estos lenguajes facilitan la representación gráfica de sistemas y procesos, permitiendo a los diseñadores y desarrolladores conceptualizar, especificar, y documentar estructuras y comportamientos de sistemas de una manera que es tanto comprensible como rigurosa.

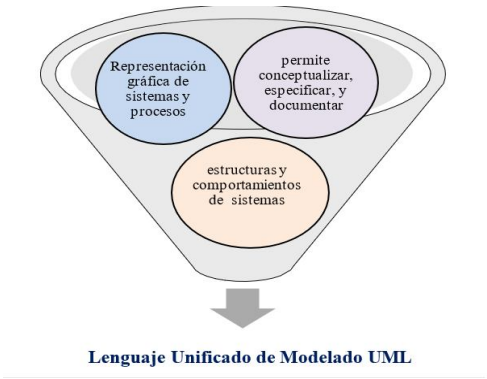


**Figura 19.** *Lenguaje UML*

*Nota: Diseño propio en base a UML*

Los lenguajes de modelado son herramientas esenciales en el diseño de arquitecturas de software seguras, ya que permiten identificar puntos críticos de seguridad y diseñar controles adecuados antes de la implementación del código. Además, facilitan la comunicación entre los equipos de desarrollo y seguridad, asegurando que todos los aspectos de la seguridad sean considerados y entendidos a lo largo del ciclo de vida del desarrollo de software.

Se concluye que la seguridad en servicios web basados en software libre requiere una atención meticulosa a la seguridad del código y las prácticas de desarrollo, beneficiándose significativamente del uso de lenguajes de modelado para planificar y ejecutar estrategias de seguridad efectivas. La colaboración y la adopción de estándares abiertos son fundamentales para el éxito en la protección de servicios web críticos, especialmente en entornos de salud donde la confidencialidad y la integridad de los datos son de suma importancia.

### *2.3.15 ArchiMate Core Framework*

ArchiMate, un lenguaje de modelado arquitectónico ampliamente reconocido, proporciona un marco integral para la descripción de las arquitecturas empresariales, abarcando desde la capa de negocio hasta la capa de tecnología de la información. (Open Group, 2024) resaltan cómo ArchiMate facilita la representación, análisis y comunicación de complejas estructuras organizacionales y sus procesos asociados, permitiendo a los arquitectos de sistemas diseñar e implementar soluciones informáticas que alineen estrechamente la tecnología de la información con los objetivos empresariales.

El Core Framework de ArchiMate se distingue por su capacidad para modelar de manera coherente y comprensible las relaciones entre diferentes dominios arquitectónicos, incluyendo aspectos de la seguridad informática. Esta capacidad es particularmente valiosa en entornos donde la seguridad de la información es crítica, como en el sector de la salud, ya que permite a los diseñadores considerar y planificar explícitamente los requisitos de seguridad a lo largo de todo el sistema y sus interacciones. En resumen, el ArchiMate Core Framework ofrece una herramienta valiosa para la planificación y documentación de sistemas de información con consideraciones de seguridad integradas.

### *2.3.16 Seguridad Informática y Seguridad de la información*

La seguridad informática y la seguridad de la información son fundamentales en la

protección contra amenazas y vulnerabilidades que enfrentan las organizaciones en el ámbito digital. Peters (2025) destacan la importancia de implementar estrategias de seguridad informática robustas para asegurar la confidencialidad, integridad y disponibilidad de la información, especialmente en el sector de la salud donde la protección de datos sensibles es primordial.

La seguridad informática se centra en la protección de la infraestructura computacional y la información contra accesos no autorizados, ataques cibernéticos y otros riesgos de seguridad. La seguridad de la información, por otro lado, aborda la protección de datos en cualquier forma, enfocándose en prácticas y políticas para gestionar y salvaguardar la información. (European Network and Information Security Agency., 2020) subrayan que una estrategia de seguridad eficaz requiere una integración de tecnologías, políticas y prácticas que abarquen tanto la seguridad física como la lógica.

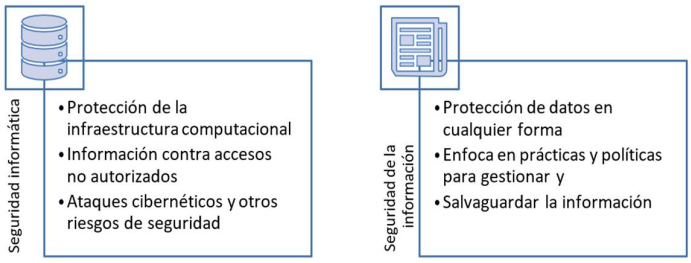



**Figura 20.** *Diferencias entre seguridad informática y de la información*

*Nota: Diseño propio*

La implementación efectiva de medidas de seguridad informática y de la información es determinante para proteger los activos digitales y físicos de una organización contra las crecientes amenazas cibernéticas.

### *2.3.17 Normativa y Estándares de Seguridad de la Información*

El cumplimiento de normativas y estándares de seguridad de la información es crucial para garantizar la protección adecuada de los datos en cualquier organización. Calle & Guanotuña Lascano (2010) destacan la importancia de adherirse a estándares internacionales como ISO/IEC 27001, que establece los requisitos para un sistema de gestión de seguridad de la información (SGSI). Estos estándares proporcionan un marco para gestionar de manera efectiva la seguridad de la información, incluidas las medidas para proteger contra accesos no autorizados, pérdida de datos y ataques cibernéticos.


**Figura 21.** *ISO/IEC 27001*

*Nota: Pasos a cumplir en Norma ISO/IEC 27001*
*(ISO International Organization for Standardization, 2022a)*

La adopción de normativas y estándares de seguridad de la información es esencial para establecer prácticas de seguridad sólidas. Proporcionan un marco confiable para la protección de datos y ayudan a las organizaciones a mitigar los riesgos asociados con la gestión de la información.

### *2.3.18 Riesgos*

La gestión de riesgos es un componente esencial de cualquier estrategia de seguridad de la información. Wasserman & Wasserman (2022) examinan cómo la identificación y evaluación de riesgos permiten a las organizaciones determinar las vulnerabilidades potenciales y las amenazas a sus sistemas de información. La evaluación de riesgos implica la determinación de la probabilidad y el impacto de eventos adversos, lo que a su vez informa la selección de medidas de mitigación adecuadas.

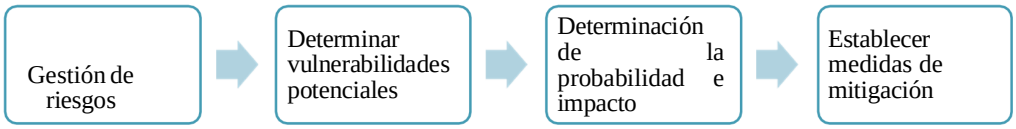



**Figura 22.** *Gestión de Riesgos de la información*

*Nota: Diseño propio*

En el sector de la salud, donde la integridad y disponibilidad de la información pueden tener implicaciones directas en la atención al paciente, la gestión de riesgos adquiere una importancia aún mayor. Identificar riesgos relacionados con la ciberseguridad, como ataques de malware, phishing y otras amenazas cibernéticas, permite a las instituciones de salud

prepararse y responder de manera efectiva para proteger la información de los pacientes y los sistemas críticos de atención de la salud. La gestión efectiva de riesgos es fundamental para la seguridad de la información en todas las organizaciones, especialmente en el ámbito de la salud. Identificar, evaluar y mitigar riesgos no solo protege la información crítica, también asegura la continuidad de las operaciones y la confianza de los pacientes en los servicios de salud.

### *2.3.19 Riesgos en ataques informáticos*

Los ataques informáticos presentan riesgos significativos para individuos, empresas y gobiernos, comprometiendo la seguridad de la información y afectando la operatividad de sistemas críticos. Ruiz Martinez (2021) señala que los riesgos asociados con ataques informáticos incluyen la pérdida de datos confidenciales, interrupciones en los servicios, daños financieros, y daño a la reputación. Los ciberataques pueden adoptar varias formas, incluyendo malware, phishing, ataques de denegación de servicio, y más, cada uno presentando desafíos únicos para la seguridad informática. La identificación de riesgos es un primer paso crucial en el desarrollo de estrategias efectivas para mitigar los efectos potenciales de los ataques informáticos. Es vital implementar un enfoque de seguridad en capas que incluya firewalls, software antivirus, protocolos de autenticación fuerte y educación en seguridad cibernética para usuarios.

La comprensión y mitigación de los riesgos asociados con ataques informáticos son fundamentales para proteger la información y asegurar la continuidad de las operaciones. La adopción de prácticas de seguridad robustas y la preparación para responder ante incidentes son esenciales para minimizar el impacto de estos ataques.

### *2.3.20 Ataques informáticos*

Los ataques informáticos son acciones malintencionadas dirigidas a acceder, alterar, robar o destruir información, interrumpir operaciones o dañar sistemas informáticos. Layme Fernández et al. (2022) exploran diversos métodos utilizados en ataques informáticos, destacando la importancia de comprender estas amenazas para implementar medidas de defensa efectivas. Entre los ataques más comunes se encuentran el ransomware, que encripta archivos exigiendo un rescate por su liberación; el phishing, que engaña a los usuarios para que revelen información personal; y los ataques a la cadena de suministro, que comprometen software de terceros para acceder a redes de organizaciones objetivo. La prevención de ataques informáticos requiere un enfoque proactivo, incluyendo la actualización regular de software, la implementación de soluciones de seguridad avanzadas y la capacitación de usuarios sobre

prácticas seguras en línea.

Los ataques informáticos continúan evolucionando, presentando desafíos continuos para la seguridad de la información. La vigilancia constante, junto con una estrategia de seguridad informática bien definida, es esencial para protegerse contra estas amenazas y asegurar la integridad de los sistemas y datos.

### *2.3.21 Ataques comunes a servicios web*

Los servicios web se enfrentan a una amplia gama de amenazas de seguridad que pueden comprometer la integridad, disponibilidad y confidencialidad de los datos. Vega (2018) resalta algunos de los ataques más comunes, incluyendo inyecciones SQL, Cross- Site Scripting (XSS), ataques de denegación de servicio (DoS), Cross-Site Request Forgery (CSRF), y la exposición de datos sensibles. Estos ataques explotan vulnerabilidades en el software de los servicios web para obtener acceso no autorizado, manipular datos, interrumpir el servicio o robar información confidencial. A continuación, se presenta las 10 principales vulnerabilidades que afectan aplicaciones web publicadas por OWASP Top 10.


**Figura 23.** *Vulnerabilidades más comunes en aplicaciones web*

*Nota: Se menciona el top 10 de vulnerabilidades más comunes (OWASP, s. f.)*

La importancia en que los desarrolladores y administradores de sistemas implementen prácticas de seguridad robustas, como la validación de entrada, cifrado de datos, autenticación y autorización fuertes, y la configuración segura de servidores y aplicaciones web, para mitigar estos riesgos.

La protección contra ataques comunes requiere una comprensión profunda de las amenazas y la implementación de medidas de seguridad adecuadas. Mantenerse informado sobre las últimas técnicas de ataque y vulnerabilidades conocidas es esencial para defender efectivamente los servicios web.

### *2.3.22 Análisis y Gestión de Riesgos*

El análisis y la gestión de riesgos son procesos fundamentales en la seguridad de la información, permitiendo a las organizaciones identificar, evaluar y priorizar riesgos para aplicar las medidas de mitigación adecuadas. Arce & Fábian (2016) discuten cómo un enfoque sistemático para el análisis de riesgos puede ayudar a las organizaciones a entender mejor las amenazas a sus sistemas y datos, y a planificar estrategias de respuesta efectivas. La gestión de riesgos incluye la evaluación continua de riesgos, el desarrollo de políticas y procedimientos de seguridad, la implementación de controles de seguridad y la realización de auditorías y pruebas de penetración regulares.

Una gestión de riesgos efectiva es esencial para proteger los recursos de información y garantizar la continuidad del negocio. Adoptar un enfoque proactivo y basado en la evaluación de riesgos permite a las organizaciones minimizar las vulnerabilidades y prepararse mejor para responder a incidentes de seguridad.


**Figura 24.** *Gestión de Riesgos y continuidad de negocio*

*Nota: Diseño propio*

### *2.3.23 Análisis de riesgos informáticos y ciberseguridad*

El análisis de riesgos informáticos y ciberseguridad es un proceso crítico que ayuda a las organizaciones a identificar, evaluar y priorizar los riesgos asociados con sus activos de información y tecnología. Greiner & Godoy Guglielmone (2023) enfatizan la importancia de este análisis como parte de una estrategia de gestión de la seguridad de la información integral.

Este proceso permite a las organizaciones comprender mejor las amenazas potenciales, las vulnerabilidades de sus sistemas y las posibles consecuencias de los ataques informáticos. Implementar una metodología sistemática para el análisis de riesgos ayuda a las organizaciones a asignar recursos de manera eficiente para mitigar los riesgos más críticos. Esto incluye la adopción de medidas preventivas, como fortalecer las defensas perimetrales, mejorar los sistemas de detección de intrusiones y promover una cultura de seguridad entre los usuarios.

Se concluye en la importancia de realizar un análisis de riesgos informáticos y de ciberseguridad permite a las organizaciones prepararse mejor contra ataques y minimizar el impacto de posibles brechas de seguridad. La clave está en adoptar un enfoque proactivo y continuo para evaluar y gestionar los riesgos de seguridad de la información.

### *2.3.24 Metodologías para el Análisis y gestión de riesgos de la Información*

Las metodologías para el análisis y gestión de riesgos de la información son fundamentales para establecer un enfoque estructurado y eficaz en la protección de los activos de información. Morales González et al. (2022) discuten la aplicación de metodologías reconocidas como ISO/IEC 27005, que proporciona directrices para la gestión de riesgos de seguridad de la información, y la Metodología MAGERIT, que se centra en el análisis y gestión de riesgos en sistemas de información.

Estas metodologías ofrecen un marco para identificar amenazas, evaluar vulnerabilidades, determinar impactos potenciales y priorizar acciones de mitigación basadas en el nivel de riesgo. La implementación de estas metodologías ayuda a las organizaciones a desarrollar planes de gestión de riesgos robustos y adaptativos, que son esenciales para proteger contra la evolución constante de las amenazas cibernéticas.

La adopción de metodologías estandarizadas para el análisis y gestión de riesgos es un paso fundamental en el fortalecimiento de la postura de seguridad de una organización. Permiten una comprensión profunda de los riesgos de seguridad de la información y facilitan la implementación de estrategias de mitigación efectivas para proteger contra amenazas informáticas y cibernéticas.

### *2.3.25 Metodología MAGERIT v.3*

La Metodología MAGERIT versión 3 es una herramienta esencial en el campo de la seguridad de la información, diseñada para analizar y gestionar los riesgos asociados a los sistemas de información. Castillo Enríquez et al. (2022) destacan la importancia de MAGERIT v.3 como un marco de referencia para identificar, evaluar y controlar los riesgos informáticos, proporcionando a las organizaciones una guía sistemática para proteger sus activos digitales. Esta metodología promueve la realización de análisis de riesgos de manera estructurada, ofreciendo un enfoque detallado para determinar las amenazas, las vulnerabilidades y el impacto potencial sobre los sistemas de información, facilitando así la implementación de medidas de seguridad adecuadas para mitigar los riesgos identificados.

La adopción de MAGERIT v.3 permite a las organizaciones mejorar su postura de seguridad a través de un entendimiento profundo y una gestión efectiva de los riesgos informáticos, asegurando la continuidad y la integridad de sus operaciones en el entorno digital.

### *2.3.26 Resiliencia Digital*

La resiliencia digital se refiere a la capacidad de una organización para anticipar, resistir, recuperarse y adaptarse a incidentes cibernéticos que pueden afectar sus operaciones o comprometer su información. Bernita et al. (2017) subrayan la relevancia de la resiliencia digital en el contexto actual, donde las amenazas cibernéticas son cada vez más sofisticadas y potencialmente devastadoras. La resiliencia digital no solo implica la implementación de robustas medidas de seguridad informática, sino también la creación de una cultura organizacional que prioriza la seguridad de la información y la preparación para la respuesta y recuperación ante incidentes.

Fomentar la resiliencia digital es fundamental para asegurar la sostenibilidad y el éxito a largo plazo de las organizaciones en un mundo cada vez más conectado. Esto requiere un enfoque holístico que integre tecnología, procesos y personas, permitiendo una respuesta ágil y efectiva frente a los desafíos de seguridad cibernética.

### *2.3.27 Continuidad de servicios*

La continuidad de servicios es un aspecto crítico de la planificación estratégica de una organización, asegurando que sus operaciones esenciales puedan continuar sin interrupciones significativas ante eventos adversos. Alonzo Gomero & Lovera Dávila (2022) resaltan la importancia de establecer planes de continuidad de servicios robustos que incluyan estrategias

de recuperación ante desastres, redundancia de sistemas y procedimientos de respaldo para garantizar la disponibilidad continua de los servicios críticos. Estos planes deben ser revisados y actualizados regularmente para adaptarse a los cambios en el entorno operativo y tecnológico de la organización.


**Figura 25.** *Continuidad de servicios*

*Nota: Diseño propio*

Se resume en la importancia de desarrollar e implementar un plan de continuidad de servicios efectivo es esencial para minimizar el impacto de interrupciones inesperadas, permitiendo a las organizaciones mantener sus operaciones críticas y proteger su reputación en el mercado.

### *2.3.28 La continuidad de servicios web*

La continuidad de los servicios web se refiere específicamente a la capacidad de mantener operativos y accesibles los servicios web de una organización ante incidentes de seguridad, fallas técnicas o desastres naturales. González Ortega et al. (2023) enfatizan la necesidad de adoptar medidas específicas para la continuidad de los servicios web, como la implementación de sistemas de gestión de tráfico web, el uso de la nube para redundancia y recuperación ante desastres, y la realización de pruebas periódicas de recuperación para garantizar la resiliencia de los servicios en línea.

Por lo tanto, asegurar la continuidad de los servicios web es vital en el mundo digital actual, donde la dependencia de las plataformas en línea para realizar negocios, comunicarse y acceder a servicios es omnipresente. Las organizaciones deben priorizar la planificación y preparación para la continuidad de sus servicios web para mantener la confianza y satisfacción de sus usuarios y clientes.

### *2.3.29 ISO/IEC 27031:2011*

La norma ISO/IEC 27031:2011, titulada "Tecnología de la información - Técnicas de seguridad - Directrices para la preparación de la continuidad del negocio de las tecnologías de la información y comunicación (TIC)", establece los principios y directrices para garantizar que las organizaciones puedan recuperar y continuar sus operaciones de TIC ante cualquier interrupción. Ávila Agreda et al. (2021) enfatizan la importancia de esta norma como marco para desarrollar y gestionar un sistema efectivo de continuidad del negocio en el ámbito de las TIC, lo que incluye la identificación de los requisitos de negocio, la evaluación de los riesgos, la implementación de estrategias y soluciones de continuidad, y la realización de pruebas y revisiones periódicas para asegurar la eficacia del plan.

La adopción de la norma ISO/IEC 27031:2011 ayuda a las organizaciones a construir una infraestructura de TIC resistente y preparada para responder eficazmente a las interrupciones, asegurando así la continuidad de sus operaciones críticas y la protección de sus activos de información.

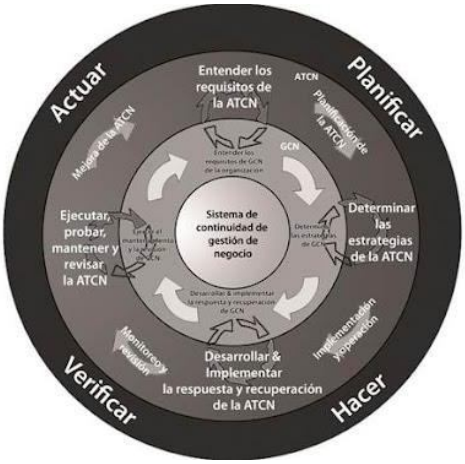



**Figura 26.** *TIC para la continuidad del negocio*

*Nota: Tomado de pasos cíclicos PDVA, adecuación TIC para la Continuidad del Negocio, (Servicio Ecuatoriano de Normalización, 2017)*

### *2.3.30 Indicadores clave de la Norma ISO 27031*

Los indicadores clave de la norma ISO 27031 proporcionan métricas y parámetros para evaluar la efectividad del sistema de gestión de continuidad del negocio de las TIC. Mejía Viteri (2015) destaca la relevancia de estos indicadores como herramientas para medir el desempeño de los planes de continuidad y realizar ajustes basados en el análisis de datos concretos. Entre estos indicadores se encuentran el tiempo de recuperación objetivo (RTO), el punto de recuperación objetivo (RPO), y la eficacia de las pruebas de continuidad, que permiten a las

organizaciones asegurar que sus estrategias de continuidad están alineadas con los objetivos de negocio y las expectativas de los stakeholders.

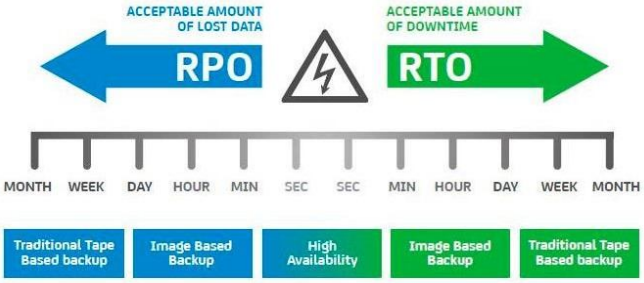



**Figura 27.** *Tiempo de recuperación objetivo (RTO) y punto de recuperación objetivo (RPO)*

*Nota: Tomado de diferencia entre RPO y RTO (2ksystems, 2017)*

Utilizar los indicadores clave de la norma ISO 27031 es fundamental para la gestión y mejora continua de los sistemas de continuidad del negocio de las TIC, proporcionando una base sólida para la toma de decisiones estratégicas y operativas en el ámbito de la recuperación ante desastres y la continuidad operativa.

## 2.4 Marco legal

La Constitución de la Republica de Ecuador, en la parte referente a los derechos en su artículo 32 establece que: la salud es un derecho que garantiza el Estado, su acceso es permanente, oportuno y sin exclusión a programas, acciones y servicios de promoción y atención integral de salud, salud sexual y salud reproductiva. La prestación de los servicios de salud se regirá por los principios de equidad, universalidad, solidaridad, interculturalidad, calidad, eficiencia, eficacia, entre otras; haciendo énfasis para nuestro caso en lo que se refiere al acceso permanente y oportuno a los servicios de salud. (Constitución de la Republica del Ecuador, 2008)

El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley, también establecido en el 66 de la carta magna, tiene relación con la confidencialidad que toda institución, especialmente del sector salud debe observar.

En el Ecuador la autoridad sanitaria nacional es el Ministerio de Salud Pública, entidad a la que corresponde el ejercicio de las funciones de rectoría en salud; así como la responsabilidad de la aplicación, control y vigilancia del cumplimiento de la ley Orgánica de

Salud.

En ese contexto el Ministerio de Salud Pública tiene bajo su responsabilidad regular y vigilar la aplicación de las normas técnicas para la detección, prevención, atención integral y rehabilitación, de enfermedades transmisibles, no transmisibles, crónico-degenerativas, discapacidades y problemas de salud pública declarados prioritarios, y determinar las enfermedades transmisibles de notificación obligatoria, garantizando la confidencialidad de la información. (Ley Orgánica de Salud 2006, 2006)

Adicionalmente podemos resaltar que en el mismo Código de Salud se establece que toda persona tiene derecho al acceso universal, equitativo, permanente, oportuno y de calidad a todas las acciones y servicios de salud. En el Registro Oficial Suplemento No. 459 de 26 de mayo de 2021 se publicó la Ley Orgánica de Protección de Datos Personales, que tiene por objeto garantizar el derecho a la protección de datos personales, proteger las libertades públicas y los derechos fundamentales de las personas.

Consagra algunas categorías especiales de datos personales, como los datos sensibles, los de niños, niñas y adolescentes, los de salud y los de las personas con discapacidad; y se refiere al tratamiento especializado de estos datos. Dentro de los principios que establece este cuerpo legal se detalla el de confidencial que trata del sigilo y secreto de los datos personales, en donde estos no deben tratarse o comunicarse para un fin distinto para el cual no fueron recogidos, para el efecto menciona que el responsable, es decir la institución deberá adecuar las medidas técnicas para cumplir con este principio.

Otro principio muy importante hace referencia a la Seguridad de los datos personales, en donde establece que los responsables y encargados de su tratamiento, deberán implementar todas las medidas de seguridad adecuadas y necesarias para proteger los datos personales frente a cualquier riesgo, amenaza, vulnerabilidad. (Ley Orgánica de Protección de Datos Personales, 2021).

Mediante Acuerdo Ministerial 006-2021 abril de 2021, el ministerio de Telecomunicaciones y de la Sociedad de la Información emite la Política de Ciberseguridad cuyo objetivo es construir y fortalecer las capacidades nacionales que permitan garantizar el ejercicio de los derechos y libertades de la población y la protección de los bienes jurídicos del Estado en el ciberespacio.

La política establece directrices que buscan afianzar un ciberespacio seguro para contribuir al desarrollo social, económico y humano del país, así como a la creación de una

confianza digital, posee un enfoque multisectorial y multidimensional que se debe al carácter transversal de la ciberseguridad.

Esta política alcanza a sectores público y privado del país, establece directrices para encaminar las acciones en ciberseguridad de las entidades de la Administración Pública Institucional y que dependen de la Función Ejecutiva, en coordinación con los otros poderes del Estado, sociedad civil y ciudadanía en general.

Dentro de los objetivos específicos de la Política de Seguridad podemos resaltar los siguientes:

Fortalecer la capacidad de protección de datos, información, activos y servicios digitales en el sector público garantizando así la seguridad de los mismos y confianza en el ciberespacio. Establecer una metodología compatible con estándares internacionales para la evaluación de riesgos y amenazas. Impulsar un marco normativo y de buenas prácticas que fundamente la protección y defensa de las infraestructuras críticas digitales y servicios esenciales. (Política de Ciberseguridad, 2021)

Las Normas Técnicas de Control Interno, emitidas por la Contraloría General del Estado de Ecuador, en su apartado relacionado con Tecnología de la Información (410), hace mención al tratamiento de contingencias para garantizar la continuidad operativa, así como a la aplicación de estándares tecnológicos y controles que aseguren la calidad y la gestión de riesgos. (Normas de Control Interno para las Entidades del Sector Público, 2023)

El Ecuador mantiene nueve zonas de planificación, en donde el Ministerio de Salud Pública tiene presencia a través de Direcciones Distritales a nivel cantonal, y a nivel parroquial con unidades de salud de primer nivel y hospitales básicos.

Dentro de los productos y servicios entregables por la Unidad de Tecnologías de la Información y Comunicaciones en los hospitales del MSP, el Estatuto Orgánico de Gestión Organizacional resalta la importancia de considerar sistemas de información para las diferentes áreas de la institución, así como servicios web y respaldos de información. (Estatuto Orgánico Gestión Organizacional por Procesos de Hospitales, 2012)

# 3 CAPITULO III MARCO METODOLÓGICO

## 3.1 Descripción del área de estudio

El trabajo de investigación se realiza en el Hospital Básico “Raúl Maldonado Mejía” de la ciudad de Cayambe, con código SGI 001787, se enfoca directamente al servicio de consulta externa, donde intervienen los procesos y servicios de Admisión y Estadística, Enfermería y Atención Integral de Salud. Como unidad de salud de segundo nivel de atención se encuentra ubicada en la ciudad de Cayambe, parroquia urbana y cantón del mismo nombre, pertenecientes a la provincia de Pichincha.

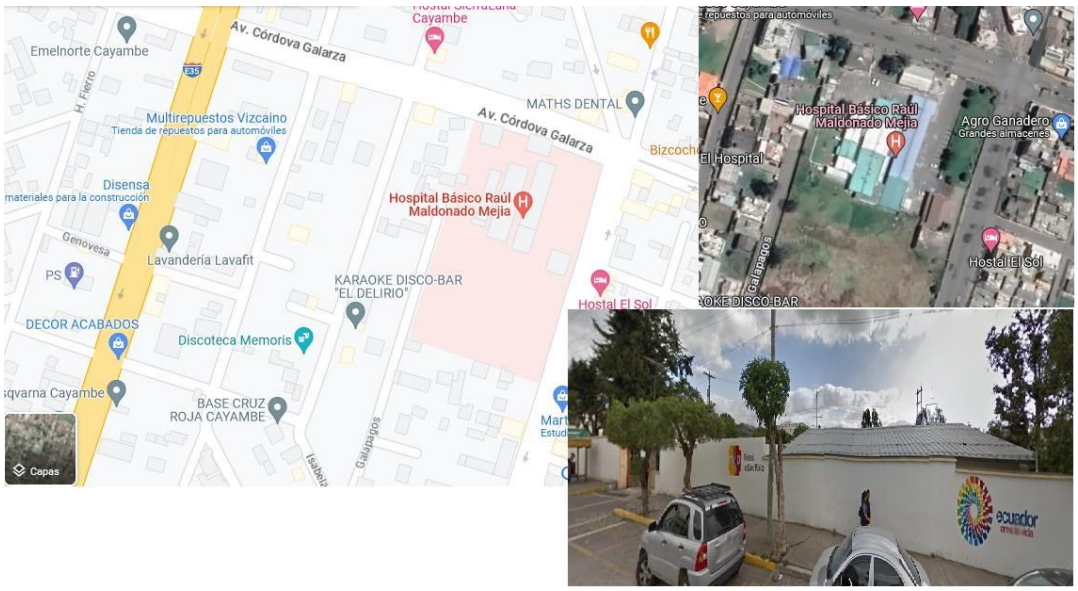



**Figura 28.** *Ubicación del HBRMM*

*Nota: Ubicación Hospital Básico Cayambe (Google Maps, s. f.)*

En su inicio esta casa de salud, funcionaba en el edificio del colegio Mariana de Jesús entre las calles Sucre y Terán de la ciudad de Cayambe, luego se trasladó al sector del río blanco de la misma ciudad y era conocido con el nombre de Hospital San José.

El nuevo edificio se inaugura en la Av. Manuel Córdova Galarza y Rocafuerte el 10 de septiembre de 1974, el hospital cantonal lleva su nombre en honor al ciudadano cayambeño, Dr. Raúl Maldonado Mejía, quien a esa época se desempeñaba como ministro de salud, coincidiendo designación con el año de construcción de sus instalaciones. (Imbaquingo, 2016)

El HBRMM es una de las 16 unidades de salud que forman parte de la Dirección Distrital de Salud 17D10 Cayambe – Pedro Moncayo, siendo el único con capacidad resolutiva de segundo nivel de atención, es decir siendo hospital de referencia para centros de salud urbanos y rurales, proporcionando atención de especialidad en el servicio de consulta externa, atención de emergencia las 24 horas, cirugía y hospitalización.

El Hospital Básico Raúl Maldonado Mejía dispone de 25 camas y en su cartera de servicios ofrece atención en medicina interna, cirugía general, ginecología, pediatría y traumatología; así como servicios de apoyo diagnóstico en imagenología, laboratorio clínico y atención de emergencia las 24 horas.

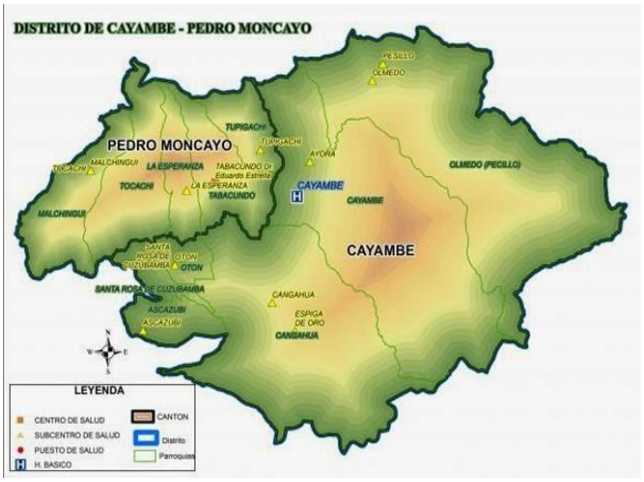



**Figura 29.** *Unidades de salud cantones Cayambe y Pedro Moncayo - Pichincha*

La infraestructura tecnológica que posee el Hospital Básico Cayambe consta de un servidor de aplicaciones basado en software libre, con un sistema operativo Linux Ubuntu Server, servidor web Apache HTTP, MySQL como sistema gestor de base de datos relacional y PHP como lenguaje de programación de la aplicación para la Gestión de Consulta Externa.

El Sistema de Gestión de Consulta Externa (SGCE) para su funcionamiento hace uso de una IP publica http://xx.xx.xx.xxx/consultaexterna, en donde se encuentra expuesto el puerto de red 80 para el servicio web mediante HTTP.

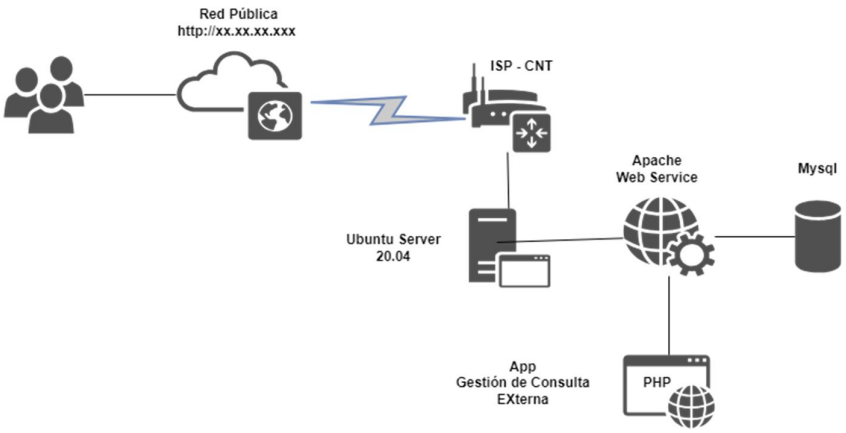



**Figura 30.** *Infraestructura de red HBRMM – Consulta Externa*

*Nota: Diseño Propio*

## 3.2 Diseño metodológico de la evaluación

La evaluación se diseñó como estudio no experimental de corte transversal con integración de evidencia técnica y percepción de usuarios, y su objetivo fue describir el desempeño del servicio sin manipular variables para vincular cada dimensión observada con los controles activos de la prueba de concepto mediante una pauta documentada con hitos claros para recolección de datos. La unidad de análisis correspondió a los activos de información del servicio web de Consulta Externa, con sus componentes de aplicación, base de datos, servidor web y conectividad, y se incluyó al personal operativo que ejecuta registro consulta y agendamiento bajo condiciones regulares de operación con definición previa de roles criterios de inclusión calendario de campo y resguardo de evidencias primarias según cronograma institucional con autorización vigente mediante actas firmadas.

**Tabla 7.**

*Alcance del diseño y unidad de análisis*

| Elemento | Definición operacional |
|---|---|
| Tipo de estudio | No experimental, corte transversal |
| Enfoque de integración | Evidencia técnica + percepción de usuarios |
| Unidad de análisis | Activos de información de CE, app, BD, servidor web, conectividad |
| Propósito analítico | Describir desempeño y vincularlo con controles de la PoC |
| Soporte documental | Pauta con hitos, actas y cronograma autorizado |

*Nota: Diseño propio*

Se definió como población a usuarios internos vinculados al flujo de Consulta Externa en medicina, enfermería, estadística, administración y tecnologías de información del hospital,

y la muestra se fijó con veinte participantes distribuidos en once médicos con dos profesionales de enfermería con cuatro administrativos o estadísticos con dos especialistas de TIC con un colaborador clasificado como otros. El muestreo fue intencional con alcance operativo sobre turnos regulares con convocatoria formal con consentimiento informado escrito, y cada invitado respondió de manera individual en sesiones breves dentro de la jornada sin interrupción del servicio bajo supervisión del investigador con resguardo de formularios en custodia controlada con archivo bajo llave con registro de entrega según protocolo aprobado.

**Tabla 8.**

*Población y muestra*

| Grupo | n |
|---|---|
| Médica | 11 |
| Enfermería | 2 |
| Administración/Estadística | 4 |
| TIC | 2 |
| Otros | 1 |
| **Total** | 20 |

*Nota: Diseño propio*

El instrumento fue un cuestionario de siete ítems con escala Likert de cinco puntos desde totalmente en desacuerdo hasta totalmente de acuerdo con codificación ordinal de uno a cinco, y las dimensiones quedaron estructuradas como perfil del encuestado en P1 usabilidad y rendimiento en P2 y P3 seguridad y confidencialidad en P4 P5 y P6 y continuidad y disponibilidad en P7 sin alterar el orden de respuesta para análisis descriptivo posterior. La codificación de categorías textuales se mapeó a valores numéricos con reglas fijas para garantizar trazabilidad sin ambigüedades, y los registros se volcaron a una matriz con identificador anónimo sello de fecha y control de consistencia por doble verificación manual con conservación de los originales en carpeta de respaldo.

**Tabla 9.**

*Ítems por dimensión*

| Dimensión | Ítems |
|---|---|
| Perfil | P1 |
| Usabilidad / Rendimiento | P2, P3 |
| Seguridad / Confidencialidad | P4, P5, P6 |
| Continuidad / Disponibilidad | P7 |

*Nota: Diseño propio*

La validez de contenido fue revisada por el tutor mediante contraste ítem a dimensión con retroalimentación documentada y ajustes menores sobre la redacción, y se declaró como limitación la ausencia de estimación del coeficiente alfa de Cronbach por tratarse de una medición focal con tamaño muestral acotado a veinte registros mediante acta firmada con fecha de revisión según pauta de evaluación archivada.

## 3.3 Enfoque y tipo de investigación

El estudio integró enfoque mixto con componente cualitativo para caracterizar prácticas operativas mediante entrevista estructurada al responsable de TIC y revisión de procedimientos institucionales, y componente cuantitativo para medir riesgos con MAGERIT v3 y PILAR junto con métricas de funcionalidad usabilidad rendimiento y seguridad a partir de logs de Apache mediciones de Pingdom y pruebas con herramientas del navegador. El diseño fue no experimental de corte transversal con alcance descriptivo y correlacional para observar variables sin intervención y relacionar su comportamiento con la aplicación de controles de seguridad definidos en la prueba de concepto segura bajo lineamientos documentados que ordenaron las tareas de campo y aseguraron la trazabilidad de cada registro hasta su fuente primaria bajo resguardo verificado.

**Tabla 10.**

*Enfoque y diseño*

| Componente | Técnica / Fuente |
|---|---|
| Cualitativo | Entrevista estructurada, revisión de procedimientos |
| Cuantitativo | MAGERIT/PILAR, logs Apache, Pingdom, herramientas del navegador |
| Diseño | No experimental, transversal, descriptivo–correlacional |

*Nota: Diseño propio*

El alcance fue exploratorio y descriptivo para activos amenazas y vulnerabilidades con fase evaluativa al valorar el desempeño de la prueba de concepto y el grado de cumplimiento frente a la NTE INEN ISO IEC 27031 mediante un checklist con evidencias, y la unidad de análisis se definió como el servicio web de Consulta Externa con su aplicación base de datos servidor web y conectividad junto con usuarios internos. La población comprendió personal médico enfermería administración estadística y TIC con participación focal en procesos del servicio, y la muestra se integró con veinte colaboradores seleccionados por rol operativo con convocatoria formal y consentimiento escrito bajo un esquema de recolección en jornada

ordinaria sin afectar la prestación de atenciones con control de cadena de custodia documental verificada.

**Tabla 11.**

*Alcance y muestra*

| Elemento | Detalle |
|---|---|
| Alcance | Exploratorio–descriptivo y evaluativo |
| Unidad de análisis | Servicio de Consulta Externa |
| Población | Médica, Enfermería, Adm/Estadística, TIC |
| Muestra | n = 20 por rol operativo |

*Nota: Diseño propio*

Las técnicas incluyeron análisis de riesgos con PILAR y escaneos con Nmap Nikto y Hostedscan más análisis de logs con Webalizer y mediciones de Pingdom además de encuesta tipo Likert de cinco puntos para percepción de acceso rendimiento y seguridad, y la entrevista estructurada al responsable de TIC sirvió para consolidar prácticas y controles existentes con guía aprobada. La validez de contenido de la guía y del cuestionario se revisó por el tutor con observaciones incorporadas y registro en acta correspondiente, y se mantuvo anonimato de participantes con resguardo de datos y enmascaramiento de IP o host en reportes públicos bajo autorización institucional con custodia de formularios y respaldos digitales cifrados según lineamientos internos vigentes para protección de la información operativa.

**Tabla 12.**

*Técnicas e instrumentos*

| Técnica / Instrumento | Propósito |
|---|---|
| PILAR / MAGERIT v3 | Valoración de riesgos |
| Nmap / Nikto / Hostedscan | Detección de exposición y configuración |
| Webalizer / Logs Apache | Métricas de uso y códigos de respuesta |
| Pingdom | Rendimiento de carga |
| Encuesta Likert | Percepción de acceso, seguridad y continuidad |
| Entrevista estructurada | Contexto operativo y controles vigentes |

*Nota: Diseño propio*

## 3.4 Procedimiento de investigación

La investigación se desarrolló en cuatro fases que se describen a continuación:

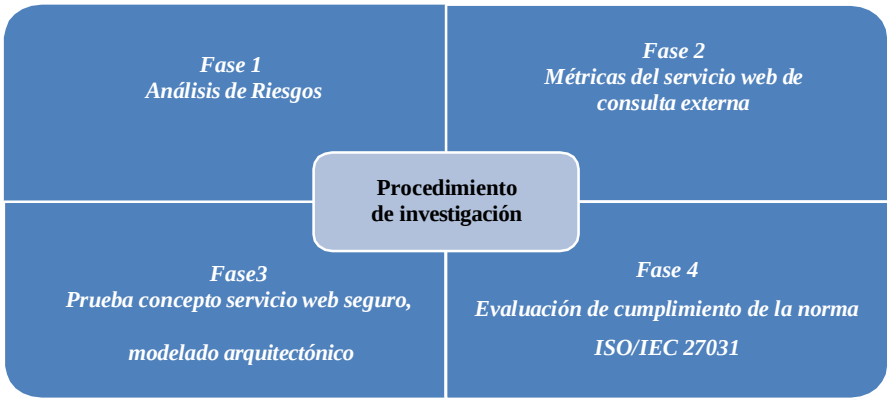



**Figura 31.** *Fases de investigación*

*Nota: Diseño Propio*

### *3.4.1 Fase 1 Análisis de Riesgos*

En la fase 1 que corresponde al Análisis de Riegos se realizó las siguientes tareas:

- Identificación de los activos principales del servicio de Consulta Externa del HBRMM.
- Aplicando la Metodología Magerit versión 3 y mediante el uso la herramienta PILAR versión 7.4.9 y artefactos propios, se realiza el análisis y gestión de riesgos sobre los activos principales del servicio de consulta externa del HBRMM.
- Para la identificación de amenazas y vulnerabilidades que afectan a los activos de información se aplicó una entrevista estructurada al responsable TIC del HBRMM, para el servicio web de Consulta Externa se llevaron a cabo pruebas de penetración y escaneos de seguridad utilizando herramientas como Nmap, Nikto y Hostedscan, seleccionadas por su capacidad para detectar configuraciones inseguras y servicios expuestos.
- Por último, para el tratamiento de riesgos se plantean medidas de seguridad o salvaguardas a los activos de información, con énfasis en las mejoras de la disponibilidad y su impacto en la continuidad del servicio web del área de consulta externa del HBRMM.

### *3.4.2 Fase 2 Métricas del servicio web de consulta externa*

Como punto de partida para la ejecución de esta fase se consideró la cultura

organizacional (misión, visión, objetivos estratégicos), además se identificó la infraestructura tecnológica del servicio de Consulta Externa, con la que cuenta el HBRMM, infraestructura que en la práctica ayuda al cumplimiento del objetivo de facilitar la accesibilidad y mejora en los tiempos de espera en la atención a pacientes. Para ello se realizó el análisis de las métricas de rendimiento, funcionalidad, usabilidad y seguridad del web service Apache y la herramienta informática que la institución utiliza para la gestión de citas y agendamiento, mediante el uso de aplicaciones como Webalizer, Pingdom y la herramienta para desarrolladores integrada en el navegador.

### *3.4.3 Fase 3 Prueba de concepto servicio web seguro, modelado arquitectónico*

Para esta fase se desarrolló una prueba de concepto mediante el despliegue del servicio web en un servidor privado virtual (VPS) con una arquitectura de seguridad modelada en UML con ArchiMate Core Framework y basada en software libre, para la implementación se considera las herramientas que se muestran en la siguiente figura:

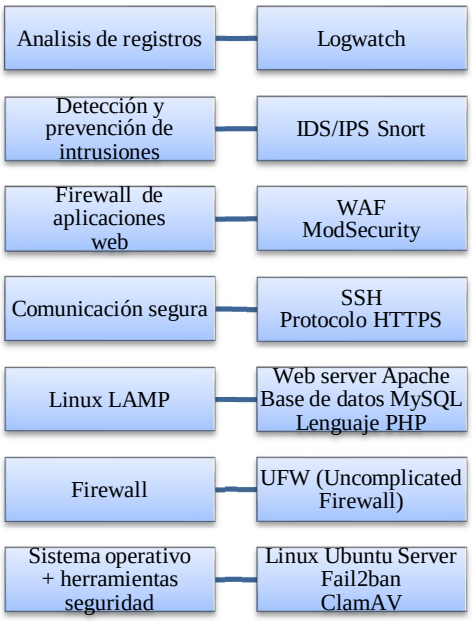



**Figura 32.** *Arquitectura de seguridad propuesta*

*Nota: Diseño Propio*

### *3.4.4 Fase 4 Evaluación de cumplimiento de la norma ISO NTE INEN-ISO/IEC 27031*

Con la identificación de las amenazas y vulnerabilidades realizadas en la Fase 1 del proyecto, se analizan los impactos en la confidencialidad, integridad y disponibilidad en los

activos de información del área de Consulta Externa del HBRMM.

Mediante el despliegue realizado en la fase 3 de la prueba de concepto, se realizó una encuesta a usuarios internos del HBRMM en donde se pretende conocer sus apreciaciones al servicio web seguro con la propuesta de mejora realizadas.

Finalmente, para cumplir con el objetivo de alinear el servicio web de Consulta Externa del HBRMM con los requisitos de la norma ISO NTE INEN-ISO/IEC 27031, se realizó análisis de: procesos críticos, impactos al Negocio (BIA), Tiempo de Recuperación (OTR) y Punto de Recuperación (OPR), que nos proporciona el grado de cumplimiento de la norma en base un checklist que contribuya a mejorar la continuidad del servicio.

## 3.5 Consideraciones bioéticas

La investigación se desarrollará considerando los principios bioéticos de beneficencia, no maleficencia y autonomía. El trabajo investigativo se llevará a cabo con la autorización explícita de las autoridades de la unidad de salud, personal administrativo y de salud del Hospital Básico “Raúl Maldonado Mejía” de Cayambe.

A los sujetos participantes de la investigación, se les informará de forma oral, los aspectos más relevantes de la investigación: objetivos, procedimientos, la importancia de su participación, tiempo de duración, leyes, códigos y normas que lo amparan, carácter voluntario en la participación y beneficios. Así mismo, se tramitarán todos los permisos respectivos para tener acceso a bases de datos y se respetará el anonimato de los involucrados.

# 4 CAPITULO IV RESULTADOS Y DISCUSIÓN

En este capítulo se presentan y analizan los hallazgos obtenidos a partir de la revisión sistemática de la literatura y la aplicación de los procedimientos de investigación relacionados con la arquitectura de seguridad para la continuidad de servicios web en el ámbito de la salud. Se dan a conocer los resultados de la aplicación de la metodología MAGERIT v3, pruebas de penetración, las métricas analizadas, la ejecución y puesta en marcha de la prueba de concepto y su impacto en la mejora de la continuidad del servicio web en conformidad con la norma ISO NTE INEN-ISO/IEC. Además, resume los principales temas y tendencias identificados en los estudios revisados, mientras que la discusión contextualiza estos hallazgos dentro del marco teórico y práctico de la investigación, proporcionando una visión crítica y sugerencias para futuras investigaciones.

## 4.1 Resultados

### *4.1.1 Metodología MAGERIT v.3*

Mediante el uso de la herramienta PILAR que usa la metodología Magerit se procedió con la recolección de datos para identificación de los activos del servicio de Consulta Externa, su clasificación, dependencias y valoración, en las dimensiones de confidencialidad, integridad y disponibilidad, esto se detallan en las siguientes figuras.

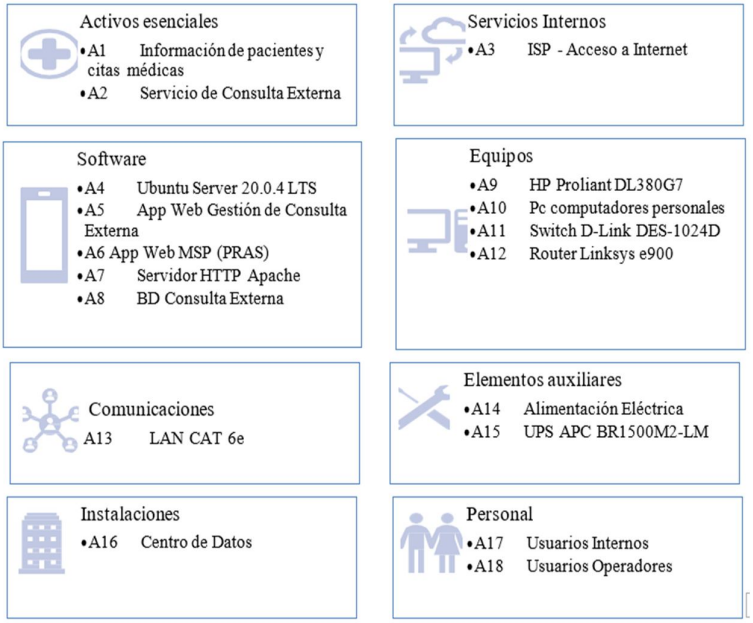



**Figura 33.** *Activos de información Consulta Externa HBRMM*

*Nota: La distribución más detallada y fichas de los activos de información se presentan en el Anexo A*


**Figura 34.** *Proyecto de análisis de riesgos con PILAR - Servicio de Consulta Externa HBRMM*


**Figura 35.** *PILAR – valoración de los activos*

*Nota: Valoración en disponibilidad, integridad y confidencialidad*

**Síntesis de la entrevista al responsable TIC**

El responsable TIC describe control de acceso físico restringido a personal de TI autorizado con ingreso supervisado por llaves y autorización previa, no existen cerraduras electrónicas ni cámaras de vigilancia que permitan trazabilidad continua de entradas y salidas. El espacio opera como sala técnica improvisada con soporte energético basado en un UPS de 1500 KVA y sin sistema de enfriamiento dedicado lo que incrementa temperatura interna y probabilidad de interrupciones por sobrecalentamiento.

En servidores Ubuntu aplica actualizaciones periódicas del sistema con SSH por clave privada en el puerto 22 con UFW limitado a 22 más 80. No configura HTTPS ni WAF en

producción y el antivirus en endpoints no se documenta, de este modo el servicio expuesto por HTTP carece de cifrado y de filtrado profundo frente a cargas maliciosas o intentos automatizados de descubrimiento.

En las tablas a continuación se presenta las escalas para valoración de probabilidad e impactos para el Análisis de Riesgos.

**Tabla 13.**

*Escalas de probabilidad*

| Valor | Probabilidad | Ocurrencia |
|---|---|---|
| **1** | Muy Baja | Poco probable > 5 años, casi nunca |
| **2** | Baja | Esporádica cada 2 a 4 años |
| **3** | Media | Una vez al año |
| **4** | Alta | Varias veces al año |
| **5** | Muy Alta | Mensual, semanal o a diario |

*Nota. Diseño propio*

**Tabla 14.**

*Escalas de impacto*

| Valor | Impacto | Afectación |
|---|---|---|
| **1** | Muy Bajo | Menor interrupción recuperable en minutos |
| **2** | Bajo | Parcial recuperación en menos de una hora |
| **3** | Medio | Moderada solución en pocas horas |
| **4** | Alto | Significativa recuperación en 24-48 horas |
| **5** | Muy Alto / Crítico | Interrupción total o pérdida irrecuperable |

*Nota. Diseño propio*

**Tabla 15.**

*Matriz de Riesgos*

| N.º | Código | Nombre del Activo | Amenazas principales | Probabilidad | Impacto | Riesgo (PXI) |
|---|---|---|---|---|---|---|

| | | | | | | |
|---|---|---|---|---|---|---|
| 1 | A1 | Información de pacientes y citas médicas | Acceso no autorizado / Fuga de datos | 3 | 5 | 15 |
| 2 | A2 | Servicio de Consulta Externa | Acceso no autorizado / Pérdida de datos | 3 | 5 | 15 |
| 3 | A3 | ISP - Acceso a Internet | Fallas en red | 5 | 2 | 10 |
| 4 | A4 | Ubuntu Server 20.04 LTS | Ransomware / Ataques de fuerza bruta | 5 | 5 | 25 |
| 5 | A5 | App Web Gestión de Consulta Externa | Ataques de XSS y/o Gestión de sesiones | 3 | 4 | 12 |
| 6 | A6 | App Web MSP PRAS | Indisponibilidad de aplicación externa | 5 | 3 | 15 |
| 7 | A7 | Servidor HTTP Apache | DoS / Intercepción de comunicaciones | 3 | 5 | 15 |
| 8 | A8 | MySQL BD Consulta Externa | Inyección SQL / Pérdida de datos | 4 | 5 | 20 |
| 9 | A9 | HP Proliant DL380G7 | Fallos eléctricos / Sobrecalentamiento | 2 | 5 | 10 |
| 10 | A10 | PC Computadores personales | Malware / Fallos de hardware y/o software | 3 | 3 | 9 |
| 11 | A11 | Switch D-Link DES-1024D | Intercepción tráfico / Fallos de hardware | 2 | 3 | 6 |
| 12 | A12 | Router Linksys e900 | Acceso indebido / Fallos de hardware | 2 | 3 | 6 |
| 13 | A13 | LAN CAT 6e | Fallas transmisión / Interrupciones | 2 | 3 | 6 |
| 14 | A14 | Alimentación eléctrica | Apagones / Sobretensiones | 5 | 1 | 5 |
| 15 | A15 | UPS APC BR1500M2-LM | Fallo baterías / Sobrecargas | 2 | 3 | 6 |
| 16 | A16 | Centro de Datos | Acceso indebido / Sobrecalentamiento | 5 | 4 | 20 |
| 17 | A17 | Usuarios Internos | Acceso indebido / Divulgación de datos | 1 | 5 | 5 |
| 18 | A18 | Usuarios Operadores | Errores humanos / Fallos de autenticación | 3 | 4 | 12 |

*Nota. Diseño propio*

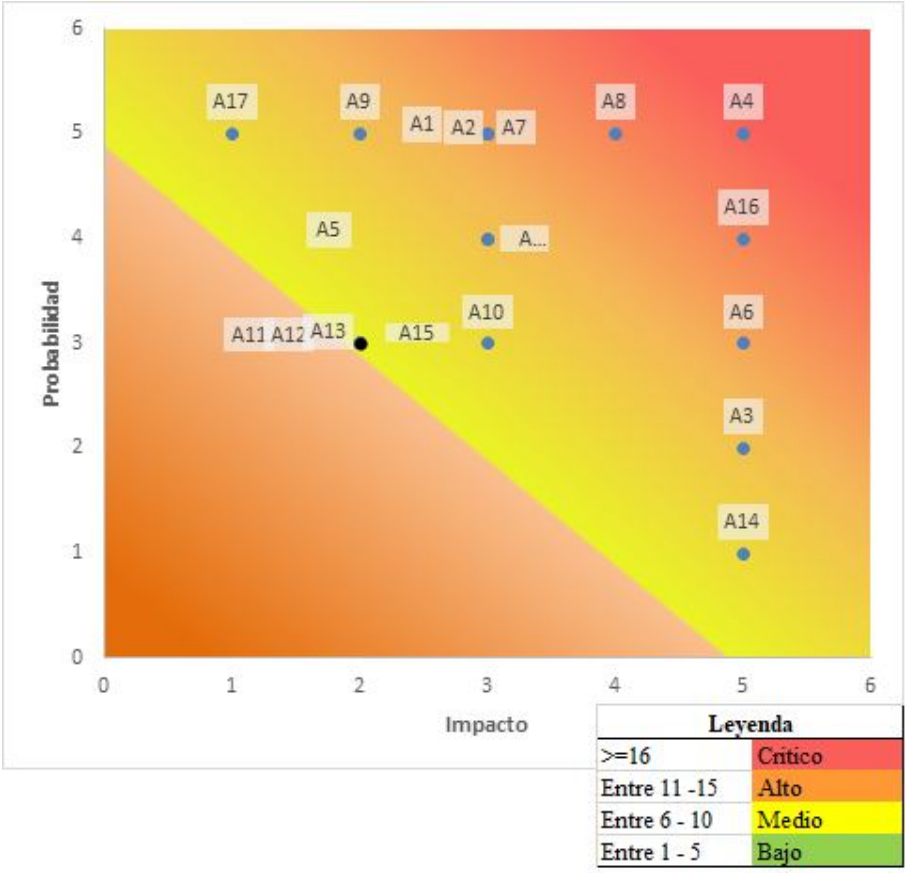



**Figura 36.** *Mapa de Calor de Riesgos MAGERIT v3*

*Nota: Diseño propio*

Ejecutando pruebas de penetración con herramientas basadas en software libre conocidas y usadas en este medio como: Nmap, Nikto y Hostedscan se logró detectar las vulnerabilidades del servicio web Apache publicado en la IP de la institución (http://XXX.XX.XX.XXX/consultaexterna), misma que por privacidad y confidencialidad, no se la expone en este proyecto de investigación. Los resultados obtenidos de las pruebas realizadas se muestran a continuación:

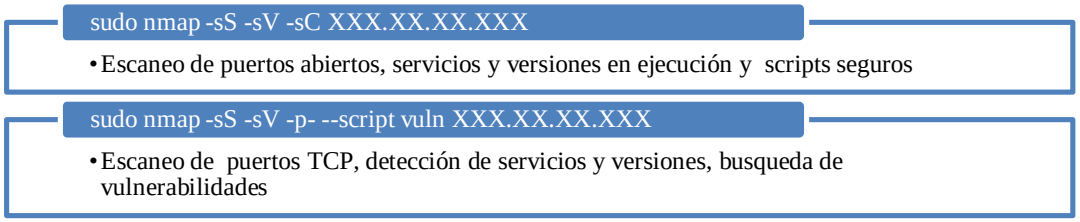


**Figura 37.** *Nmap – escaneo de puertos y vulnerabilidades*

*Nota: Comandos ejecutados escaneo al host de servicio web con IP pública*

```
msp@E0163:~$ sudo nmap -sS -sV -sC [redacted]
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-15 14:37 -05
Nmap scan report for 108.99.47.186.static.anycast.cnt-grms.ec (186.47.99.108)
Host is up (0.0043s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE              VERSION
22/tcp    open  ssh                  OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http                 Apache httpd 2.4.41 ((Ubuntu))
|_http-server-header: Apache/2.4.41 (Ubuntu)
|_http-title: Redireccionando...
10000/tcp open  ssl/snet-sensor-mgmt?
```

**Figura 38.** *Nmap – puertos abiertos*

*Nota: Resultado de escaneo puertos abiertos host de servicio web con IP pública*

```
msp@E0163:~$ sudo nmap -f -sS --script vuln [redacted]
Starting Nmap 7.80 ( https://nmap.org ) at 2025-08-15 14:44 -05
Pre-scan script results:
| broadcast-avahi-dos:
|   Discovered hosts:
|     224.0.0.251
|   After NULL UDP avahi packet DoS (CVE-2011-1002).
|_  Hosts are all up (not vulnerable).
Nmap scan report for [redacted]
Host is up (0.0068s latency).
Not shown: 997 filtered ports
PORT      STATE SERVICE
22/tcp    open  ssh
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
80/tcp    open  http
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|   /phpmyadmin/: phpMyAdmin
|   /img/: Potentially interesting directory w/ listing on 'apache/2.4.41 (ubuntu)'
|   /public/: Potentially interesting directory w/ listing on 'apache/2.4.41 (ubuntu)'
|_  /webalizer/: Potentially interesting folder
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
10000/tcp open  snet-sensor-mgmt
|_clamav-exec: ERROR: Script execution failed (use -d to debug)
| http-vuln-cve2006-3392:
|   VULNERABLE:
|   Webmin File Disclosure
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2006-3392
|       Webmin before 1.290 and Usermin before 1.220 calls the simplify_path function before decoding HTML.
|       This allows arbitrary files to be read, without requiring authentication, using "..%01" sequences
|       to bypass the removal of "../" directory traversal sequences.
```

***Figura 39. Nmap – vulnerabilidades***

*Nota: Resultado de escaneo vulnerabilidades host de servicio web con IP pública*

```
sudo nikto -h http://XXX.XX.XX.XXX/consultaexterna/

• Escaneo de vulnerabilidades
• Archivos y directorios inseguros.
• Versiones obsoletas del servidor
• Configuraciones incorrectas.
• Módulos vulnerables
• Errores comunes de seguridad
```

***Figura 40. Nikto – escaneo de vulnerabilidades***

*Nota: Comandos ejecutados para escaneo al host de servicio web con IP pública*

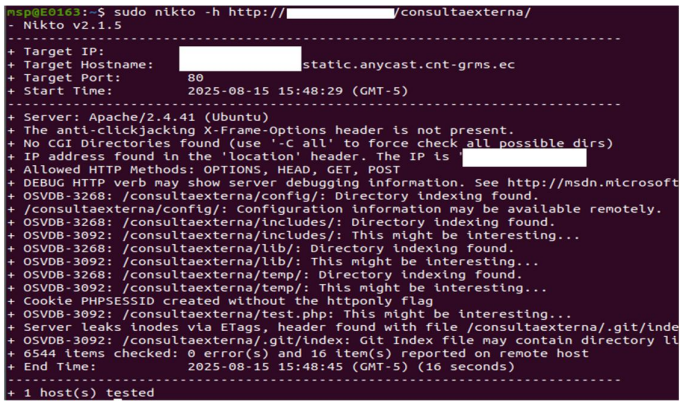



**Figura 41.** *Nikto – vulnerabilidades*

*Nota: Resultado de escaneo al host de servicio web con IP pública*

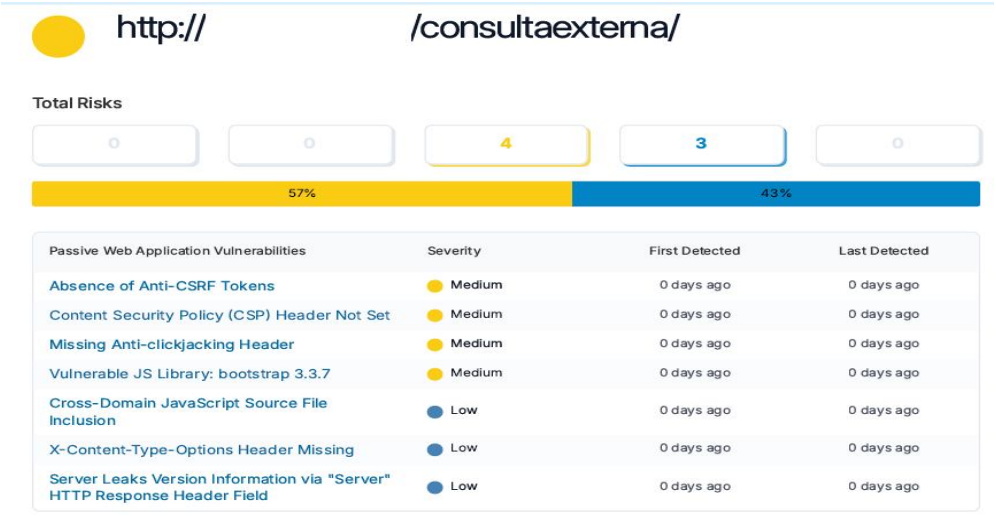



**Figura 42.** *Hostedscan – informe de Vulnerabilidades*

*Nota: Resultado de escaneo al host de servicio web con IP pública desde https://hostedscan.com*

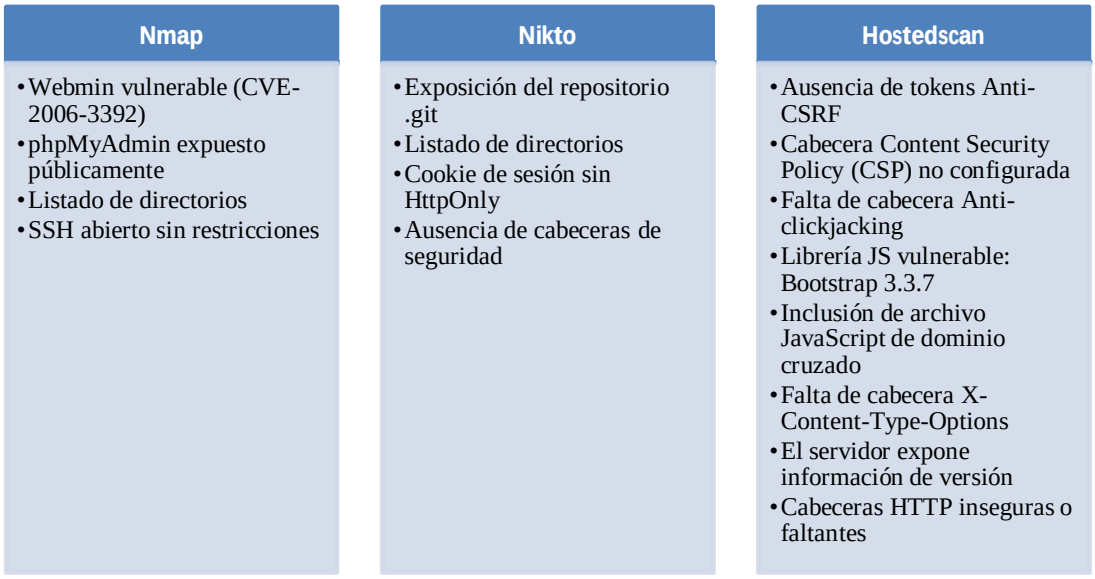



**Figura 43.** *Resumen de vulnerabilidades por herramienta de escaneo*

*Nota: Vulnerabilidades aplicación web servicio de Consulta Externa*

**Tabla 16.**

*Vulnerabilidades y salvaguardas activos de información*

| Código | Activos de Información | Vulnerabilidades | | Salvaguardias |
|---|---|---|---|---|
| **A1** | Información de pacientes y citas médicas | V1 | Controles de acceso no adecuados | H.IA Identificación y autenticación |
| | | V2 | Transmisión de datos sin cifrado | H.AC Control de acceso lógico |
| | | V3 | Falta de respaldos periódicos | D Protección de la Información |
| **A2** | Servicio de Consulta Externa | V4 | Controles de acceso no adecuados | D.A Copias de seguridad de los datos (backup) |
| | | V5 | Falta de respaldo y recuperación de datos | S.A Aseguramiento de la disponibilidad |
| **A3** | ISP - Acceso a Internet | V6 | Falta de medidas de seguridad de red | IP.SPP Sistema de protección perimetral |
| | | V7 | Dependencia a única ruta de conexión | NEW.COM Comunicaciones: Adquisición o contratación |
| | | V8 | Sin redundancia de conexión | (Redundancia de red, enlaces y dispositivos) |
| **A4** | Ubuntu Server 20.0.4 LTS | V9 | Actualizaciones de seguridad periódicas | SW Protección de las Aplicaciones Informáticas |
| | | V10 | Contraseñas débiles o predeterminadas | SW.CM Cambios (actualizaciones y mantenimiento) |
| | | V11 | Controles de acceso no adecuados | H.AC Control de acceso lógico |

| | | | | |
|---|---|---|---|---|
| | | | | H.tools Herramientas de seguridad |
| **A5** | App Web Gestión de Consulta Externa | V12 | Validación y sanitización de entradas | S.www Protección de servicios y aplicaciones web |
| | | V13 | Implementación segura de autenticación y gestión de sesiones | SW.SC Se aplican perfiles de seguridad |
| | | V14 | Controles de acceso no adecuados | SW.CM Cambios (actualizaciones y mantenimiento) |
| | | | | COM.A Aseguramiento de la disponibilidad |
| **A6** | App Web MSP PRAS | V15 | Intermitencia de aplicaciones Web externas | Redundancia de red, enlaces y dispositivos |
| **A7** | Servidor HTTP Apache | V16 | Protocolo no seguro HTTP | S.www Protección de servicios y aplicaciones web |
| | | V17 | Sin medidas de protección contra DoS. | H.tools.IDS IDS/IPS: Herramienta de detección / prevención de intrusión |
| | | | | H.tools.LA Herramienta para análisis de logs |
| **A8** | MySQL BD Consulta Externa | V18 | Contraseñas débiles o predeterminadas | H.tools.IDS IDS/IPS: Herramienta de detección / prevención de intrusión |
| | | V19 | Falta de redundancia y respaldo | H.tools Herramientas de seguridad |
| | | | | D.A Copias de seguridad de los datos (backup) |
| **A9** | HP Proliant DL380G7 | V20 | Protección contra sobretensiones | HW Protección de los Equipos Informáticos |
| | | V21 | Falta de sistema de climatización | HW.A Aseguramiento de la disponibilidad |
| | | | | HW.CM Cambios (actualizaciones y mantenimiento) |
| **A10** | Pc computadores personales | V22 | Contraseñas débiles o predeterminadas | SW Protección de las Aplicaciones Informáticas |
| | | V23 | Protección anti malware | HW.A Aseguramiento de la disponibilidad |
| | | V24 | Ausencia de mantenimiento preventivo | HW.CM Cambios (actualizaciones y mantenimiento) |
| | | V25 | Intermitencia, caidas del servicio de internet | NEW.COM Comunicaciones: Adquisición o contratación |
| **A11** | Switch D-Link DES-1024D | V26 | Contraseñas débiles o predeterminadas | HW.A Aseguramiento de la disponibilidad |
| | | V27 | Daño de dispositivo por obsolescencia o uso prolongado | HW.CM Cambios (actualizaciones y mantenimiento) |
| | | | | H.tools.TM Herramienta de monitorización de tráfico |
| **A12** | Router Linksys e900 | V28 | Contraseñas débiles o predeterminadas | HW.A Aseguramiento de la disponibilidad |

| | | | | |
|---|---|---|---|---|
| | | V29 | Daño de dispositivo por obsolescencia o uso prolongado | HW.CM Cambios y mantenimiento) |
| | | V30 | Ausencia de Firewall de borde | H.tools.TM Herramienta de monitorización de tráfico |
| **A13** | LAN CAT 6e | V31 | Daños físicos del cableado | HW.CM Cambios y mantenimiento) |
| | | V32 | Manipulación o instalación incorrecta | |
| **A14** | Alimentación Eléctrica | V33 | Fallos en generador eléctrico de respaldo | AUX.power Suministro eléctrico |
| | | V34 | Sin protección contra sobretensiones | HW.CM Cambios y mantenimiento) |
| **A15** | UPS APC BR1500M2-LM | V35 | Sobretensiones eléctricas | HW.CM Cambios y mantenimiento) |
| | | V36 | Falta de mantenimiento preventivo | |
| **A16** | Centro de Datos | V37 | Acceso físico no restringido | L.AC Control de los accesos físicos |
| | | V38 | Espacio físico inadecuado | AUX.AC Climatización |
| **A17** | Usuarios Internos | V39 | Contraseñas débiles o predeterminadas | H.AC Control de acceso lógico |
| | | V40 | Falta de controles de acceso aplicaciones | D Protección de la Información |
| **A18** | Usuarios Operadores | V41 | Falta de planes de capacitación | PS.AT Formación y concienciación |
| | | V42 | Sin monitoreo de actividades | H.ST Segregación de tareas |
| | | | | H.AC Control de acceso lógico |

*Nota: Diseño propio*

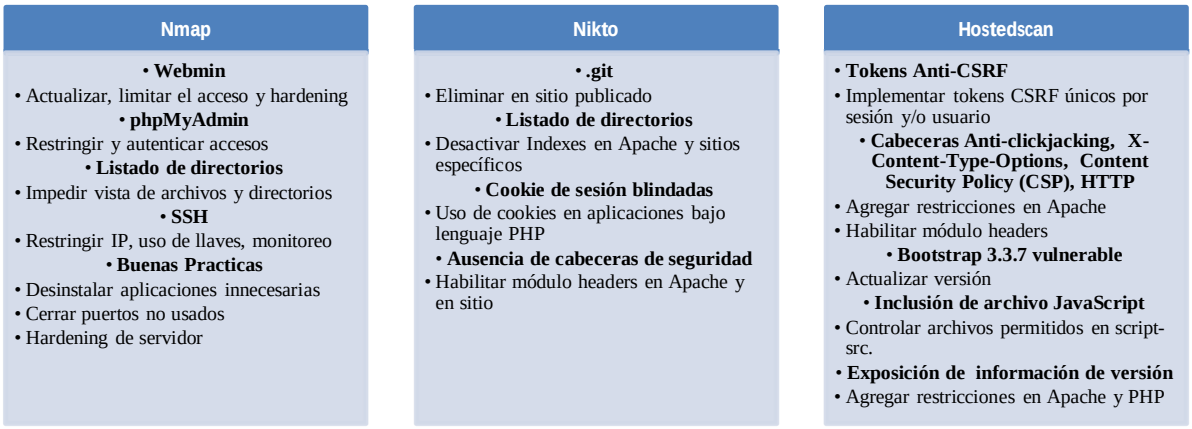



**Figura 44.** *Salvaguardias servicio web Consulta Externa*

*Nota: Diseño propio*

### *4.1.2 Métricas del servicio web de consulta externa*

En las siguientes figuras se representa la cultura organizacional y la infraestructura tecnológica del servicio de Consulta Externa con la que la cuenta el HBRMM.

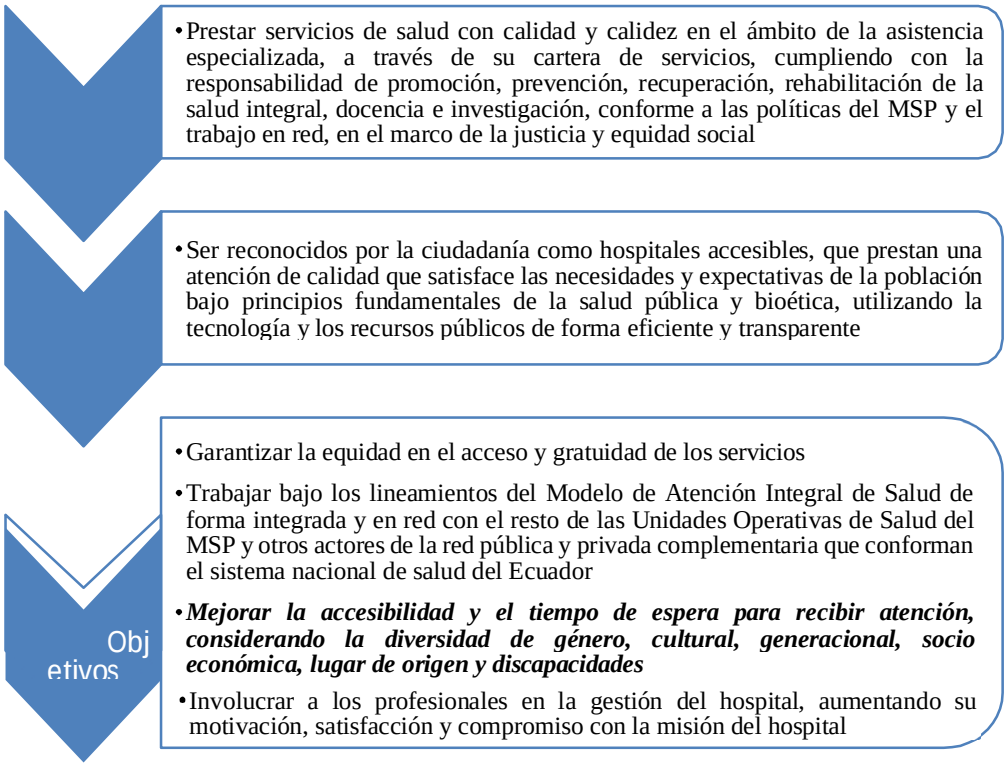



**Figura 45.** *Cultura Organizacional HBRMM*

*Nota: Basado en Estatuto Orgánico de Hospitales del MSP*

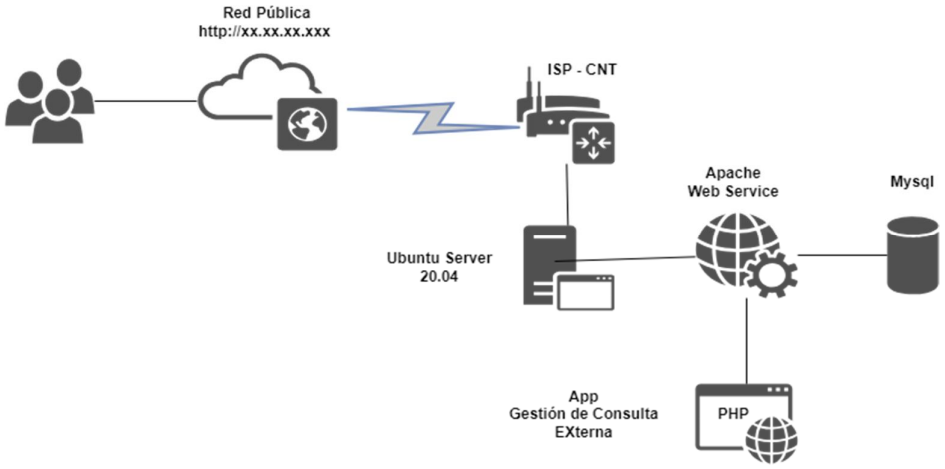



**Figura 46.** *Infraestructura tecnológica servicio web de Consulta Externa*

*Nota: Diseño propio*


**Figura 47.** *Objetivo estratégico relación servicio web de Consulta Externa*

*Nota: Diseño propio*

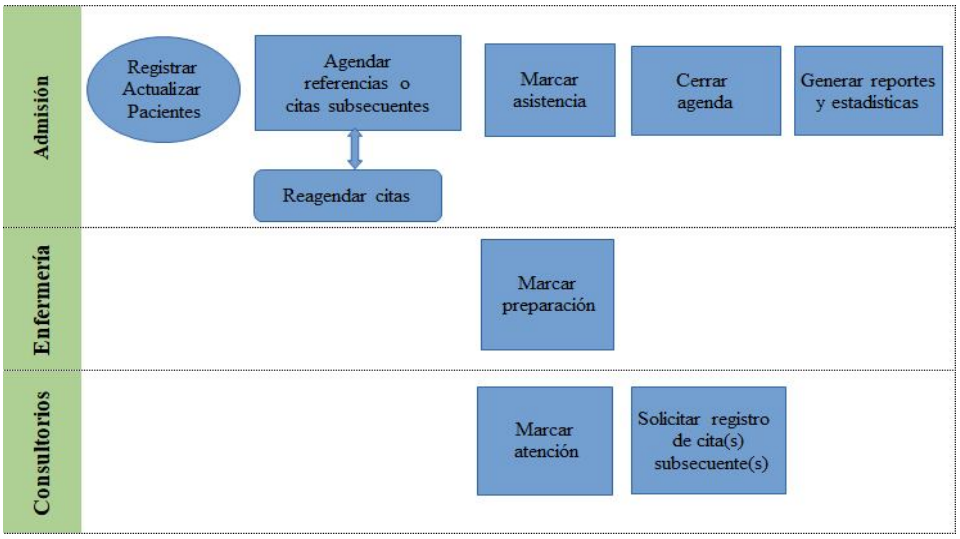



**Figura 48.** *Funcionalidad de App web de Consulta Externa*

*Nota: Diseño propio*

A continuación, se presenta el resultado del análisis de archivos de registro (logs) del servicio web Apache, estos fueron extraídos con la herramienta webalyzer y tienen relación con la funcionalidad, usabilidad y seguridad.

**Summary by Month**

| Month | Daily Avg | | | | Monthly Totals | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | Hits | Files | Pages | Visits | Sites | kB F | Visits | Pages | Files | Hits |
| Jun 2025 | 93129 | 77603 | 69972 | 450 | 4141 | 34032602 | 11268 | 1749314 | 1940090 | 2328248 |
| May 2025 | 73199 | 61576 | 54808 | 367 | 4100 | 47639989 | 11403 | 1699069 | 1908858 | 2269197 |
| Apr 2025 | 78632 | 67949 | 60289 | 305 | 3103 | 41657624 | 9157 | 1808695 | 2038492 | 2358972 |
| Mar 2025 | 72534 | 63641 | 55412 | 322 | 3599 | 41118823 | 9983 | 1717782 | 1972874 | 2248564 |
| Feb 2025 | 72630 | 63693 | 54712 | 376 | 4521 | 42986949 | 10541 | 1531939 | 1783418 | 2033667 |
| Jan 2025 | 65179 | 56123 | 48241 | 292 | 3098 | 82294434 | 9062 | 1495500 | 1739837 | 2020556 |
| Dec 2024 | 44909 | 38669 | 32139 | 186 | 1120 | 19378257 | 2615 | 449946 | 541373 | 628738 |
| **Totals** | | | | | | **309108678** | **64029** | **10452245** | **11924942** | **13887942** |

**Figura 49.** *Resumen mensual de estadísticas y tráfico de servicio web Apache*

*Nota: Obtenidos con webalizer a partir de logs del servidor*

**Tabla 17.**

*Páginas o recursos más usados del sitio logs Apache*

| Métrica | Número de URLs | Hits Totales | URLs principales |
|---|---|---|---|
| Funcionalidad | 6 | 39,436 | turnos_llamar.php, tur_insertar_profesional.php, tur_preparacion_procesar_confirmar.php, tur_insertar_procesar.php |
| Usabilidad | 5 | 44,505 | bootstrap.min.css, bootstrap-datepicker.js, all.min.css, fontello.css, jquery-3.1.1.min.js, bootstrap-datepicker.css |
| Funcionalidad / Usabilidad | 3 | 27,565 | hcu-search.php, tur_preparacion.php, menu_agendamiento.php, tarjeta_indice_consultas.php |

*Nota. Obtenidos con webalizer /var/log/apache2/access.log junio 2025*

Interpretación: la funcionalidad está relacionada con procesos críticos del sistema, como el registro de citas, la usabilidad corresponde archivos de CSS y JS que afectan la interfaz y experiencia de usuario, la funcionalidad / usabilidad representan páginas funcionales y de experiencia de usuario, como buscadores o menús.

| Métrica | Código http | Descripción | Porcentaje | Hits |
|---|---|---|---|---|
| Funcionalidad Seguridad | Undefined | Código indefinido | 12.30% | 13,715 |
| Funcionalidad | 200 | OK | 83.33% | 92,918 |
| Funcionalidad | 201 | Created | 0.43% | 479 |
| Funcionalidad | 204 | No Content | 0.03% | 33 |
| Funcionalidad Usabilidad | 206 | Partial Content | 0.01% | 11 |
| Funcionalidad | 301 | Moved Permanently | 0.02% | 22 |
| Funcionalidad | 302 | Found | 0.65% | 725 |
| Funcionalidad | 303 | See Other | 0.26% | 290 |
| Usabilidad Rendimiento | 304 | Not Modified | 0.34% | 379 |

| | | | | |
|---|---|---|---|---|
| Funcionalidad Seguridad | 400 | Bad Request | 0.04% | 45 |
| Seguridad | 401 | Unauthorized | 0.01% | 11 |
| Seguridad | 403 | Forbidden | 0.00% | 0 |
| Usabilidad Funcionalidad | 404 | Not Found | 2.42% | 2,698 |
| Seguridad Funcionalidad | 405 | Method Not Allowed | 0.00% | 0 |
| Usabilidad Seguridad | 408 | Request Timeout | 0.15% | 167 |
| Funcionalidad | 409 | Conflict | 0.00% | 0 |
| Funcionalidad | 412 | Precondition Failed | 0.00% | 0 |
| Funcionalidad Seguridad | 500 | Internal Server Error | 0.00% | 0 |

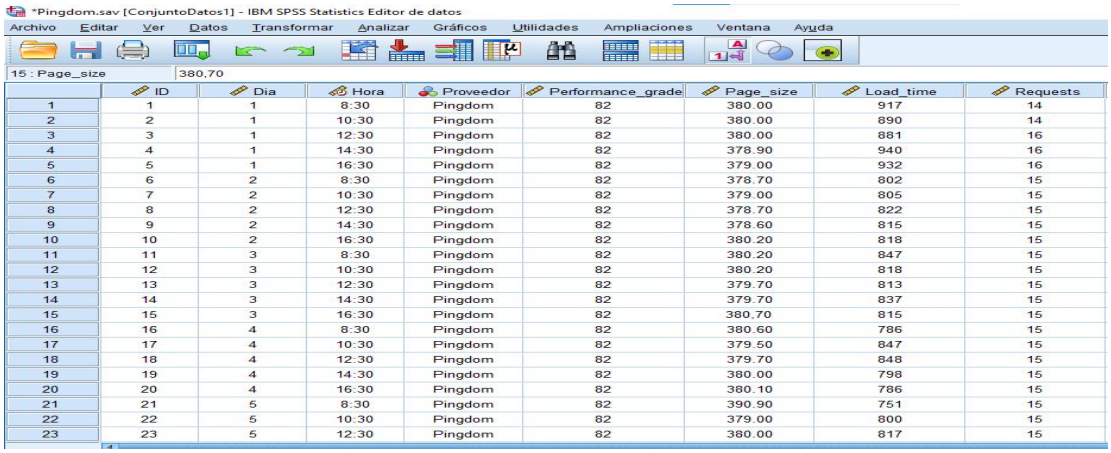
*Nota. Obtenidos con webalizer /var/log/apache2/error.log junio 2025*

Interpretación: El rendimiento y funcionalidad indica que la mayoría de hits (83.33%) son 200 OK, indica que el servidor funciona correctamente y la aplicación responde bien a la mayoría de las solicitudes, en seguridad pocos hits con códigos 401 (Unauthorized) y 400 (Bad Request) indica intentos mínimos de accesos no autorizados o errores de entrada. No hay códigos 500 ni 403, es decir no se reportan fallos graves ni accesos bloqueados.

Mediante el uso de herramienta Pingdom Speed Test a se evaluó el rendimiento del servicio web (http://XXX.XX.XX.XXX/consultaexterna/), la cual proporcionó indicadores relevantes como tamaño de la página, tiempo de carga, número de solicitudes y calificación de rendimiento.

**Tabla 18.**

*Registro de datos para análisis de rendimiento App Consulta Externa*



*Pingdom.sav [ConjuntoDatos1] - IBM SPSS Statistics Editor de datos

Archivo Editar Ver Datos Transformar Analizar Gráficos Utilidades Ampliaciones Ventana Ayuda

15 : Page_size 380,70

| | ID | Dia | Hora | Proveedor | Performance_grade | Page_size | Load_time | Requests |
|---|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 8:30 | Pingdom | 82 | 380.00 | 917 | 14 |
| 2 | 2 | 1 | 10:30 | Pingdom | 82 | 380.00 | 890 | 14 |
| 3 | 3 | 1 | 12:30 | Pingdom | 82 | 380.00 | 881 | 16 |
| 4 | 4 | 1 | 14:30 | Pingdom | 82 | 378.90 | 940 | 16 |
| 5 | 5 | 1 | 16:30 | Pingdom | 82 | 379.00 | 932 | 16 |
| 6 | 6 | 2 | 8:30 | Pingdom | 82 | 378.70 | 802 | 15 |
| 7 | 7 | 2 | 10:30 | Pingdom | 82 | 379.00 | 805 | 15 |
| 8 | 8 | 2 | 12:30 | Pingdom | 82 | 378.70 | 822 | 15 |
| 9 | 9 | 2 | 14:30 | Pingdom | 82 | 378.60 | 815 | 15 |
| 10 | 10 | 2 | 16:30 | Pingdom | 82 | 380.20 | 818 | 15 |
| 11 | 11 | 3 | 8:30 | Pingdom | 82 | 380.20 | 847 | 15 |
| 12 | 12 | 3 | 10:30 | Pingdom | 82 | 380.20 | 818 | 15 |
| 13 | 13 | 3 | 12:30 | Pingdom | 82 | 379.70 | 813 | 15 |
| 14 | 14 | 3 | 14:30 | Pingdom | 82 | 379.70 | 837 | 15 |
| 15 | 15 | 3 | 16:30 | Pingdom | 82 | 380,70 | 815 | 15 |
| 16 | 16 | 4 | 8:30 | Pingdom | 82 | 380.60 | 786 | 15 |
| 17 | 17 | 4 | 10:30 | Pingdom | 82 | 379.50 | 847 | 15 |
| 18 | 18 | 4 | 12:30 | Pingdom | 82 | 379.70 | 848 | 15 |
| 19 | 19 | 4 | 14:30 | Pingdom | 82 | 380.00 | 798 | 15 |
| 20 | 20 | 4 | 16:30 | Pingdom | 82 | 380.10 | 786 | 15 |
| 21 | 21 | 5 | 8:30 | Pingdom | 82 | 390.90 | 751 | 15 |
| 22 | 22 | 5 | 10:30 | Pingdom | 82 | 379.00 | 800 | 15 |
| 23 | 23 | 5 | 12:30 | Pingdom | 82 | 380.00 | 817 | 15 |

*Nota: Pruebas realizadas durante 30 días con pingdom.com*

**Tabla 19.**

*Resumen de análisis de rendimiento App Consulta Externa*

**Estadísticos descriptivos**

| | N | Mínimo | Máximo | Media | Desv. Desviación |
|---|---|---|---|---|---|
| Calificación de rendimiento | 155 | 82 | 82 | 82,00 | ,000 |
| Tamaño de la página | 155 | 378.60 | 390.90 | 382.7587 | 2.54560 |
| Tiempo de carga | 155 | 711 | 2,200 | 837.15 | 121.143 |
| Solicitudes | 155 | 14 | 16 | 15,01 | ,180 |
| N válido (por lista) | 155 | | | | |

*Nota. Media de pruebas realizadas con https://tools.pingdom.com*

**Tabla 20.**

*Análisis con https://tools.pingdom.com*

| Métrica | Indicador | Valor |
|---|---|---|
| Funcionalidad<br>Requests (Solicitudes) | Número de recursos necesarios para cargar la página. | 14 – 16 solicitudes |
| Usabilidad<br>Load_time (Tiempo de carga) | Tiempo en ms/segundos | Promedio ~830 ms (picos hasta 2200 ms) |
| Usabilidad<br>Page_size (Tamaño de la página) | Peso total en KB/MB | 378 – 390 KB |
| Usabilidad<br>Performance_grade | Calificación (0–100) de optimización web | 82/100 |

| | | |
|---|---|---|
| Seguridad | Encabezados de seguridad y configuración del servidor | 82 sin tráfico https |
| Performance_grade (parcial) | | |

*Nota. Mediciones al sitio (http://XXX.XX.XX.XXX/consultaexterna/)*

Interpretación: La funcionalidad en requests (14 – 16 solicitudes) permite consistencia funcional, en usabilidad load_time (~830 ms promedio) es aceptable sin embargo existen intermitencias, page_size (378 – 390 KB) revela un sitio ligero, performance_grade (82/100 sin https) aceptable, pero requiere optimización (>90), en seguridad la ausencia de https representa un riesgo crítico.

Mediante el uso de la herramienta para desarrolladores integrada en el navegador web Google Chrome se presenta el resultado del análisis a las funciones principales de la aplicación web, como se muestra en la siguiente figura.

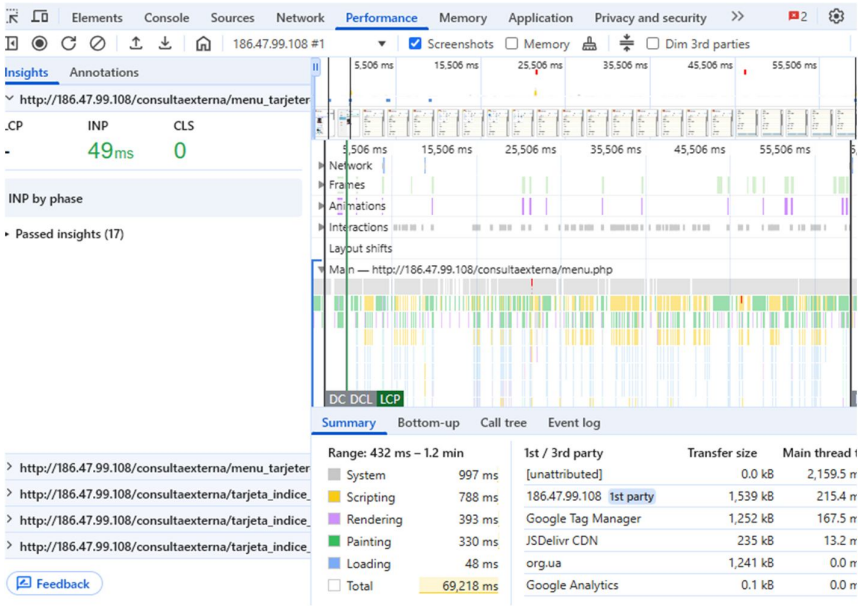



**Figura 50.** *Análisis con herramienta integrada en el navegador Google Chrome*

*Nota: Pruebas de rendimiento a http://XXX.XX.XX.XXX/consultaexterna/*

**Tabla 21.**

*Análisis de funciones con herramienta para desarrolladores*

| Función en servicio Web | Métrica | Indicador | Valor esperado | Valor observado |
|---|---|---|---|---|
| Registro de paciente | Usabilidad | Tiempo promedio | <= 3 min | 1.50 min |
| Actualización de datos | Usabilidad | Tiempo promedio | <= 3 min | 1.50 min |

| | | | | |
|---|---|---|---|---|
| Registro y actualización de datos | Seguridad | Acceso controlado | 100% | 100% |
| Agendamiento de cita | Usabilidad | Tiempo promedio | <= 3 min | 2 min |
| | Seguridad | Acceso controlado | 100% | 100% |
| Generación de reportes y estadísticas | Usabilidad | Tiempo promedio | <= 5 min | 1 min |
| | Seguridad | Acceso controlado | 100% | 100% |
| Confirmación de registro de signos vitales | Usabilidad | Tiempo promedio | <= 2 min | 1 min |
| | Seguridad | Integridad y confidencialidad | 100% | 100% |
| | Seguridad | Acceso controlado a registro | 100% | 100% |
| Notificación a sala de espera | Usabilidad | Tiempo promedio | <= 30 seg | 30 seg |
| | Seguridad | Acceso seguro | 100% | 0% |
| Registro de citas subsecuente | Usabilidad | Tiempo promedio de registro | <= 3 min | 2 min |
| | Seguridad | Acceso controlado | 100% | 100% |

*Nota. Mediciones al sitio (http://XXX.XX.XX.XXX/consultaexterna/)*

Interpretación: La usabilidad (tiempos) se cumplen con los tiempos esperados refleja un aplicación rápida y eficiente, la seguridad es parcial con accesos controlados, la confidencialidad e integridad no están aseguradas para datos sensibles, acceso inseguro en notificación a la sala de espera, no se encuentra implementado el cifrado de datos en tránsito (TLS/HTTPS).

### *4.1.3 Prueba de concepto*

A continuación, se muestra el modelado de la arquitectura de seguridad con ArchiMate Core Framework (UML), donde se representan las aplicaciones, servicios, actores y componentes que son desplegados en un servidor VPS con alta disponibilidad, con el uso de herramientas de software libre.

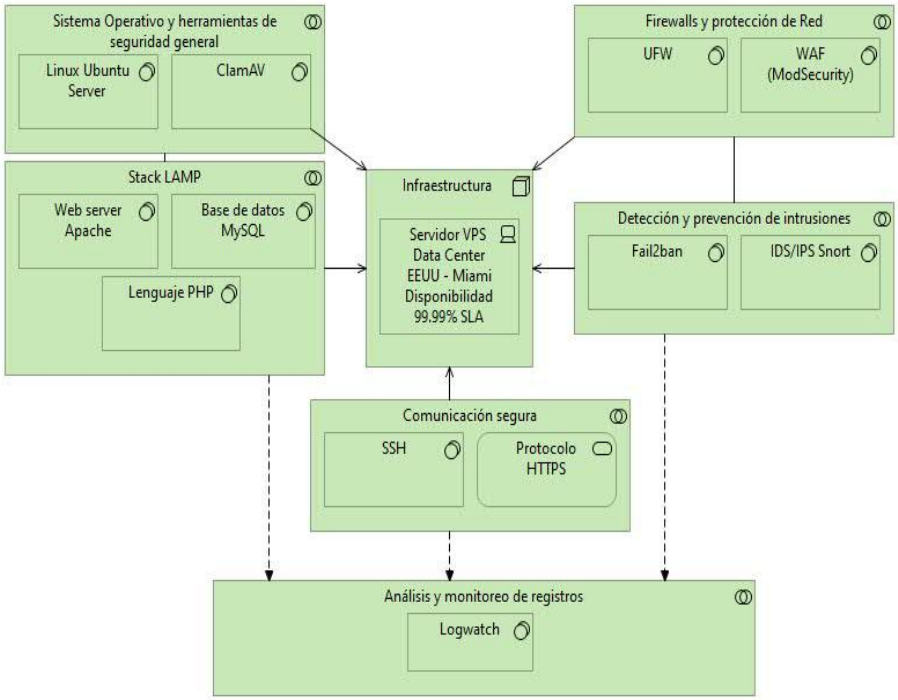



**Figura 51.** *Capa de Tecnología – Infraestructura y software*

*Nota: Diseño propio*

Explicación: El diagrama muestra en la capa de tecnología el uso de un servidor VPS remoto con alta disponibilidad, con un SO Ubuntu Server y antivirus ClamAV, pila LAMP (Apache, MySQL, PHP) para despliegue de aplicaciones en lenguaje PHP, Firewall de sistema (UFW) y de aplicaciones web (WAF), prevención de ataques de fuerza bruta (Fail2ban), detección y prevención de intrusiones (Snort IDS/IPS), comunicación segura (SSH y HTTPS) y Logwatch para monitorización de registros.

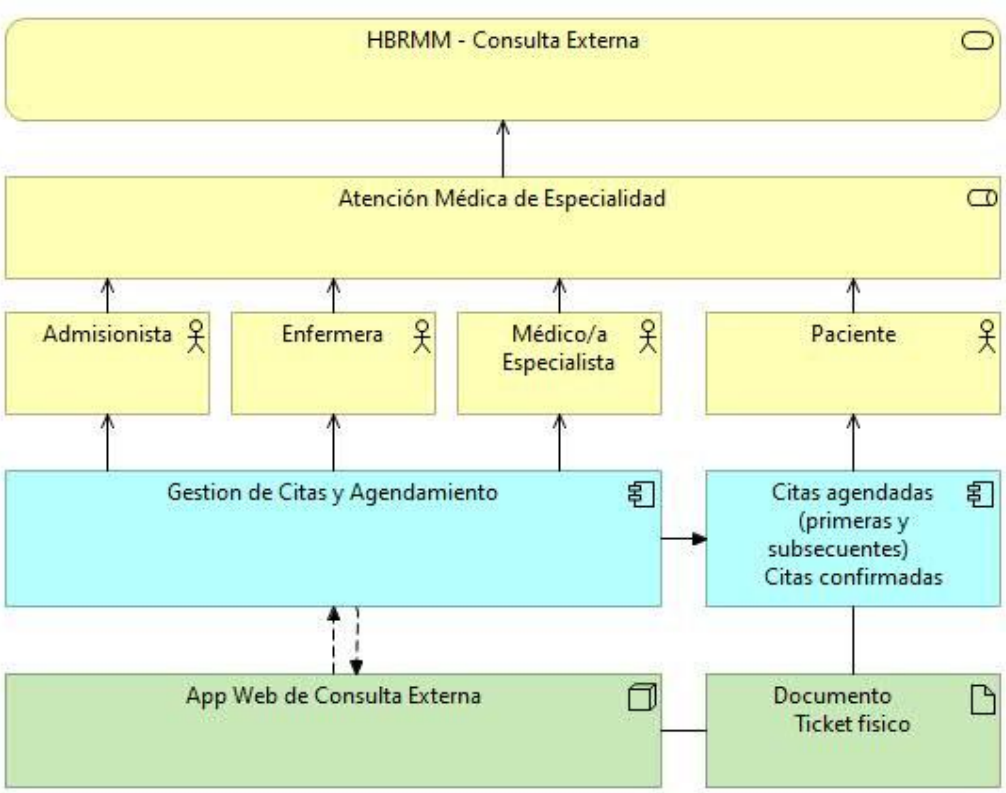



**Figura 52.** *Servicio de Consulta Externa - Capas de negocio, aplicación y tecnología*

*Nota: Diseño propio*

Explicación: El diagrama integra las capas de negocio, aplicación y tecnología, mostrando la interacción entre roles, servicios y aplicaciones del área de consulta externa del HBRMM. La capa de negocio refleja la provisión de atenciones médicas de especialidad como unidad operativa de segundo nivel del MSP. Los actores de negocio se alinean a las actividades desarrolladas por Admisión, Enfermería y Consulta, que como actores clave involucran al personal administrativo, médicos y enfermeras.

La capa de aplicación permite la gestión de citas y agendamiento, facilitando la creación, confirmación y seguimiento de citas hasta el día que se realiza la atención del paciente, en base a su cita programada. En este caso, el ticket físico evidencia el registro de citas, sean estas primeras o subsecuentes.

En la capa de tecnología la aplicación Web de la institución mantiene y respalda la continuidad del servicio de consulta externa.

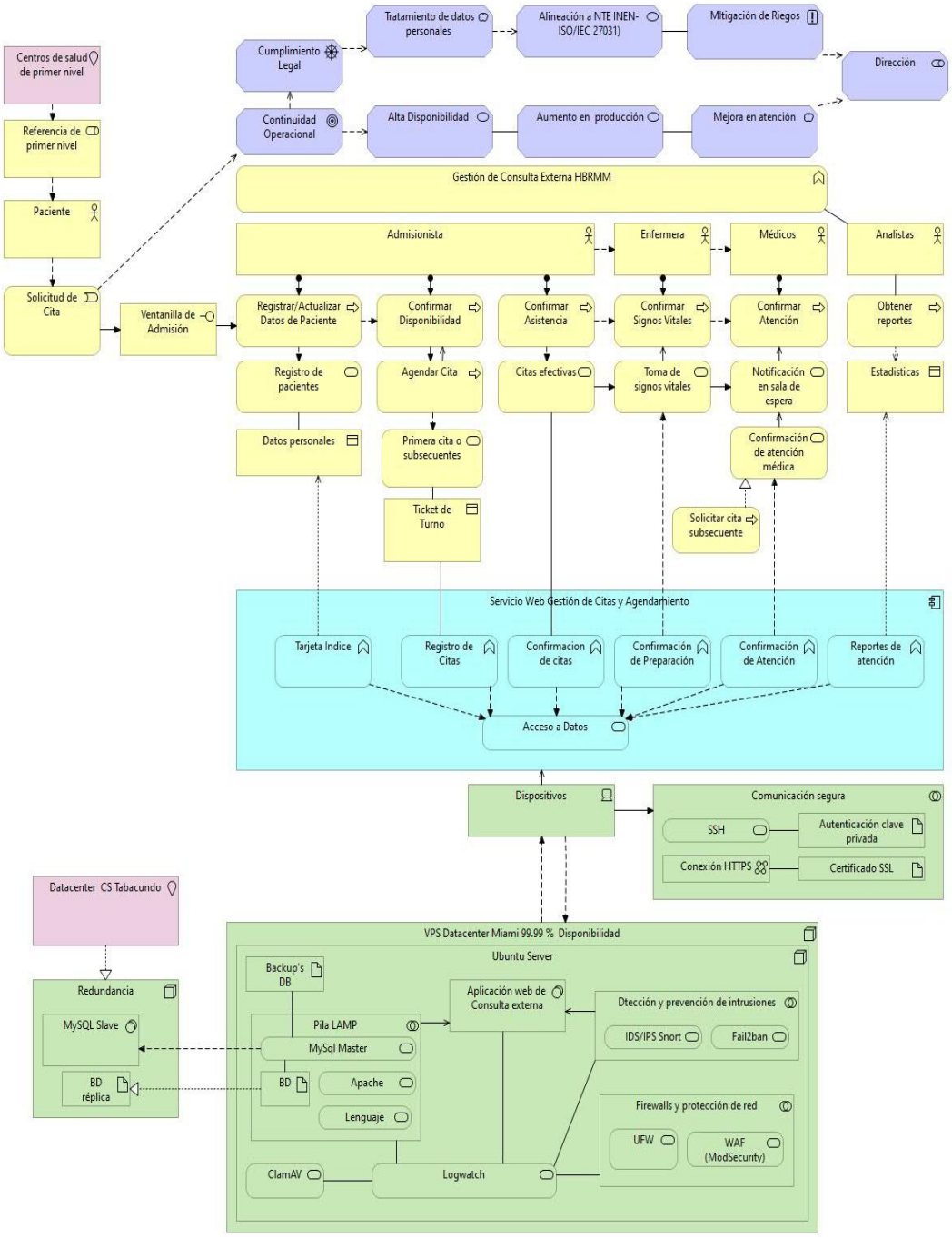



**Figura 53.** *Arquitectura de seguridad desplegada en https://hospitalbasicocayambe.online/*

*Nota: Diseño propio*

Explicación: La figura representa la gestión del servicio de Consulta Externa del HBRMM modelada en cuatro capas. Establece el punto de partida desde los centros de salud de primer nivel del MSP para la atención de especialidad. En la capa de negocio se definen actores, roles, procesos y funciones. En la capa de aplicación se modela el Sistema Web de Gestión Citas y Agendamiento, que soporta el flujo administrativo y de atención médica. La

capa de tecnología define la infraestructura, software y las herramientas necesarias para el funcionamiento de la capa de aplicación, además de mecanismos de seguridad y redundancia. Finalmente, en la capa de motivación se justifica este modelo que permite garantizar el cumplimiento legal, continuidad y la disponibilidad, esto se traduce en la mejora del servicio de atención el área de Consulta Externa del HBRMM.

En las siguientes figuras se muestran los componentes principales desplegados para la arquitectura de seguridad propuesta para el servicio web de Consulta Externa del HBRMM de Cayambe, usando como infraestructura un servidor VPS ubicado en la ciudad de Miami que cuenta con una disponibilidad del 99.99 % y basado en herramientas de software libre.

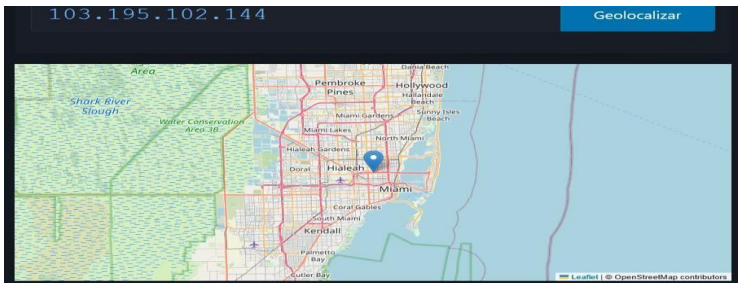



**Figura 54.** *Geolocalización de IP pública servidor VPS Miami*

*Nota: Obtenido de https://www.cual-es-mi-ip.net/geolocalizar-ip-mapa*


**Figura 55.** *Página inicial aplicación web de Consulta Externa desplegada*

*Nota: Acceso a sitio de prueba de concepto https://hospitalbasicocayambe.online/*

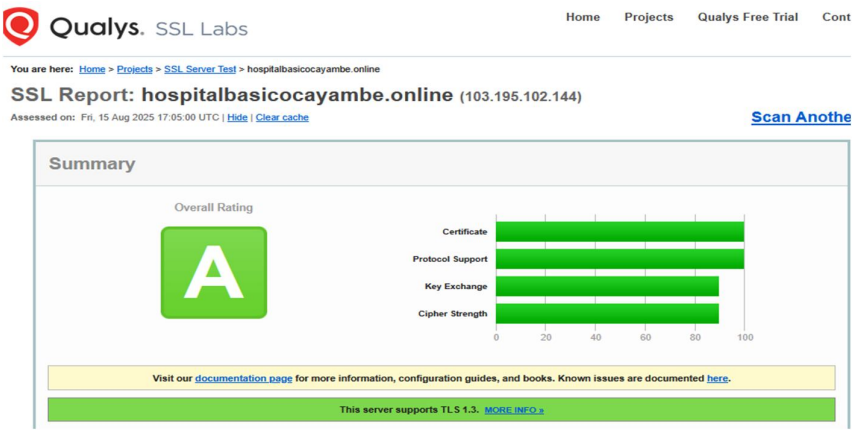



**Figura 56.** *Informe SSL de hospitalbasicocayambe.online*

*Nota: Prueba realizada desde [https://www.ssllabs.com/ssltest/](https://www.ssllabs.com/ssltest/)*

```
msp@E0163:~$ ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/msp/.ssh/id_rsa): hbconline
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in hbconline
Your public key has been saved in hbconline.pub
The key fingerprint is:
SHA256:UGpOM4HM+zoQISQVo8deY+RVYFZZe1KublGcqF/RVgA msp@E0163
The key's randomart image is:
+---[RSA 4096]----+
|oo++..*++o. E....|
|oo.+++ +.  * o . |
|..o.=.B   + B o  |
| o.o.= + . = o   |
|  .. .. S o .    |
|  .   .  o o     |
|   . .    +      |
|    o    .       |
|     .           |
+----[SHA256]-----+
```

**Figura 57.** *Generación de claves privada y pública para acceso vía SSH*

*Nota: Se usa el algoritmo RSA de 4096 bits*

```
root@hospitalbasicocayambe: /home/franklin
root@hospitalbasicocayambe:/home/franklin# sudo service fail2ban status
● fail2ban.service - Fail2Ban Service
     Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vend
     Active: active (running) since Fri 2025-09-19 17:28:35 -05; 3 days
       Docs: man:fail2ban(1)
   Main PID: 3235271 (f2b/server)
      Tasks: 5 (limit: 9413)
     Memory: 20.1M
     CGroup: /system.slice/fail2ban.service
             └─3235271 /usr/bin/python3 /usr/bin/fail2ban-server -xf sta

sep 19 17:28:35 hospitalbasicocayambe.online systemd[1]: Stopped Fail2Ba
sep 19 17:28:35 hospitalbasicocayambe.online systemd[1]: Starting Fail2B
sep 19 17:28:35 hospitalbasicocayambe.online systemd[1]: Started Fail2Ba
sep 19 17:28:36 hospitalbasicocayambe.online fail2ban-server[3235271]: S
root@hospitalbasicocayambe:/home/franklin#
```

**Figura 58.** *Servicio Fail2ban en ejecución*

*Nota: Habilitado al arranque del SO consumo de recursos mínimo*

```
root@hospitalbasicocayambe:/home/franklin# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip

To                         Action      From
--                         ------      ----
80,443/tcp (Apache Full)   ALLOW IN    Anywhere
10000/tcp                  DENY IN     Anywhere
10022/tcp                  ALLOW IN    Anywhere
80,443/tcp (Apache Full (v6)) ALLOW IN    Anywhere (v6)
10000/tcp (v6)             DENY IN     Anywhere (v6)
10022/tcp (v6)             ALLOW IN    Anywhere (v6)
```

**Figura 59.** *UFW reglas activas de firewall*

*Nota: Tráfico HTTP/HTTPS (80/443) permitido y SSH no expuesto en puerto estándar*

```
root@hbcayambe: ~
root@hbcayambe:~# dpkg -l libapache2-mod-security2
Deseado=desconocido(U)/Instalar/eliminaR/Purgar/retener(H)
| Estado=No/Inst/ficheros-Conf/desempaqUetado/medio-conF/medio-inst(H)/espera-disparo(W)/pendienTe-disparo
|/ Err?=(ninguno)/requiere-Reinst (Estado,Err: mayúsc.=malo)
||/ Nombre                 Versión          Arquitectura Descripción
+++-======================-================-============-=================================================
ii  libapache2-mod-security2 2.9.3-1ubuntu0.1 amd64        Tighten web applications security for Apache
root@hbcayambe:~#
```

**Figura 60.** *Web Aplication Firewall (WAF) en ejecución*

*Nota: Firewall de aplicación web filtrado, monitoreo y bloqueo de tráfico HTTP/S malicioso*

En la siguiente figura se muestra el resultado de la ejecución del comando curl -v https://hospitalbasicocayambe.online?param=<script>alert(1)</script> que envía un payload de prueba XSS al servidor, el resultado en términos de ModSecurity / WAF.

```
root@hospitalbasicocayambe:~# curl -v "https://hospitalbasicocayambe.online
*   Trying 103.195.102.144:443...
* TCP_NODELAY set
* Connected to hospitalbasicocayambe.online (103.195.102.144) port 443 (#0)
* ALPN, offering h2
* ALPN, offering http/1.1
* successfully set certificate verify locations:
*   CAfile: /etc/ssl/certs/ca-certificates.crt
  CApath: /etc/ssl/certs
* TLSv1.3 (OUT), TLS handshake, Client hello (1):
* TLSv1.3 (IN), TLS handshake, Server hello (2):
* TLSv1.3 (IN), TLS handshake, Encrypted Extensions (8):
* TLSv1.3 (IN), TLS handshake, Certificate (11):
* TLSv1.3 (IN), TLS handshake, CERT verify (15):
* TLSv1.3 (IN), TLS handshake, Finished (20):
* TLSv1.3 (OUT), TLS change cipher, Change cipher spec (1):
* TLSv1.3 (OUT), TLS handshake, Finished (20):
* SSL connection using TLSv1.3 / TLS_AES_256_GCM_SHA384
* ALPN, server accepted to use http/1.1
* Server certificate:
*  subject: CN=hospitalbasicocayambe.online
*  start date: Sep 11 05:07:38 2025 GMT
*  expire date: Dec 10 05:07:37 2025 GMT
*  subjectAltName: host "hospitalbasicocayambe.online" matched cert's "hosp
*  issuer: C=US; O=Let's Encrypt; CN=R12
*  SSL certificate verify ok.
> GET /?param=<script>alert(1)</script> HTTP/1.1
> Host: hospitalbasicocayambe.online
> User-Agent: curl/7.68.0
> Accept: */*
>
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
* TLSv1.3 (IN), TLS handshake, Newsession Ticket (4):
* old SSL session ID is stale, removing
* Mark bundle as not supporting multiuse
< HTTP/1.1 403 Forbidden
< Date: Fri, 19 Sep 2025 21:11:22 GMT
< Server: Apache/2.4.41 (Ubuntu)
< Content-Length: 294
< Content-Type: text/html; charset=iso-8859-1
<
<!DOCTYPE HTML PUBLIC "-//IETF//DTD HTML 2.0//EN">
<html><head>
<title>403 Forbidden</title>
```

**Figura 61.** *Aplication Firewall (WAF) resultado test con payload OWASP CRS 3.2.0*

*Nota: ModSecurity activo payload de prueba, detección de patrones de XSS cmf y bloqueo de petición*

El resultado de la aplicación de seguridad para cabeceras recomendadas por OWASP, incluyendo HTTP Strict Transport Security. (HSTS) y anti-clickjacking, mediante el comando (curl -I https://hospitalbasicocayambe.online), i se muestra figura siguiente:

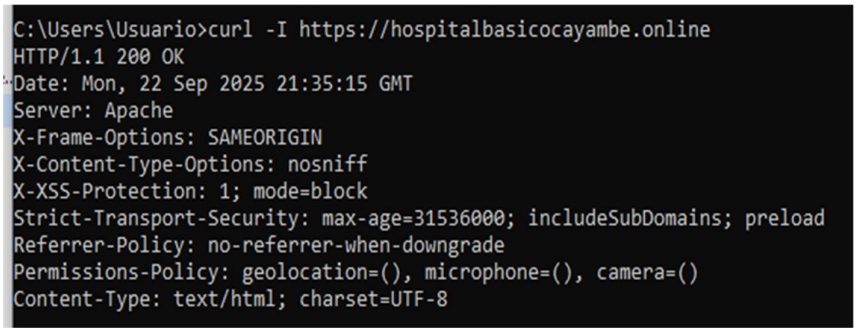



**Figura 62.** *Respuesta Cabeceras HTTP de seguridad*

*Nota: Envío mediante el comando curl -I*

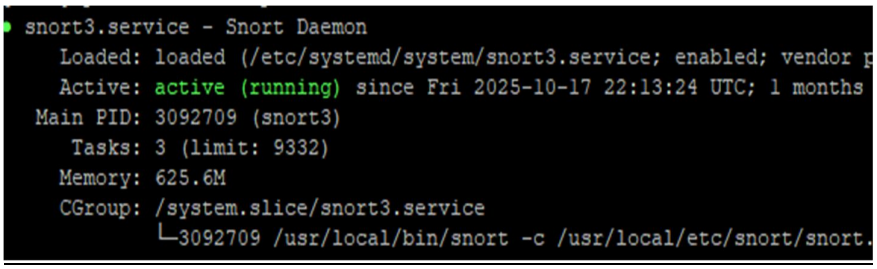



**Figura 633.** *Servicio de Snort activo y en ejecución*

*Nota: En modo IDS escucha el tráfico (passive mode)*

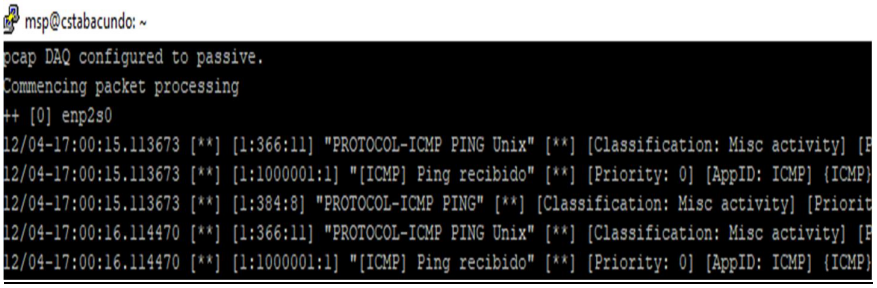



**Figura 644.** *Snort IDS analizando tráfico*

*Nota: Muestra por consola la alerta de ping recibido*

### *4.1.4 Evaluación de cumplimiento*

Como punto de partida para el análisis de cumplimento, se aplicó una encuesta a la prueba de concepto desplegada en el VPS contratado (https://hospitalbasicocayambe.online/), esta recoge las apreciaciones de 20 usuarios internos del HBRMM respecto al servicio web seguro con mejoras planteadas, considerando la limitación de la prueba de concepto que permite mantener en paralelo dos aplicaciones de agendamiento y gestión de citas médicas , además tratándose de servicios de salud públicos, la confidencialidad de los pacientes no debe ser expuesta en pruebas con registros reales.

#### 4.1.4.1 Caracterización de la muestra

La muestra incluyó veinte colaboradores del Hospital Básico Raúl Maldonado Mejía con distribución por área que respeta el peso operativo del servicio: Médica once casos equivalentes al 55% con Enfermería dos casos que representan el 10% con Administración-Estadística cuatro casos para el 20% con Tecnologías de la Información dos casos que suman el 10% con Otros un caso que alcanza el 5%. La cobertura resultante integra perfiles asistenciales con operativos que intervienen en el flujo de Consulta Externa con peso preponderante del grupo médico.

Pregunta 1 Área de trabajo del encuestado

**Tabla 22.**

*Pregunta 1*

**Área de trabajo**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Administrativa | 4 | 20,0 | 20,0 | 20,0 |
| | Enfermería | 2 | 10,0 | 10,0 | 30,0 |
| | Médica | 11 | 55,0 | 55,0 | 85,0 |
| | Otro | 1 | 5,0 | 5,0 | 90,0 |
| | TIC | 2 | 10,0 | 10,0 | 100,0 |
| | Total | 20 | 100,0 | 100,0 | |

*Nota. Identificación del área de trabajo de personal interno encuestado*

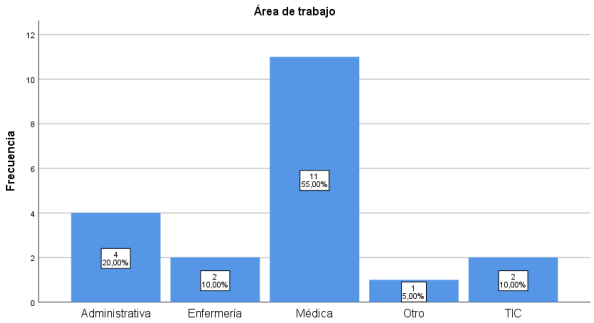



**Figura 655.** *Pregunta 1*

*Nota: Diseño propio*

**Análisis e interpretación**

El resultado a esta pregunta indica que: el 55% de los encuestados corresponde a profesionales de la salud del área médica, el 20% del área administrativa que comprende a personal de estadística y directivo, de manera similar 10% a profesionales de enfermería y de TIC, el de 5% restante a otros profesionales de la salud; lo que demuestra que todo el talento humano que interviene en el servicio fue considerado.

Pregunta 2 ¿Considera que el acceso al servicio web de Consulta Externa es sencillo y rápido?

**Tabla 23.**

*Pregunta 2*

**Acceso sencillo y rápido**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | De acuerdo | 3 | 15,0 | 15,0 | 15,0 |
| | Muy de acuerdo | 15 | 75,0 | 75,0 | 90,0 |
| | Neutral | 2 | 10,0 | 10,0 | 100,0 |
| | Total | 20 | 100,0 | 100,0 | |

*Nota. Se asocia a usabilidad del sistema*

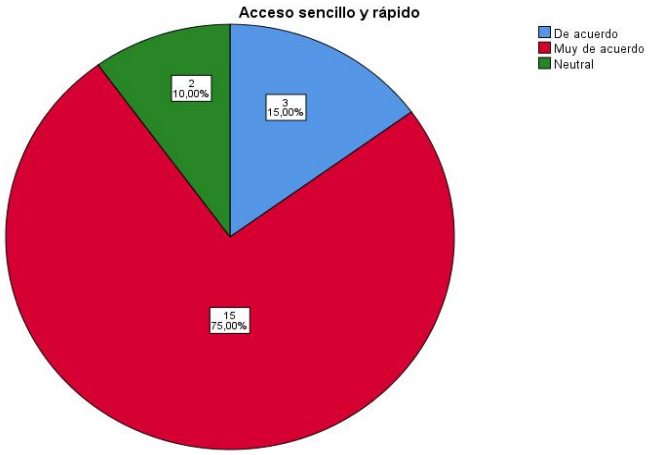



**Figura 666.** *Pregunta 2*

*Nota: Diseño propio*

**Análisis e interpretación**

El resultado a esta pregunta indica que: 90% de los usuarios internos ofrecen una apreciación favorable sobre el acceso sencilla y rápido a la aplicación, considerando que esto ya no se realiza con el número de IP, sino con un nombre de dominio, el restante 10% se pronuncia de manera neutral y ningún usuario está en desacuerdo.

El rendimiento percibido coincide con la evidencia técnica porque la página reduce redirecciones con un dominio estable, además el servidor VPS limita esperas por lectura de disco gracias a los recursos asignados.

Pregunta 3 ¿Ha notado alguna mejora en la velocidad de respuesta del sistema web después del despliegue de la arquitectura de seguridad?

**Tabla 24.**

*Pregunta 3*

**Mejora en velocidad respuesta**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Sí ligeramente | 1 | 5,0 | 5,0 | 5,0 |
| | Sí notablemente | 19 | 95,0 | 95,0 | 100,0 |
| | Total | 20 | 100,0 | 100,0 | |

*Nota. Se asocia a la experiencia del usuario*

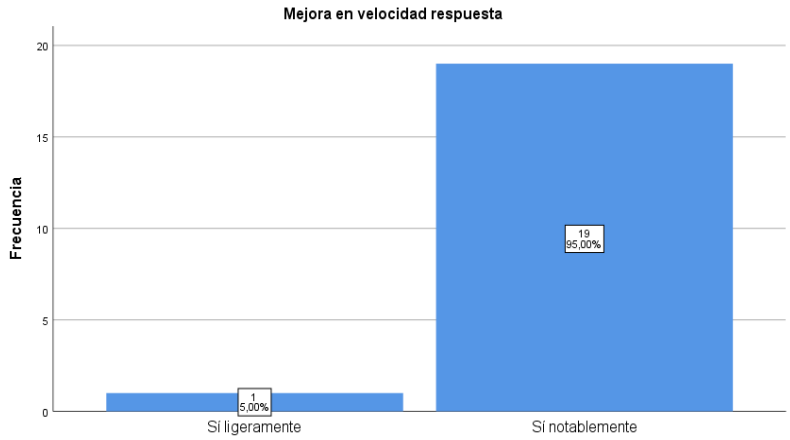



**Figura 677.** *Pregunta 3*

*Nota: Diseño propio*

**Análisis e interpretación**

El resultado a esta pregunta menciona que: 95% de los encuestados afirman que la velocidad y respuesta de es notable, un 5% en cambio considera una ligera mejora, considerando que el servidor VPS donde fue desplegado ofrece mejora en la disponibilidad del servicio, no existen opiniones que indiquen que no han notado cambios o que la aplicación se despliega más lenta.

Pregunta 4 ¿Se siente más seguro/a al utilizar el sistema web de Consulta Externa luego de la implementación de la arquitectura de seguridad?

**Tabla 25.**

*Pregunta 4*

**App más seguro tras implementación**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Sí bastante | 16 | 80,0 | 80,0 | 80,0 |
| | Sí en parte | 4 | 20,0 | 20,0 | 100,0 |
| | Total | 20 | 100,0 | 100,0 | |

*Nota. Apreciación de seguridad y confianza*

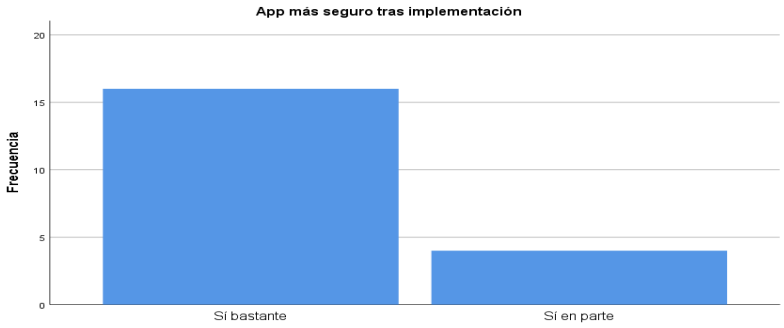



**Figura 688.** *Pregunta 4*

*Nota: Diseño propio*

**Análisis e interpretación**

El resultado a esta pregunta muestra que: el 80% de usuarios internos opinan sentirse bastante seguros con las mejoras de seguridad aplicadas, esto gracias a que el sitio ya cuenta con cifrado SSL/HTTPS, el 20% se sentirse en parte más seguros, porque la seguridad del 100% no existe, ningún encuestado se siente indiferente o menos seguro.

Pregunta 5 ¿Confía en que la información de pacientes y agendamiento está protegida adecuadamente?

**Tabla 26.**

*Pregunta 5*

**Confianza en protección de datos**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | De acuerdo | 6 | 30,0 | 30,0 | 30,0 |
| | Muy de acuerdo | 14 | 70,0 | 70,0 | 100,0 |
| | Total | 20 | 100,0 | 100,0 | |

*Nota. Relación con la confidencialidad e integridad*

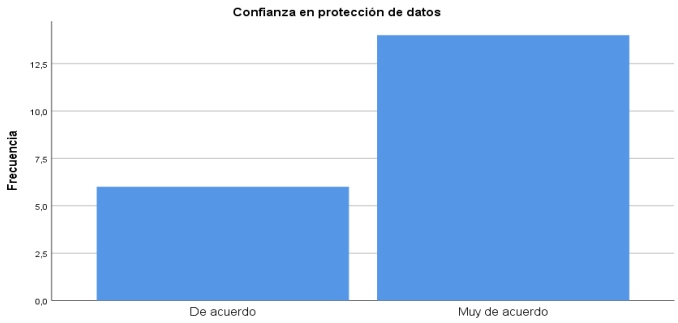


**Figura 699.** *Pregunta 5*

*Nota: Diseño propio*

**Análisis e interpretación**

El resultado a esta pregunta indica que: 70% de encuestados manifiesta estar muy de acuerdo en que la arquitectura de seguridad propuesta protege la información de los pacientes, el 30% restante de la misma manera está de acuerdo en que el servicio web desplegado se alinea con el objetivo proteger la confidencialidad e integridad de los datos, no existen opiniones neutrales o en desacuerdo.

Pregunta 6 ¿Considera que la aplicación de Consulta Externa implementa medidas adecuadas para garantizar la confidencialidad, integridad y disponibilidad de los datos?

**Tabla 27.**

*Pregunta 6*

**Mejora en Confidencialidad, Integridad y Disponibilidad**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Sí | 20 | 100,0 | 100,0 | 100,0 |

*Nota. Percepción de confidencialidad, integridad y disponibilidad*

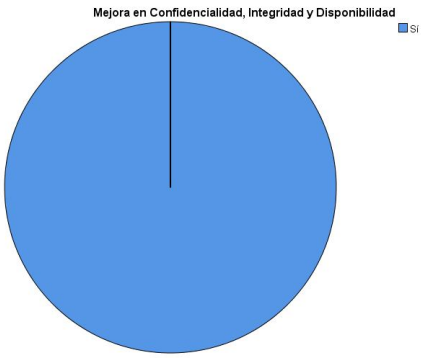



**Figura 70.** *Pregunta 6*

*Nota: Diseño propio*

**Análisis e interpretación**

El resultado a esta pregunta menciona que: 100% de los encuestados perciben que la aplicación protege el acceso información sensible, existe confianza que los datos registrados no serán alterados y que accesible de forma permanente, lo cual garantiza la continuidad del

servicio. Aunque el 100% puede ser considerado un indicador ideal refleja una percepción, por lo que recomienda complementar esta opinión con pruebas de penetración y monitoreo permanente.

Pregunta 7 ¿Considera que la arquitectura de seguridad desplegada puede mejorar la disponibilidad y continuidad del sistema web de Consulta Externa?

**Tabla 28.**

*Pregunta 7*

**Disponibilidad y continuidad del servicio**

| | | Frecuencia | Porcentaje | Porcentaje válido | Porcentaje acumulado |
|---|---|---|---|---|---|
| Válido | Sí | 20 | 100,0 | 100,0 | 100,0 |

*Nota. Relación con la disponibilidad del servicio y continuidad de operaciones*

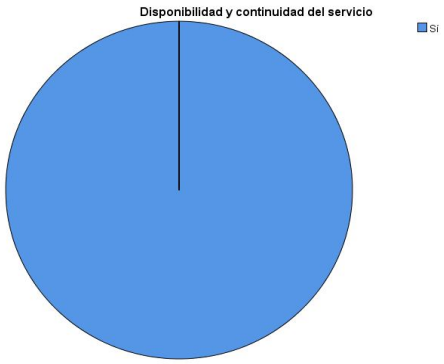



**Figura 71.** *Pregunta 7*

*Nota: Diseño propio*

**Análisis e interpretación**

El resultado a esta pregunta muestra que: 100% de los usuarios internos reconocen que la arquitectura propuesta permite que la aplicación web este accesible en todo momento, herramientas de seguridad instaladas fortalecen la capacidad del sistema para mantenerse operativo promoviendo la continuidad de negocio y alinea a la norma ISO NTE INEN-ISO/IEC 27031.

#### 4.1.4.2 Impactos por activo en C–I–D

Para cumplir con el objetivo de evaluar el cumplimiento de la continuidad de servicios web de consulta externa, mediante la norma NTE INEN-ISO/IEC 27031 es necesario primero considerar los impactos en la confidencialidad, integridad y disponibilidad de los activos de la información del servicio de Consulta Externa del HBRMM, como a continuación se detalla en la siguiente tabla:

**Tabla 29.**

*Impactos en la disponibilidad, integridad y confidencialidad*

| N.º | Activos de Información | [D] Disponibilidad | [I] Integridad de los datos | [C] Confidencialidad |
|---|---|---|---|---|
| **A1** | Información de pacientes y citas médicas | Datos inaccesibles temporalmente<br>Dificultad de acceso y gestión de citas | Errores en datos de pacientes y/o citas médicas<br>Inconsistencia en los registros de citas médicas | Exposición de datos personales<br>Revelación de datos personales<br>Acceso información confidencial<br>Divulgación de información confidencial |
| **A3** | ISP - Acceso a Internet | Interrupción del servicio de internet | Pérdida o corrupción de datos | |
| **A4** | Ubuntu Server 20.0.4 LTS | Bloqueo de acceso al sistema<br>Afectación al rendimiento del SO<br>Interrupción, degradación del SO | Cifrado o daño de datos<br>Modificación de archivos críticos<br>Alteración de configuración de SO | |
| **A5** | App Web Gestión de Consulta Externa | Afectación a funcionalidad<br>Interrupción en el acceso al sistema | Modificación de datos de pacientes y/o citas médicas | |
| **A6** | App Web MSP PRAS | Indisponibilidad para el registro de atenciones | Modificación de datos de pacientes, citas médicas, registros de atención | |
| **A7** | Servidor HTTP Apache | Interrupción en las comunicaciones<br>Interrupción completa del servicio | Intercepción y modificación de datos | |
| **A8** | MySQL BD Consulta Externa | Afectación al rendimiento<br>Interrupción del servicio | Manipulación y/o eliminación de datos de la BD | |
| **A9** | HP Proliant DL380G7 | Indisponibilidad de sistema informático | Corrupción de datos en BD<br>Daños físicos en componentes del servidor | Acceso a datos personales y/o citas médicas de dispositivo en inactividad |
| **A10** | | | | |

| | | | | |
|---|---|---|---|---|
| | Pc computadores personales | Restricción, denegación de acceso a la aplicación | Modificación de datos de citas médicas Pérdida, cifrado o daño de datos | Acceso información confidencial, datos personales, resultados de exámenes, diagnósticos |
| **A11** | Switch D-Link DES-1024D | Interrupción temporal del servicio Sin acceso al sistema | Errores de transmisión por fallos físicos Pérdida o daño de datos por hardware defectuoso | |
| **A12** | Router Linksys e900 | | | |
| **A13** | LAN CAT 6e | | | |
| **A14** | Alimentación Eléctrica | Daño de equipos Interrupción temporal del servicio | | |
| **A15** | UPS APC BR1500M2-LM | Sin respaldo de energía para equipos críticos | | |
| **A16** | Centro de Datos | Interrupción de servicios críticos | | Robo de datos del servidor central Copia no autorizada de datos |
| **A17** | Usuarios Internos | Interrupciones en accesos legítimos Interrupción temporal del servicio Omisión en gestión de citas médicas | Inserción de datos incorrectos Alteración, pérdida de datos | Revelación de datos personales Divulgación de información confidencial |
| **A18** | Usuarios Operadores | | | |

*Nota. Diseño propio*

#### 4.1.4.3 BIA y parámetros RTO/RPO

El Análisis de Impacto al Negocio identifica qué procesos deben restablecerse primero, con base en sus efectos sobre la atención y la continuidad operativa, según las definiciones de RTO y RPO de la NTE INEN-ISO/IEC 27031 mostradas en la Figura 70. La lectura integra los procesos críticos de Tabla 31 con la carga real de trabajo evidenciada en las Tablas 32–35, para vincular prioridades de recuperación con ritmos de demanda sin ambigüedades.

**Tabla 30.**

*Análisis de procesos críticos y prioridad de recuperación*

| Proceso Crítico | Tiempo aproximado de restablecimiento | Prioridad de recuperación |
|---|---|---|
| Registro de pacientes | 8 horas | Alta |
| Agendamiento de citas | 8 horas | Alta |
| Registro de citas subsecuentes | 8 horas | Alta |

| | | |
|---|---|---|
| Consulta y acceso a datos de pacientes | 8 horas | Alta |
| Consulta de citas del día | 8 horas | Media |
| Reportes de estadísticas de atención | 24 horas | Baja |

*Nota. Elaborado por el autor*

Los procesos críticos priorizados son registro de pacientes, agendamiento de citas, y registro de citas subsecuentes, mientras que la consulta de citas del día y los reportes estadísticos presentan una urgencia operativa menor. La Tabla 31 fija un tiempo aproximado de restablecimiento de ocho horas para los cuatro primeros procesos con prioridad alta, y ubica los reportes con veinticuatro horas en prioridad baja.

**Tabla 31.**

*Citas agendadas por especialidad año 2024*

| Especialidad | No. Registros | % |
|---|---|---|
| Anestesiología | 439 | 2% |
| Audiometría | 1657 | 9% |
| Cirugía | 2069 | 11% |
| Ginecología | 5471 | 30% |
| Medicina Interna | 2836 | 15% |
| Nutrición | 1605 | 9% |
| Pediatría | 1811 | 10% |
| Psicología | 1731 | 9% |
| Salud Ocupacional | 907 | 5% |
| Total citas agendadas | 18526 | 100% |

*Nota. Obtenido de App web de Gestión de Consulta Externa*

**Tabla 32.**

*Promedio de citas agendadas año 2024*

| Citas agendadas | Promedio Mensual | Promedio Diario | Promedio por Hora |
|---|---|---|---|
| 18526 | 1544 | 77 | 10 |

*Nota. Basado en atenciones agendadas en App web de Gestión de Consulta Externa*

La carga operativa sustenta esas prioridades con datos verificables, pues durante 2024 se registraron 18.526 citas agendadas con promedios 1.544 mensuales, 77 diarias y 10 por hora, de acuerdo con la Tabla 33. En paralelo, las citas confirmadas sumaron 12.811 con promedios 1.068 mensuales, 53 diarias y 7 por hora conforme a la Tabla 35, lo que evidencia una cadencia constante que exige ventanas de recuperación breves.

**Tabla 33.**

*Citas confirmadas por especialidad año 2024*

| Especialidad | No. Registros | % |
|---|---|---|
| Anestesiología | 322 | 3% |
| Audiometría | 953 | 7% |
| Cirugía | 1626 | 13% |
| Ginecología | 3616 | 28% |
| Medicina Interna | 2145 | 17% |
| Nutrición | 934 | 7% |
| Pediatría | 1207 | 9% |
| Psicología | 1125 | 9% |
| Salud Ocupacional | 883 | 7% |
| Total citas confirmadas | 12811 | 100% |

*Nota. Obtenido de App web de Gestión de Consulta Externa*

**Tabla 34.**

*Promedio de citas confirmadas año 2024*

| Citas confirmadas en App Web de Consulta Externa año 2024 | | | |
|---|---|---|---|
| Año | Promedio Mensual | Promedio Diario | Promedio por Hora |
| 12811 | 1068 | 53 | 7 |

*Nota. Basado en atenciones agendadas en App web de Gestión de Consulta Externa*

**Tabla 35.**

*Análisis de Impacto al Negocio (BIA) – Consulta Externa*

| Proceso crítico | Activo asociado | Impacto si se interrumpe | Tiempo de interrupción | Prioridad de recuperación |
|---|---|---|---|---|
| Registro de pacientes | Servidor, aplicación web CE | *No se pueden registrar pacientes y demora en atención | 8 horas | Alta |
| Agendamiento de citas | Servidor, aplicación web CE | *Pacientes no pueden agendarse | 8 horas | Alta |
| Registro de citas subsecuentes | Servidor, aplicación web CE | *No pueden agendarse citas subsecuentes | 8 horas | Alta |
| Acceso a datos de pacientes | Base de datos MySQL, servidor Apache | No se puede consultar datos personales, duplicidad - errores en registros | 8 horas | Alta |
| Consulta de citas del día | Servidor y aplicación web CE | Tiempos de atención elevados, malestar en pacientes | 8 horas | Media |
| Generación de estadísticas | Base de datos, servidor Apache | Retrasos en reportes de producción | 24 horas | Baja |

*Nota: Se considera como aceptable el registro manual y uso de reportes físicos para el registro de citas*

A continuación, se presenta el análisis de RTO/OTR y RPO/OPR conforme a la NTE INEN-ISO/IEC 27031 del servicio web de Consulta Externa del HBRMM, para la preparación de las TIC en la continuidad del negocio (IRBC – ICT Readiness for Business Continuity), considerando los siguientes parámetros:

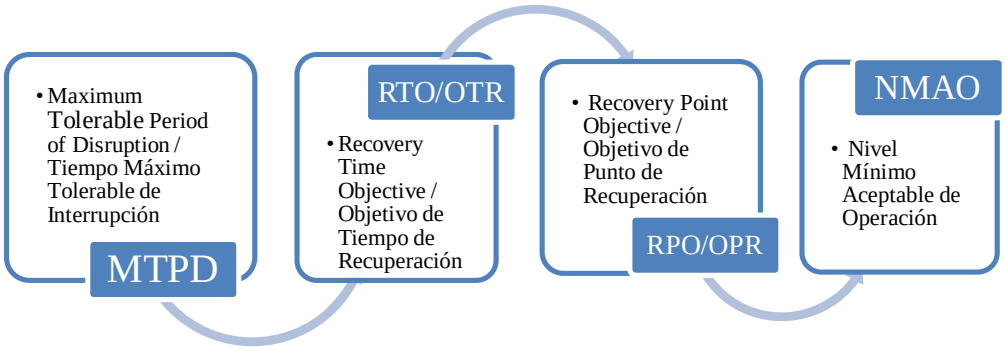



**Figura 702.** *Definiciones NTE INEN-ISO/IEC 27031 / ISO/IEC 27031*

*Nota: Diseño propio*

**Tabla 36.**

*Análisis de impacto RTO y RPO en citas y atención médica*

| | Impacto calculado en citas médicas | |
|---|---|---|
| Situación actual | Agendamiento | Confirmación |
| Citas mensuales | 1600 (80 citas x 20 días) | 1120 (56*20 días) |
| RTO/OTR actual 8 horas | 80 (10 citas x 8 horas) | 56 (7 citas x 8horas) |
| RPO/OPR actual 15 días. | 1200 (80 citas x 15 días) | 840 (56 citas x 15 días) |
| % de Afectación | 75% | 75% |

*Nota. Considerando la jornada laboral de horas con el RPO de 15 días se perderían hasta 1.200 citas agendadas y se afectaría la atención a 840 usuarios, equivalentes al 75% de citas de un mes*

Para evaluar el cumplimiento de la continuidad del servicio web de consulta externa, se aplicó un checklist con los requisitos de la norma NTE INEN-ISO/IEC 27031, considerando evidencias y asignando un grado de cumplimiento.

**Tabla 37.**

*Análisis de requisitos*

| Requisito NTE INEN-ISO/IEC 27031 | Evidencia esperada | Cumple (Sí/Parcial/No) | Puntaje |
|---|---|---|---|

| | | | |
|---|---|---|---|
| Existe Plan de Continuidad documentado | Documento BCP aprobado | Parcial | 1 |
| Existe Plan de Recuperación ante Desastres | Documento DRP aprobado | Parcial | 1 |
| Se definieron RTO y RPO | RTO y RPO definidos por servicio | Si | 2 |
| Estrategias de continuidad (sitio alterno, VPS) | Infraestructura de sitio alterno y VPS | Si | 2 |
| Respaldos de base de datos periódicos | Registro de copias de seguridad | Si | 2 |
| Procedimientos manuales definidos | Procedimiento de citas manuales | Si | 2 |
| Pruebas del plan realizadas | Actas de simulacros o pruebas | Parcial | 1 |
| Actualización periódica del plan | Informe de actualización semestral | No | 0 |
| Roles y responsabilidades documentados | Lista de responsables con contactos | Parcial | 1 |
| Plan de comunicación en caso de crisis | Procedimiento de comunicación en crisis | Parcial | 1 |
| Identificación de activos TIC críticos | Inventario de activos TIC | Si | 2 |
| Análisis de impacto al negocio (BIA) realizado | Informe de BIA | Si | 2 |
| Evaluación de amenazas y riesgos documentada | Matriz de riesgos | Si | 2 |
| Mantenimiento de UPS y respaldo eléctrico | Registro de mantenimiento de UPS | Parcial | 1 |
| Protección contra accesos no autorizados | Políticas de seguridad de acceso | Si | 2 |
| Porcentaje total de cumplimiento | | | 73.33% |

**Análisis e interpretación**

El nivel de cumplimiento obtenido es 73.33% considerado como intermedio-alto en la implementación de la norma NTE INEN-ISO/IEC 27031, se cumplen con varios requisitos como RTO/RPO, respaldos, identificación de activos, BIA, existen brechas relacionadas la legalización de planes, pruebas regulares de continuidad y actualización periódica de la documentación.

### *4.1.5 Principales temas abordados*

Para resumir los principales temas identificados en la literatura con relación a la arquitectura de seguridad, se consideran siguientes áreas clave relacionadas con prácticas de ciberseguridad, normativas y estándares aplicados en el sector salud. A continuación, se presenta un resumen en formato de tabla:

**Tabla 38.**

*Resultados de temas abordados*

| Tema | Descripción | Referencias |
|---|---|---|
| **Prácticas de ciberseguridad** | Incluyen la implementación de medidas como validación de entrada, cifrado de datos, autenticación y autorización fuertes, y configuración segura de servidores y aplicaciones web. | Acosta & Quetama (2015); Arce & Fábian (2016); Carbajo Martín et al. (2021) |
| **Normativas y estándares aplicados en el sector salud** | Se destacó la importancia de adherirse a normas internacionales como ISO/IEC 27001 y regulaciones específicas como HIPAA para asegurar la protección de datos de salud. | Calle & Guanotuña Lascano (2010); Martinez & Hernandez (2019); Williams & Taylor (2021) |

#### 4.1.5.1 Prácticas de ciberseguridad

Acosta y Quetama (2015) subrayan la importancia de implementar validación de entrada y cifrado de datos para proteger la integridad de la información en sistemas de salud. Arce y Fábian (2016) discuten cómo estas prácticas son esenciales para mitigar riesgos y asegurar la confidencialidad de los datos. Carbajo Martín et al. (2021) enfatizan la configuración segura de servidores y aplicaciones web para prevenir ataques comunes como inyecciones SQL y XSS.

#### 4.1.5.2 Normativas y estándares aplicados en el sector salud

ISO/IEC 27001: Calle y Guanotuña Lascano (2010) destacan la importancia de esta norma internacional para establecer sistemas de gestión de seguridad de la información en el sector salud.

Continuidad del negocio: Williams y Taylor (2021) indican que la aplicación de marcos como ISO/IEC 27031 mejora significativamente la resiliencia de los servicios de salud en línea.

### *4.1.6 Análisis de la funcionalidad*

#### 4.1.6.1 Desempeño del sistema

***Métricas de rendimiento***

Según los estudios revisados, la tasa de éxito de transacciones en sistemas de salud bien implementados puede alcanzar el 99.9%. Esta alta tasa es indicativa de sistemas robustos y bien diseñados que minimizan errores y fallas durante la transacción de datos.

Tiempos de respuesta: El tiempo de respuesta es otro indicador crucial del desempeño del sistema. Este se refiere al tiempo que toma un sistema para responder a una solicitud del

usuario. En el ámbito de la salud, tiempos de respuesta rápidos son esenciales para la satisfacción del usuario y la eficiencia operativa.

***Factores que afectan el desempeño***

La infraestructura de red, incluyendo el ancho de banda disponible y la latencia de la red, también impacta en el desempeño del sistema. Las instituciones de salud deben invertir en infraestructuras de red de alta calidad para asegurar tiempos de respuesta rápidos y minimizar interrupciones.

***Mejora del desempeño***

Una infraestructura robusta es esencial para asegurar un desempeño óptimo y proporcionar una experiencia de usuario satisfactoria. Las instituciones de salud deben priorizar estas áreas para mejorar la eficiencia operativa y la satisfacción del paciente.

#### 4.1.6.2 Fiabilidad y disponibilidad

Fiabilidad y disponibilidad en servicios web de salud

La fiabilidad y disponibilidad de los servicios web son componentes fundamentales para la operación continua y segura en el sector de la salud.

***Métricas de fiabilidad y disponibilidad***

La tasa de disponibilidad se refiere al porcentaje de tiempo que un sistema está operativo y accesible. En el contexto de la salud, una alta disponibilidad es crucial para garantizar que los pacientes y profesionales de la salud tengan acceso constante a los sistemas necesarios para la atención médica. Los estudios revisados indican que los sistemas de salud de alta calidad deben mantener una disponibilidad superior al 99.95%.

***Estrategias para mejorar la fiabilidad y disponibilidad***

La implementación de redundancia y replicación de datos es una estrategia común para mejorar la disponibilidad y fiabilidad de los sistemas web. Al replicar datos y servicios críticos en múltiples ubicaciones, las instituciones de salud pueden asegurar que los sistemas permanezcan operativos incluso en caso de fallos de hardware o desastres locales.

El mantenimiento preventivo regular es indispensable para identificar y corregir problemas potenciales antes de que resulten en fallos del sistema. Esto incluye actualizaciones de software, reemplazo de hardware obsoleto y pruebas de sistemas de respaldo.

### *4.1.1. Evaluación de la usabilidad*

#### 4.1.6.3 Facilidad de uso

La facilidad de uso de los servicios web en el sector salud puede asegurar que los pacientes, médicos y otros usuarios internos puedan interactuar eficientemente con las aplicaciones, un método sugerido para la evaluación de la usabilidad incluye pruebas de usuarios y encuestas de satisfacción.

***Pruebas de usuario***

Este método implica observar a los usuarios mientras interactúan con el servicio web, permitiendo identificar problemas de navegación y funcionalidad. En el contexto de los servicios de salud, las pruebas de usuario han revelado que interfaces simples y bien organizadas mejoran significativamente la experiencia del usuario

***Encuestas de satisfacción***

Estas encuestas recopilan la percepción de los usuarios sobre la facilidad de uso del servicio web. Los resultados de estas encuestas indican que los usuarios valoran altamente las interfaces intuitivas y la rapidez en el acceso a la información. Espinoza et al. (2016) encontraron que la satisfacción del usuario aumenta cuando los sistemas proporcionan feedback inmediato y claras instrucciones de uso.

***Principales problemas de usabilidad***

A pesar de los avances, varios estudios han identificado problemas de usabilidad que afectan la experiencia del usuario. Entre los más comunes se encuentran:

Tiempos de carga largos y errores técnicos pueden frustrar a los usuarios y disminuir su confianza en el sistema. Castillo Enríquez et al. (2022) subrayan la importancia de optimizar el rendimiento técnico del servicio web para mantener la satisfacción del usuario.

### *4.1.7 Seguridad de los servicios web*

La seguridad de los servicios web en el sector salud es esencial para proteger la información sensible de los pacientes y garantizar la continuidad de los servicios. La detección de intrusiones se enfoca en identificar y mitigar actividades maliciosas que puedan comprometer la seguridad de los sistemas.

#### 4.1.7.1 Detección de Intrusiones

La seguridad de los servicios web en el sector salud es una prioridad debido a la sensibilidad de los datos manejados y la necesidad de asegurar su integridad, confidencialidad

y disponibilidad. La detección de intrusiones es una de las estrategias clave para proteger estos servicios.

***Estrategias de Detección de Intrusiones***

Las estrategias de detección de intrusiones se dividen principalmente en dos categorías: sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS). Los IDS monitorean el tráfico de red y alertan sobre actividades sospechosas, mientras que los IPS no solo detectan, también pueden bloquear estas actividades.

Ruiz Martinez (2021) destaca el uso de técnicas de Machine Learning en la ciberseguridad para mejorar la detección de comportamientos anómalos en la web, subrayando la importancia de aplicaciones web dinámicas y su capacidad para adaptarse a nuevas amenazas.

***Tecnologías de Detección de Intrusiones***

Las tecnologías empleadas para la detección de intrusiones incluyen una combinación de hardware y software diseñados para proteger los servicios web:

- Firewalls Avanzados: Integran capacidades de detección y prevención de intrusiones, filtrando el tráfico de red según reglas predefinidas y aprendidas. Cueva Delgado (2015) subraya cómo un esquema de seguridad con un firewall de borde mejora la protección de información sensible en sistemas de salud.
- Herramientas de Monitoreo Continuo: Aplicaciones que permiten la supervisión en tiempo real del tráfico de red y el comportamiento del sistema. Estas herramientas alertan automáticamente sobre cualquier actividad sospechosa que requiera atención inmediata.

***Normativas y Estándares Aplicados***

Las normativas y estándares internacionales, como ISO/IEC 27001 y la Ley de Portabilidad y Responsabilidad del Seguro de Salud (HIPAA) en los Estados Unidos, establecen directrices específicas para la implementación de medidas de seguridad en el sector salud. Estas normativas sugieren la implementación de controles de seguridad adecuados para proteger los datos de salud y asegurar la continuidad de los servicios

## 4.2 Discusión

### *4.2.1 Comparación con estudios previos*

En este apartado se realiza una comparación entre los hallazgos obtenidos en la revisión sistemática de la literatura y estudios previos en el campo de la seguridad de los servicios web en el sector salud.

#### 4.2.1.1 Consistencia de los resultados

En este apartado, se compararán los hallazgos obtenidos con estudios previos en el campo, destacando las similitudes y diferencias para evaluar la consistencia de los resultados.

***Similitudes en los resultados***

La mayoría de los estudios revisados coinciden en la importancia crítica de implementar sistemas robustos de detección de intrusiones (IDS) y prevención de intrusiones (IPS) para proteger los servicios web de salud. Por ejemplo, Ruiz Martínez (2021) destaca el uso de técnicas de Machine Learning para mejorar la detección de comportamientos anómalos en las aplicaciones web, una estrategia que también fue identificada en nuestra revisión sistemática como fundamental para mejorar la precisión y eficiencia en la detección de intrusiones.

***Análisis basado en firmas y anomalías***

Tanto en la revisión sistemática como en estudios previos, se encuentra una fuerte dependencia de las técnicas basadas en firmas y anomalías para la detección de intrusiones. Los sistemas basados en firmas son efectivos para identificar amenazas conocidas, mientras que los basados en anomalías pueden detectar ataques desconocidos al identificar desviaciones del comportamiento normal del sistema. Este doble enfoque es ampliamente respaldado en la literatura, incluyendo trabajos de Cueva Delgado (2015), quien subraya la importancia de utilizar ambos métodos para una protección integral

***Uso de firewalls avanzados***

La revisión sistemática y los estudios anteriores coinciden en que los firewalls avanzados, que integran capacidades de detección y prevención de intrusiones, son esenciales para proteger los servicios web de salud. La implementación de firewalls avanzados se ha destacado como una práctica estándar que proporciona una capa adicional de seguridad al filtrar el tráfico de red según reglas predefinidas. Este enfoque es consistente con las recomendaciones de Espinoza et al. (2016), quienes demuestran que los firewalls avanzados son cruciales para mantener la integridad y disponibilidad de los datos de salud.

***Normativas y estándares internacionales***

Los estudios revisados enfatizan la importancia de adherirse a normativas y estándares

internacionales como ISO/IEC 27001 y HIPAA. Estas normativas proporcionan un marco estructurado para implementar medidas de seguridad adecuadas y asegurar la continuidad de los servicios web en el sector salud. La consistencia en la aplicación de estos estándares se refleja en la literatura revisada, destacando su papel en la creación de entornos seguros y confiables para el manejo de datos sensibles.

***Diferencias en los resultados***

Aunque existen varias coincidencias, también existen diferencias notables en los enfoques y tecnologías recomendadas por los estudios revisados. Estas diferencias pueden atribuirse a varios factores, incluyendo el contexto específico de cada estudio, las tecnologías disponibles en el momento de la investigación, y las particularidades de cada entorno de salud.

***Enfoques de monitoreo continuo***

Aunque la revisión sistemática y varios estudios previos coinciden en la importancia del monitoreo en tiempo real, algunos estudios destacan el uso de herramientas específicas como OpenVAS o Nessus para escanear continuamente la infraestructura y detectar vulnerabilidades potenciales. En contraste, otros estudios recomiendan herramientas propietarias o desarrolladas internamente que ofrecen capacidades de monitoreo personalizadas según las necesidades específicas del entorno de salud.

***Implementación de IPS Basados en Host (HIPS)***

La revisión sistemática encontró una menor frecuencia en la implementación de IPS basados en host (HIPS) en comparación con los IPS basados en red (NIPS). Sin embargo, algunos estudios previos, como el de Castillo Enríquez et al. (2022), destacan la eficacia de los HIPS en la protección de servidores individuales y aplicaciones críticas. Esta discrepancia puede reflejar diferentes prioridades y capacidades tecnológicas entre las instituciones de salud, así como las variaciones en el tamaño y la complejidad de las infraestructuras de TI.

***Adopción de tecnologías de código abierto***

Un punto de divergencia notable es la adopción de tecnologías de código abierto versus soluciones propietarias. Algunos estudios revisados, como los de Greiner y Godoy Guglielmone (2023), abogan por el uso de software de código abierto debido a su transparencia y flexibilidad, permitiendo auditorías de seguridad más exhaustivas y personalización según las necesidades específicas de la organización. Sin embargo, otros estudios prefieren soluciones propietarias que ofrecen soporte técnico y actualizaciones continuas, argumentando que estas

pueden ser más seguras y confiables en entornos críticos de salud.

***Variabilidad en la aplicación de normativas***

Aunque existe un consenso general sobre la importancia de las normativas internacionales, la aplicación de estas normativas varía significativamente entre los estudios. Algunos trabajos, como el de Mejía Viteri (2015), enfatizan una implementación estricta y detallada de las normativas ISO/IEC 27001 y HIPAA, mientras que otros estudios indican una adopción más flexible y adaptada a las circunstancias específicas de cada institución. Esta variabilidad puede estar influenciada por factores regulatorios locales, recursos disponibles y prioridades organizacionales.

La revisión sistemática de la literatura sobre la seguridad de los servicios web en el sector salud revela una alta consistencia en la identificación de estrategias y tecnologías clave, como la implementación de IDS e IPS, el uso de firewalls avanzados y la adherencia a normativas internacionales. Sin embargo, también se observan diferencias significativas en los enfoques y tecnologías específicas recomendadas, reflejando la diversidad de contextos y necesidades en el sector salud.

#### 4.2.1.2 Innovaciones y avances recientes

Los resultados obtenidos en la revisión sistemática de la literatura sobre la seguridad de los servicios web en el sector salud han permitido identificar diversas innovaciones y avances recientes que contribuyen significativamente al conocimiento actual.

***Uso de inteligencia artificial y machine learning***

Uno de los avances más notables en la seguridad de los servicios web en el sector salud es la integración de inteligencia artificial (IA) y machine learning (ML) para la detección de intrusiones y la gestión de riesgos. Estudios recientes, como el de Ruiz Martinez (2021), han mostrado que los modelos de ML pueden mejorar significativamente la precisión y la rapidez de la detección de intrusiones, permitiendo una respuesta más proactiva y eficaz ante amenazas emergentes.

***Sistemas de detección y prevención de intrusiones (IDPS) avanzados***

La evolución de los sistemas de detección y prevención de intrusiones (IDPS) es otro avance crucial identificado en la literatura. Los IDPS modernos no solo detectan y alertan sobre actividades sospechosas, sino que también pueden tomar medidas preventivas de manera autónoma para mitigar posibles ataques.

***Tecnologías de blockchain para la seguridad de datos***

El uso de tecnologías de blockchain para mejorar la seguridad y la integridad de los datos en el sector salud es una innovación emergente que ha ganado atención en los últimos años. Blockchain proporciona un registro inmutable de todas las transacciones, lo que hace extremadamente difícil para los atacantes alterar la información sin ser detectados. Greiner y Godoy Guglielmone (2023) destacan cómo blockchain puede ser utilizado para asegurar registros médicos electrónicos (EMR) y otros datos críticos en los servicios web de salud, ofreciendo una capa adicional de seguridad y transparencia.

***Arquitecturas de seguridad basadas en la nube***

La implementación de soluciones como el Zero Trust Architecture (ZTA) y Secure Access Service Edge (SASE) ha permitido a las organizaciones mejorar su postura de seguridad al asegurar el acceso a los servicios web de salud desde cualquier ubicación y dispositivo. Castillo Enríquez et al. (2022) enfatizan que estas arquitecturas no solo mejoran la seguridad, sino que también facilitan la gestión de riesgos y la continuidad operativa.

***Autenticación multifactor (MFA) y gestión de identidades***

La autenticación multifactor (MFA) y la gestión de identidades (IAM) son áreas en las que se han producido avances significativos. La implementación de MFA, que requiere múltiples formas de verificación para acceder a los sistemas, ha demostrado ser una medida efectiva para prevenir accesos no autorizados. Mejía Viteri (2015) señala que la integración de MFA con sistemas IAM avanzados permite una gestión más eficiente y segura de las identidades digitales, garantizando que solo usuarios autorizados puedan acceder a los datos sensibles.

***Evaluación de vulnerabilidades y pruebas de penetración automatizadas***

Las herramientas automatizadas de evaluación de vulnerabilidades y pruebas de penetración han mejorado considerablemente, permitiendo a las organizaciones de salud identificar y mitigar vulnerabilidades de manera más rápida y eficiente. Las plataformas como OpenVAS y Nessus ofrecen capacidades avanzadas para escanear y evaluar la seguridad de los sistemas web, proporcionando informes detallados y recomendaciones para la remediación. La revisión sistemática identifica que la adopción de estas herramientas ha sido clave para mantener la integridad y seguridad de los servicios web en el sector salud.

***Adopción de estándares y normativas internacionales***

El cumplimiento de estándares y normativas internacionales, como ISO/IEC 27001, sigue siendo una prioridad para las organizaciones de salud. La revisión sistemática y estudios previos, como los de Carbajo Martín et al. (2021), indican que la adopción de estos estándares proporciona un marco sólido para la implementación de prácticas de seguridad efectivas y para la evaluación continua de riesgos.

***Desarrollo de software seguro y DevSecOps***

El enfoque en el desarrollo de software seguro y la adopción de prácticas DevSecOps (Desarrollo, Seguridad y Operaciones) han sido identificados como avances importantes. Integrar la seguridad en cada fase del ciclo de vida del desarrollo de software garantiza que las aplicaciones web sean diseñadas y construidas con consideraciones de seguridad desde el inicio. Ávila Agreda et al. (2021) destacan que DevSecOps permite a las organizaciones responder rápidamente a nuevas amenazas y asegurar que las aplicaciones se mantengan seguras a lo largo de su vida útil.

Los resultados de la revisión sistemática han identificado varias innovaciones y avances recientes en la seguridad de los servicios web en el sector salud. La integración de inteligencia artificial y machine learning, la evolución de los sistemas de detección y prevención de intrusiones, los avances en encriptación y gestión de claves, el uso de blockchain, y las arquitecturas de seguridad basadas en la nube son algunas de las innovaciones clave que están transformando la seguridad en el sector salud. Además, la implementación de autenticación multifactor, la adopción de estándares internacionales, y las prácticas DevSecOps están mejorando significativamente la protección de los datos y la continuidad de los servicios web de salud.

### *4.2.2 Implicaciones prácticas*

#### 4.2.2.1 Mejora de la funcionalidad

***Desempeño del sistema***

Para mejorar el rendimiento, se recomienda la implementación de prácticas como el uso de servidores más potentes y escalables, optimización del código y la infraestructura de red, y el uso de tecnologías avanzadas como la computación en la nube. La adopción de técnicas de balanceo de carga también puede distribuir eficazmente el tráfico entre varios servidores, reduciendo los tiempos de respuesta y mejorando la disponibilidad del servicio.

***Fiabilidad y disponibilidad***

La fiabilidad y disponibilidad de los servicios web son otras áreas críticas destacadas en la revisión. Los servicios web en salud deben estar disponibles en todo momento, dado que cualquier interrupción puede afectar seriamente la atención a los pacientes. Las estrategias para minimizar el tiempo de inactividad incluyen el uso de sistemas redundantes y soluciones de recuperación ante desastres.

Los estudios también sugieren el uso de servicios en la nube que ofrecen alta disponibilidad y recuperación ante desastres, ya que estas plataformas están diseñadas para ser robustas y escalables, con capacidades integradas de respaldo y recuperación.

A continuación, recomendaciones para la mejora del rendimiento:

- Invertir en servidores de alto rendimiento y utilizar la computación en la nube.
- Implementar balanceadores de carga para distribuir el tráfico de usuarios entre múltiples servidores.
- Emplear herramientas de monitoreo para supervisar el rendimiento del sistema en tiempo real.
- Realizar pruebas regulares de estrés y carga para identificar posibles puntos débiles en las aplicaciones.

Recomendaciones para la mejora de la fiabilidad:

Configurar servidores redundantes para asegurar que haya siempre un respaldo disponible en caso de fallo del servidor principal.

Desarrollar e implementar un plan de recuperación ante desastres que incluya copias de seguridad regulares y pruebas periódicas para asegurar que los datos puedan ser restaurados rápidamente en caso de pérdida.

Implementar medidas de seguridad robustas, como firewalls, sistemas de detección de intrusiones y protocolos de autenticación, para proteger el sistema de ataques cibernéticos que podrían comprometer la disponibilidad del servicio.

Asegurar que el personal técnico esté bien entrenado en la gestión de la infraestructura de servicios web y en la implementación de planes de contingencia.

Las implicaciones prácticas de los hallazgos sobre la funcionalidad de los servicios web en el sector salud recalcan la necesidad de una infraestructura tecnológica sólida, estrategias de monitoreo, optimización continuas y planes de contingencia robustos. La implementación de

estas recomendaciones puede conducir a una mejora significativa en el rendimiento y la fiabilidad de los servicios web, lo que se traduce en una mejor experiencia para el usuario y una mayor eficiencia operativa para las instituciones de salud.

#### 4.2.2.2 Optimización de la usabilidad

Implementar un ciclo iterativo de evaluación y mejora puede asegurar que los servicios web evolucionen en respuesta a las necesidades y expectativas de los usuarios. Además, la capacitación sobre cómo utilizar el sistema puede aumentar la eficiencia y reducir la frustración.

Para mejorar la satisfacción del usuario, es fundamental optimizar los tiempos de carga de las páginas y asegurar que la información esté bien organizada y sea fácilmente accesible.

#### 4.2.2.3 Fortalecimiento de la seguridad

La seguridad de los servicios web en el sector salud es una preocupación crítica, dado que estos servicios manejan información sensible y deben cumplir con estrictas regulaciones de privacidad y protección de datos. A partir de la revisión sistemática de la literatura, se han identificado mejores prácticas y estrategias que pueden ser implementadas para fortalecer la seguridad de los servicios web en el Hospital Básico "Raúl Maldonado Mejía" del cantón Cayambe. Estas recomendaciones se alinean con los objetivos del proyecto y permiten establecer una arquitectura de seguridad robusta basada en el marco MAGERIT y ArchiMate.

Primero, la implementación de tecnologías avanzadas de detección de intrusiones es esencial para proteger los servicios web contra amenazas externas. Los estudios revisados han demostrado la eficacia de los sistemas de detección de intrusiones (IDS) y los sistemas de prevención de intrusiones (IPS) en identificar y mitigar ataques en tiempo real.

Segundo, adoptar una estrategia de defensa en profundidad, que implica múltiples capas de seguridad para proteger los datos sensibles. Esta estrategia debe incluir controles de acceso estrictos, autenticación multifactor y encriptación de datos tanto en tránsito como en reposo.

Tercero, la gestión de parches y actualizaciones es fundamental para mantener la seguridad del sistema, los estudios han señalado que muchas brechas de seguridad se deben a la explotación de vulnerabilidades conocidas en software desactualizado, este proceso debe ser automatizado en la medida de lo posible.

Cuarto, la formación y concienciación del personal es un componente vital de la seguridad, según la literatura revisada, una proporción significativa de incidentes de seguridad

se deben a errores humanos.

Quinto, la implementación de políticas y procedimientos de seguridad bien definidos es esencial para asegurar una respuesta coherente y efectiva a los incidentes de seguridad. Estos documentos deben incluir planes de respuesta a incidentes y directrices para la gestión de accesos.

Sexto, la auditoría y el monitoreo continuo son esenciales para mantener la seguridad de los servicios web, la implementación de herramientas de monitoreo de seguridad puede proporcionar visibilidad en tiempo real del estado del sistema y detectar posibles amenazas.

Fortalecer la seguridad de los servicios web en el sector salud requiere un enfoque integral que incluya tecnologías avanzadas, una estrategia de defensa en profundidad, una gestión efectiva de parches, la formación del personal, políticas de seguridad claras, auditorías regulares y la colaboración con otros actores del sector. Implementar estas recomendaciones puede ayudar a proteger la información sensible, cumplir con las regulaciones de privacidad y asegurar la continuidad de los servicios web, alineándose con los objetivos del proyecto y estableciendo una base sólida para la propuesta de arquitectura de seguridad.

### *4.2.3 Limitaciones de la revisión*

#### 4.2.3.1 Limitaciones metodológicas

Una de las principales limitaciones es el posible sesgo de selección, que puede haber afectado la representatividad de los estudios incluidos. Dado que la selección de estudios se basó en criterios específicos de inclusión y exclusión, algunos estudios relevantes pueden haber sido omitidos

La disponibilidad de estudios relevantes es otra limitación. En algunas áreas clave, como la arquitectura de seguridad para servicios web fue limitado. Esto puede haber restringido la capacidad para realizar conclusiones definitivas y puede indicar la necesidad de más investigación en estas áreas.

#### 4.2.3.2 Áreas no abordadas

Existen varias áreas de investigación que no fueron suficientemente cubiertas en la revisión y que requieren más atención en futuros estudios. Una de estas áreas es la integración de tecnologías emergentes, como la inteligencia artificial y el aprendizaje automático, en la seguridad de los servicios web

### *4.2.4 Recomendaciones para futuras investigaciones*

#### 4.2.4.1 Nuevas líneas de investigación

Se sugieren varias áreas para futuras investigaciones, como profundizar en la integración de tecnologías emergentes y la IA, estos estudios deberían explorar cómo estas tecnologías pueden mejorar la precisión y la rapidez de la respuesta a las amenazas.

Además, se recomienda investigar la efectividad de las estrategias de defensa en profundidad específicas para el sector salud. Esto incluiría estudios sobre cómo diferentes capas de seguridad interactúan y cómo se pueden optimizar para maximizar la protección sin comprometer la funcionalidad y la eficiencia operativa.

# CONCLUSIONES Y RECOMENDACIONES

## Conclusiones

La aplicación de la metodología MAGERIT v.3 permitió realizar un diagnóstico detallado de los riesgos inherentes a los activos de información del servicio de Consulta Externa del Hospital Básico “Raúl Maldonado Mejía”, en relación al web server Apache las pruebas de penetración permitieron identificar amenazas leves que pueden afectar a la disponibilidad, integridad y confidencialidad de los datos almacenados en el servidor de la aplicaciones de la institución, destacándose vulnerabilidades en la aplicación como los controles de acceso y configuraciones del sistema.

El análisis de métricas tomando como base los archivos de access.log y error.log del servidor web Apache, no permitieron diferenciar los accesos y errores específicos de las aplicaciones desplegadas, ya que estas no están configuradas con host virtuales que permitirían observaciones más objetivas del rendimiento, funcionalidad, usabilidad y seguridad de la aplicación de Consulta Externa, esto dificulta auditorías, monitoreos de seguridad y cumplimiento normativo.

El diseño de una arquitectura robusta y alineada a buenas prácticas y la utilización de ArchiMate Core Framework permitió modelar una arquitectura de seguridad integral, reflejando la relación entre los componentes tecnológicos, procesos, actores y servicios. El diseño propuesto fortalece la resiliencia del entorno tecnológico del HBRMM ante eventos disruptivos.

Se comprobó que es posible implementar soluciones de seguridad eficaces utilizando herramientas de software libre, garantizando sostenibilidad técnica y económica, herramientas como WAF, implementación de certificados de seguridad HTTPS/TLS resultaron claves en el despliegue de la prueba de concepto.

La evaluación basada en la norma NTE INEN-ISO/IEC 27031 demostró que el RTO de 8 horas apenas se encuentra en un límite tolerable, mientras que el RPO que se fundamenta en copias de seguridad cada 15 días es inaceptable, de materializarse una amenaza que afecte la continuidad del servicio web de consulta externa, esto tendría un impacto negativo para alcanzar el objetivo institucional de mejorar la accesibilidad y el tiempo de espera para brindar atención a los usuarios.

**Recomendaciones**

Dado que los entornos tecnológicos evolucionan, es indispensable revisar y actualizar la arquitectura de seguridad al menos una vez al año, considerando la aparición de nuevas amenazas, tecnologías y requerimientos normativos, desarrollando pruebas de seguridad más estrictas y la adoptando nuevas herramientas tecnologías que permitan disminuir los riesgos y mantener la continuidad del servicio.

Se sugiere evaluar la posibilidad de escalar la arquitectura diseñada a otros servicios hospitalarios (emergencia, hospitalización, nube de almacenamiento), promoviendo una estrategia de seguridad integral en toda la institución.

Considerando la obsolescencia del equipamiento tecnológico actual del hospital, se recomienda evaluar la migración de los servicios web de consulta externa a un servidor VPS (Servidor Privado Virtual). Esta transición permitiría aprovechar recursos computacionales más modernos y escalables, mejorando significativamente la disponibilidad del servicio hasta un 99.99%, en comparación con la infraestructura física local. Además, se reducirían los riesgos asociados a fallos de hardware, y se facilitaría la implementación de copias de seguridad, redundancia y recuperación ante desastres.

Es fundamental capacitar a todo el personal de TIC en el uso de las herramientas de seguridad basadas en software libre que pueden ser implementadas, así como la adopción de buenas prácticas de seguridad informática y gestión de riesgos a todos los usuarios internos del HBRMM.

Considerando la evaluación con la norma NTE INEN-ISO/IEC 27031 se recomienda reducir el RTO de 8 horas a menos de 4 horas, considerando servidores alternos o VPS, automatizando despliegues y restauración, reducir el RPO de 15 días a menos de 24h, generando respaldos automáticos a diario o replicación de base de datos en un sitio alterno, definir formalmente MTPD a máximo 8 horas de interrupción tolerable y el NMAO manteniendo el agendamiento manual de citas para garantizar la atención básica.

Adicionalmente y como parte del cumplimiento de la norma NTE INEN-ISO/IEC y de la mejora continua, se recomienda desarrollar e institucionalizar el plan de contingencia, de continuidad y de recuperación ante desastres pare el servicio web de consulta externa, que integre el modelo de arquitectura de seguridad propuesto y permita su escalamiento para el resto de servicios críticos del HBRRMM.

**Referencias**

Admass, W. S., Munaye, Y. Y., & Diro, A. A. (2024). Cyber security: State of the art, challenges and future directions. *Cyber Security and Applications*, *2*, 100031. https://doi.org/10.1016/j.csa.2023.100031

Al-Sarayreh, K., Alyabroodi, Z., & Abuasal, S. (2024). Designing A Standard-Based Approach for Security of Healthcare Systems. *Journal of Statistics Applications & Probability*, *13(2024)*, 419. https://doi.org/10.18576/jsap/130129

Carbajo Martín, L., Martín Álvarez, R., Astier Peña, M. P., Rotaeche Del Campo, R., Navarro Pérez, J., & Párraga Martínez, I. (2021). Descripción de la implantación y grado de desarrollo de tecnología de comunicación e informática de los equipos de Atención Primaria en los servicios autonómicos de salud en España. *Revista Clínica de Medicina de Familia*. https://doi.org/10.55783/rcmf.140206

Carreño Arce, C. F. (2016). *Reingeniería de sistema web para pacientes del hospital Naval Guayaquil utilizando arquitectura de cuatro capas, con sistema de autenticación único, e implementación de servidor web de aplicaciones, con certificado de seguridad SSI.* [bachelorThesis]. http://dspace.ups.edu.ec/handle/123456789/12325

Castillo Enríquez, A. S. (2021). *Pruebas de penetración para la seguridad informática al servidor web del laboratorio de ciberseguridad en la Universidad Politécnica Estatal del Carchi* [UPEC]. http://repositorio.upec.edu.ec/handle/123456789/1302

Christy, V., Andry, J., Kamila, A., & Lee, F. (2024). Information system architecture for healthcare company based on TOGAF. *International Journal of Advances in Applied Sciences*, *13*, 806. https://doi.org/10.11591/ijaas.v13.i4.pp806-813

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. *The Geneva Papers on Risk and Insurance. Issues and Practice*, *47*(3), 698-736. https://doi.org/10.1057/s41288-022-00266-6

España León, A. R. (2016). *Estrategia informática con arquitectura MVC y Responsive Web Design en la gestión de datos de los pacientes del hospital maternidad Babahoyo en el área de estadística* [masterThesis]. https://dspace.uniandes.edu.ec/handle/123456789/3680

European Network and Information Security Agency. (2020). *Guideline on security measures under the EECC*. Publications Office. https://data.europa.eu/doi/10.2824/44013

European Union Agency for Cybersecurity. (2024). *ENISA threat landscape 2024: July 2023 to June 2024*. Publications Office. https://data.europa.eu/doi/10.2824/0710888

*FICHA METODOLÓGICA DE DEFINICIÓN DE METAS DEL PLAN NACIONAL DE DESARROLLO, 2024*. (s. f.). Recuperado 9 de octubre de 2025, de https://www.planificacion.gob.ec/wp-content/uploads/2021/09/Meta-10.1.1.pdf?

Fuentes, G., Ruiz, F., & Caro, A. (2024). *Arquitectura empresarial y gobernanza de TI para respaldar el enfoque de BizDevOps: Un estudio de mapeo sistemático*. https://www.researchgate.net/publication/378343028_Enterprise_Architecture_and_IT_Governance_to_Support_the_BizDevOps_Approach_a_Systematic_Mapping_Study

González, P. M., Reyes, S. V., Barraza, S. V., Elizondo, P. V., Ramírez, C. H. C., & González, A. M. (2022). Metodología para detectar riesgos en seguridad informática en la universidad autónoma de zacatecas basada en pruebas de penetración. *South Florida Journal of Development*, *3*(6), 6793-6802. https://doi.org/10.46932/sfjdv3n6-030

Haseeb-ur-rehman, R. M. A., Aman, A. H. M., Hasan, M. K., Ariffin, K. A. Z., Namoun, A., Tufail, A., & Kim, K.-H. (2023). High-Speed Network DDoS Attack Detection: A Survey. *Sensors*, *23*(15), 6850. https://doi.org/10.3390/s23156850

*ISO/IEC 27032:2023—ISO/IEC 27032:2023*. (s. f.). Recuperado 9 de octubre de 2025, de https://cdn.standards.iteh.ai/samples/76070/be57667fdd0b432490c253ca538c9938/ISO-IEC-27032-2023.pdf?

Martin. (s. f.). Health. *United Nations Sustainable Development*. Recuperado 9 de octubre de 2025, de https://www.un.org/sustainabledevelopment/health/

Martín Vega, D. (2018). *Prototipo de Sistema de Información Web Aplicando Desarrollo Guiado por Pruebas del Sistema de Gestión de la Seguridad y Salud en el Trabajo en Empresas de Producción: Caso de Estudio Munkys SAS*. http://hdl.handle.net/11349/13632

Nagua, C., & Andrés, K. (2020). *Desarrollo de una Aplicación Web para el Control de citas y manejo de historial médico en la Unidad Médica Family care de la ciudad de Guayaquil*.

Open Group. (2024). *Lenguaje de modelado de arquitectura—Certificación ArchiMate® | www.opengroup.org*. https://www.opengroup.org/certifications/archimate

Ortega, K., Aguilar, E., Aizprúa, A., Cedeño, E., & Sanchez Galan F, J. (2023). Estructuración de un sistema de información geoespacial para el análisis de datos de seguridad alimentaria, intervenciones nutricionales y de salud humana en Panamá. *Congreso Nacional de Ciencia y Tecnología – APANAC*, 356-362. https://doi.org/10.33412/apanac.2023.3959

Ortega, K. G., Aguilar, E., Aizprúa, A. G., Eddy Cedeño, & Sánchez-Galán, J. (2023). Estructuración de un sistema de información geoespacial para el análisis de datos de seguridad alimentaria, intervenciones nutricionales y de salud humana en Panamá. *Congreso Nacional de Ciencia y Tecnología – APANAC*, 356-362. https://doi.org/10.33412/apanac.2023.3959

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., … Moher, D. (2021b). The PRISMA 2020 statement: An updated guideline for reporting systematic reviews. *BMJ*, n71. https://doi.org/10.1136/bmj.n71

Peters, S. (2025). What is ISO/IEC 27001, The Information Security Standard. *Https://Www.Isms.Online/*. https://www.isms.online/iso-27001/

*PLAN-NACIONAL-DE-DESARROLLO-2021-2025.pdf*. (s. f.). Recuperado 9 de octubre de 2025, de https://iste.edu.ec/wp-content/uploads/2022/08/PLAN-NACIONAL-DE-DESARROLLO-2021-2025.pdf?

Relativiti. (2023). *Infrastructure planning considerations overview—Server2023*. https://help.relativity.com/Server2023/Content/System_Guides/Infrastructure_planning_considerations.htm?

Rethlefsen, M. L., Kirtley, S., Waffenschmidt, S., Ayala, A. P., Moher, D., Page, M. J., Koffel, J. B., Blunt, H., Brigham, T., Chang, S., Clark, J., Conway, A., Couban, R., de Kock, S., Farrah, K., Fehrmann, P., Foster, M., Fowler, S. A., Glanville, J., … PRISMA-S Group. (2021). PRISMA-S: An extension to the PRISMA Statement for Reporting Literature Searches in Systematic Reviews. *Systematic Reviews*, *10*(1), 39. https://doi.org/10.1186/s13643-020-01542-z

Rodríguez, M. (2021). *Ciberseguridad en la justicia digital: Recomendaciones para el caso colombiano—Dialnet*. https://dialnet.unirioja.es/servlet/articulo?codigo=9514571

Romero, G. J. (2024). La ética informática en el sector de la salud Computer ethics in the health sector. *Revista Cubana de Salud y Trabajo*, *25*(1). http://revsaludtrabajo.sld.cu/index.php/revsyt/article/view/446

Sheffer, Y., Saint-Andre, P., & Fossati, T. (2022). *Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)* (Request for Comments No. RFC 9325). Internet Engineering Task Force. https://doi.org/10.17487/RFC9325

Soto, L. L. (2024). *Proceso de Control de La Gestión de Seguridad y Medio Ambiente Mediante La Aplicación de Un Sistema Web | PDF | Mi sql | La seguridad informática*. https://es.scribd.com/document/732917811/23?

Sparx. (2022). *ArchiMate Core Framework | Enterprise Architect User Guide*. https://sparxsystems.com/enterprise_architect_user_guide/17.1/modeling_frameworks/archimate_framework_core.html?

Ștefan, A., Rusu, N., Ovreiu, E., & Ciuc, M. (2024). *Empowering Healthcare: A Comprehensive Guide to Implementing a Robust Medical Information System—Components, Benefits, Objectives, Evaluation Criteria, and Seamless Deployment Strategies*. https://www.mdpi.com/2571-5577/7/3/51?

Svarre, T., & Russell-Rose, T. (2025). Think outside the search box: A comparative study of visual and form-based query builders. *Journal of Information Science, 51*(2), 354-367. https://doi.org/10.1177/01655515221138536

Tea, F., Groh, A. M. R., Lacey, C., & Fakolade, A. (2024). A scoping review assessing the usability of digital health technologies targeting people with multiple sclerosis. *NPJ Digital Medicine*, *7*, 168. https://doi.org/10.1038/s41746-024-01162-0

Technology, N. I. of S. and. (2024). *The NIST Cybersecurity Framework (CSF) 2.0* (No. NIST CSWP 29). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.29

Velasquez Moreno, G. A., & Parra Duran, J. J. (2020). *Desarrollo de un aplicativo web para la administración de las historias clínicas de salud ocupacional DE Mobile System E. U.* http://hdl.handle.net/11371/2906

Wasserman, L., & Wasserman, Y. (2022). *Frontiers | Hospital cybersecurity risks and gaps: Review (for the non-cyber professional)*. https://www.frontiersin.org/journals/digital-health/articles/10.3389/fdgth.2022.862221/full

World Health Statistics. (2024). *SDG Target 3.8 | Achieve universal health coverage, including financial risk protection, access to quality essential health-care services and access to safe, effective, quality and affordable essential medicines and vaccines for all.* https://www.who.int/data/gho/data/themes/topics/indicator-groups/indicator-group-details/GHO/sdg-target-3.8-achieve-universal-health-coverage-%28uhc%29-including-financial-risk-protection?

Zaid, T., & Garai, S. (2024). Emerging Trends in Cybersecurity: A Holistic View on Current Threats, Assessing Solutions, and Pioneering New Frontiers. *Blockchain in Healthcare Today*, *7*, 10.30953/bhty.v7.302. https://doi.org/10.30953/bhty.v7.302

Centro Criptológico Nacional. (s. f.). PILAR - ¿Qué es PILAR? Recuperado 20 de junio de 2025, de https://pilar.ccn-cert.cni.es/pilar/que-es-pilar

Centro Criptológico Nacional. (2012). MAGERIT – Metodología de análisis y gestión de riesgos de los sistemas de Información. Versión 3.0. Libro II: Catálogo de elementos. Ministerio de Hacienda y Administraciones Públicas.

Constitución de la Republica del Ecuador, Registro Oficial núm. 449, de 20 de octubre de 2008 (2008). https://www.defensa.gob.ec/wp-content/uploads/downloads/2021/02/Constitucion-de-la-Republica-del-Ecuador_act_ene-2021.pdf

# 5 ANEXOS

**Anexo A.**

*Fichas de activos de información Consulta Externa*

| **[info] información** | | | |
|---|---|---|---|
| **código** | A1 | **nombre** | Información de pacientes y citas médicas |
| **descripción**<br>Código único de expediente, datos personales, números de contacto, citas médicas, historial de atenciones | | | |
| **propietario** | Gestión de Admisiones | | |
| **responsable** | Analista de Estadística y Admisiones | | |
| **tipo**<br>Datos de carácter personal | | | |
| **Valoración** | | | |
| **dimensión** | **valor** | **justificación** | |
| Confidencialidad **[C]** | alta | Datos personales sensibles, ley de protección de datos personales | |
| Integridad **[I]** | media | Alteración de datos de pacientes y/o citas médicas afecta atención en el servicio de consulta externa | |
| Disponibilidad **[C]** | media | Imprescindible para agendamiento de citas y atención programada de usuarios | |
| **Dependencias de activos inferiores** | | | |
| **grado** | **activo** | | |
| alto | A3, A4, A5, A7, A8, A9 | | |

| **[service] servicios** | | | |
|---|---|---|---|
| **código** | A2 | **nombre** | Servicio de Consulta Externa |
| **descripción**<br>Atención médica ambulatoria de especialidad en pacientes referidos de unidades de salud de primer de atención. | | | |
| **propietario** | Gestión de Especialidades Clínicas, Quirúrgicas o Clínico Quirúrgicas | | |
| **responsable** | Director/a de Hospital Básico | | |
| **tipo** | | | |

| Servicios (procesos de gestión asistencial apoyados por TIC) | | |
|---|---|---|
| **Valoración** | | |
| **dimensión** | **valor** | **justificación** |
| Confidencialidad **[C]** | despreciable | |
| Integridad **[I]** | despreciable | |
| Disponibilidad **[C]** | medio | Afectación directa a la atención, retrasos |
| **Dependencias de activos inferiores** | | |
| **grado** | **activo** | |
| alto | A1, A5, A8, A18 (+ infraestructura tecnológica) | |

| **[3rd] contratado a terceros** | |
|---|---|
| **código** A3 | **nombre** ISP - Acceso a Internet |
| **descripción**<br>Servicio de internet por fibra óptica proporcionado por CNT | |
| **propietario** | Proveedor de servicio CNT |
| **responsable** | Analista de Soporte Técnico |
| **tipo**<br>ISP Acceso a Internet servicios contratados a terceros | |

| **Valoración** | | |
|---|---|---|
| **dimensión** | **valor** | **justificación** |
| Confidencialidad **[C]** | baja | Intercepción de tráfico en caso de datos no cifrados |
| Integridad **[I]** | baja | En caso de alteración del canal |
| Disponibilidad **[C]** | alta | Indisponibilidad puede acarrear suspensión de registro de atenciones o citas medicas |
| **Dependencias de activos inferiores** | | |

| grado | activo |
|---|---|
| alto | A12, A14 |

| [so] sistema operativo | |
|---|---|
| **código** A4 | **nombre** Ubuntu Server 20.0.4 LTS |
| **descripción**<br>S.O de código abierto donde se ejecuta App Web de Consulta Externa y se almacena la base de datos | |
| **propietario** | Gestión de Tecnologías de la Información y Comunicaciones |
| **responsable** | Analista de Soporte Técnico |
| **tipo**<br>Sistema operativo Linux | |

| Valoración | | |
|---|---|---|
| **dimensión** | **valor** | **justificación** |
| Confidencialidad **[C]** | media | Puede contener archivos de configuración y datos sensibles |
| Integridad **[I]** | alta | Cambios o alteraciones pueden comprometer su funcionamiento |
| Disponibilidad **[C]** | alta | S.O base donde se ejecuta el servidor web, su caída afecta directamente a los pacientes |

| Dependencias de activos inferiores | |
|---|---|
| **grado** | **activo** |
| alto | A14, A15, A16 |

| [prp] desarrollo propio (in house) | |
|---|---|
| **código** A5 | **nombre** App Web Gestión de Consulta Externa |
| **descripción**<br>Aplicación para registro de tarjeta índice, agendamiento de citas, marcado de asistencia, generación de datos estadísticos e historial de atención de pacientes | |

| | |
|---|---|
| **propietario** | Gestión de Tecnologías de la Información y Comunicaciones |
| **responsable** | Analista de Soporte Técnico |
| **tipo**<br>Aplicación de desarrollo propio en lenguaje de programación PHP | |

| **Valoración** | | |
|---|---|---|
| **dimensión** | **valor** | **justificación** |
| Confidencialidad **[C]** | media | Gestiona datos personales sensibles |
| Integridad **[I]** | alta | Cambios o alteraciones afectan la atención a pacientes |
| Disponibilidad **[C]** | alta | Su indisponibilidad retrasa o paraliza la atención, altos tiempos de espera, daño reputacional |

| **Dependencias de activos inferiores** | |
|---|---|
| **grado** | **activo** |
| alto | A1, A3, A4, A7, A8, A9, A14 |

| **[sub] desarrollo a medida (Nivel Nacional)** | |
|---|---|
| **código** A6 | **nombre** App Web MSP PRAS |
| **descripción**<br>Plataforma para el registro de atenciones en salud y gestión de datos | |
| **propietario** | Ministerio de Salud Pública |
| **responsable** | Dirección Nacional de TIC |
| **tipo**<br>Aplicación desarrolla por el MSP para uso a nivel nacional, gestionada por planta central | |

| **Valoración** | | |
|---|---|---|
| **dimensión** | **valor** | **justificación** |
| Confidencialidad **[C]** | media | Datos de salud sensibles, no directamente administrados por la organización |

| | | |
|---|---|---|
| Integridad **[I]** | baja | La alteración de datos no repercute directamente en la organización |
| Disponibilidad **[C]** | alta | Caídas o intermitencias del sistema retrasan la atención de citas y generan altos tiempos de espera |

| **Dependencias de activos inferiores** | |
|---|---|
| **grado** | **activo** |
| alto | A3, A14, A18 |

| **[app] servidor de aplicaciones** | |
|---|---|
| **código** A7 | **nombre** Servidor HTTP Apache |
| **descripción**<br>Servidor web de código abierto que permite la ejecución de aplicaciones web dinámicas | |
| **propietario** | Gestión de Tecnologías de la Información y Comunicaciones |
| **responsable** | Analista de Soporte Técnico |
| **tipo**<br>Servidor de aplicaciones, App Web Gestión de Consulta Externa | |

| **Valoración** | | |
|---|---|---|
| **dimensión** | **valor** | **justificación** |
| Confidencialidad **[C]** | media | Acceso no autorizado puede permitir exposición de datos personales sensibles |
| Integridad **[I]** | alta | La alteración de configuración puede inhabilitar las aplicaciones alojadas |
| Disponibilidad **[C]** | media | Caída del servicio impide la gestión automatizada de citas médicas de consulta externa. |

| **Dependencias de activos inferiores** | |
|---|---|
| **grado** | **activo** |
| alto | A3, A4, A8, A9 |

| **[dbms] sistema de gestión de bases de datos** |
|---|

| **código** A8 | **nombre** MySQL BD Consulta Externa |
|---|---|
| **descripción**<br>Servidor de código abierto, almacena información de personal de pacientes y citas médicas | |
| **propietario** | Gestión de Tecnologías de la Información y Comunicaciones |
| **responsable** | Analista de Soporte Técnico |
| **tipo**<br>Servidor de base de datos relacional | |

| **Valoración** | | |
|---|---|---|
| **dimensión** | **valor** | **justificación** |
| Confidencialidad **[C]** | alta | Acceso no autorizado puede permitir exposición de datos personales sensibles |
| Integridad **[I]** | alta | La corrupción o modificación no autorizada podría comprometer la atención ambulatoria |
| Disponibilidad **[C]** | alta | La indisponibilidad afecta la atención médica en consulta externa y el agendamiento de citas |

| **Dependencias de activos inferiores** | |
|---|---|
| **grado** | **activo** |
| alto | A1, A4, A5, A7 |

| **[host] grandes equipos (1)** | |
|---|---|
| **código** A9 | **nombre** HP Proliant DL380G7 |
| **descripción**<br>Servidor físico con SO base Ubuntu Server 20.04 LTS, LAMP (Linux -Apache -MySQL -PHP) para la aplicación web de gestión de consulta externa. | |
| **propietario** | Gestión de Tecnologías de la Información y Comunicaciones |
| **responsable** | Analista de Soporte Técnico |
| **tipo**<br>Equipo servidor, soporte de ejecución de las aplicaciones informáticas | |

| Valoración | | |
|---|---|---|
| **dimensión** | **valor** | **justificación** |
| Confidencialidad **[C]** | baja | Acceso físico podría comprometer los datos almacenados |
| Integridad **[I]** | alta | Daños al hardware pueden afectar el sistema de Gestión de Consulta Externa y datos almacenados |
| Disponibilidad **[C]** | alta | Fallo puede paralizar servicios esenciales como consultas a la base de datos y aplicaciones web |
| **Dependencias de activos inferiores** | | |
| **grado** | **activo** | |
| alto | A13, A14 | |

| [pc] informática personal (3) | |
|---|---|
| **código** A10 | **nombre** Pc computadores personales |
| **descripción**<br>Equipos de escritorio utilizados por médicos, enfermeras y personal administrativo para gestionar la atención en consulta externa | |
| **propietario** Activos Fijos | |
| **responsable** Profesionales operativos o administrativos | |
| **tipo**<br>Equipos personales de soporte de ejecución de las aplicaciones informáticas | |

| Valoración | | |
|---|---|---|
| **dimensión** | **valor** | **justificación** |
| Confidencialidad **[C]** | baja | Acceso indebido puede exponer información personal |
| Integridad **[I]** | baja | Daño físico, mal uso o malware puede comprometer la integridad de datos almacenados |
| Disponibilidad **[C]** | baja | Su falla o daño puede afectar la atención de manera temporal o aislada |
| **Dependencias de activos inferiores** | | |
| **grado** | **activo** | |

| | |
|---|---|
| alto | A3, A13, A14 |

| **[switch] conmutadores** | | |
|---|---|---|
| **código** A11 | **nombre** | Switch D-Link DES-1024D |
| **descripción**<br>Dispositivo de red, conmutadores que sirven para interconectar los computadores, servidores y otros dispositivos de red LAN | | |
| **propietario** | Gestión de Tecnologías de la Información y Comunicaciones | |
| **responsable** | Analista de Soporte Técnico | |
| **tipo**<br>Soporte de red para equipos personales, servidores y otros dispositivos. | | |
| **Valoración** | | |
| **dimensión** | **valor** | **justificación** |
| Confidencialidad **[C]** | baja | Podría permitir intercepción de tráfico |
| Integridad **[I]** | baja | Errores en transmisión de datos |
| Disponibilidad **[C]** | media | Su falla o daño puede afectar la conectividad entre equipos, por ende el acceso aplicaciones |
| **Dependencias de activos inferiores** | | |
| **grado** | **activo** | |
| alto | A13, A14 | |

| **[router] encaminadores** | | |
|---|---|---|
| **código** A12 | **nombre** | Router Linksys e900 |
| **descripción**<br>Dispositivo de red que permite enrutamiento IP para acceso a internet, permite la asignación de IP dinámica (DHCP) para la red interna. | | |
| **propietario** | Gestión de Tecnologías de la Información y Comunicaciones | |

| | |
|---|---|
| **responsable** | Analista de Soporte Técnico |
| **tipo**<br>Soporte de red, puerta de enlace para diferentes dispositivos | |

| **Valoración** | | |
|---|---|---|
| **dimensión** | **valor** | **justificación** |
| Confidencialidad **[C]** | baja | Incorrecta configuración puede exponer la red local (LAN) |
| Integridad **[I]** | baja | Puede permitir redirección o interceptación de tráfico de red. |
| Disponibilidad **[C]** | media | Daño o fallo impiden el acceso a internet o sistemas internos, afectando los servicios administrativos y operativos |

| **Dependencias de activos inferiores** | |
|---|---|
| **grado** | **activo** |
| alto | A13, A14 |

| **[com] red de datos** | | | |
|---|---|---|---|
| **código** | A13 | **nombre** | LAN CAT 6e |
| **descripción**<br>Infraestructura de cableado estructurado para conexión de estaciones de trabajo, servidores, routers, switches y otros dispositivos de red, transmisión de red de 100 Mbps | | | |
| **propietario** | Gestión de Tecnologías de la Información y Comunicaciones | | |
| **responsable** | Analista de Soporte Técnico | | |
| **tipo**<br>Red de comunicaciones | | | |

| **Valoración** | | |
|---|---|---|
| **dimensión** | **valor** | **justificación** |
| Confidencialidad **[C]** | baja | Acceso físico no autorizado al cableado puede permitir interceptación de datos. |

| | | |
|---|---|---|
| Integridad **[I]** | media | Daños físicos pueden ocasionar problemas en la transmisión de datos. |
| Disponibilidad **[C]** | media | Daños o corte en el cableado puede afectar el acceso aplicaciones o servicios de red |

| **Dependencias de activos inferiores** | |
|---|---|
| **grado** | **activo** |
| alto | A16 (condiciones en patch panel, conectores, tomas de red) |

| **[power] fuentes de alimentación** | |
|---|---|
| **código** A14 | **nombre** Alimentación Eléctrica |
| **descripción**<br>Suministro de energía eléctrica de red pública | |
| **propietario** | Mantenimiento HBRMM |
| **responsable** | Auxiliar de Mantenimiento |
| **tipo**<br>Equipamiento auxiliar uso como soporte a los sistemas de información | |

| **Valoración** | | |
|---|---|---|
| **dimensión** | **valor** | **justificación** |
| Confidencialidad **[C]** | despreciable | No almacena información |
| Integridad **[I]** | media | Cortes de energía pueden provocar daños en aplicaciones o pérdida de datos |
| Disponibilidad **[C]** | alta | Interrupción energía eléctrica detiene la operación de los sistemas de información |

| **Dependencias de activos inferiores** | |
|---|---|
| **grado** | **activo** |
| alto | A15 |

| **[ups] sai - sistemas de alimentación ininterrumpida** |
|---|

| **código** A15 | **nombre** UPS APC BR1500M2-LM |
|---|---|
| **descripción**<br>Sistema de alimentación ininterrumpida que permite respaldo eléctrico temporal | |
| **propietario** | Gestión de Tecnologías de la Información y Comunicaciones |
| **responsable** | Analista de Soporte Técnico |
| **tipo**<br>Equipamiento auxiliar uso como soporte a los sistemas de información | |

| **Valoración** | | |
|---|---|---|
| **dimensión** | **valor** | **justificación** |
| Confidencialidad **[C]** | despreciable | No almacena información |
| Integridad **[I]** | media | Cortes de energía pueden provocar daños en equipos o corrupción de datos |
| Disponibilidad **[C]** | alta | Fallo o daño en cortes de energía eléctrica detiene la operación de los sistemas de información |

| **Dependencias de activos inferiores** | |
|---|---|
| **grado** | **activo** |
| alto | A14 |

| **[local] cuarto** | |
|---|---|
| **código** A16 | **nombre** Centro de Datos |
| **descripción**<br>Espacio físico que aloja servidores, equipos de red y otros dispositivos esenciales para el funcionamiento del HBRMM y el servicio de consulta externa. | |
| **propietario** | Gestión de Tecnologías de la Información y Comunicaciones |
| **responsable** | Analista de Soporte Técnico |
| **tipo**<br>Instalaciones que hospedan los sistemas de información y comunicaciones | |

| Valoración | | |
|---|---|---|
| **dimensión** | **valor** | **justificación** |
| Confidencialidad **[C]** | media | Acceso físico no autorizado compromete dispositivos que contienen información sensible. |
| Integridad **[I]** | alta | Daños físicos, eléctricos o ambientales pueden dañar dispositivos y comprometer datos y servicios. |
| Disponibilidad **[C]** | alta | Indisponibilidad puede generar interrupciones de servicios TIC |
| **Dependencias de activos inferiores** | | |
| **grado** | **activo** | |
| alto | A13, A14, A15 | |

| [ui] usuarios internos | | | |
|---|---|---|---|
| **código** | A17 | **nombre** | Usuarios Internos |
| **descripción**<br>Personal administrativo que requiere de reportes y estadísticas de sistemas de información | | | |
| **propietario** | Dirección / Calidad | | |
| **responsable** | Director , Analistas. Asistentes | | |
| **tipo**<br>Personas relacionadas con los sistemas de información | | | |
| **Valoración** | | | |
| **dimensión** | **valor** | **justificación** | |
| Confidencialidad **[C]** | baja | Puede exponer datos personales sensibles | |
| Integridad **[I]** | despreciable | Manejo de reportes más no procesamiento de informacion | |
| Disponibilidad **[C]** | baja | Reportes y estadísticas de atenciones no son consideradas activos esenciales | |
| **Dependencias de activos inferiores** | | | |
| **grado** | **activo** | | |

| | |
|---|---|
| bajo | A1, A5 |

| **[op] operadores** | | |
|---|---|---|
| **código** A18 | **nombre** | Usuarios Operadores |
| **descripción**<br>Personal administrativo y operativo (profesionales de salud, analistas, técnicos) que usan sistemas y recursos informáticos para acceder a información, registrar atenciones, gestionar citas y generar reportes | | |
| **propietario** | Admisión / Estadística / Enfermería / Consultorios | |
| **responsable** | Profesionales de la salud, analistas, asistentes | |
| **tipo**<br>Personas que operan los sistemas de información | | |
| **Valoración** | | |
| **dimensión** | **valor** | **justificación** |
| Confidencialidad **[C]** | alta | Puede exponer datos personales sensibles |
| Integridad **[I]** | alta | Errores pueden afectar registros de datos y citas médicas |
| Disponibilidad **[C]** | alta | Ausencia o indisponibilidad del personal impide agendamiento de citas y atenciones programadas |
| **Dependencias de activos inferiores** | | |
| **grado** | **activo** | |
| alto | A1, A5 | |

REPÚBLICA DEL ECUADOR

Coordinación Zonal de Salud 2
Dirección Distrital 17 D10 Cayambe – Pedro Moncayo – SALUD
Hospital Básico Cayambe

Cayambe 21 de agosto del 2025

Dra. Lucia Yépez

**DECANA FACULTAD DE POSTGRADO UTN**

Me permito informar a usted que el Sr. Segundo Franklin Lara Cartagena con CI. 1714632575, estudiante del Programa de Maestría en Computación con mención en Seguridad Informática, de la Universidad Técnica del Norte, ha sido aceptado en el Hospital Básico Cayambe, para realizar su trabajo de titulación. La institución brindara las facilidades e información necesarias para el desarrollo de la investigación.

Agradezco su atención.

Mgs.Luis Esteban Visarrea

**Director Hospital Básico Cayambe**

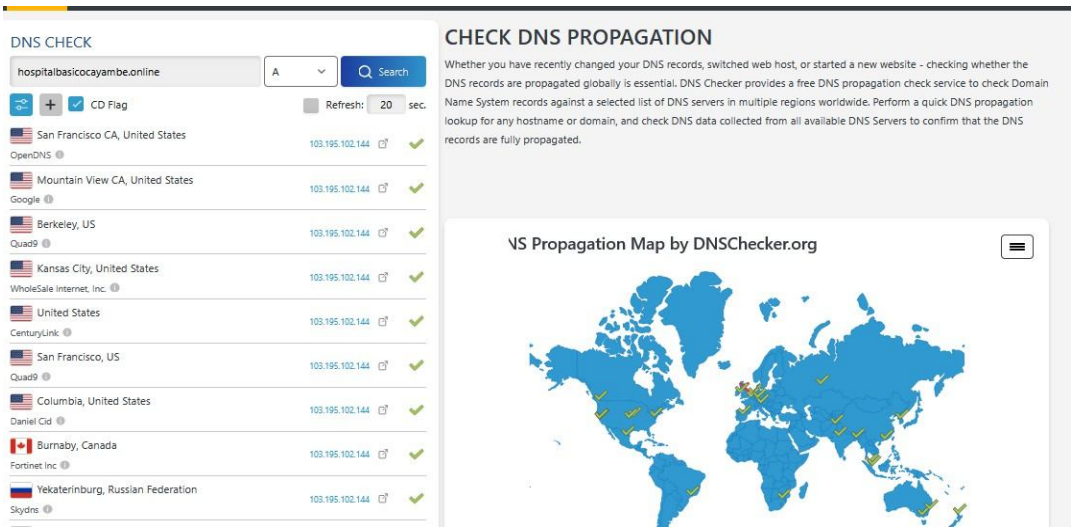
MINISTERIO DE SALUD PÚBLICA
SECRETARÍA
HOSPITAL BÁSICO CAYAMBE

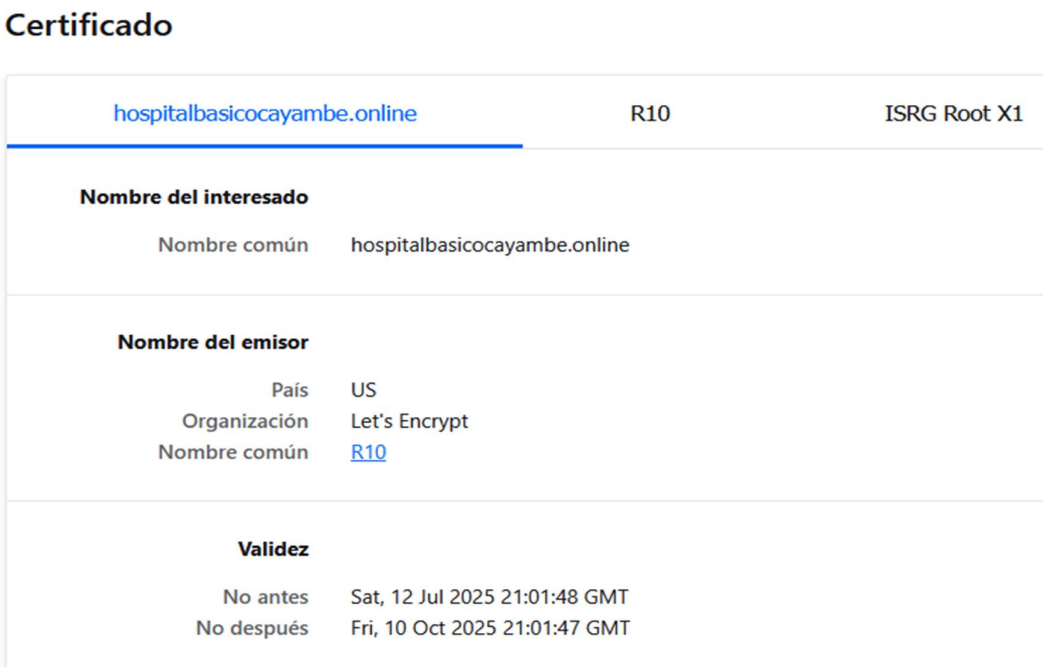
Dirección: Av. 15 de Noviembre y Zamora
Código postal: 150150 / Tena - Ecuador
Teléfono: +593-6-2886-420
www.salud.gob.ec

EL NUEVO ECUADOR

**Anexo B.**

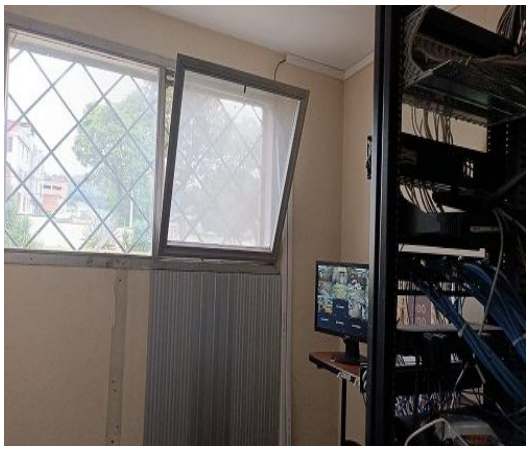
*VPS Propagación de DNS, Certificado SSL Let´s Encrypt*

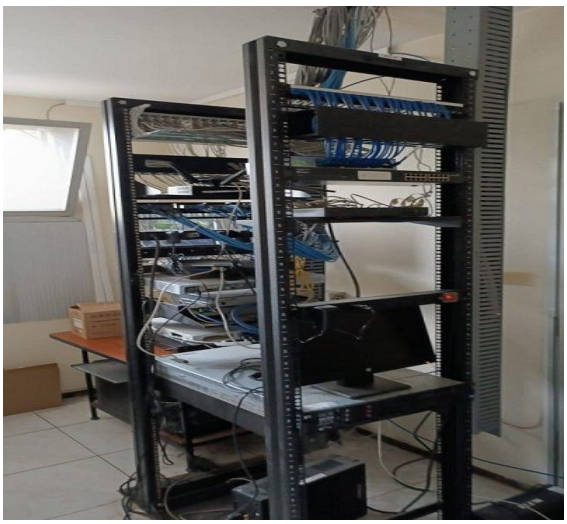


**Anexo C.**

*Centro de datos y Consulta Externa HBRMM*




**Anexo D.**

*Transcripción de entrevista al responsable TIC*

| Pregunta | Respuesta |
|---|---|
| ¿Cuál es su cargo actual en la institución? | Analista de Soporte Técnico |
| ¿Cuánto tiempo ha estado en este cargo? | 5 años |
| Principales funciones y responsabilidades | Soporte técnico a usuarios; Administración de aplicaciones: correo institucional, Quipux, Consulta Externa, Emergencia |
| ¿Cómo se relacionan sus funciones con la gestión de la seguridad de los sistemas? | Mantenimiento preventivo de equipos, que incluye actualizaciones de sistema operativo y antivirus; Administración de acceso a sistemas para usuarios |
| ¿Cómo controla y gestiona el acceso físico al centro de datos? | Se permite el acceso solo a personal de TI y a empleados con autorización |
| ¿Qué medidas de seguridad física y controles de acceso están implementados? | No existen mecanismos tecnológicos de seguridad física |
| ¿El equipamiento del centro de datos asegura la disponibilidad de los servicios web considerando una vida útil de tres años? | No, los equipos están obsoletos; se trabaja con los equipos disponibles |
| ¿Cómo asegura soporte de energía y sistemas de enfriamiento en el centro de datos? | No se cuenta con soporte adecuado de energía ni de enfriamiento; el centro de datos opera en un espacio no apropiado |
| ¿Qué medidas toma para garantizar la continuidad operativa ante fallos de energía o problemas de enfriamiento? | Se cuenta con un UPS de **1500 KVA**; no hay sistema de enfriamiento |
| ¿Qué prácticas de seguridad implementa regularmente en Ubuntu Server? | Actualización periódica del sistema operativo; Uso de firewall UFW; Uso de SSH para conexiones remotas |
| ¿Qué prácticas de seguridad utiliza para la administración del acceso SSH a los servidores? | Actualización periódica del servidor SSH |
| ¿Cómo gestiona las claves SSH y el acceso remoto? | Acceso remoto habilitado con llave privada por el puerto 22 |
| ¿Cómo configura la protección de los servicios web? | No está configurado |
| ¿Qué reglas y políticas de firewall implementa? | Reglas para habilitar los puertos 22 (SSH) y 80 (Apache) |