

INSTITUTO SUPERIOR TECNOLÓGICO SUDAMERICANO



INSTITUTO TECNOLÓGICO
SUDAMERICANO
Hacemos gente de talento!



CIBERSEGURIDAD
TECNOLOGÍA SUPERIOR

TECNOLOGÍA SUPERIOR EN CIBERSEGURIDAD

EMPRENDIMIENTO TECNOLÓGICO PARA EL DESARROLLO DE UN DISPOSITIVO
DE SEGURIDAD CON RASPBERRY PI ORIENTADO A LA PROTECCIÓN DE LA
INFORMACIÓN Y MITIGACIÓN DE RANSOMWARE EN CLÍNICAS Y CENTROS DE
ESPECIALIDADES PRIVADOS DE LA CIUDAD DE MACHALA.

INFORME DEL PROYECTO DE INVESTIGACIÓN PREVIO A LA OBTENCIÓN DEL
TÍTULO DE TECNÓLOGO EN LA TECNOLOGÍA SUPERIOR EN CIBERSEGURIDAD

AUTORES:

Jose Xavier Mocha Quichimbo

Anthony Edinson Yaguachi Cárdenas

TUTOR

Ing. Linder Fernando Bravo Pardo, Mgs

Machala, Junio 2026

Certificación Del Director Del Proyecto De Inv. Fin De Carrera

Ingeniero

Linder Fernando Bravo Pardo, Mgs

DIRECTOR DE PROYECTO DE FIN DE CARRERA

CERTIFICO:

Que he supervisado el siguiente proyecto de investigación titulado Emprendimiento tecnológico para el desarrollo de un dispositivo de seguridad con raspberry pi orientado a la protección de la información y mitigación de ransomware en clínicas y centros de especialidades privados de la ciudad de Machala, realizado por los estudiantes Jose Xavier Mocha Quichimbo y Anthony Edinson Yaguachi Cárdenas, el mismo que cumple con lo establecido por el Instituto Superior Tecnológico Sudamericano; por consiguiente, autorizo su presentación ante el tribunal respectivo.

Machala, junio del 2026



Ing. Linder Fernando Bravo Pardo, Mgs

C.I.: 1104635089

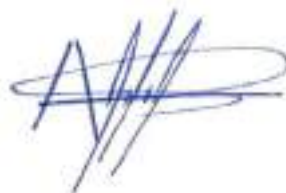
Autoría

Nosotros, Jose Xavier Mocha Quichimbo y Anthony Edinson Yaguachi Cárdenas, estudiantes del Instituto Superior Tecnológico Sudamericano a continuación certificamos que los criterios, opiniones, afirmaciones, análisis, interpretaciones, conclusiones, recomendaciones y todos los demás aspectos vertidos en el presente proyecto de investigación de fin de carrera son de nuestra absoluta responsabilidad.

Machala, 01 de junio 2026



Firma
C.I. 0705609857



Firma
C.I. 0705528008

Dedicatoria

Quiero dedicar este trabajo de titulación a mi amada esposa Arleth Cruz Potes, quien ha estado a mi lado en cada paso de este proceso. Gracias por tu inmensa paciencia, por escucharme en los momentos más complicados y por darme el impulso necesario cuando sentía que ya no podía más.

Tu apoyo constante, tus palabras de aliento y tu compañía fueron fundamentales para que hoy pueda estar aquí. Cada esfuerzo puesto en este proyecto y cada logro alcanzado llevan impregnados una parte de ti, porque siempre creíste en mí y nunca permitiste que me rindiera.

Este trabajo no es solo una meta académica cumplida, sino el reflejo de todo el amor y el respaldo que recibí de tu parte a lo largo de este camino.

Jose Xavier Mocha Quichimbo

Este fruto quiero dedicarlo primero a Dios, quien ha sabido guiarme y bendecirme con su inmensa sabiduría a lo largo de mis estudios. A mi amada Mercedes Cárdenas Jiménez, por todas las veces que me animó a seguir adelante con su ejemplo y su infinita ayuda. A mi guerrero Jaime Yaguachi Bustamante, porque sin su paciencia no lo habría logrado, y por brindarme su incondicional amor. También quiero dedicárselo a mis amados hermanos, ya que sin sus alegrías no habría sido capaz de lograr esto. Por último, a mi familia, en especial a mi resiliente Jimmy Cárdenas Jiménez, quien siempre me salvó con sus consejos y charlas. Este trabajo es una demostración de mí para ustedes, por nunca dejarme rendir.

Anthony Edinson Yaguachi Cárdenas

Agradecimiento

Empezamos agradeciendo a Dios, porque él es la razón de nuestra existencia y quien nos guía para encontrar nuestro propósito de ayudar a los demás. Al Instituto Superior Tecnológico Sudamericano, nuestro hogar de estudios, por darnos las herramientas para enfrentar los desafíos del mundo digital. Un agradecimiento especial al Ing. Samaniego por sus enseñanzas en las aulas, y a nuestro tutor, el Ing. Linder Bravo Pardo; sus orientaciones fueron el faro que nos permitió aterrizar nuestras ideas en un proyecto tecnológico real.

Este logro también es un reconocimiento a nuestro propio esfuerzo. Nos agradecemos mutuamente como compañeros, por no rendirnos cuando las materias se ponían difíciles. Alcanzar este título de tercer nivel es algo que siempre anhelamos, un sueño cumplido que hoy le dedicamos con todo el amor y orgullo a nuestras madres.

Finalmente, a nuestras familias y a todas las personas que nos sostuvieron con su paciencia infinita y sus sacrificios silenciosos cuando las cosas se complicaban. Gracias a quienes nos salvaron con un buen consejo y una palabra de aliento; hoy cerramos este peldaño con la inmensa satisfacción de haberlo logrado y listos para salir al campo profesional.

Con agradecimiento los autores.

Acta de Cesión de Derechos

ACTA DE CESIÓN DE DERECHOS DE PROYECTO DE INVESTIGACIÓN DE FIN DE CARRERA

Conste por el presente documento la Cesión de los Derechos de proyecto de investigación de fin de carrera, de conformidad con las siguientes cláusulas:

PRIMERA. - Por sus propios derechos; Ing. Linder Fernando Bravo Pardo, Mgs, en calidad de Director del proyecto de investigación de fin de carrera; y, Jose Xavier Mocha Quichimbo y Anthony Edinson Yaguachi Cárdenas, en calidad de autores del proyecto de investigación de fin de carrera; mayores de edad emiten la presente acta de cesión de derechos.

SEGUNDA. - Jose Xavier Mocha Quichimbo y Anthony Edinson Yaguachi Cárdenas, realizaron la investigación titulada “EMPRENDIMIENTO TECNOLÓGICO PARA EL DESARROLLO DE UN DISPOSITIVO DE SEGURIDAD CON RASPBERRY PI ORIENTADO A LA PROTECCIÓN DE LA INFORMACIÓN Y MITIGACIÓN DE RANSOMWARE EN CLÍNICAS Y CENTROS DE ESPECIALIDADES PRIVADOS DE LA CIUDAD DE MACHALA”; para optar por el título de Tecnólogo en Ciberseguridad, en el Instituto Superior Tecnológico Sudamericano de Machala, bajo la dirección Ing. Ana Cordero Clavijo, Mgs.

TERCERA. - Es política del Instituto que los proyectos de investigación de fin de carrera se apliquen y materialicen en beneficio de la comunidad.

CUARTA. - Los Ing. Linder Fernando Bravo Pardo, Mgs, en calidad de Director del proyecto de investigación de fin de carrera y Jose Xavier Mocha Quichimbo y Anthony

Edinson Yaguachi Cárdenas como autores, por medio del presente instrumento, tienen a bien ceder en forma gratuita sus derechos de proyecto de investigación de fin de carrera titulado “EMPRENDIMIENTO TECNOLÓGICO PARA EL DESARROLLO DE UN DISPOSITIVO DE SEGURIDAD CON RASPBERRY PI ORIENTADO A LA PROTECCIÓN DE LA INFORMACIÓN Y MITIGACIÓN DE RANSOMWARE EN CLÍNICAS Y CENTROS DE ESPECIALIDADES PRIVADOS DE LA CIUDAD DE MACHALA” a favor del Instituto Superior Tecnológico Sudamericano de Machala; y, conceden autorización para que el Instituto pueda utilizar esta investigación en su beneficio y/o de la comunidad, sin reserva alguna.

QUINTA. - Aceptación. - Las partes declaran que aceptan expresamente todo lo estipulado en la presente cesión de derechos.

Para constancia suscriben la presente cesión de derechos, en la ciudad de Machala, en el mes de junio del año 2026



.....
Ing. Linder Fernando
Bravo Pardo, Mgs
C.I. 1104635089



.....
Jose Xavier
Mocha Quichimbo
C.I. 0705609857



.....
Anthony Edinson
Yaguachi Cárdenas
C.I. 0705528008

Declaración Juramentada

DECLARACIÓN JURAMENTADA

Machala, 01 de junio del 2026

Nombres: Jose Xavier

Apellidos: Mocha Quichimbo

Cédula de Identidad: 0705609857

Carrera: Ciberseguridad

Semestre de ejecución del proceso de titulación: Noviembre 2025 – Marzo 2026

Tema de proyecto de investigación de fin de carrera con fines de titulación: Emprendimiento tecnológico para el desarrollo de un dispositivo de seguridad con raspberry pi orientado a la protección de la información y mitigación de ransomware en clínicas y centros de especialidades privados de la ciudad de Machala.

En calidad de estudiante del Instituto Tecnológico Superior Sudamericano de la ciudad de Machala;

Declaro bajo juramento que:

1. Soy autor del trabajo intelectual y de investigación del proyecto de fin de carrera.
2. El trabajo de investigación de fin de carrera no ha sido plagiado ni total ni parcialmente, para la cual se han respetado las normas internacionales de citas y referencias para las fuentes consultadas.
3. El trabajo de investigación de fin de carrera presentada no atenta contra derechos de terceros.
4. El trabajo de investigación de fin de carrera no ha sido publicado ni presentada anteriormente para obtener algún grado académico previo o título profesional.

5. Los datos presentados en los resultados son reales, no han sido falsificados, ni duplicados, ni copiados. Las imágenes, tablas, gráficas, fotografías y demás son de mi autoría; y en el caso contrario aparecen con las correspondientes citas o fuentes.

Por lo expuesto; mediante la presente asumo frente al INSTITUTO cualquier responsabilidad que pudiera derivarse por la autoría, originalidad y veracidad del contenido del trabajo de investigación de fin de carrera.

En consecuencia, me hago responsable frente al INSTITUTO y frente a terceros, de cualquier daño que pudiera ocasionar al INSTITUTO o a terceros, por el incumplimiento de lo declarado o que pudiera encontrar causa en el trabajo de investigación de fin de carrera presentada, asumiendo todas las cargas pecuniarias que pudieran derivarse de ello.

Asimismo, por la presente me comprometo a asumir además todas las cargas pecuniarias que pudieran derivarse para EL INSTITUTO en favor de terceros por motivo de acciones, reclamaciones o conflictos derivados del incumplimiento de lo declarado o las que encontraren causa en el contenido del trabajo de investigación de fin de carrera.

De identificarse fraude, piratería, plagio, falsificación o que el trabajo de investigación haya sido publicado anteriormente; asumo las consecuencias y sanciones que de mi acción se deriven, sometiéndome a la normatividad vigente dispuesta por la LOES y sus respectivos reglamentos y del Instituto Tecnológico Superior Sudamericano de la ciudad de Machala.



Jose Xavier Mocha Quichimbo
Nro. Cédula 0705609857

DECLARACIÓN JURAMENTADA

Machala, 01 de junio del 2026

Nombres: Anthony Edinson

Apellidos: Yaguachi Cárdenas

Cédula de Identidad: 0705528008

Carrera: Ciberseguridad

Semestre de ejecución del proceso de titulación: Noviembre 2025 – Marzo 2026

Tema de proyecto de investigación de fin de carrera con fines de titulación: Emprendimiento tecnológico para el desarrollo de un dispositivo de seguridad con raspberry pi orientado a la protección de la información y mitigación de ransomware en clínicas y centros de especialidades privados de la ciudad de Machala.

En calidad de estudiante del Instituto Tecnológico Superior Sudamericano de la ciudad de Machala;

Declaro bajo juramento que:

6. Soy autor del trabajo intelectual y de investigación del proyecto de fin de carrera.
7. El trabajo de investigación de fin de carrera no ha sido plagiado ni total ni parcialmente, para la cual se han respetado las normas internacionales de citas y referencias para las fuentes consultadas.
8. El trabajo de investigación de fin de carrera presentada no atenta contra derechos de terceros.
9. El trabajo de investigación de fin de carrera no ha sido publicado ni presentada anteriormente para obtener algún grado académico previo o título profesional.

10. Los datos presentados en los resultados son reales, no han sido falsificados, ni duplicados, ni copiados. Las imágenes, tablas, gráficas, fotografías y demás son de mi autoría; y en el caso contrario aparecen con las correspondientes citas o fuentes.

Por lo expuesto; mediante la presente asumo frente al INSTITUTO cualquier responsabilidad que pudiera derivarse por la autoría, originalidad y veracidad del contenido del trabajo de investigación de fin de carrera.

En consecuencia, me hago responsable frente al INSTITUTO y frente a terceros, de cualquier daño que pudiera ocasionar al INSTITUTO o a terceros, por el incumplimiento de lo declarado o que pudiera encontrar causa en el trabajo de investigación de fin de carrera presentada, asumiendo todas las cargas pecuniarias que pudieran derivarse de ello.

Asimismo, por la presente me comprometo a asumir además todas las cargas pecuniarias que pudieran derivarse para EL INSTITUTO en favor de terceros por motivo de acciones, reclamaciones o conflictos derivados del incumplimiento de lo declarado o las que encontraren causa en el contenido del trabajo de investigación de fin de carrera.

De identificarse fraude, piratería, plagio, falsificación o que el trabajo de investigación haya sido publicado anteriormente; asumo las consecuencias y sanciones que de mi acción se deriven, sometiéndome a la normatividad vigente dispuesta por la LOES y sus respectivos reglamentos y del Instituto Tecnológico Superior Sudamericano de la ciudad de Machala.



Anthony Edinson Yaguachi Cárdenas
Nro. Cédula 0705528008

Índice

Certificación Del Director Del Proyecto De Inv. Fin De Carrera	ii
Autoría	iii
Dedicatoria.....	iv
Agradecimiento	vi
Acta de Cesión de Derechos.....	vii
Declaración Juramentada.....	ix
Índice	xiii
Índice de figuras	xviii
Índice de tablas	xix
Resumen	xx
Abstract.....	xxi
1. Planteamiento Del Problema	1
2. Determinación Del Tema.....	3
3. Lineamientos De Investigación	4
3.1. Línea de Investigación.....	4
3.1.1. Sublínea de Investigación.....	4
3.2. Objetivo de Desarrollo Sostenible.....	4
3.3. Programa de Investigación	4
4. Justificación	5
5. Objetivos.....	7
5.1. Objetivo General.....	7
5.2. Objetivos Específicos	7

6.	Marco Teórico.....	8
6.1.	Marco Contextual	8
6.2.	Marco Conceptual.....	11
6.2.1.	Introducción Teórica.....	11
6.2.2.	Antecedentes Conceptuales y Estudios Previos	11
6.2.3.	Conceptos Fundamentales	12
6.2.4.	Teorías, Modelos y Estándares Aplicados	14
6.2.5.	Variables y Componentes de Análisis.....	16
6.2.6.	Integración Conceptual.....	16
7.	Diseño Metodológico	17
7.1.	Herramientas De Aplicación.....	17
7.1.1.	Herramientas Propias De La Metodología De Cada Área De Especialidad	17
7.1.2.	Herramientas Generales.....	18
7.2.	Encuesta.....	18
7.3.	Técnicas De Aplicación	19
8.	Desarrollo De Investigación Y Propuesta De Acción.....	20
8.1.	Determinación del universo y de la muestra	20
8.2.	Diseño de herramienta	23
8.2.1.	Estudio de mercado	25
8.3.	Aplicación de herramientas de investigación	26
8.4.	Análisis de resultados	28
8.4.1.	Análisis de mercado.....	29

8.4.2. Análisis de Vulnerabilidad y Riesgo Tecnológico.....**¡Error!**

Marcador no definido.

9.	Propuesta De Acción	39
9.1.	Construcción de la propuesta.....	39
9.1.1.	Arquitectura de Hardware (Capa Física)	40
9.1.2.	Escudo Pasivo: Bóveda Virtual e Inmutabilidad (Capa Lógica)	40
9.1.3.	Escudo Activo: Sistema de Prevención de Intrusiones (IDPS) y Kill-Switch	41
9.2.	Recursos y Requerimientos	42
9.2.1.	Requerimientos de Software y Tiempo de Ejecución.....	43
9.2.2.	Recursos Materiales y Presupuesto de Implementación.....	43
9.3.	Validación Técnica (Pruebas de Estrés en Laboratorio)	44
9.3.1.	Fase 1: Validación del Escudo Activo (Ataque de Denegación de Servicio y Kill-Switch).....	45
9.3.2.	Fase 2: Validación del Escudo Pasivo (Simulación de Infección por Ransomware y RPO).....	46
10.	Modelo de Emprendimiento	48
10.1.	CANVA(F)*	48
10.2.	Descripción Empresarial(F)*	51
10.3.	Flujo Financiero Esperado(F)*	52
10.3.1.	Presupuesto de Inversión Inicial	53
10.3.2.	Flujo de Dinero Proyectado	54

11.	Prototipo De Producto	59
11.1.	Identidad corporativa.....	59
11.2.	Descripción de producto o servicio	61
11.3.	Canal de promoción.....	63
11.4.	Validación del Prototipo	66
11.4.1.	Oportunidades de mejora detectadas	68
11.4.2.	Evidencia Documental.....	68
12.	Presupuesto	69
13.	Cronograma	70
14.	Conclusiones.....	71
15.	Recomendaciones	72
16.	Bibliografía.....	73
17.	Anexos	76
	Anexo A: Certificado de aprobación de Vicerrectorado de Innovación y Desarrollo ..	76
	Anexo B: Certificado de aprobación de la entidad para la ejecución del proyecto	77
	Anexo C: Acta de socialización de la propuesta de acción	78
	Anexo D: Certificado de Abstract	79
	Anexo E: Presupuesto.....	80
	Anexo F: Cronograma	81
	Anexo G: Formato de encuesta	82
	Anexo H: Formato de encuesta validado.....	84
	Anexo I: Encuesta de satisfacción realizada de forma virtual.....	86
	Anexo J: Base de datos.....	87

Anexo K: Evidencias fotográficas sobre la realización de encuestas y tabulación	88
Anexo M: Evidencias de desarrollo de la aplicación	89
Anexo N: Evidencias del funcionamiento de la aplicación	90
Anexo Ñ: Solicitud de Aprobación del Tema de Titulación	91
Anexo O: Solicitud de Aprobación del Tema del Anteproyecto.....	92
Anexo P: Registro de Coordinación de Manera Virtual del Equipo de Investigación .	93

Índice de figuras

Figura 1 ¿Qué método utiliza actualmente para respaldar la información médica de sus pacientes?	29
Figura 2 ¿Con qué frecuencia se realizan las copias de seguridad en su institución? ...	30
Figura 3 ¿Qué tan preocupado está frente a un hackeo o pérdida de datos (Ransomware)?.....	31
Figura 4 ¿Conoce el concepto de "Almacenamiento Inmutable" (Copias que no se pueden borrar ni cifrar)?	32
Figura 5 ¿Qué tan preparado considera que está su centro para cumplir con la Ley de Protección de Datos (LOPD)?	33
Figura 6 ¿Cuál es el principal motivo por el que no tiene un servidor de seguridad profesional?.....	34
Figura 7 ¿Confiaría en un dispositivo local de bajo costo (Raspberry Pi) con soporte técnico en Machala?	35
Figura 8 ¿Qué característica valoraría más en una solución de respaldo?	36
Figura 9 ¿Qué rango de inversión mensual consideraría razonable para este servicio?	37
Figura 10 ¿Estaría interesado en una prueba piloto de este dispositivo en su institución?	38
Figura 11 Archivo Logs de devbox_auditoria	46
Figura 12 Comandos de restauración	47

Índice de tablas

Tabla 1	Comparativa entre Seguridad Tradicional y el Modelo Propuesto.....	15
Tabla 2	Desglose de presupuesto para el proyecto	43
Tabla 3	Lienzo de Modelo de Negocio (Canvas) de Corporación PhylaxTech.....	50
Tabla 4	Formato de la descripción empresarial.....	51
Tabla 5	Presupuesto de inversión inicial.....	53
Tabla 6	Modelo de Flujo de Dinero Proyectado	55
Tabla 7	TIR.....	57
Tabla 8	Presupuesto referencial para la ejecución del proyecto de titulación	69

Resumen

Las clínicas privadas de Machala enfrentan una vulnerabilidad crítica debido al secuestro de datos clínicos (ransomware), agravada por la gestión de información en equipos locales sin protección o nubes personales inseguras. Esta problemática surge de la falta de protocolos estandarizados y presupuestos limitados para ciberseguridad, lo que genera riesgos legales y la posible paralización de la atención médica ante ataques digitales.

El objetivo principal es desarrollar la "DevBox", un dispositivo de bajo costo basado en Raspberry Pi. Se plantearon objetivos específicos como crear un sistema de almacenamiento inmutable que garantice que la información de los pacientes siempre esté disponible e íntegra. Para esto se aplicó una metodología mixta con diseño secuencial exploratorio, que incluyó entrevistas y encuestas a 63 representantes del sector salud en Machala para diagnosticar vulnerabilidades, seguido de pruebas de estrés en laboratorio para validar la resistencia del hardware bajo estándares internacionales.

Como resultado final se obtuvo una herramienta que utiliza tecnología de archivos BTRFS para crear copias de solo lectura imposibles de cifrar por atacantes. El sistema incorpora un Sistema de Prevención de Intrusiones (IDPS) con un "Kill-Switch" automático que desconecta el equipo ante tráfico sospechoso y notifica vía Telegram; en pruebas de laboratorio, el prototipo recuperó el 100% de la información en menos de tres minutos tras una infección simulada.

En conjunto la DevBox no solo neutraliza la amenaza del ransomware, sino que garantiza la continuidad operativa de las clínicas, el cumplimiento de la normativa legal vigente y la protección de la privacidad de los datos sensibles de los pacientes.

Abstract

Private clinics in Machala face a critical vulnerability due to clinical data ransomware attacks, exacerbated by the management of information on unprotected local computers or insecure personal cloud services. This problem stems from a lack of standardized protocols and limited cybersecurity budgets, which creates legal risks and the potential for medical care to grind to a halt in the event of a cyberattack.

The main objective is to develop the “DevBox,” a low-cost device based on Raspberry Pi. Specific objectives were set, such as creating an immutable storage system that ensures patient information is always available and intact. To achieve this, a mixed methodology with an exploratory sequential design was applied, including interviews and surveys of 63 healthcare sector representatives in Machala to identify vulnerabilities, followed by laboratory stress tests to validate the hardware’s resilience under international standards.

The final result was a tool that uses BTRFS file system technology to create read-only copies that cannot be encrypted by attackers. The system incorporates an Intrusion Detection and Prevention System (IDPS) with an automatic “kill switch” that disconnects the device upon detecting suspicious traffic and sends a notification via Telegram; in laboratory tests, the prototype recovered 100% of the data in less than three minutes following a simulated infection.

Overall, the DevBox not only neutralizes ransomware threats but also ensures operational continuity for clinics, compliance with current legal regulations, and the protection of sensitive patient data.

TRADUCIDO POR: Lic. Karla Juliana Castillo Abendaño, Mgs./ 1105213019

1. Planteamiento Del Problema

A nivel mundial, los hospitales y centros de salud se han convertido en blancos vulnerables para los ciberataques. Por ende, el secuestro de datos clínicos o ransomware es hoy en día la principal causa de paralización de operaciones en este sector. Un ejemplo claro de esto ocurrió en el Reino Unido, cuando el malware WannaCry infectó las redes de más de 60 hospitales del Servicio Nacional de Salud (NHS). Este evento dejó una lección muy dura: digitalizar historiales médicos sin tener escudos de protección sólidos termina poniendo en riesgo directo la vida de los pacientes (Department of Health and Social Care, 2018).

En Latinoamérica, se ha evidenciado su situación ante estas amenazas, convirtiéndose en un objetivo principal para grupos de ciberdelincuentes. Por ejemplo, en Costa Rica, donde la Caja Costarricense de Seguro Social sufrió un ataque masivo por parte del grupo de ransomware "Hive". La magnitud del ataque obligó al gobierno a declarar "Estado de Emergencia Nacional", tras la desconexión de sus sistemas informáticos, lo que forzó al personal médico a retomar el uso de papel y lápiz, retrasando miles de citas y diagnósticos críticos (Swissinfo, 2022).

En Ecuador estas crisis enfrentan un escenario de alto riesgo. Centros importantes como el IESS han tenido que suspender sus plataformas en línea por ataques informáticos, dejando a los afiliados sin la posibilidad de agendar citas o realizar trámites vitales de urgencia. Esto simplemente demuestra que la infraestructura sanitaria del país carece de seguridad (El Comercio, 2020). Según el “Quinto estudio sobre el estado de la ciberseguridad en Ecuador”, revela que el 45% ha sufrido incidentes relacionados con secuestro de datos, siendo el sector con menos inversión en defensa cibernética (IT Ahora & Deloitte, 2024).

Esta crisis es uno de los escenarios de las Clínicas y Centros de Especialidades del sector privado del cantón Machala. El modo en que operan esta información evidencia una gestión de historiales médicos muy insegura. Áreas importantes, registran la información de los pacientes en hojas de cálculo dentro computadoras compartidas. Mientras que documentos con suma mayor importancia son guardados en nubes públicas de uso personal, sin que exista detrás de ellos políticas corporativas de respaldo.

Esta práctica que los centros de salud han desarrollado a lo largo de este tiempo tanto por la falta de recursos y errores humanos, hacen que frecuentemente se pierdan muchos historiales clínicos. El origen de esta situación es muy claro y tiene mucho que ver con los recursos: las clínicas locales no tienen para adquirir soluciones de ciberseguridad corporativas (nivel “Enterprise”) y tampoco presupuesto para un personal de TI a tiempo completo encargado en la seguridad de los equipos. Al no cumplir estas 2 prioridades, un ataque no solo paralizaría por completo las actividades, también traería consigo fuertes sanciones legales por incumplir la LOPDP (Asamblea Nacional del Ecuador, 2021).

Extrañamente, a pesar del riesgo tan alto que existe de sufrir un ciberataque, el mercado local sufre de un gran vacío tecnológico. La revisión de estudios demuestra que no existen soluciones de hardware de bajo costo diseñadas específicamente para la protección de datos en este tipo de infraestructuras de salud en Machala. Por tanto, este estudio es necesario y original, pues propone la implementación de un dispositivo de seguridad basado en Raspberry Pi con almacenamiento inmutable (WORM) (SNIA, 2022), adaptado a la realidad económica del sector, llenando el vacío entre la necesidad de seguridad avanzada y la optimización de recursos.

2. Determinación Del Tema

Emprendimiento tecnológico para el desarrollo de un dispositivo de seguridad con raspberry pi orientado a la protección de la información y mitigación de ransomware en clínicas y centros de especialidades privados de la ciudad de Machala.

3. Lineamientos De Investigación

3.1. Línea de Investigación

Desarrollo tecnológico, internet de las cosas, big data e innovación en procesos de automatización y sistematización organizacional.

3.1.1. Sublínea de Investigación

Desafíos de la Industria 4.0.

3.2. Objetivo de Desarrollo Sostenible

ODS alineado: ODS9 - Industria, Innovación e Infraestructura.

Justificación de la alineación: El proyecto contribuye a la Meta 9.5, orientada a modernizar la infraestructura y reconvertir las industrias para que sean sostenibles (PNUD, s.f.). La implementación del dispositivo de seguridad en las Clínicas y Centros de Especialidades de Machala fortalece la resiliencia tecnológica frente a ciberataques, garantizando la continuidad operativa mediante una solución de hardware innovadora y accesible.

3.3. Programa de Investigación

Programa alineado: Gestión e Innovación Tecnológica para el Desarrollo Económico y Humano.

Justificación: Nuestro proyecto se alinea con este programa porque integra la ciberseguridad con el bienestar de la sociedad. La propuesta de blindar las historias clínicas mediante tecnología accesible garantiza tanto la privacidad de los pacientes (desarrollo humano) y, pérdidas financieras para los centros (apoyando el desarrollo económico). De esta forma, logramos que una innovación tecnológica se traduzca en un beneficio social real.

4. Justificación

Este proyecto se enmarca en la línea de investigación "Desarrollo tecnológico, internet de las cosas, big data e innovación", apuntando específicamente a la sublínea de los "Desafíos de la Industria 4.0". La razón de esta elección es directa: la transformación digital y la conexión de equipos a la red carecen de valor si no están respaldadas por escudos de ciberseguridad fuertes que cuiden la información (NIST, 2018). Con este estudio se busca demostrar en la práctica que el concepto de "seguridad por diseño" es urgente para que las clínicas puedan defenderse de amenazas tan destructivas como el ransomware.

A nivel académico, este trabajo representa el paso final para alcanzar el título de Tecnólogo Superior en Ciberseguridad otorgado por el Instituto Superior Tecnológico Sudamericano (ISTS). Más allá de cumplir con un requisito formal, el documento pone a prueba los conocimientos adquiridos a lo largo de la carrera. Al combinar el diseño de arquitecturas de red, el endurecimiento de sistemas operativos y la respuesta a incidentes, se demuestra la capacidad técnica necesaria para solucionar problemas reales en el mercado laboral.

Desde el punto de vista técnico, la propuesta se materializa en el desarrollo de la "DevBox". Se decidió utilizar una Raspberry Pi porque es un hardware sumamente eficiente que permite ejecutar un entorno Linux totalmente blindado. Este equipo tiene la capacidad de gestionar almacenamiento inmutable tipo WORM, que actualmente es el estándar internacional para la protección de datos (SNIA, 2022). De esta forma, se rompe el paradigma de que se necesitan servidores corporativos excesivamente costosos para alcanzar una seguridad lógica aceptable, comprobando que las herramientas Open Source son una defensa real para infraestructuras críticas locales.

En cuanto a la viabilidad económica, el enfoque principal de la investigación es cuidar el presupuesto de las instituciones. Al reemplazar las tradicionales y costosas licencias privadas por hardware accesible, las clínicas privadas tienen la oportunidad de alcanzar un nivel de seguridad empresarial sin comprometer su estabilidad financiera. Prevenir que un ciberataque paralice sus servicios significa evitarles pérdidas monetarias considerables, ayudando a que el sector salud local se vuelva mucho más competitivo.

El impacto social del proyecto representa uno de los puntos más críticos. Blindar las historias clínicas equivale a proteger el derecho a la intimidad de los pacientes, dando fiel cumplimiento a las exigencias de la Ley Orgánica de Protección de Datos Personales (Asamblea Nacional del Ecuador, 2021). Si se garantiza que el historial médico esté siempre disponible, se protege de manera indirecta el bienestar físico de la comunidad, evitando el escenario donde un virus informático termine retrasando una atención de emergencia vital.

Para finalizar, la investigación se estructuró con un fuerte enfoque de emprendimiento, lo cual encaja perfectamente con el perfil de egreso del instituto. La DevBox no se diseñó para archivarse como un simple producto académico; constituye la base de un modelo de negocio escalable bajo la modalidad de "Seguridad como Servicio" (SECaaS). Con esta propuesta comercial, se busca cubrir una demanda que el mercado de Machala mantenía descuidada, ofreciendo a los centros médicos un servicio de respaldo continuo mediante una suscripción accesible.

5. Objetivos

5.1. Objetivo General

Desarrollar un prototipo de dispositivo de almacenamiento inmutable basado en Raspberry Pi, mediante el desarrollo del marco teórico, aplicación de la metodología mixta, elaboración de la propuesta de acción y validación del proyecto, para la protección de historias clínicas en establecimientos de salud y centros de especialidades privados de Machala con el fin de asegurar la disponibilidad e integridad de la información frente a ataques de ransomware.

5.2. Objetivos Específicos

Desarrollar el marco teórico referente a la arquitectura de almacenamiento seguro y vectores de ataque tipo Ransomware, mediante la revisión bibliográfica y normativa especializada, para sustentar el proyecto en bases conceptuales y legales sólidas.

Aplicar la metodología mixta, a través de entrevistas a personal técnico y encuestas a administradores de las clínicas de Machala, para diagnosticar las vulnerabilidades actuales y determinar los requisitos del sistema.

Elaborar la propuesta de acción consistente en la arquitectura del dispositivo "DevBox" basado en Raspberry Pi, integrando configuraciones de endurecimiento y protocolos de inmutabilidad, para generar una solución de seguridad funcional.

Validar la viabilidad técnica y comercial del proyecto, mediante simulaciones de ataques controlados en laboratorio y el análisis de aceptación de mercado, para asegurar la efectividad de la recuperación de datos y la pertinencia de la solución propuesta.

6. Marco Teórico

6.1. Marco Contextual

Para ubicar geográficamente este estudio, nos situamos en el cantón Machala, capital de la provincia de El Oro, en el sur de Ecuador. Por su cercanía a Puerto Bolívar, la ciudad es el gran motor económico de la región. De hecho, los datos del último censo (Instituto Nacional de Estadística y Censos, 2023a) confirman que ya superamos los 306.309 habitantes, volviéndonos una de las zonas urbanas más densamente pobladas del país.

Naturalmente, a medida que la ciudad se expande de forma acelerada, también lo hace la necesidad de atención médica especializada. Si revisamos el Plan de Desarrollo y Ordenamiento Territorial (PDOT) de Machala, notamos que casi todas las instalaciones de salud están amontonadas en el casco urbano. Esto genera un tráfico altísimo de pacientes en una zona céntrica que, como problema añadido, suele sufrir inestabilidad en el suministro eléctrico, un detalle ambiental que golpea directamente la disponibilidad de los equipos informáticos (GAD Municipal de Machala, 2020).

Para no abarcar más de lo operativamente posible, delimitamos el proyecto de forma exclusiva al sector salud privado (clínicas y centros de especialidades), ya que son ellos quienes evitan que la red pública colapse. Los reportes recientes muestran que estas instalaciones privadas han ido aumentando su capacidad para atender a la gente (Instituto Nacional de Estadística y Censos, 2023b). A nivel local, el PDOT contabiliza alrededor de 68 equipamientos de salud formales; de este universo, filtramos únicamente a los establecimientos Tipología B y C. Dejamos por fuera a los consultorios pequeños porque el verdadero riesgo está en las infraestructuras grandes que manejan volúmenes pesados de historiales médicos.

Aunque todos estos centros médicos operan vigilados por el ACCESS, existe un punto ciego enorme: casi ninguno tiene un departamento de sistemas estructurado. Resulta contradictorio ver clínicas que manejan una facturación altísima, pero que no cuentan con un área dedicada a la seguridad de la información. Al final del día, las decisiones sobre qué tecnología comprar la toma la gerencia administrativa, reaccionando solo cuando ya ocurrió una emergencia. Esta realidad es el pan de cada día en el país, donde invertir en ciberdefensa rara vez es prioridad (IT Ahora & Deloitte, 2024).

El problema del dinero pesa bastante en esto. Cuando las clínicas arman sus presupuestos, la prioridad se la llevan las máquinas o equipos médicos tangibles, dejando la protección de la red en un segundo plano. El Observatorio Ecuador Digital lo deja muy claro: aunque hay buen acceso a internet en el sector productivo nacional, armar redes corporativas seguras y digitalizar bien los procesos sigue siendo una materia pendiente (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2023).

A este escenario hay que sumarle la presión que ejercen los mismos pacientes. Hoy en día la gente exige agendar su cita en línea o revisar sus exámenes desde el celular. Para cumplir con esa inmediatez, las clínicas terminan implementando plataformas a la carrera sin revisar la seguridad, cayendo en el "Shadow IT". Al digitalizar los procesos a la fuerza y tener personal que no aplica una buena "ciber-higiene", cometen errores humanos graves. Como advierte Kaspersky (2020), esto deja a los hospitales servidos en bandeja de plata para los atacantes, convirtiendo estos secuestros digitales casi en actos de terrorismo por el daño que causan a los pacientes.

Técnicamente hablando, al diagnosticar a las clínicas de Machala nos topamos exactamente con lo que dicen los estudios nacionales (IT Ahora & Deloitte, 2024): usan

equipos viejos y redes completamente planas. Al no separar la red médica de la administrativa mediante VLANs, cualquier virus que entre por el área de recepción puede llegar hasta los equipos de quirófano sin obstáculos. Además, siguen respaldando la información a mano usando discos duros externos que dejan conectados a las computadoras. Frente a las versiones modernas de Ransomware, hacer esto no sirve de nada, porque el virus termina cifrando la computadora y el disco de respaldo al mismo tiempo (Avila Niño, 2023).

Para empeorar la situación, en Machala no abundan las empresas de ciberseguridad especializadas en normativas de salud que les puedan dar soporte técnico. Al no contar con proveedores expertos locales, los médicos terminan pasándose resultados muy sensibles por canales o chats que no están cifrados. Básicamente, el entorno actual es de altísima criticidad, pero con muy baja defensa. Y es justamente por esta carencia local que la implementación de la "DevBox" pasa de ser una simple opción para convertirse en una medida de protección económica y urgente para nuestra ciudad.

6.2. Marco Conceptual

6.2.1. Introducción Teórica

Para entender el enfoque de esta investigación, partimos de unir dos grandes mundos: la Ciberseguridad Operativa (OpSec) y la arquitectura del Internet de las Cosas (IoT) llevada a entornos críticos. Cuando hablamos de clínicas, proteger una base de datos ya no es solo un tema técnico, sino una responsabilidad bioética y legal. Por eso, este estudio se apoya fuertemente en el concepto de Ciber-resiliencia. A diferencia de la vieja idea de la "prevención perimetral" (que consistía básicamente en poner un antivirus, un firewall y cruzar los dedos), la ciber-resiliencia asume que los ataques van a ocurrir tarde o temprano. Su meta real es garantizar que la organización pueda seguir funcionando pase lo que pase (Carvajal, 2023).

Como pilar principal utilizamos la estrategia de Defensa en Profundidad (Defense in Depth), que consiste en poner varias capas de obstáculos para proteger la información. En este esquema, nuestro dispositivo no opera en la puerta de entrada de la red. La DevBox se sitúa estratégicamente en la capa más profunda, que es la de Seguridad de Datos y Recuperación. Su trabajo es funcionar como el último escudo de defensa para mantener todo íntegro en caso de que una amenaza avanzada logre burlar todas las demás barreras de la clínica.

6.2.2. Antecedentes Conceptuales y Estudios Previos

Revisando la literatura actual, queda claro que las amenazas contra los centros de salud se han vuelto sumamente agresivas. Antes, el Ransomware era un ataque al azar, pero hoy ha evolucionado a operaciones dirigidas conocidas como "Caza Mayor" (Big Game Hunting). Peor aún, con el modelo actual de Ransomware-as-a-Service (RaaS), se ha bajado la barrera de entrada para que cualquier delincuente pueda alquilar un virus y atacar infraestructuras críticas en Latinoamérica (Avila Niño, 2023).

En este escenario, las clínicas y centros de especialidades descentralizados resultan ser el blanco más fácil. El principal problema es lo que llamamos "deuda técnica": siguen operando con sistemas viejos y no separan sus redes de forma segura. Investigaciones previas sobre dispositivos de seguridad de bajo costo demuestran que el uso de Commodity Hardware configurado con software de código abierto puede ofrecer niveles de protección comparables a soluciones corporativas (Enterprise), siempre que se apliquen rigurosamente principios de Hardening (endurecimiento) y Aislamiento de red (Raspberry Pi Foundation, 2023).).

6.2.3. Conceptos Fundamentales

Para la correcta operacionalización de la propuesta tecnológica, se definen los siguientes conceptos técnicos bajo estándares internacionales:

- Internet de las Cosas Médicas (IoMT): Se refiere a la infraestructura interconectada de dispositivos médicos y aplicaciones de software que recopilan y transmiten datos de salud a través de redes informáticas. La seguridad del IoMT es crítica, dado que un dispositivo comprometido puede actuar como puerta de entrada lateral a la red hospitalaria o afectar directamente la seguridad del paciente (Hatton et al., 2021).
- Gateway de Seguridad IoT: Se define como un dispositivo físico o lógico que actúa como punto de conexión y control entre la red interna (LAN) y los dispositivos críticos o el almacenamiento externo. En el contexto de este proyecto, el prototipo funciona como una "Pasarela Segura" que filtra el tráfico malicioso y aísla los respaldos del resto de la red infectada (ITU-T, 2018).

- Arquitectura ARM y SBC: Los Single Board Computers (SBC) como el Raspberry Pi se basan en la arquitectura de procesadores RISC (ARM). A diferencia de la arquitectura x86 tradicional, los SBC ofrecen una superficie de ataque reducida, bajo consumo energético y control directo sobre interfaces de hardware (GPIO), permitiendo crear appliances de seguridad dedicados que no comparten las vulnerabilidades comunes de los entornos Windows (Upton & Halfacree, 2022).
- Almacenamiento Immutable (WORM): Acrónimo de *Write Once, Read Many*. Es una técnica de almacenamiento donde los datos, una vez escritos, quedan bloqueados y no pueden ser modificados ni eliminados por un periodo definido, independientemente de los privilegios del usuario. Esta tecnología se considera la contramedida técnica definitiva contra el cifrado no autorizado del *Ransomware* (SNIA, 2022).
- Shadow IT: Se refiere al uso de sistemas, dispositivos, software, aplicaciones y servicios de tecnología de la información dentro de una organización sin la aprobación explícita del departamento de TI. En el sector salud, esto se manifiesta comúnmente cuando el personal médico utiliza nubes personales o unidades USB no cifradas para transferir datos de pacientes, creando brechas de seguridad invisibles para los administradores de la red (IT Ahora & Deloitte, 2024).
- Proveedor de Servicios de Seguridad Gestionada (MSSP): Modelo de prestación de servicios donde un proveedor externo gestiona y monitorea la

seguridad de la infraestructura de TI de una organización. A diferencia del soporte técnico tradicional (que repara daños), un MSSP se enfoca en la prevención continua, la gestión de copias de seguridad y la respuesta ante incidentes, alineándose con el modelo de negocio SECaaS (Security as a Service) propuesto en esta investigación (NIST, 2018).

6.2.4. Teorías, Modelos y Estándares Aplicados

Para armar la lógica del sistema no improvisamos, sino que nos guiamos estrictamente por normativas internacionales y nacionales pensadas para el sector salud:

Primero, tomamos como base la Norma ISO 27799, que dicta cómo manejar la seguridad informática en entornos médicos. De todo este documento, el proyecto ataca directamente el control de Integridad y Disponibilidad. La norma exige, de forma clara, que las copias de seguridad sean imposibles de alterar y que puedan recuperarse lo suficientemente rápido para no poner en riesgo la atención del paciente (ISO/IEC, 2016).

Por otro lado, utilizamos el Marco de Ciberseguridad del NIST (CSF 2.0), centrándonos de lleno en su función Recover (RC). El dispositivo propuesto materializa la categoría RC.RP (Recovery Planning), automatizando la creación de puntos de restauración aislados (NIST, 2024). Para complementar esto, la DevBox trabaja bajo la filosofía Zero Trust ("Nunca confiar, siempre verificar"). Básicamente, el equipo asume por defecto que la red de la clínica ya es un entorno infectado; por eso, exige autenticación y cifra toda la comunicación que intenta ingresar a él. Las diferencias operativas entre este enfoque y la seguridad perimetral convencional se detallan en la Tabla 1.

Tabla 1
Comparativa entre Seguridad Tradicional y el Modelo Propuesto.

Criterio de Comparación	Seguridad Perimetral Tradicional (Situación Actual)	Modelo Zero Trust con "DevBox" (Propuesta)
Principio de Confianza	"Confiar, pero verificar". Se confía en todo lo que está dentro de la red local (LAN).	"Nunca confiar, siempre verificar". Se asume que la red local ya podría estar infectada.
Ubicación de la Defensa	En el borde (Firewall/Router). Una vez dentro, el atacante tiene libertad de movimiento.	En el dato. La seguridad está adherida a la información (Microsegmentación).
Gestión de Respaldos	Discos USB conectados permanentemente o carpetas compartidas en red sin aislamiento.	Almacenamiento Inmutable (WORM). El dispositivo de respaldo es "invisible" a la red.
Respuesta ante Ransomware	El malware cifra la PC y se propaga al disco de respaldo conectado (Pérdida Total).	El malware cifra la PC, pero no puede alterar los datos bloqueados en el DevBox (Recuperación Exitosa).
Dependencia Humana	Alta. Requiere que el personal médico recuerde conectar o desconectar discos.	Nula. El proceso es 100% automatizado mediante scripts en el Raspberry Pi.

Nota. *Elaboración propia basada en los principios de arquitectura Zero Trust y análisis de riesgos del sector salud local.

Finalmente, el proyecto se fundamenta legalmente en la Ley Orgánica de Protección de Datos Personales (LOPD) de Ecuador. Los Artículos 30, 31 y 32 categorizan los datos de salud como sensibles y obligan a las clínicas (responsables del tratamiento) a implementar medidas técnicas de seguridad verificables (Asamblea Nacional del Ecuador, 2021).

6.2.5. Variables y Componentes de Análisis

Para medir el impacto de nuestro proyecto de forma estrictamente cuantitativa, definimos las variables de trabajo de una manera muy directa y técnica:

- Variable Independiente: La puesta en marcha de la "DevBox", es decir, la implementación de nuestro dispositivo físico basado en Raspberry Pi con su respectivo almacenamiento inmutable.
- Variable Dependiente: La capacidad de supervivencia de los historiales médicos. Esto lo vamos a medir con números reales utilizando el RTO (Recovery Time Objective), cronometrando exactamente cuánto tardamos en recuperar los datos completamente intactos después de sufrir un ataque.

6.2.6. Integración Conceptual

En Para cerrar esta sección, toda la revisión teórica nos deja una lección muy clara: salvar a las clínicas de Machala de las garras del ransomware no depende de obligarlas a comprar licencias de software carísimas, el verdadero secreto está en cómo se diseña la arquitectura de red. Al juntar un hardware que cuida el bolsillo con la tecnología de inmutabilidad (WORM), y alinear todo esto con lo que exige la ley actual (LOPD) y la norma ISO 27799, logramos armar un escudo sumamente sólido.

Básicamente, con este proyecto demostramos que llevar ciberseguridad de primer nivel a los centros de salud locales es totalmente posible. Se trata de democratizar la protección de los datos, demostrando que la innovación tecnológica puede ir de la mano con las exigencias legales y el ritmo acelerado que necesitan los médicos hoy en día.

7. Diseño Metodológico

El desarrollo de esta investigación se rige estrictamente por un enfoque cuantitativo. Elegimos este camino porque, para resolver el problema de ciberseguridad en las clínicas privadas de Machala, no necesitamos suposiciones, sino datos duros y métricas exactas. A través de este enfoque logramos validar numéricamente qué tan eficaz es la DevBox en el laboratorio y, al mismo tiempo, confirmamos con encuestas estructuradas si el dispositivo tiene una viabilidad económica real en el mercado local (Fresno Chávez, 2019).

7.1. Herramientas De Aplicación

Tanto para levantar los datos comerciales como para someter a prueba nuestro prototipo, seleccionamos instrumentos muy puntuales. Estas herramientas no se escogieron al azar, sino que encajan directamente con la naturaleza técnica de nuestro proyecto y cumplen con las exigencias del manual de titulación institucional.

7.1.1. *Herramientas Propias De La Metodología De Cada Área De Especialidad*

Como todo el corazón de este proyecto gira en torno a la programación y configuración de hardware basado en Raspberry Pi, necesitábamos un mecanismo exacto para comprobar que la herramienta funciona. Por ello, aplicamos el siguiente instrumento técnico:

Matriz de Pruebas de Seguridad y Funcionamiento: Básicamente, utilizamos este documento para registrar paso a paso cómo reacciona el dispositivo cuando le lanzamos ataques controlados en nuestro laboratorio. En la matriz fuimos anotando de forma secuencial si la Raspberry Pi lograba ejecutar los scripts de automatización sin fallos y verificamos que el bloqueo de escritura (tecnología WORM) se activara cumpliendo con los estándares internacionales de almacenamiento (SNIA, 2022). Toda esta documentación técnica nos sirve

para comprobar si el sistema operativo resiste intentos de intrusión lateral, validando así la robustez técnica del prototipo antes de su despliegue en campo.

7.1.2. Herramientas Generales

7.1.2.1. Herramientas Cuantitativas. Para obtener métricas exactas sobre el rendimiento de nuestra solución, nos apoyamos en la siguiente herramienta avalada por el manual institucional:

- **Ficha de Medición técnica:** Siguiendo la clasificación de la Tabla 4 del Manual de Titulación, usamos esta ficha en el laboratorio para registrar los números reales durante nuestras pruebas piloto. Nuestro objetivo central aquí fue medir la variable "Tiempo" para calcular el RTO (Recovery Time Objective). Básicamente, nos sentamos a cronometrar con exactitud cuántos minutos tardaba el dispositivo "DevBox" en recuperar un historial clínico completo frente a un ataque, comparándolo con los métodos manuales. Tener esta métrica es indispensable para validar que el equipo asegura la continuidad del negocio bajo estándares internacionales (NIST, 2018).

7.2. Encuesta

De acuerdo con los lineamientos de titulación, la encuesta funcionó como nuestra herramienta transversal para validar el modelo de negocio. Su propósito fue muy claro: descubrir las necesidades reales de protección de los gerentes de clínicas en Machala, conocer sus preferencias y medir cuánto estarían dispuestos a pagar mensualmente por el servicio (Willingness to Pay).

Para llevar a cabo esto de forma eficiente, visitamos presencialmente los establecimientos, pero hicimos que los directivos y médicos respondieran el formulario directamente desde sus propios celulares. Esta decisión logística nos permitió ahorrarles el mayor tiempo posible, respetando sus agendas que siempre están saturadas. Los datos que recolectamos aquí son los que transforman este proyecto académico en un modelo de emprendimiento real, comprobando que la DevBox sí responde a una demanda insatisfecha en el mercado local de TI.

7.3. Técnicas De Aplicación

El procedimiento metodológico lo operativizamos de forma secuencial y netamente cuantitativa, dividiendo el trabajo en dos grandes momentos lógicos.

En primera instancia, realizamos el trabajo de campo desplegando la encuesta estructurada a los tomadores de decisiones de los centros de salud privados. El objetivo de esta etapa es identificar los vectores de riesgo específicos, como el uso de dispositivos personales no seguros o el temor a sanciones normativas, para definir con precisión los requisitos funcionales que debe cumplir el hardware.

Posteriormente, con esos datos claros, pasamos a la fase de validación técnica. En este punto fue donde configuramos la "DevBox" y la sometimos a nuestras pruebas de estrés controladas en el laboratorio. Utilizamos la Matriz de Pruebas para constatar la seguridad lógica del sistema y la Ficha de Medición Técnica para registrar los tiempos de recuperación (RTO). Al finalizar este ciclo, conseguimos una investigación redonda: generamos evidencia empírica que demuestra la superioridad técnica del prototipo frente a los respaldos tradicionales de las clínicas, y confirmamos que el proyecto posee viabilidad comercial real en la ciudad.

8. Desarrollo De Investigación Y Propuesta De Acción

8.1. Determinación del universo y de la muestra

Para asegurarnos de que el prototipo "DevBox" responda a una necesidad real del mercado y no se quede como un simple experimento de laboratorio, no podíamos elegir nuestra población haciendo un conteo superficial. Tuvimos que realizar una depuración técnica muy rigurosa.

Universo poblacional:

Nuestro universo de estudio agrupa exclusivamente a las clínicas y centros de especialidades privados de Machala que verdaderamente manejan infraestructura de red, bases de datos de pacientes y sistemas de historias clínicas.

Para dar con el número exacto y oficial de esta población ($N = 68$), cruzamos la información de cuatro fuentes estratégicas. Esto nos sirvió como un filtro contundente para aterrizar en la realidad operativa actual de la ciudad:

- **Agencia de Aseguramiento de la Calidad de los Servicios de Salud:** Esta fue nuestra fuente legal principal. La usamos para confirmar que los centros existan jurídicamente, mantengan sus permisos de funcionamiento en regla y para verificar su tipología (ACCESS, 2024).
- **Plan de Desarrollo y Ordenamiento Territorial de Machala:** Revisar el PDOT nos dio el marco estadístico macro y nos indicó el tope de cuánta infraestructura de salud formal hay operando en el cantón (GAD Municipal de Machala, 2024).

- **Red Privada Complementaria del IESS:** Analizar los listados de prestadores externos del Seguro Social funcionó como un excelente filtro técnico. El IESS obliga a estas clínicas a tener una infraestructura tecnológica formal para poder cruzar datos y facturar; si están en esa lista, manejan información crítica (IESS, 2024).
- **Directorios Comerciales y Médicos:** Finalmente, contrastamos con estos directorios para comprobar que los establecimientos sigan activos comercialmente y tengan presencia (Solidario Medical Center, 2024).

Criterios de Inclusión y Exclusión:

Como nuestra investigación pertenece a la rama dura de la ciberseguridad, aplicamos filtros muy estrictos para no desviar el objetivo. Solo incluimos a las instituciones de Nivel II (Hospital Básico) y Nivel III (Especializado), metiendo también en el grupo a los policonsultorios que gestionan sus bases de datos de forma centralizada.

Por el otro lado, dejamos completamente fuera del radar a los siguientes establecimientos:

- **Laboratorios de toma de muestras:** Su dinámica diaria se basa en el procesamiento de exámenes, no en la atención clínica integral o la hospitalización de pacientes.
- **Consultorios médicos individuales:** La gran mayoría de estos consultorios no tienen servidores locales complejos ni manejan una red corporativa. Por lo tanto, su nivel de riesgo frente a un ataque de ransomware sistémico es menor y no justificaba la implementación de un hardware perimetral como el nuestro.

Muestra:

Una vez definida y validada nuestra población total (conformada por los 68 establecimientos de salud), procedimos a determinar el tamaño exacto de la muestra aplicando el cálculo estadístico para poblaciones finitas.

Fórmula para el cálculo de la muestra:

$$n = \frac{N \cdot Z^2 \cdot p \cdot q}{e^2 \cdot (N - 1) + Z^2 \cdot p \cdot q}$$

Donde:

n: tamaño de la muestra a encuestar

N: tamaño de la población

Z: nivel de confianza (1.96 para 95%)

p: probabilidad de éxito (0.5 si se desconoce)

q: probabilidad de fracaso (1 - p)

e: margen de error permitido (0.05 = 5%)

Resolución:

Población de 68 establecimientos de salud (N=68), con un 95% de confianza y 5% de error:

$$n = \frac{68 \cdot 1.96^2 \cdot 0.5 \cdot 0.5}{0.05^2 \cdot (68 - 1) + 1.96^2 \cdot 0.5 \cdot 0.5}$$

$$n = \frac{68 \cdot 3.8416 \cdot 0.25}{0.0025 \cdot 67 + 3.8416 \cdot 0.25}$$

$$n = \frac{65.3072}{0.1675 + 0.9604}$$

$$n = \frac{65.3072}{1.1279}$$

$$n = 57.89$$

La fórmula determina una muestra mínima requerida de 58 establecimientos. Sin embargo, durante el despliegue del trabajo de campo, la excelente receptividad del sector permitió recolectar 63 encuestas válidas, superando la cuota mínima, reduciendo el margen de error proyectado y consolidando la viabilidad del estudio.

8.2. Diseño de herramienta

De acuerdo con el diseño metodológico cuantitativo establecido, la técnica seleccionada para el levantamiento de información fue la encuesta.

El diseño de esta herramienta obedece a la necesidad de obtener datos estandarizados, objetivos y medibles sobre el estado actual de la infraestructura tecnológica de las clínicas privadas en Machala. La elección de la encuesta mediante un cuestionario estructurado permitió recopilar información crítica de los jefes de TI y administradores de las 63 instituciones sin interrumpir la operatividad vital de los centros de salud.

Estructura del Cuestionario

El instrumento de recolección fue diseñado en formato digital hecho en Google Forms y consta de un total de 10 preguntas de opción múltiple y escala cerrada. Para garantizar la coherencia metodológica y el flujo lógico de la información, el cuestionario se estructuró en tres bloques temáticos fundamentales:

- **Bloque I Perfilamiento de Infraestructura y Gestión de Datos:** Preguntas orientadas a identificar el tipo de almacenamiento que utilizan actualmente las clínicas como servidores locales, nubes o dispositivos vulnerables como USB y también la criticidad de las historias clínicas digitales.
- **Bloque II Diagnóstico de Ciberseguridad y Exposición al Riesgo:** Interrogantes diseñadas para medir el nivel de conocimiento sobre amenazas informáticas específicamente ransomware, la frecuencia de incidentes previos de pérdida de información y la existencia de protocolos de respaldo continuo.
- **Bloque III Viabilidad y Aceptación de la Propuesta:** Preguntas enfocadas en evaluar la disposición presupuestaria y técnica de las instituciones para adoptar una solución de red perimetral automatizada, el dispositivo "DevBox", como mecanismo de mitigación de ataques.

Validación de la herramienta

Antes de salir al campo y encuestar a nuestro universo de estudio, le presentamos el cuestionario a la tutoría del proyecto para que pasara por una revisión técnica exhaustiva. Nuestro principal reto era asegurarnos de que la terminología de ciberseguridad no resultara confusa para el personal médico o administrativo. Con esta validación, logramos garantizar que las opciones de respuesta fueran lo suficientemente claras y, sobre todo, que abarcaran todas las variables que necesitábamos para justificar la creación de nuestro prototipo tecnológico.

8.2.1. Estudio de mercado

Llevamos a cabo esta fase del estudio para entender de primera mano cómo se comportan los centros de salud privados en Machala, descubriendo sus verdaderas vulnerabilidades y carencias tecnológicas. En el fondo, nuestro objetivo central era comprobar si fabricar e introducir la "DevBox" como una barrera contra el ransomware era una jugada viable tanto a nivel técnico como comercial.

Para lograrlo, estructuramos el trabajo de campo bajo las siguientes etapas:

- **Definición del público meta:** Nos dirigimos estratégicamente a los directores médicos, administradores y jefes de TI de las 63 clínicas encuestadas. Elegimos a este perfil en específico porque ellos son los responsables directos de aprobar los presupuestos tecnológicos y, legalmente, son quienes tienen la custodia de los historiales de los pacientes.
- **Selección del tipo de estudio:** Como mencionamos en nuestra metodología, aplicamos un diseño netamente descriptivo y cuantitativo. Necesitábamos dejar de lado las suposiciones y obtener porcentajes exactos que nos demostraran qué tan alto es el riesgo informático local y cuánta disposición real existe para comprar hardware de seguridad.
- **Diseño del instrumento:** Construimos el cuestionario de 10 preguntas cerradas y fuimos directo al grano en tres ejes: cómo hacen sus respaldos hoy (comparando el uso de memorias USB frente a la nube), qué tanto perciben el riesgo de sufrir un ciberataque, y cuáles son sus expectativas comerciales (precios y soporte local).

- **Análisis de viabilidad y conclusiones preliminares:**

- **Viabilidad Técnica:** Las encuestas nos confirmaron que las clínicas suelen huir de los servidores profesionales tradicionales por considerarlos demasiado caros o complejos de manejar. Esto nos dio luz verde y justificó por completo nuestra idea de crear un dispositivo automatizado tipo Plug-and-Play (conectar y usar).
- **Viabilidad Comercial y Económica:** Validamos que la oportunidad de mercado existe. Los administradores mostraron una gran aceptación hacia el uso de un hardware basado en Raspberry Pi, siempre y cuando cuenten con soporte técnico en la misma ciudad. Además, logramos establecer rangos de inversión mensual (entre \$30 y más de \$100 USD) y notamos un interés real por realizar pruebas piloto, lo cual nos asegura que el retorno de inversión y el modelo de negocio "Seguridad como Servicio" sí es rentable.

8.3. Aplicación de herramientas de investigación

Esta fase detalla cómo llevamos la teoría a la práctica en el trabajo de campo. Como sabíamos que íbamos a manejar información tecnológica muy sensible de las clínicas, la aplicación del instrumento se planificó bajo estrictos protocolos operativos, priorizando la agilidad de recolección, el contacto directo y la protección de datos.

Cronograma, lugares y medios de levantamiento:

Salimos a recolectar los datos durante todo el mes de febrero de 2026. Para hacerlo bien, organizamos un despliegue de campo que combinó las visitas presenciales con la

recolección digital. Visitamos personalmente las 63 clínicas y centros de especialidades en Machala; queríamos establecer un contacto directo, cara a cara y muy formal con el personal médico, administrativo y los encargados de TI.

Sin embargo, éramos muy conscientes de la alta carga laboral y la dinámica de emergencias que se viven a diario en estos lugares. Por eso, nuestra estrategia operativa fue hacer un abordaje presencial rápido para explicarles de qué trataba el proyecto (dejando constancia con el registro fotográfico que está en los anexos). Acto seguido, para no interrumpir sus labores críticas, les compartimos el enlace de la encuesta por mensajería instantánea para que la llenaran directamente desde sus celulares. Esta modalidad híbrida fue clave: nos garantizó una excelente tasa de respuesta y nos permitió procesar los datos de forma inmediata.

Población involucrada y rol de los participantes:

Logramos involucrar con éxito a los representantes de todas las instituciones que habíamos validado en nuestro universo de estudio. Ellos se convirtieron en nuestros informantes clave. Gracias a esta dinámica, nos contaron de primera mano cómo es su día a día, cuáles son las verdaderas fallas en sus métodos de respaldo actuales y, lo más importante, nos ayudaron a validar comercialmente si existe una necesidad real por nuestro hardware.

Normas éticas: Consentimiento y Confidencialidad

Como estábamos investigando vulnerabilidades cibernéticas frente a extorsiones digitales, tuvimos muchísimo cuidado con el manejo ético de los datos durante todo el proceso:

- **Consentimiento informado:** En la primera pantalla del formulario digital incluimos una cláusula de aceptación. Antes de que respondieran, les explicamos personalmente que este estudio era puramente académico e investigativo, y que nuestro único fin era diseñar un prototipo de protección local para ayudarlos.
- **Anonimato estratégico:** No queríamos crear "mapas de vulnerabilidad" que algún ciberdelincuente o tercero pudiera usar para atacar a estas instituciones. Por eso, diseñamos el instrumento de tal forma que las respuestas de seguridad jamás se vincularan con el nombre exacto de la clínica. Toda la información la capturamos y analizamos estadísticamente en bloque.
- **Confidencialidad absoluta:** Les dimos nuestra palabra (y garantía formal) de que datos tan delicados como su presupuesto disponible o los detalles de sus redes (si usan USB o nubes inseguras) quedarían estrictamente protegidos. Su uso se limitó única y exclusivamente a calcular y dimensionar los componentes que iba a llevar la "DevBox".

8.4. Análisis de resultados

Para realizar el análisis de los resultados, nos apegamos estrictamente a las exigencias del manual de titulación institucional. Al haber estructurado nuestro trabajo bajo un enfoque cien por ciento cuantitativo mediante la encuesta de escala cerrada, recopilamos datos duros y medibles.

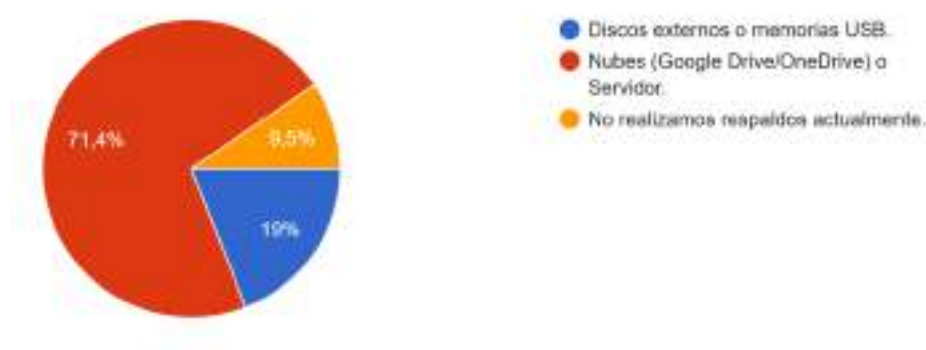
Sin embargo, nuestro análisis no se limitó a simplemente graficar pasteles y exponer estadística descriptiva vacía. Lo que hicimos fue tomar cada porcentaje obtenido y

contrastarlo con la cruda realidad operativa que se vive en las clínicas de Machala. Evaluamos esos números poniendo sobre la mesa las fuertes exigencias de la actual Ley Orgánica de Protección de Datos Personales (LOPDP) y el nivel real de vulnerabilidad que tienen los médicos frente a una amenaza tan destructiva como el ransomware. Esta interpretación integral permite validar de forma técnica y económica la pertinencia de la solución de ciberseguridad "DevBox" desarrollada en este proyecto.

8.4.1. *Análisis de mercado*

Figura 1

¿Qué método utiliza actualmente para respaldar la información médica de sus pacientes?



Nota. Pregunta 1

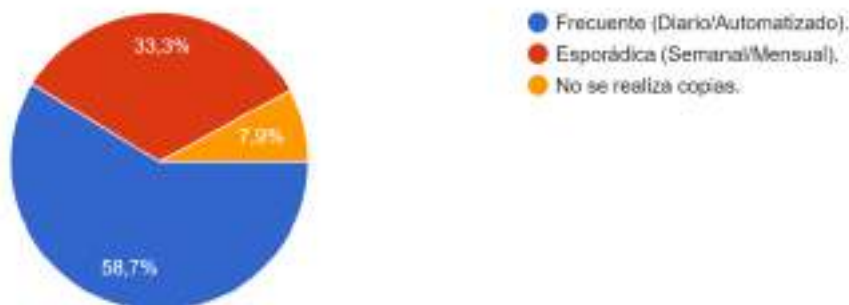
- **Interpretación de los resultados:**

Al tabular esta primera interrogante, confirmamos de entrada la vulnerabilidad de la infraestructura local. Una preocupante mayoría de las clínicas (71.4%) admitió que resguarda sus historiales médicos utilizando discos externos o memorias USB, mientras que otro grupo (19%) confía en nubes públicas comerciales. Prácticamente nadie maneja servidores profesionales. Para nosotros, esto justifica inmediatamente la creación de la "DevBox", ya que nos demuestra que el sector salud está operando de

forma improvisada, utilizando dispositivos domésticos vulnerables para guardar datos altamente sensibles.

Figura 2

¿Con qué frecuencia se realizan las copias de seguridad en su institución?



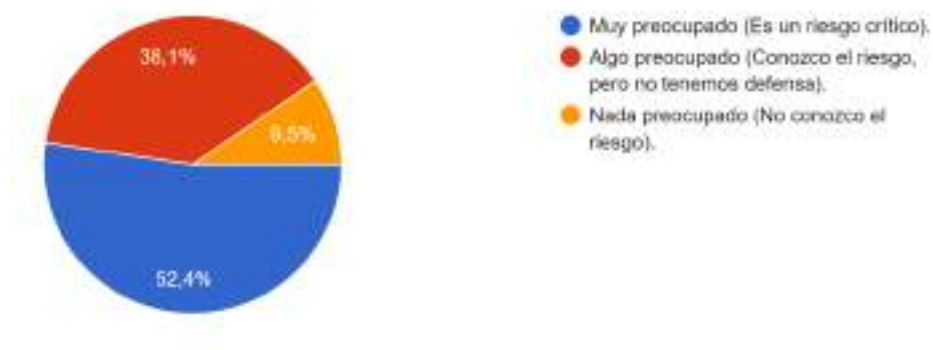
Nota. Pregunta 2

- **Interpretación de los resultados:**

Cuando indagamos sobre la constancia de estos respaldos, descubrimos que el 58.7% de los establecimientos realiza copias de manera esporádica (apenas una vez a la semana o al mes), y un alarmante 33.3% confesó que ni siquiera realiza copias. Desde la perspectiva técnica, un respaldo semanal es inútil frente a un ataque de ransomware; si el virus entra un viernes, la clínica perdería todos los diagnósticos de la semana. Este dato valida la urgencia de nuestro dispositivo, pues su principal fuerte es automatizar los respaldos diarios sin depender de la memoria del personal.

Figura 3

¿Qué tan preocupado está frente a un hackeo o pérdida de datos (Ransomware)?



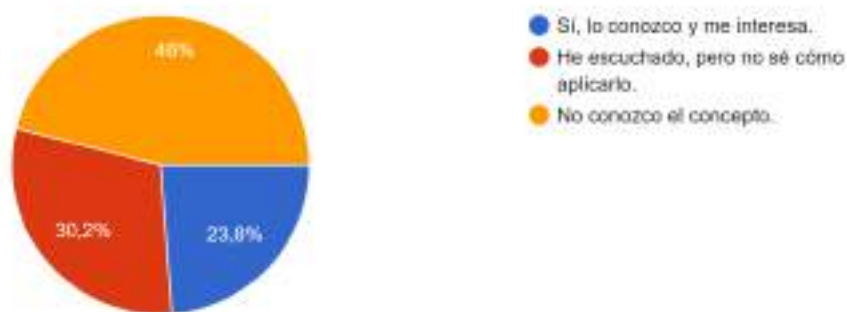
Nota. Pregunta 3

- **Interpretación de los resultados:**

Aquí buscamos medir el pulso sobre el miedo real a perder la operatividad. Las respuestas reflejaron que el 52.4% de los encuestados está "Muy preocupado", reconociéndolo como un riesgo crítico, mientras que un 38.1% sabe que el riesgo existe, pero sienten que no tienen defensas. Al cruzar esto con las preguntas anteriores, notamos una contradicción evidente: los médicos saben que un secuestro digital arruinaría su clínica, pero siguen sin invertir en protección adecuada.

Figura 4

¿Conoce el concepto de "Almacenamiento Inmutable" (Copias que no se pueden borrar ni cifrar)?



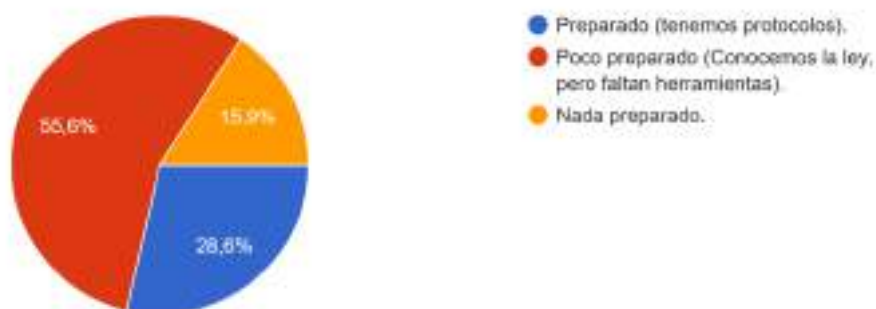
Nota. Pregunta 4

- **Interpretación de los resultados:**

Esta interrogante nos reveló una enorme brecha de conocimiento en el sector. A pesar de su preocupación por los hackeos, el 46% de los encuestados desconoce por completo qué es el almacenamiento inmutable, y un 30.2% ha escuchado del tema, pero no tiene idea de cómo aplicarlo. Que más del 76% de nuestra población de estudio carezca de alfabetización en ciberseguridad avanzada explica por qué los ataques cibernéticos tienen tanto éxito en Machala. Esto hace imperativa la instalación de un hardware como el nuestro, que actúe de forma autónoma sin depender del conocimiento técnico del médico.

Figura 5

¿Qué tan preparado considera que está su centro para cumplir con la Ley de Protección de Datos (LOPD)?



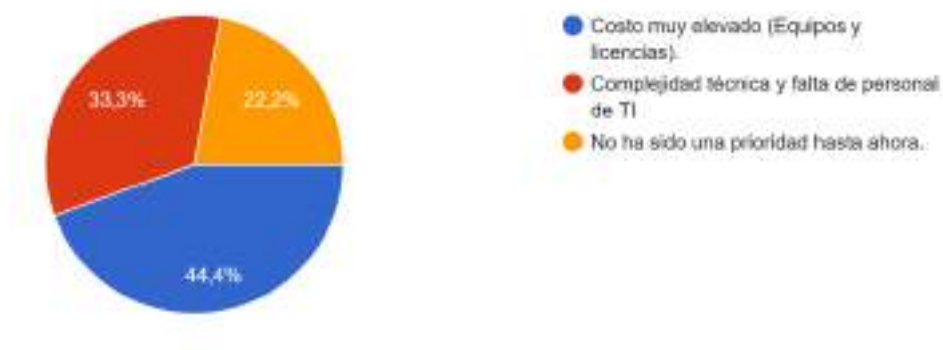
Nota. Pregunta 5

- **Interpretación de los resultados:**

Desde una perspectiva legal, los números que arrojó esta pregunta son alarmantes. Más del 84% de las clínicas encuestadas incumple abiertamente con la LOPDP (el 55.6% se considera "Poco preparado" y el 28.6% está "Nada preparado"). Esto significa que, además de estar expuestos a la pérdida de información de sus pacientes, corren el riesgo de enfrentar multas gubernamentales severas. La "DevBox" entra a solucionar justamente este vacío, ofreciéndoles una herramienta rápida para alcanzar el cumplimiento normativo.

Figura 6

¿Cuál es el principal motivo por el que no tiene un servidor de seguridad profesional?



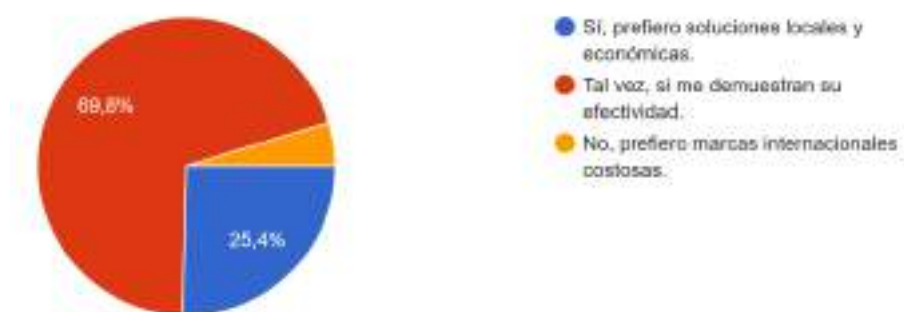
Nota. Pregunta 6

- **Interpretación de los resultados:**

Queríamos entender cuál era la verdadera barrera que les impedía protegerse. Al tabular los datos, la gran mayoría apuntó a dos grandes culpables: el costo tan elevado de comprar licencias y equipos (44.4%) y la enorme complejidad técnica de manejar un servidor sin tener personal de sistemas (33.3%). A esto se suma un 22.2% que admitió que la ciberseguridad simplemente no había sido su prioridad. Este hallazgo fue oro puro para nuestra investigación, porque nos confirma que si diseñamos un dispositivo que sea económico y fácil de usar, estaríamos derribando exactamente las principales excusas que tienen las clínicas hoy en día para no respaldar su información.

Figura 7

¿Confiaría en un dispositivo local de bajo costo (Raspberry Pi) con soporte técnico en Machala?



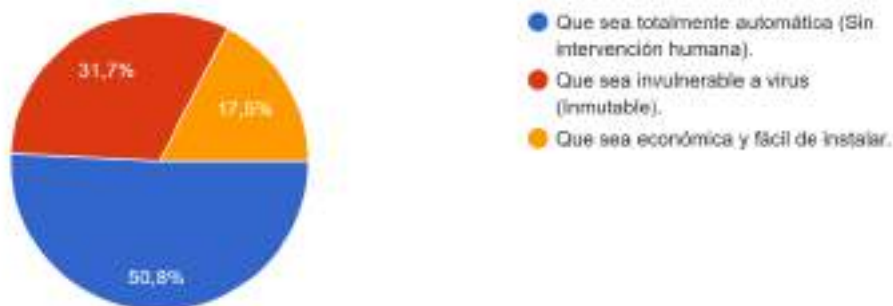
Nota. Pregunta 7

- **Interpretación de los resultados:**

Entrando ya en la evaluación de nuestro modelo de negocio, la respuesta fue sumamente positiva. El 69.8% de los administradores afirmó que preferiría una solución local y económica, y un 25.4% adicional estaría dispuesto a confiar si le demostramos la efectividad del equipo en vivo. Apenas un 4.8% se aferra a la idea de comprar marcas internacionales costosas. Esto rompe el mito de que en el sector salud solo se vende lo extranjero, y nos demuestra que el factor "soporte técnico local en Machala" genera muchísima confianza y viabilidad comercial para la DevBox.

Figura 8

¿Qué característica valoraría más en una solución de respaldo?



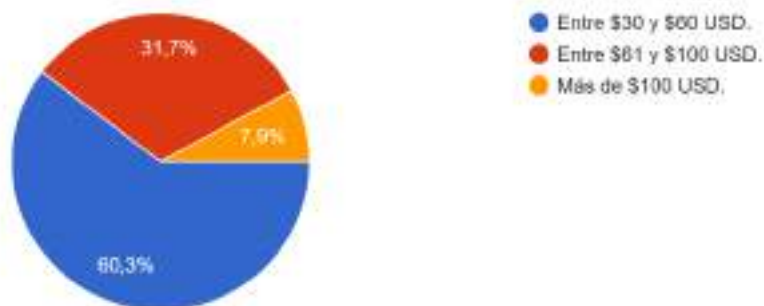
Nota. Pregunta 8

- **Interpretación de los resultados:**

Para saber cómo perfilar el desarrollo final del hardware, les dimos a elegir entre varias opciones técnicas. La tendencia fue clara: más de la mitad de los encuestados (50.8%) prioriza que la solución sea totalmente automática, sin que el personal tenga que intervenir. Además, un 31.7% exige que sea invulnerable a virus. Sabiendo esto, el diseño técnico de la DevBox se justifica por sí solo, ya que nosotros integramos precisamente la inmutabilidad (WORM) y la automatización de respaldos en un solo entorno de bajo costo.

Figura 9

¿Qué rango de inversión mensual consideraría razonable para este servicio?



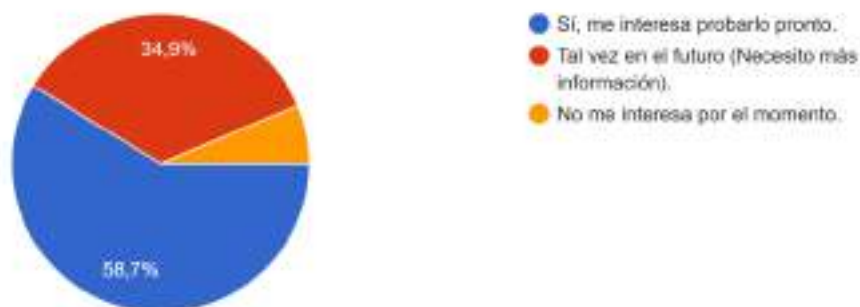
Nota. Pregunta 9

- **Interpretación de los resultados:**

Esta fue la pregunta financiera clave. Comprobamos que existe un mercado local dispuesto a pagar por el servicio, con un fuerte volumen de respuestas (60.3%) concentradas en el rango de los \$30 a \$60 USD, y otro sector nada despreciable (31.7%) dispuesto a pagar entre \$61 y \$100 USD mensuales. Estos números aterrizan nuestra tesis académica, validando matemáticamente que ofrecer la DevBox bajo un modelo de "Seguridad como Servicio" es un emprendimiento rentable y sostenible en el tiempo para nuestra ciudad.

Figura 10

¿Estaría interesado en una prueba piloto de este dispositivo en su institución?



Nota. Pregunta 10

- **Interpretación de los resultados:**

Finalmente, un aplastante 58.7% de los centros de salud manifestó estar interesado en instalar el prototipo pronto, mientras que un 34.9% estaría abierto a evaluarlo a futuro (apenas un 6.3% no mostró interés). Terminar la encuesta con esta tasa de aceptación concluye de manera contundente nuestro estudio de mercado: existe una demanda insatisfecha urgente, y las clínicas de Machala están listas para abrirnos las puertas e implementar nuestra tecnología.

9. Propuesta De Acción

Con todo el diagnóstico y los datos de campo listos, pasamos a la fase aplicativa de nuestra investigación. Aquí es donde transformamos los problemas que detectamos en el sector salud de Machala en una solución tecnológica real, tangible y escalable. Sabemos que las clínicas tienen un nivel crítico de vulnerabilidad frente al ransomware, principalmente porque los atacantes se aprovechan de que estos centros operan con recursos limitados y carecen de protocolos robustos (Coventry & Branley, 2018). Además, existe la obligación legal urgente de cumplir con el principio de seguridad técnica que dicta la Ley Orgánica de Protección de Datos Personales (2021). Para responder a esta doble necesidad, desarrollamos el diseño, la configuración y el modelo de despliegue de nuestro propio prototipo de seguridad perimetral: la "DevBox".

Nos regimos estrictamente por la norma ISO/IEC 27799 (2016), la cual nos exige garantizar que los datos médicos estén siempre disponibles e íntegros utilizando controles de respaldo automáticos. Siguiendo esta regla, la DevBox cierra la enorme brecha técnica local al crear respaldos inmutables por su cuenta. Así evitamos que la clínica tenga que depender de la intervención constante de un experto en TI, mitigando casi a cero el riesgo de un error humano. A nivel comercial, planteamos un modelo de despliegue basado en Hardware as a Service (HaaS); básicamente, diseñamos el proyecto para que sea financieramente viable y garantice la sostenibilidad operativa incluso en los centros de salud más pequeños (Tipología B y C).

9.1. Construcción de la propuesta

Diseñamos la "DevBox" con un enfoque Plug-and-Play (conectar y usar). Nuestro objetivo era que el dispositivo pudiera integrarse de forma totalmente transparente en entornos

médicos que manejan redes Windows, sin interrumpir el trabajo de los doctores. Para lograrlo, dividimos su arquitectura en tres escudos fundamentales: Capa Física, Escudo Pasivo (Inmutabilidad) y Escudo Activo (IDPS). Si el lector desea revisar al detalle los comandos exactos y los códigos de programación que utilizamos para su despliegue, puede referirse al Anexo D: Manual Técnico de Configuración y Despliegue.

9.1.1. Arquitectura de Hardware (Capa Física)

Como cerebro de operaciones para este equipo, seleccionamos una Raspberry Pi 5 de 8GB de RAM. Necesitábamos esta capacidad de memoria específica para que la placa logre procesar las auditorías de red y gestionar los sistemas de archivos avanzados sin colapsar.

- **Almacenamiento NVMe:** Instalamos un disco SSD NVMe M.2 de 256GB y lo conectamos directamente a la placa mediante una interfaz PCIe (usando un adaptador M.2 HAT+). Esto blindo el disco dentro de la carcasa, protegiéndolo contra desconexiones y garantizando altas tasas de transferencia.
- **Refrigeración y Energía:** El hardware opera con refrigeración activa y es alimentado por una fuente dedicada de 45W USB-C PD, garantizando la continuidad operativa del dispositivo.

9.1.2. Escudo Pasivo: Bóveda Virtual e Inmutabilidad (Capa Lógica)

Para la protección criptográfica de los datos, el dispositivo prescinde de entornos gráficos, utilizando Raspberry Pi OS Lite. La comunicación con las estaciones de los médicos se realiza mediante el protocolo SMB/CIFS (Samba).

- **Aislamiento por Bóveda Virtual (Loop Device):** En lugar de utilizar particiones físicas tradicionales, el sistema reserva dinámicamente un espacio

de almacenamiento (ej. 50GB) encapsulado en un disco virtual. Este contenedor es formateado con el sistema de archivos B-Tree File System (BTRFS).

- **Snapshots de Solo Lectura (RPO 60 min):** Los médicos guardan las historias clínicas directamente en la red. En segundo plano, mediante tareas programadas (Cron Jobs), el núcleo de Linux genera una instantánea (Snapshot) a nivel de bloques cada hora. Estas instantáneas son marcadas criptográficamente como de "Solo Lectura". Ante una infección de ransomware en la red local, el malware es incapaz de alterar estas fotografías, permitiendo una recuperación total e inmediata de los datos.

9.1.3. Escudo Activo: Sistema de Prevención de Intrusiones (IDPS) y Kill-Switch

Buscando asegurar que la DevBox no sea solo una bóveda estática de archivos, la dotamos de una capa de seguridad dinámica. Desarrollamos un script de monitoreo continuo escrito en Python que se ejecuta silenciosamente en segundo plano usando el servicio systemd. Lo configuramos de esta manera para garantizar que nuestro programa de defensa persista, sobreviva y vuelva a arrancar por sí solo, incluso si la clínica sufre apagones o reinicios bruscos.

- **Monitoreo de Sockets TCP:** El Básicamente, pusimos al sistema a auditar las conexiones concurrentes de la red (como el tráfico del Puerto 22) sin que el usuario lo note. Si nuestro script detecta un comportamiento anómalo que supere el umbral de conexiones que le configuramos en el laboratorio —por ejemplo, un Ataque de Denegación de Servicio o un intento de saturar los

sockets— hace saltar automáticamente el protocolo de emergencia (Acha Araya, 2017).

- **Alerta Temprana y Amputación de Red:** Cuando ese umbral de seguridad se rompe, la DevBox reacciona en cuestión de milisegundos. Primero, extrae un rápido reporte forense y dispara un mensaje de alerta "SOS" directamente al celular del administrador aprovechando la API de Telegram. Acto seguido, ejecuta un "Kill-Switch" lógico: le ordenamos al equipo que apague sus propias tarjetas de red (eth0 y wlan0). Con esta amputación de red logramos que el dispositivo se aíse por completo del entorno infectado, salvando la integridad de todos los respaldos médicos antes de que el virus logre alcanzar el disco.

9.2. Recursos y Requerimientos

Para sacar la propuesta del papel y asegurar que sea viable tanto técnica como operativamente, estructuramos una matriz de requerimientos con todos los elementos indispensables que necesitamos para construir, configurar y desplegar la "DevBox" en un entorno real.

Nuestra filosofía principal en esta fase fue la optimización financiera. Decidimos aprovechar todo el ecosistema de tecnologías de código abierto (Open Source) para evadir el pago de esas costosas licencias anuales que tanto asustan a las clínicas. Gracias a esta decisión, pudimos concentrar la inversión exclusivamente en comprar hardware de altísimo rendimiento y en nuestro tiempo de desarrollo para armar la arquitectura de seguridad.

9.2.1. *Requerimientos de Software y Tiempo de Ejecución*

- **Software:** Armamos todo el cerebro del dispositivo utilizando estrictamente herramientas libres y lenguajes de código abierto. Decidimos instalar una distribución de Linux orientada a servidores, formateamos el disco bajo el sistema de archivos BTRFS, levantamos los protocolos de red con Samba, escribimos todo el IDPS en Python 3 y enlazamos las alertas usando la API gratuita de Telegram. Es justamente este apilamiento de tecnologías libres lo que nos permite eliminar de raíz cualquier gasto recurrente de licenciamiento comercial para el cliente.
- **Tiempo estimado de ejecución:** El ensamblaje físico del hardware, la creación de la bóveda inmutable BTRFS, la programación del demonio systemd para el Kill-Switch y las pruebas de estrés en laboratorio toman un tiempo estimado de 4 horas reloj por unidad. La instalación física en la clínica y su integración a la red médica requiere 2 horas adicionales de trabajo de campo.

9.2.2. *Recursos Materiales y Presupuesto de Implementación*

A continuación, se desglosa el presupuesto validado en el mercado local para la ejecución del proyecto y el costo unitario de producción del prototipo de hardware.

Tabla 2
Desglose de presupuesto para el proyecto

Categoría	Rubro / Descripción	Unidad de medida	Cant.	Costo Unitario	Costo Total
Hardware (Prototipo DevBox)	Kit CanaKit Raspberry Pi 5 Integrado (Placa 8GB, Fuente 45W PD, Case con refrigeración activa, expansión M.2 HAT+ y Disco SSD NVMe de 256GB)	Unidad	1	\$240,87	\$240,87

Operatividad e Infraestructura Web	Dominio Web (.com) para panel y emprendimiento	Anual	1	\$20,00	\$20,00
	Internet (Plan Básico para pruebas y soporte remoto - 5 meses)	Mensual	5	\$20,00	\$100,00
Logística y Trabajo de Campo	Transporte (Visitas a clínicas en Machala)	Global	1	\$40,00	\$40,00
	Alimentación (Días de levantamiento de información)	Global	1	\$40,00	\$40,00
Gastos Académicos y Administrativos	Suministros de Oficina (Papelería)	Global	1	\$20,00	\$20,00
	Impresión y Empastado (Documento Final)	Unidad	3	\$12,00	\$36,00
	Especie Valorada (Trámites ISTS)	Unidad	1	\$5,00	\$5,00
Subtotal					\$501,87
Imprevistos (5%)					\$25,09
TOTAL GENERAL					\$526,96

Nota. Elaboración propia. La tabla detalla la inversión inicial requerida para el diseño, configuración y validación técnica del prototipo de seguridad "DevBox". Los rubros de hardware están calculados con base en los precios del mercado actual para la arquitectura Raspberry Pi 5, e incluyen los gastos logísticos y académicos necesarios para la culminación del proyecto. Este presupuesto representa estrictamente el costo de producción unitario e implementación, el cual sirve como base financiera para estructurar el modelo comercial de Hardware as a Service (HaaS) propuesto para los centros de salud.

9.3. Validación Técnica (Pruebas de Estrés en Laboratorio)

Para certificar la efectividad de los tres escudos que componen la arquitectura de la "DevBox", el prototipo fue sometido a pruebas de penetración y simulación de estrés en un entorno de laboratorio aislado, emulando la infraestructura de red típica de una clínica privada.

La validación técnica se estructuró en dos fases críticas, diseñadas para poner a prueba los mecanismos de respuesta autónoma frente a los vectores de ataque más comunes en el sector salud.

9.3.1. Fase 1: Validación del Escudo Activo (Ataque de Denegación de Servicio y Kill-Switch)

El objetivo de esta prueba fue validar la capacidad del Sistema de Prevención de Intrusiones (IDPS) para auditar el tráfico y ejecutar una desconexión autónoma antes de que la máquina sufriera una caída crítica.

- **Vector de ataque:** Se utilizó una máquina virtual con Kali Linux. Mediante un script automatizado en Python, se lanzó un ataque de Agotamiento de Sockets hacia el puerto TCP 22 (SSH) del prototipo, generando 30 hilos de conexión simultáneos sin transmitir carga útil, con el objetivo de saturar el tráfico de red de la bóveda.
- **Respuesta del Prototipo:** El algoritmo `systemd` que ejecuta el escudo en segundo plano detectó la anomalía al instante en que el tráfico superó el umbral seguro preestablecido.
- **Resultado Forense:** Como se evidencia en el archivo log del sistema, el prototipo logró emitir una alerta externa y ejecutó la amputación inmediata de sus propias interfaces de red (`eth0` y `wlan0`), aislándose exitosamente del entorno hostil en milisegundos. Tras 5 segundos de aislamiento, el servicio se reinició automáticamente para continuar el escaneo de forma pasiva.

Figura 11

Archivo Logs de devbox_auditoria

```

devbox_auditoria: Mac OS/Unix
Archivo: /var/log/devbox_auditoria.log
2026-04-27 16:18:04,043 - INFO - Escudo DevBox Iniciado. Vigilando puerto 22...
2026-04-27 16:18:04,238 - WARNING - ATAQUE DETECTADO. Umbral de 3 conexiones superado en puerto 22...
2026-04-27 16:18:07,007 - INFO - Alerta de Telegram enviada con éxito al administrador.
2026-04-27 16:18:07,054 - INFO - Interfaz eth0 DESCONECTADA exitosamente.
2026-04-27 16:18:07,574 - INFO - Interfaz wlan0 DESCONECTADA exitosamente.
2026-04-27 16:18:07,586 - INFO - AISLAMIENTO COMPLETADO. Máquina segura. Superando intervención manual.
2026-04-27 16:18:11,793 - INFO - Escudo DevBox Iniciado. Vigilando puerto 22...
2026-04-27 16:18:11,799 - WARNING - ATAQUE DETECTADO. Umbral de 3 conexiones superado en puerto 22.
2026-04-27 16:18:12,090 - ERROR - Fallo al enviar alerta de Telegram: curl: (6) curl: (6) Temporary failure in n
2026-04-27 16:18:12,093 - INFO - Interfaz eth0 DESCONECTADA exitosamente.
2026-04-27 16:18:12,854 - INFO - Interfaz wlan0 DESCONECTADA exitosamente.
2026-04-27 16:18:12,859 - INFO - AISLAMIENTO COMPLETADO. Máquina segura. Esperando intervención manual.
2026-04-27 16:18:18,008 - INFO - Escudo DevBox Iniciado. Vigilando puerto 22...
2026-04-27 16:18:18,070 - WARNING - ATAQUE DETECTADO. Umbral de 3 conexiones superado en puerto 22.
2026-04-27 16:18:18,132 - ERROR - Fallo al enviar alerta de Telegram: curl: (6) curl: (6) Temporary failure in n
2026-04-27 16:18:18,135 - INFO - Interfaz eth0 DESCONECTADA exitosamente.
2026-04-27 16:18:18,138 - INFO - Interfaz wlan0 DESCONECTADA exitosamente.
2026-04-27 16:18:18,142 - INFO - AISLAMIENTO COMPLETADO. Máquina segura. Esperando intervención manual.
  
```

Nota. Registro forense de auditoría (/var/log/devbox_auditoria.log) evidenciando la amputación de interfaces tras el ataque de Kali Linux.

9.3.2. Fase 2: Validación del Escudo Pasivo (Simulación de Infección por Ransomware y RPO)

El objetivo de esta prueba fue demostrar la invulnerabilidad del almacenamiento BTRFS frente a un secuestro de datos con cifrado masivo (Ransomware), partiendo del escenario en que una estación de trabajo Windows (la computadora del médico) fue comprometida.

- **Vector de ataque:** Se programó un simulador de ransomware en PowerShell ejecutado directamente en la máquina Windows conectada a la red de la clínica. Este script localizó la carpeta de historias clínicas compartidas por la DevBox a través del protocolo Samba, procediendo a sobrescribir todo el texto médico

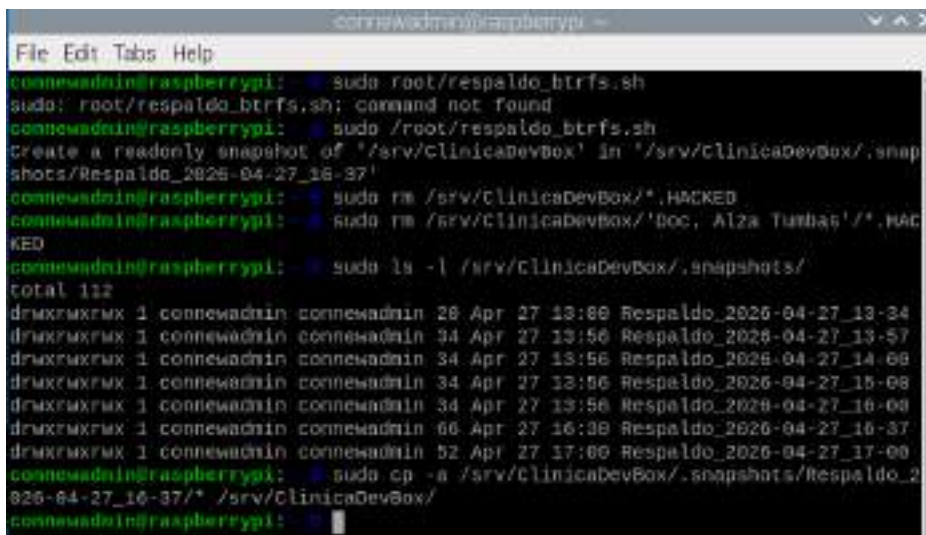
con una nota de extorsión y alterando las extensiones de los archivos a.

HACKED.

- **Respuesta del Prototipo:** Debido a la arquitectura de aislamiento por particionamiento lógico, el malware solo logró afectar los archivos expuestos en la zona de intercambio. Las instantáneas (Snapshots) de respaldo, almacenadas en la partición oculta y marcadas como de "Solo Lectura", resultaron criptográficamente inaccesibles para el atacante.
- **Resultado de Recuperación:** Desde la terminal del administrador, se procedió a la eliminación de los archivos corruptos en la zona de intercambio. Mediante el comando de copiado rápido desde el último Snapshot inmutable generado por Cron, se logró una restauración exitosa del 100% de la información clínica original, sin requerir el pago de un rescate y cumpliendo con el RTO establecido para la continuidad del negocio.

Figura 12

Comandos de restauración



```

connnewadmin@raspberrypi: ~$ sudo root/respaldo_btrfs.sh
sudo: root/respaldo_btrfs.sh: command not found
connnewadmin@raspberrypi: ~$ sudo /root/respaldo_btrfs.sh
create a readonly snapshot of '/srv/ClinicaDevBox' in '/srv/ClinicaDevBox/.snapshots/Respaldo_2026-04-27_16-37'
connnewadmin@raspberrypi: ~$ sudo rm /srv/ClinicaDevBox/*.HACKED
connnewadmin@raspberrypi: ~$ sudo rm /srv/ClinicaDevBox/'Doc, Alza Tumbas'/*.HACKED
connnewadmin@raspberrypi: ~$ sudo ls -l /srv/ClinicaDevBox/.snapshots/
total 112
drwxrwxrwx 1 connnewadmin connnewadmin 28 Apr 27 13:00 Respaldo_2026-04-27_13-34
drwxrwxrwx 1 connnewadmin connnewadmin 34 Apr 27 13:56 Respaldo_2026-04-27_13-57
drwxrwxrwx 1 connnewadmin connnewadmin 34 Apr 27 13:56 Respaldo_2026-04-27_14-08
drwxrwxrwx 1 connnewadmin connnewadmin 34 Apr 27 13:56 Respaldo_2026-04-27_15-08
drwxrwxrwx 1 connnewadmin connnewadmin 34 Apr 27 13:56 Respaldo_2026-04-27_16-08
drwxrwxrwx 1 connnewadmin connnewadmin 66 Apr 27 16:38 Respaldo_2026-04-27_16-37
drwxrwxrwx 1 connnewadmin connnewadmin 52 Apr 27 17:00 Respaldo_2026-04-27_17-00
connnewadmin@raspberrypi: ~$ sudo cp -a /srv/ClinicaDevBox/.snapshots/Respaldo_2026-04-27_16-37/* /srv/ClinicaDevBox/
connnewadmin@raspberrypi: ~$

```

Nota. Proceso de restauración de historias clínicas desde la bóveda inmutable BTRFS tras el cifrado por ransomware.

10. Modelo de Emprendimiento

En este apartado materializaremos los resultados obtenidos en la encuesta, en una propuesta comercial práctica, viable y escalable para el futuro del “DevBox”. Una vez validada la arquitectura de seguridad del prototipo y comprobado la necesidad de este en el mercado frente a la amenaza de ataques de ransomware, el proyecto está enfocado netamente en el ámbito académico para consolidarse como una empresa proveedora de servicios tecnológicos corporativos.

A fin de llevar a cabo esta propuesta hemos creado "Corporación Phylax Tech", la cual emplea una metodología de emprendimiento enfocada en el modelo de negocio Hardware as a Service (HaaS). Esta estrategia no solo garantiza la protección continua de la información crítica de las instituciones de salud en el cantón Machala, sino también la sostenibilidad financiera e innovación del proyecto a largo plazo.

10.1. CANVA(F)*

La siguiente estructura tiene una propuesta de valor que demuestra la viabilidad operativa y financiera del emprendimiento, usa la metodología Business Model Canvas (Lienzo de Modelo de Negocio) que permite visualizar de forma íntegra y sistémica cómo la empresa crea, entrega y captura valor dentro del mercado de la ciberseguridad B2B (Business-to-Business). A continuación, se detallan los nueve bloques estructurales del modelo en la siguiente tabla:

Tabla 3
Lienzo de Modelo de Negocio (Canvas) de Corporación PhylaxTech

Modelo Negocio CANVAS		Diseñado para: Corporación PhylaxTech	Diseñado por: Anthony Edinson Yaguachi Cardenas Jose Xavier Mocha Quichimbo	Fecha: 23/02/2026	Versión: 1.0
Socios Clave - Proveedores internacionales de hardware tecnológico (Ej. CanaKit). - Proveedores locales de Servicios de Internet (ISP) para garantizar la conexión remota.	Actividades Clave - Ensamblaje y configuración de los nodos de seguridad (DevBox). - Despliegue de red en las instalaciones del cliente. - Monitoreo remoto de respaldos y mantenimiento preventivo.	Propuesta de Valor - Bóveda de red inmutable ("DevBox") contra ransomware. Modelo Hardware as a Service (HaaS): Protección corporativa sin compra de costosos servidores. - Implementación rápida (Plug-and-Play) y recuperación inmediata de historias clínicas.	Relaciones con los Clientes - Asistencia personal exclusiva. - Acuerdos de Nivel de Servicio (SLA) con soporte telemático continuo. - Visitas físicas prioritarias para emergencias de ciberseguridad.	Segmentos de Clientes Nicho de Mercado (B2B): Clínicas, hospitales y centros de especialidades privadas (Nivel II y III) en Machala. - Instituciones sujetas a la Ley de Protección de Datos (LOPD).	
	Recurso Clave Físicos: Stock de hardware (Kits, NVMe) y herramientas de red. Intelectuales: Arquitectura de inmutabilidad (BTRFS) y marca registrada (PhylaxTech). Humanos: Talento especializado en Linux y ciberseguridad.		Canales - Venta directa corporativa (Reuniones B2B). - Demostraciones presenciales y pruebas piloto en las clínicas. - Página web corporativa (Informativa y soporte).		
Estructura de Costo Costos Variables: Adquisición de hardware (placas, discos NVMe, fuentes de poder) para nuevos clientes. Costos Fijos: Viáticos/movilización para soporte técnico, mantenimiento de infraestructura web y gastos de formalización (patentes, RUC).		Flujo de Ingresos Modelo de Suscripción Mensual: - Plan Essential (\$49.99/mes) - Soporte remoto. - Plan Clinic Pro (\$99.99/mes) - Mayor capacidad NVMe y soporte físico. Cobros variables: Tarifas por visitas técnicas presenciales ocasionadas por errores de usuario.			

Nota. Representación del modelo comercial B2B para la implementación del prototipo "DevBox" bajo el esquema Hardware as a Service (HaaS).

A través de este esquema demostramos en números reales que blindar los historiales médicos de nuestra ciudad contra los secuestros digitales no solo es técnicamente posible, sino que es un proyecto totalmente viable y sostenible a nivel financiero. Elaboración propia.

10.2. Descripción Empresarial(F)*

En este apartado dejamos atrás la teoría y pasamos a definir estratégicamente la identidad, el propósito y la orientación comercial de nuestro proyecto. Básicamente, aquí explicamos cómo la "DevBox" da el salto de ser una simple investigación para convertirse en una empresa real.

A través de esta descripción, detallamos cómo vamos a operar en el día a día para hacerle frente a las enormes vulnerabilidades tecnológicas que detectamos en las clínicas de Machala. Además, dejamos muy clara cuál es nuestra propuesta de valor en el mercado local y trazamos la hoja de ruta que seguiremos para asegurar que el negocio sea rentable, sostenible y pueda escalar a futuro.

Tabla 4
Formato de la descripción empresarial

Elemento	Descripción
Información del estudiante	Anthony Edinson Yaguachi Cardenas Jose Xavier Mocha Quichimbo
Nombre del emprendimiento/empresa	Corporación PhylaxTech
Tecnología o especialidades	Tecnología Superior en Ciberseguridad - ISTS
Misión	Proteger la continuidad operativa y la confidencialidad de los datos críticos del sector empresarial y de salud en Machala, mediante la implementación de infraestructura inmutable automatizada que garantice la mitigación de secuestros digitales (ransomware) y el estricto cumplimiento de la Ley Orgánica de Protección de Datos Personales (LOPDP).
Visión	Posicionarnos en un plazo de 5 años como la corporación líder en soluciones de ciberseguridad B2B en la provincia de El Oro, siendo el socio estratégico por excelencia para la protección de infraestructuras críticas y auditoría de redes en los sectores de salud, educación y servicios corporativos.

Objetivos estratégicos	1. Desplegar el servicio de bóvedas inmutables en al menos 15 instituciones médicas del cantón Machala durante el primer año de operaciones. 2. Mantener una tasa de éxito del 99.9% en la retención y recuperación de datos clínicos frente a incidentes de ciberseguridad. 3. Diversificar la cartera de clientes hacia el sector educativo e industrial a partir del tercer año, empleando una estrategia comercial Land and Expand.
Descripción del negocio	Somos una iniciativa tecnológica local dedicada de lleno a la seguridad perimetral corporativa. Nuestro trabajo diario se centra en proveer, instalar y monitorear la "DevBox", apoyándonos en la tecnología de inmutabilidad lógica para blindar la información médica. El negocio democratiza la ciberseguridad en grado empresarial, ofreciendo una solución Plug-and-Play con soporte técnico presencial especializado, lo cual elimina la necesidad de que los clientes realicen altas inversiones en servidores tradicionales o licencias extranjeras.
Contexto del mercado y clientes	Nuestro público objetivo directo abarca a las clínicas, los hospitales y los centros de especialidades privados que operan en Machala. Hoy en día, todos estos centros médicos guardan historiales clínicos digitales extremadamente delicados, pero operan sin escudos reales frente al ransomware o a la denegación de acceso. Detectamos una oportunidad comercial muy clara al cruzar dos realidades locales: por un lado, los médicos tienen la urgencia de cumplir con la LOPDP para evitar multas; y por el otro, el sector salud cuenta con la liquidez suficiente para sostener un modelo de pago mensual a cambio de que nosotros les garanticemos protección continua.

Nota. Resumen de la identidad corporativa de nuestra empresa, el rumbo estratégico que tomamos y la propuesta de valor real de este emprendimiento tecnológico. Elaboración propia.

10.3. Flujo Financiero Esperado(F)*

Con el objetivo de que nuestro proyecto no se quede simplemente como un buen experimento tecnológico guardado en un cajón, necesitábamos aterrizarlo en números reales. Este flujo financiero es exactamente eso: el puente que traduce toda la ingeniería detrás de la "DevBox" en un negocio viable y que pueda sostenerse por sí solo en el tiempo.

Al armar este análisis buscamos cumplir con tres metas muy claras: primero, pasar de la teoría a la acción planificada; segundo, medir la rentabilidad calculando en cuánto tiempo

exacto recuperaremos el dinero invertido; y tercero, demostrar responsabilidad emprendedora al mantener nuestros costos a raya. Lo que presentamos a continuación es la proyección financiera de cómo se verían las cuentas claras de nuestra empresa, "Corporación PhylaxTech", operando desde Machala y cobrando mensualmente bajo el esquema de Hardware as a Service (HaaS).

10.3.1. Presupuesto de Inversión Inicial

Arrancar una empresa de ciberseguridad desde cero requiere capital, y este presupuesto refleja nuestro primer paso real. Aquí calculamos cuánto dinero necesitamos tener sobre la mesa para comprar las piezas y levantar la operación antes de siquiera facturar nuestro primer mes de servicio.

Como en PhylaxTech decidimos movernos rápido y sin desperdiciar recursos (aplicando la filosofía Lean Startup), no vamos a inflar los números con gastos innecesarios. Hemos concentrado toda nuestra inversión inicial estratégicamente en dos frentes: comprar el hardware necesario para ensamblar las primeras DevBox de prueba, y costear las herramientas que nos permitirán golpear puertas para meter el producto en el mercado médico local (Go-to-Market).

Tabla 5
Presupuesto de inversión inicial

Categoría de inversión	Ítem / Descripción	Costo unitario (USD)	Cantidad	Costo total (USD)
1. Equipos y herramientas	Stock inicial "DevBox" (Kit CanaKit NVMe M.2)	240,87	3	722,61
	Herramientas de red (Cables Cat6, probador, ponchadora)	80,00	1	80,00

2. Materiales e insumos iniciales	Insumos de instalación (Canaletas, amarras)	20,00	1	20,00
3. Mobiliario e infraestructura	(Operación en terreno B2B - No requiere local inicial)	0,00	0	0,00
4. Marketing y promoción	Material impreso B2B y publicidad digital	50,00	1	50,00
5. Permisos y licencias	Trámites legales: RUC y Patente Municipal	120,00	1	120,00
6. Capital de trabajo (1er mes)	Transporte y distribución local (visitas médicas)	80,00	1	80,00
7. Desarrollo tecnológico	Dominio web corporativo y Hosting (Plan anual)	100,00	1	100,00
8. Otros gastos iniciales	Imprevistos y caja chica operativa	100,00	1	100,00
TOTAL INVERSIÓN INICIAL (USD)				1.272,61

Nota. Este valor total de la inversión inicial lo trasladamos directamente al Año 0 de nuestro flujo de caja proyectado, usándolo como el punto de partida real para evaluar la viabilidad financiera de PhylaxTech. Elaboración propia.

10.3.2. Flujo de Dinero Proyectado

Con el propósito de no caminar a ciegas en el manejo financiero de nuestra empresa, estructuramos este flujo de dinero proyectado. Su verdadera utilidad va más allá de un simple papel; nos permite visualizar con precisión milimétrica cómo se va a mover nuestro capital en el día a día, dejando en claro la relación real entre los ingresos que entren, los costos operativos que debemos asumir y el flujo neto que nos quedará libre en la caja para reinvertir.

Al momento de calcular estas proyecciones, decidimos ser muy prudentes. Fijamos un "Ticket Promedio" bastante conservador de \$70.00 USD mensuales por cliente, el cual resulta de promediar las tarifas de los planes Essential y Clinic Pro que ofreceremos. Con esta base

financiera, nos trazamos la meta comercial de captar un grupo inicial de 15 clínicas privadas durante nuestro primer año de operaciones en Machala. Este número de clientes es el punto de partida clave para estabilizar la caja, cubrir los gastos fijos y demostrar la rentabilidad real del negocio en marcha.

Tabla 6
Modelo de Flujo de Dinero Proyectado

Categoría / Concepto	Año 0	Año 1	Año 2	Año 3	Año 4	Año 5
INGRESOS						
Ventas o prestación de servicios (Suscripción HaaS)	-	12.600,00	21.000,00	29.400,00	37.800,00	50.400,00
Total ingresos (A)	-	12.600,00	21.000,00	29.400,00	37.800,00	50.400,00
COSTOS DIRECTOS (Producción / Servicio)						
Materia prima o insumos (Nuevos kits DevBox)	-	3.613,05	2.408,70	2.408,70	2.408,70	3.613,05
Mantenimiento de equipos / herramientas	-	150,00	200,00	250,00	300,00	400,00
Total costos directos (B)	-	3.763,05	2.608,70	2.658,70	2.708,70	4.013,05
GASTOS OPERATIVOS (Administración y Comercialización)						
Servicios básicos (Internet corporativo)	-	400,00	450,00	500,00	550,00	600,00
Marketing, publicidad y web	-	150,00	200,00	250,00	300,00	350,00
Transporte interno (Movilización soporte)	-	350,00	450,00	550,00	650,00	800,00
Otros gastos generales / imprevistos	-	150,00	200,00	250,00	300,00	400,00

Total gastos operativos (C)	-	1.050,00	1.300,00	1.550,00	1.800,00	2.150,00
FLUJO OPERATIVO (A - B - C)	-	7.786,95	17.091,30	25.191,30	33.291,30	44.236,95
INVERSIÓN INICIAL (del presupuesto)	-	1.272,61	-	-	-	-
FLUJO DE DINERO LIBRE (ACUMULADO)	-	1.272,61	6.514,34	23.605,64	48.796,94	82.088,24
						126.325,19

Nota. Esta línea del flujo de dinero libre acumulado nos muestra la ganancia neta que el proyecto va sumando a lo largo del tiempo. Elaboración propia.

Interpretación del modelo

- Año 0: Representa nuestra inversión inicial de USD 1.272,61, que es el capital neto que necesitamos inyectar para adquirir los componentes y poner en marcha la operación.
- Año 1: A diferencia de los modelos de negocio tradicionales que tardan años en salir de los números rojos, la enorme eficiencia de la arquitectura de red que diseñamos para la DevBox permite que el emprendimiento genere un flujo positivo desde el primer año, logrando una recuperación prácticamente inmediata del negocio.
- Año 5: Al llegar al quinto año, vemos que el flujo de dinero libre acumulado escala hasta alcanzar los USD 126.325,19. Esta cifra nos confirma con absoluta certeza que el proyecto produce excedentes económicos que vuelven a la propuesta altamente rentable y atractiva.

Cálculo del VAN y la TIR

Para poner a prueba la verdadera salud financiera de nuestra propuesta y demostrar su viabilidad económica con bases matemáticas sólidas, calculamos el Valor Actual Neto (VAN) y la Tasa Interna de Retorno (TIR). Para asegurarnos de que este análisis sea completamente realista y esté bien aterrizado al contexto financiero ecuatoriano, aplicamos una tasa de descuento del 10% anual, que es el estándar técnico utilizado a nivel local para evaluar proyectos de inversión tecnológica.

Tabla 7
TIR

Año	0	1	2	3	4	5	Fórmulas de cálculo	Resultados
Flujo	- 1.272,61	7.786,95	17.091,30	25.191,30	33.291,30	44.236,95		
Tasa de descuento (r)							10% anual	
Fórmula del VAN							$VAN = -I_0 + \sum_{n=1}^N \frac{C_n}{(1+r)^n}$	+89.064,15 USD
Fórmula de la TIR							$\sum_{t=0}^n \frac{C_t}{(1+TIR)^t} = 0$	> 100% anual
Interpretación							Si VAN > 0 y TIR > 10%, el proyecto es rentable y	Proyecto viable y altamente rentable

recupera la inversión.	e rentable
---------------------------	---------------

Nota. Elaboración propia.

11. Prototipo De Producto

11.1. Identidad corporativa

A fin de darle vida a nuestra identidad corporativa, no queríamos quedarnos solo con un logotipo estético. Decidimos estructurar todo un enfoque visual que logre transmitir, de un solo vistazo, esa fusión entre la ciberseguridad de más alto nivel y un diseño tecnológico moderno. Para lograrlo, elegimos trabajar con un estilo Flat Design (diseño plano); esto nos garantiza que el imago tipo sea completamente escalable y no pierda calidad, sin importar si lo imprimimos en un documento pequeño o lo proyectamos en una pantalla grande.

A continuación, detallamos las decisiones detrás de cada elemento visual que consolida la imagen de nuestra propuesta:

- **Nombre comercial y marca:** Bautizamos a nuestra empresa matriz como "Corporación Phylax Tech". Elegimos la palabra "Phylax" porque en griego antiguo significa "Guardián", y esa es exactamente la premisa narrativa de nuestro negocio: convertirnos en la línea de defensa definitiva para garantizar la continuidad operativa de cualquier organización. Bajo esta misma sombrilla corporativa, nuestro hardware protector lleva el nombre comercial que ya conocemos: "DevBox".
- **Logotipo o símbolo gráfico:**



Construimos nuestro núcleo visual basándonos en un isotipo minimalista.

Jugamos con la geometría para fusionar dos conceptos clave en una sola imagen:

- **El Escudo:** Es la representación universal de la invulnerabilidad y la protección de los activos más valiosos de nuestros clientes.
- **La Red Geométrica:** Dibujamos el interior del escudo formando una perspectiva cúbica. Con esto simbolizamos el corazón de nuestro hardware: el almacenamiento físico de datos y toda la interconectividad técnica.
- **Slogan o frase complementaria:** "Guardianes de tu continuidad".
Necesitábamos una frase contundente que le comunicara directamente al cliente nuestra promesa de valor. Al leerla, el administrador de la clínica sabe inmediatamente que nuestra misión es asegurar la resiliencia de su organización y evitar que sus procesos médicos se detengan ante una amenaza digital.
- **Paleta de colores:**
 - **Azul Marino:** Lo usamos como color dominante porque transmite la sensación de estabilidad, confidencialidad y confianza institucional que todo centro médico busca.
 - **Verde Esmeralda:** Lo incorporamos para representar la vitalidad clínica; además, en el mundo del software y los servidores, es el indicador universal de que un sistema está seguro y operando sin fallos.

- **Blanco Puro:** Aprovechamos este espacio negativo para darle limpieza visual a la marca, emulando la asepsia y pulcritud que se respira en los entornos hospitalarios.
- **Tipografía:** Nos decantamos por la familia tipográfica Montserrat. Al ser una fuente sans-serif (sin remates) y geométrica, sus trazos uniformes reflejan una precisión casi de ingeniería. Además, nos asegura que los textos sean legibles de inmediato, ya sea en pantallas de monitoreo o en formatos impresos.
- **Aplicaciones visuales:** Diseñamos toda esta identidad pensando en el mundo físico. Los trazos están optimizados para que podamos aplicar un grabado láser impecable directamente sobre la carcasa de la DevBox, y por supuesto, para que resalte en toda la papelería corporativa que usaremos para salir a captar nuevas clínicas.

11.2. Descripción de producto o servicio

Con el diseño visual ya definido, el siguiente paso fue materializar todos los meses de investigación en un modelo comercial real, estructurado bajo el esquema de Hardware as a Service.

- **Nombre del producto o servicio:** DevBox – Sistema de Bóveda Inmutable de Red Perimetral.
- **Descripción general:** Es un appliance de seguridad física que automatiza el resguardo de la información crítica sin depender del usuario. Lo que hace el equipo en la práctica es utilizar tecnología de inmutabilidad para tomar instantáneas de los archivos en modo de "solo lectura". De esta manera, si un

ransomware ataca a la clínica e intenta cifrar la red, nuestra bóveda bloquea el acceso malicioso y garantiza que podamos restaurar las operaciones del centro médico de forma casi inmediata.

- **Características o componentes principales:**
 - **Infraestructura:** Armamos el núcleo sobre una placa Raspberry Pi 5 de 8GB de RAM. Le integramos un almacenamiento sólido SSD NVMe M.2 y un sistema de refrigeración activa para asegurar un alto rendimiento continuo sin que el equipo sufra sobrecalentamientos.
 - **Lógica de Seguridad:** Configuramos el sistema de archivos BTRFS para gestionar las instantáneas inmutables y levantamos el protocolo Samba para que la caja se integre de forma transparente con las computadoras empresariales. Como ya detallamos antes, todo este ecosistema está vigilado por nuestro Sistema de Prevención de Intrusiones (IDPS) y su capacidad de amputación de red (Kill-Switch).
 - **Alertas:** Enlazamos el código con la API de Telegram. Si ocurre una anomalía, el administrador del centro de salud recibe un mensaje de auxilio directo en su teléfono en tiempo real.
- **Presentación final o portafolio:** El dispositivo se entrega en una unidad compacta y sellada, rotulada con la marca institucional, lista para su integración Plug-and-Play en el nodo central de red del cliente.
- **Valor agregado o diferenciación:** Su innovación radica en la autonomía operativa y la eliminación de licencias comerciales recurrentes. Ofrece una

defensa activa y pasiva sin requerir la intervención técnica constante del usuario final, democratizando el acceso a ciberseguridad de nivel corporativo.

- **Segmento de mercado:** Empresas, instituciones privadas y organizaciones profesionales que gestionan datos sensibles y requieren garantizar la continuidad de su negocio frente a amenazas digitales.
- **Beneficio o impacto esperado:** Asegura la resiliencia operativa, evita pérdidas financieras por secuestro de datos y garantiza el cumplimiento de los estándares de seguridad técnica exigidos por las normativas vigentes de protección de datos.

11.3. Canal de promoción

Cuando nos sentamos a definir cómo íbamos a vender la "DevBox" bajo la firma de Corporación Phylax Tech, tuvimos claro desde el primer minuto que no podíamos usar publicidad masiva tradicional. Al involucrarnos con información médica tan confidencial, nuestra ruta obligatoria era el marketing corporativo (B2B). En lugar de desperdiciar recursos en anuncios genéricos de redes sociales, concentramos nuestra estrategia comercial en medios específicos que nos permitan construir verdadera autoridad técnica, ganarnos la confianza del sector salud y demostrar empíricamente que nuestra solución funciona.

Desglosamos la estructura de este canal promocional bajo los siguientes ejes

- **Objetivo del canal de promoción:** Nuestra meta central es lograr que el mercado corporativo de Machala reconozca a la DevBox como su estándar tecnológico. Queremos posicionarnos como la alternativa definitiva y accesible

que les quitará a las clínicas el dolor de cabeza de cumplir con la LOPDP, asegurando que ninguna extorsión digital paralice sus operaciones.

- **Público objetivo:** Apuntamos directamente a quienes firman los cheques y asumen el riesgo legal: directores médicos, gerentes generales y administradores de clínicas o centros de especialidades locales (Tipología B y C). Buscamos a esos tomadores de decisiones que necesitan optimizar sus presupuestos, pero sin dejar desprotegidos los datos de sus pacientes.
- **Estrategia de promoción:** Nos decidimos por un modelo de ventas "Híbrido y Consultivo". Básicamente, esto significa que primero construimos nuestra reputación como expertos en plataformas digitales y, acto seguido, cerramos el trato yendo físicamente a las instalaciones médicas para demostrar el valor real de nuestro hardware.
- **Medios y canales utilizados (Tipología):**
 - **Canal Digital:** Levantaremos un sitio web institucional que funcione no solo como nuestra vitrina principal, sino como un embudo de ventas y centro de soporte técnico. A la par, manejaremos perfiles activos en LinkedIn, publicando artículos que concienticen al sector salud sobre los riesgos cibernéticos, logrando así atraer la atención de los gerentes de forma orgánica.
 - **Canal Promocional y Demostrativo:** Ejecución de simulaciones de ataques controlados ("Pruebas de Estrés") directamente en las oficinas de los clientes potenciales utilizando un prototipo de demostración.

- **Canal Institucional:** Gestión de alianzas estratégicas o charlas técnicas con gremios locales, como el Colegio de Médicos de El Oro, para concientizar sobre el impacto legal de la pérdida de historias clínicas.
- **Mensaje o propuesta comunicacional:** El mensaje central es directo y enfocado en mitigar el riesgo: "Protege los datos de tu empresa y garantiza tu cumplimiento legal sin la necesidad de comprar costosos servidores. Phylax Tech: Guardianes de tu continuidad".
- **Frecuencia y alcance estimado:**
 - **Digital:** Publicaciones quincenales de artículos técnicos/legales en LinkedIn.
 - **Presencial:** Proyección de 2 demostraciones técnicas agendadas por semana.
 - **Alcance:** Se estima impactar de manera directa a las 63 instituciones del universo de estudio durante el primer trimestre de operaciones.
- **Indicadores de efectividad (KPIs):** La campaña no se medirá por "Likes" en redes sociales, sino por métricas de negocio reales:
 - Número de reuniones ejecutivas o "Pruebas Piloto" agendadas por mes.
 - Tasa de conversión (Porcentaje de clínicas que adquieren la suscripción Hardware as a Service después de ver la demostración).
 - Tráfico orgánico y formularios de contacto completados en el sitio web corporativo.

11.4. Validación del Prototipo

La validación constituye la etapa final del desarrollo del emprendimiento "Corporación Phylax Tech", donde se demuestra de manera objetiva la aceptación, pertinencia comercial y funcionalidad técnica de la "DevBox". Con estos resultados en mano, logramos comprobar sin dejar lugar a dudas que nuestra propuesta realmente soluciona la vulnerabilidad informática de las clínicas en Machala y que el modelo de cobro Hardware as a Service (HaaS) tiene todo el potencial para implementarse con éxito.

Como necesitábamos estar completamente seguros de que nuestro equipo no iba a fallar en ninguna circunstancia real, sometimos el proyecto a dos frentes de prueba extremadamente rigurosos, adaptándonos a lo que exige un emprendimiento tecnológico de este nivel:

1. Validación técnica o profesional (Pruebas de Estrés en Laboratorio)

- **Propósito y participantes:** Necesitábamos someter a la DevBox a un escenario de desastre real para verificar si su arquitectura cumplía con los estándares de la LOPDP y la normativa ISO 27799 frente a un ciberataque. Estas pruebas las validamos nosotros mismos en conjunto con la tutoría técnica.
- **Herramientas aplicadas:** Lanzamos ataques controlados contra nuestro propio equipo. Simulamos una intrusión agresiva saturando la red (Ataque DoS desde Kali Linux) y ejecutamos un código malicioso de Ransomware que creamos en PowerShell.

- **Resultados técnicos:** El equipo se defendió con una efectividad del 100%. Apenas lanzamos el ataque, nuestro Sistema de Prevención de Intrusiones (IDPS) detectó la anomalía y ejecutó el Kill-Switch (amputación de red) en milisegundos. Inmediatamente después, gracias a la configuración del sistema de archivos BTRFS, recuperamos absolutamente todas las historias clínicas que el virus intentó encriptar. Logramos un Tiempo Objetivo de Recuperación (RTO) de menos de 3 minutos y, lo más importante, sin perder un solo byte de información.

2. Validación comercial y Encuesta de validación (Estudio de Mercado)

- **Propósito y participantes:** Debíamos medir qué tanta intención de compra real existe en el mercado local. Para esto, acudimos directamente a los 63 directores, administradores y jefes de TI de las clínicas de Machala (Tipología B y C) que conformaron nuestro universo de estudio.
- **Herramientas aplicadas:** Nos apoyamos en el cuestionario digital estructurado que aplicamos in situ durante nuestras visitas de campo.
- **Nivel de aceptación comercial:** La aceptación comercial fue contundente. El 95.2% de los encuestados nos confirmó que sí confiaría en una solución de hardware local si le demostramos su efectividad. Pero el dato que verdaderamente dio luz verde a nuestro negocio es que el 93.6% de las instituciones nos pidió directamente ejecutar una prueba piloto de la DevBox en sus instalaciones, validando que están dispuestos a pagar la mensualidad recurrente en el rango de los \$30 a \$60 USD.

11.4.1. Oportunidades de mejora detectadas

Al evaluar cómo se comportó el equipo en el laboratorio y escuchar las necesidades puntuales que nos comentaron los médicos durante el trabajo de campo, identificamos dos grandes oportunidades para escalar las futuras versiones de nuestro servicio:

- Soporte energético local: Nos dimos cuenta de que es vital incorporarle a la placa de la Raspberry Pi un módulo de respaldo de energía propio (Micro-UPS HAT). Tomando en cuenta los constantes cortes de suministro eléctrico que sufre el cantón Machala, esto garantizará que el equipo siga generando sus instantáneas inmutables aunque la clínica se quede a oscuras.
- Expansión de hardware: Vimos la necesidad de escalar el almacenamiento NVMe para ofrecer capacidades de 1TB y 2TB. Este upgrade va dirigido específicamente a las clínicas más grandes (Tipología C), ya que manejan volúmenes altísimos de imágenes médicas pesadas, como radiografías o tomografías en formato DICOM.

11.4.2. Evidencia Documental

Con el fin de transparentar al máximo la veracidad de estas pruebas, documentamos absolutamente todo. Los registros forenses del sistema operativo (Logs), las capturas de pantalla del momento exacto en que recuperamos los datos, los gráficos y el formato final de las encuestas los dejamos detallados de forma íntegra en el apartado 9.3 de Validación Técnica y en la sección de Anexos del presente documento.

12. Presupuesto

Tabla 8

Presupuesto referencial para la ejecución del proyecto de titulación

Rubros	Unidad de medida	Cantidad	Costo unitario	Costo total
Recurso material y tecnológico				
Kit Raspberry Pi 5 (Placa + Fuente + Case)	Unidad	1	\$190,87	\$190,87
Disco SSD 256Gb Externo (Alta Velocidad)	Unidad	1	\$50,00	\$50,00
Internet (Plan Básico - 5 meses)	Mensual	5	\$20,00	\$100,00
Dominio Web (.com) para el emprendimiento	Anual	1	\$20,00	\$20,00
Suministros de Oficina (Papelería)	Global	1	\$20,00	\$20,00
Servicios varios				
Transporte (Visitas a clínicas en Machala)	Global	1	\$40,00	\$40,00
Alimentación (Días de trabajo de campo)	Global	1	\$40,00	\$40,00
Impresión y Empastado (Documento Final)	Unidad	3	\$12,00	\$36,00
Especie Valorada (Trámites ISTS)	Unidad	1	\$5,00	\$5,00
SUBTOTAL				\$501,87
Imprevistos 5%				\$25,09
TOTAL				\$526,96

Nota. Elaboración propia basada en la proforma de costos de mercado local (2025).

13. Cronograma

Actividades	Noviembre				Diciembre				Enero				Febrero					Marzo				Abril				
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	5	1	2	3	4	1	2	3	4	5
Taller de investigación y formulación del proyecto de investigación de fin de carrera.	x	x																								
Identificación del problema.				x																						
Planteamiento del tema.					x																					
Elaboración de justificación.						x																				
Planteamiento de objetivo general y objetivos específicos.							x																			
Elaboración del marco institucional y marco teórico.								x																		
Elaboración de diseño metodológico, metodologías y técnicas de investigación a ser utilizadas en la investigación.									x																	
Determinar la muestra, recursos y bibliografía.										x																
Presentación del ante proyecto al Vicerrectorado.											x															
Aprobación de temas de proyectos de la investigación de fin de carrera.												x														
Desarrollo de investigación y propuesta de acción.													X	x	x	x	x	x	x	x	x	x				
Elaboración de conclusiones y recomendaciones y levantamiento del documento final del borrador de proyecto de investigación																							x		x	
Entrega de proyectos de investigación de fin de carrera.																									x	x

Nota. Cronograma de actividades a completar del proyecto de investigación

14. Conclusiones

En base al primer objetivo específico, se logró un marco teórico que sustenta la necesidad de infraestructuras de seguridad perimetral en el sector salud. Las investigaciones permitieron establecer que el diseño de arquitecturas de almacenamiento inmutable no solo obedece a una necesidad de protección frente al ransomware, sino que garantiza el cumplimiento del principio de seguridad y confidencialidad exigido por la Ley Orgánica de Protección de Datos Personales en el Ecuador.

Respecto al segundo objetivo, la aplicación de encuestas en el universo de clínicas privadas de Machala permitió diagnosticar un nivel crítico de vulnerabilidades. Se evidenció la falta de protocolos de respaldo automatizados y una alta dependencia de personal externo, permitiendo definir una solución autónoma y asequible para los centros de salud.

Mediante el tercer objetivo, se construyó el dispositivo DevBox por ende se integró eficientemente el Raspberry Pi 5 con un sistema de archivos BTRFS para la generación de instantáneas inmutables. Así mismo, se superaron las expectativas de endurecimiento del sistema al desarrollar e integrar un Sistema de Prevención de Intrusiones autónomo, dotando al dispositivo de una capacidad de amputación de red frente a comportamientos anómalos.

Finalmente, se validó de manera técnica las simulaciones de laboratorio con una efectividad del 100%, logrando que el dispositivo aisle la red ante ataques de denegación de servicio y recupere la totalidad de las historias clínicas tras una infección simulada por ransomware. A nivel comercial, el estudio de mercado validó una intención de adopción, demostrando que el modelo de negocio Hardware as a Service propuesto por "Corporación Phylax Tech" es altamente pertinente, escalable y financieramente viable para el entorno local.

15. Recomendaciones

A nivel de Hardware: Se recomienda integrar un módulo de alimentación ininterrumpida (Micro-UPS HAT) a la placa de procesamiento. Esto permitirá que, ante cortes eléctricos, el sistema finalice correctamente la escritura de bloques y cierre el ciclo de instantáneas inmutables, eliminando cualquier riesgo de corrupción de datos en el disco NVMe.

A nivel de Arquitectura de Red: Se sugiere escalar el sistema mediante una sincronización cifrada hacia un almacenamiento externo o nube. Esta mejora permitirá cumplir con la regla "3-2-1" de ciberseguridad, asegurando la recuperación de la información corporativa incluso frente a desastres físicos como incendios, inundaciones o robo del hardware en las instalaciones del cliente.

A nivel de Desarrollo de Software: Se aconseja evolucionar el Sistema de Prevención de Intrusiones (IDPS) integrando algoritmos de aprendizaje automático de bajo consumo. Esta actualización permitirá analizar patrones de tráfico de forma heurística, mejorando la detección de variantes de malware de día cero y reduciendo significativamente la tasa de falsos positivos.

A nivel Comercial y de Mercado: Se recomienda a "Corporación Phylax Tech" ejecutar planes piloto de mediana duración en entornos de producción reales para recopilar métricas de rendimiento en vivo. Asimismo, dado que la arquitectura de inmutabilidad es transversal, se sugiere expandir este modelo Hardware as a Service más allá del sector salud, abarcando firmas legales y estudios contables que requieran cumplir con la Ley Orgánica de Protección de Datos Personales.

16. Bibliografía

- Asamblea Nacional de la República del Ecuador. (2021, 26 de mayo). Ley Orgánica de Protección de Datos Personales. Registro Oficial Suplemento 459.
<https://www.telecomunicaciones.gob.ec>
- Acha Araya, E. (2017). Monitoreo activo de seguridad sobre la red chilena. Disponible en <https://repositorio.uchile.cl/handle/2250/148367>
- Avila Niño, F. Y. (2023). Ransomware, una amenaza latente en Latinoamérica. *InterSedes*, 24(49), 92–119. <https://doi.org/10.15517/isucr.v24i49.50765>
- Coventry, L., & Branley, D. (2018). Cybersecurity in healthcare: A narrative review of trends, threats and ways forward [Ciberseguridad en la atención sanitaria: una revisión narrativa de tendencias, amenazas y caminos a seguir]. *Maturitas*, 113, 48-52. doi.org
- Department of Health and Social Care. (2018). *Lessons learned review of the WannaCry Ransomware Cyber Attack*. National Health Service (NHS).
<https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf>
- El Comercio. (2020, 12 de agosto). *IESS suspende servicios en línea por ataques informáticos*. Diario El Comercio. <https://www.elcomercio.com/sociedad/ieess-suspende-servicios-internet-ataques/>
- Fresno Chávez, C. (2019). *Metodología de la investigación: así de fácil*. Ciudad Educativa.
<https://elibro.net/en/lc/sudamericanoloja/titulos/98278>
- GAD Municipal de Machala. (2020). *Plan de Desarrollo y Ordenamiento Territorial del Cantón Machala 2020-2023*. Gaceta Oficial. <https://www.machala.gob.ec>

- Instituto Nacional de Estadística y Censos (INEC). (2023a). *Resultados del Censo Ecuador 2022: Población y Vivienda*. <https://www.censoecuador.gob.ec/>
- Instituto Nacional de Estadística y Censos (INEC). (2023b). *Registro Estadístico de Camas y Egresos Hospitalarios 2023*. <https://www.ecuadorencifras.gob.ec/>
- International Organization for Standardization. (2016). *Health informatics — Information security management in health using ISO/IEC 27002 (ISO/IEC 27799:2016)*. ISO. (Agregada por necesidad técnica del Marco Teórico).
- International Telecommunication Union (ITU). (2018). *Security framework for the Internet of things based on the gateway model (ITU-T Recommendation X.1361)*. <https://www.itu.int/rec/T-REC-X.1361>
- IT Ahora & Deloitte. (2024). *Quinto estudio sobre el estado de la ciberseguridad en Ecuador: Sector privado*. IT Ahora. <https://itahora.com/2024/06/04/presentacion-5to-informe-estado-actual-de-la-ciberseguridad-ecuador-2024-sector-privado/>
- Kaspersky. (2020, 13 de mayo). *Eugene Kaspersky: los ciberataques a hospitales durante el COVID-19 equivalen a terrorismo*. <https://www.kaspersky.es/about/press-releases/eugene-kaspersky-los-ciberataques-a-hospitales-durante-el-covid-19-equivalen-a-terrorismo>
- Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL). (2023). *Resultados de Conectividad y Gobierno Digital*. Observatorio Ecuador Digital. <https://observatorioecuadordigital.mintel.gob.ec/>
- National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1)*. U.S. Department of Commerce. <https://doi.org/10.6028/NIST.CSWP.04162018>

National Institute of Standards and Technology (NIST). (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. National Institute of Standards and Technology.

<https://doi.org/10.6028/NIST.CSWP.29>

Peleteiro Rey, H. (2025). Análisis de soluciones para la implementación de sistemas de almacenamiento jerárquicos. <http://hdl.handle.net/2183/41301>

Presidencia de la República del Ecuador. (2023). *Reglamento General a la Ley Orgánica de Protección de Datos Personales*. Registro Oficial.

<https://www.telecomunicaciones.gob.ec/>

Programa de las Naciones Unidas para el Desarrollo (PNUD). (s.f.). *Objetivos de Desarrollo Sostenible*. <https://www.undp.org/es/sustainable-development-goals>

Storage Networking Industry Association (SNIA). (2022). *The definition of WORM (Write Once, Read Many) in the era of Ransomware*. SNIA Technical Whitepaper. (Agregada por necesidad técnica del Marco Teórico).

Swissinfo. (2022, 31 de mayo). *El Seguro Social de Costa Rica sufre ciberataque que afecta a hospitales*. <https://www.swissinfo.ch/spa/el-seguro-social-de-costa-rica-sufre-ciberataque-que-afecta-a-hospitales/47637614>

Upton, E., & Halfacree, G. (2022). *Raspberry Pi User Guide* (5th ed.). Wiley. (Agregada por necesidad técnica del Marco Teórico).

17. Anexos

Anexo A: Certificado de aprobación de Vicerrectorado de Innovación y Desarrollo

Oficio Nro. 032-PT-INV-ISTS-SEDE-2026
Loja, 17 de febrero de 2026



Sr. Jose Xavier Mocha Quichimbo
Sr. Anthony Edinson Yaguachi Cárdenas
ESTUDIANTES DE LA CARRERA DE CIBERSEGURIDAD

De mi consideración:

Por medio de la presente, me permito comunicarle que el Departamento de Investigación, Desarrollo e Innovación ha revisado su anteproyecto de trabajo de titulación, titulado:

**“EMPRENDIMIENTO TECNOLÓGICO PARA EL DESARROLLO DE UN
DISPOSITIVO DE SEGURIDAD CON RASPBERRY PI ORIENTADO A LA
PROTECCIÓN DE LA INFORMACIÓN Y MITIGACIÓN DE RANSOMWARE
EN CLÍNICAS Y CENTROS DE ESPECIALIDADES PRIVADOS DE LA
CIUDAD DE MACHALA.”;**

el mismo ha sido evaluado a través de un proceso de revisión por pares, tanto internos como externos, y se constata que cumple con los lineamientos establecidos por la institución. En consecuencia, **se autoriza su ejecución y puesta en marcha.** Para tal efecto, se nombra como director de su proyecto de fin de carrera al(la) esp **Linder Bravo Pardo,**

Particular que le hago conocer para los fines pertinentes.

Atentamente,



Ing. Jackson Michael Quevedo, Mgs.
Coordinador de Investigación, D+I

Anexo B: Certificado de aprobación de la entidad para la ejecución del proyecto

Ingeniero

Linder Fernando Bravo Pardo, Mgs

COORDINADOR DE LA CARRERA DE CIBERSEGURIDAD DEL ISTS MACHALA

De mi consideración

Por medio del presente, me permito aprobar el proyecto de investigación titulado

“Emprendimiento tecnológico para el desarrollo de un dispositivo de seguridad con raspberry pi orientado a la protección de la información y mitigación de ransomware en clínicas y centros de especialidades privados de la ciudad de Machala.”, desarrollado por los estudiantes Jose Xavier Mocha Quichimbo, con C.I. 0705609857, y Anthony Edinson Yaguachi Cárdenas, con C.I. 0705528008.

Dicho proyecto cuenta con la autorización para el levantamiento de información, investigación in situ o virtual, así como para la socialización de la propuesta de acción en el Instituto Superior Tecnológico Sudamericano.

Machala, 10 de noviembre del 2025



Ing. Linder Fernando Bravo Pardo, Mgs

Coordinador Carrera Ciberseguridad

C.I.: 1104635089

Anexo C: Acta de socialización de la propuesta de acción

Ingeniero

Linder Fernando Bravo Pardo, Mgs

COORDINADOR DE LA CARRERA DE CIBERSEGURIDAD DEL ISTS MACHALA

De mi consideración

Por medio del presente, me permito aprobar el proyecto de investigación titulado

“Emprendimiento tecnológico para el desarrollo de un dispositivo de seguridad con raspberry pi orientado a la protección de la información y mitigación de ransomware en clínicas y centros de especialidades privados de la ciudad de Machala.”, desarrollado por los estudiantes Jose Xavier Mocha Quichimbo, con C.I. 0705609857, y Anthony Edinson Yaguachi Cárdenas, con C.I. 0705528008, dejando asimismo constancia de que se han realizado las pruebas y validaciones correspondientes al proyecto, verificando el cumplimiento de los objetivos propuestos y la funcionalidad de la aplicación desarrollada; los resultados obtenidos demuestran su correcto desempeño en las etapas de implementación y uso, garantizando su aplicabilidad en el entorno real, por lo cual se certifica y da fe de su adecuado funcionamiento y validez técnica.

Machala, 13 de marzo del 2026



Ing. Linder Fernando Bravo Pardo, Mgs

Coordinador Carrera Ciberseguridad

C.I.: 1104635089

Anexo D: Certificado de Abstract



CERTF ABS. N°. 020-JP-CISM-2026
Loja, 27 de Mayo de 2026

El suscrito, Lic. Juan Pablo Quezada Rosales, **DOCENTE DEL ÁREA DE INGLÉS - CIS DEL INSTITUTO SUPERIOR TECNOLÓGICO "SUDAMERICANO"**, a petición de la parte interesada y en forma legal,

CERTIFICO:

Que el apartado **ABSTRACT** del Proyecto de Investigación de Fin de Carrera de los señores **ANTHONY EDINSON YAGUACHI CARDENAS & JOSE XAVIER MOCHAQUICHIMBO** estudiantes en proceso de titulación periodo Noviembre 2025 - Marzo 2026 de la carrera de **CIBERSEGURIDAD**, modalidad presencial está correctamente traducido, luego de haber ejecutado las correcciones emitidas por mi persona; por cuanto se autoriza la impresión y presentación dentro del empastado final previo a la disertación del proyecto.

Particular que comunico en honor a la verdad para los fines académicos pertinentes.

English is a piece of cake with CIS.



Firmado digitalmente por JUAN PABLO QUEZADA ROSALES
Motivo: Legitimación

Checked by:
Juan Pablo Quezada R.
E.P.L. Teacher

Lic. Juan Pablo Quezada Rosales.
DOCENTE DEL ÁREA DE INGLÉS ISTS - CIS

Anexo E: Presupuesto

Rubros	Unidad de medida	Cantidad	Costo unitario	Costo total
Recurso material y tecnológico				
Kit Raspberry Pi 5 (Placa + Fuente + Case)	Unidad	1	\$190,87	\$190,87
Disco SSD 256Gb Externo (Alta Velocidad)	Unidad	1	\$50,00	\$50,00
Internet (Plan Básico - 5 meses)	Mensual	5	\$20,00	\$100,00
Dominio Web (.com) para el emprendimiento	Anual	1	\$20,00	\$20,00
Suministros de Oficina (Papelería)	Global	1	\$20,00	\$20,00
Servicios varios				
Transporte (Visitas a clínicas en Machala)	Global	1	\$40,00	\$40,00
Alimentación (Días de trabajo de campo)	Global	1	\$40,00	\$40,00
Impresión y Empastado (Documento Final)	Unidad	3	\$12,00	\$36,00
Especie Valorada (Trámites ISTS)	Unidad	1	\$5,00	\$5,00
SUBTOTAL				\$501,87
Imprevistos 5%				\$25,09
TOTAL				\$526,96

Anexo F: Cronograma

Actividades	Noviembre				Diciembre				Enero				Febrero				Marzo				Abril				
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	5
Taller de investigación y formulación del proyecto de investigación de fin de carrera.	X	X																							
Identificación del problema.				X																					
Planteamiento del tema.				X																					
Elaboración de justificación.					X																				
Planteamiento de objetivo general y objetivos específicos.					X																				
Elaboración del marco institucional y marco teórico.						X																			
Elaboración de diseño metodológico, metodología y técnicas de investigación a ser utilizados en la investigación.							X																		
Determinar la muestra, recursos y bibliografía.								X																	
Presentación del ante proyecto al Vicerrectorado.									X																
Aprobación de temas de proyectos de la investigación de fin de carrera.									X																
Desarrollo de investigación y propuesta de acción.										X	X	X	X	X	X	X	X	X	X	X					
Elaboración de conclusiones y recomendaciones y levantamiento del documento final del borrador de proyecto de investigación.																					X	X			
Entrega de proyectos de investigación de fin de carrera.																						X	X	X	

Nota. Cronograma de actividades a completar del proyecto de investigación

Anexo G: Formato de encuesta



Encuesta de Seguridad y Respaldo de Información en el Sector Salud de Machala

Título del Proyecto:

Emprendimiento tecnológico para el desarrollo de un dispositivo de seguridad con raspberry pi orientado a la protección de la información y mitigación de ransomware en clínicas y centros de especialidades privados de la ciudad de Machala.

Objetivo:

Identificar las necesidades actuales de protección de datos médicos para el desarrollo de soluciones tecnológicas locales que aseguren la continuidad de la atención al paciente.

1. **¿Qué método utiliza actualmente para respaldar la información médica de sus pacientes?**
 - ☐ Discos externos o memorias USB.
 - ☐ Nubes (Google Drive/OneDrive) o Servidor.
 - ☐ No realizamos respaldos actualmente.
2. **¿Con qué frecuencia se realizan las copias de seguridad en su institución?**
 - ☐ Frecuente (Diario/Automatizado).
 - ☐ Esporádica (Semanal/Mensual).
 - ☐ No se realiza copias.
3. **¿Qué tan preocupado está frente a un hackeo o pérdida de datos (Ransomware)?**
 - ☐ Muy preocupado (Es un riesgo crítico).
 - ☐ Algo preocupado (Conozco el riesgo, pero no tenemos defensa).
 - ☐ Nada preocupado (No conozco el riesgo).
4. **¿Conoce el concepto de "Almacenamiento Inmutable" (Copias que no se pueden borrar ni cifrar)?**
 - ☐ Sí, lo conozco y me interesa.
 - ☐ He escuchado, pero no sé cómo aplicarlo.
 - ☐ No conozco el concepto.
5. **¿Qué tan preparado considera que está su centro para cumplir con la Ley de Protección de Datos (LOPD)?**
 - ☐ Preparado (tenemos protocolos).
 - ☐ Poco preparado (Conocemos la ley, pero faltan herramientas).
 - ☐ Nada preparando.



6. **¿Cuál es el principal motivo por el que no tiene un servidor de seguridad profesional?**
- ☐ Costo muy elevado (Equipos y licencias).
 - ☐ Complejidad técnica y falta de personal de TI.
 - ☐ No ha sido una prioridad hasta ahora.
7. **¿Confiaría en un dispositivo local de bajo costo (Raspberry Pi) con soporte técnico en Machala?**
- ☐ Sí, prefiero soluciones locales y económicas.
 - ☐ Tal vez, si me demuestran su efectividad.
 - ☐ No, prefiero marcas internacionales costosas.
8. **¿Qué característica valoraría más en una solución de respaldo?**
- ☐ Que sea totalmente automática (Sin intervención humana).
 - ☐ Que sea invulnerable a virus (Immutable).
 - ☐ Que sea económica y fácil de instalar.
9. **¿Qué rango de inversión mensual consideraría razonable para este servicio?**
- ☐ Entre \$30 y \$60 USD.
 - ☐ Entre \$61 y \$100 USD.
 - ☐ Más de \$100 USD.
10. **¿Estaría interesado en una prueba piloto de este dispositivo en su institución?**
- ☐ Sí, me interesa probarlo pronto.
 - ☐ Tal vez en el futuro (Necesito más información).
 - ☐ No me interesa por el momento.

Anexo H: Formato de encuesta validado



Encuesta de Seguridad y Respaldo de Información en el Sector Salud de Machala

Título del Proyecto:

Emprendimiento tecnológico para el desarrollo de un dispositivo de seguridad con raspberry pi orientado a la protección de la información y mitigación de ransomware en clínicas y centros de especialidades privados de la ciudad de Machala.

Objetivo:

Identificar las necesidades actuales de protección de datos médicos para el desarrollo de soluciones tecnológicas locales que aseguren la continuidad de la atención al paciente.

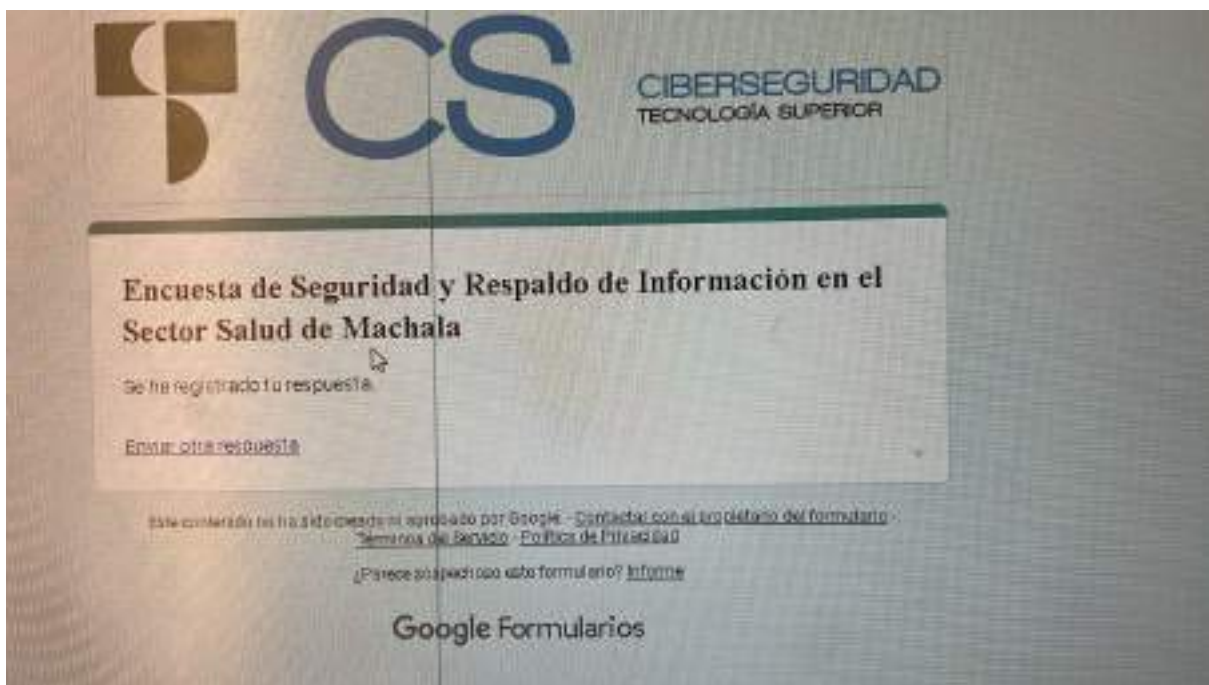
1. **¿Qué método utiliza actualmente para respaldar la información médica de sus pacientes?**
 - ☐ Discos externos o memorias USB.
 - ☐ Nubes (Google Drive/OneDrive) o Servidor.
 - ☐ No realizamos respaldos actualmente.
2. **¿Con qué frecuencia se realizan las copias de seguridad en su institución?**
 - ☐ Frecuente (Diario/Automatizado).
 - ☐ Esporádica (Semanal/Mensual).
 - ☐ No se realiza copias.
3. **¿Qué tan preocupado está frente a un hackeo o pérdida de datos (Ransomware)?**
 - ☐ Muy preocupado (Es un riesgo crítico).
 - ☐ Algo preocupado (Conozco el riesgo, pero no tenemos defensa).
 - ☐ Nada preocupado (No conozco el riesgo).
4. **¿Conoce el concepto de "Almacenamiento Inmutable" (Copias que no se pueden borrar ni cifrar)?**
 - ☐ Sí, lo conozco y me interesa.
 - ☐ He escuchado, pero no sé cómo aplicarlo.
 - ☐ No conozco el concepto.
5. **¿Qué tan preparado considera que está su centro para cumplir con la Ley de Protección de Datos (LOPD)?**
 - ☐ Preparado (tenemos protocolos).
 - ☐ Poco preparado (Conocemos la ley, pero faltan herramientas).
 - ☐ Nada preparando.



6. **¿Cuál es el principal motivo por el que no tiene un servidor de seguridad profesional?**
- ☐ Costo muy elevado (Equipos y licencias).
 - ☐ Complejidad técnica y falta de personal de TI.
 - ☐ No ha sido una prioridad hasta ahora.
7. **¿Confiaría en un dispositivo local de bajo costo (Raspberry Pi) con soporte técnico en Machala?**
- ☐ Sí, prefiero soluciones locales y económicas.
 - ☐ Tal vez, si me demuestran su efectividad.
 - ☐ No, prefiero marcas internacionales costosas.
8. **¿Qué característica valoraría más en una solución de respaldo?**
- ☐ Que sea totalmente automática (Sin intervención humana).
 - ☐ Que sea invulnerable a virus (Immutable).
 - ☐ Que sea económica y fácil de instalar.
9. **¿Qué rango de inversión mensual consideraría razonable para este servicio?**
- ☐ Entre \$30 y \$60 USD.
 - ☐ Entre \$61 y \$100 USD.
 - ☐ Más de \$100 USD.
10. **¿Estaría interesado en una prueba piloto de este dispositivo en su institución?**
- ☐ Sí, me interesa probarlo pronto.
 - ☐ Tal vez en el futuro (Necesito más información).
 - ☐ No me interesa por el momento.

Anexo I: Encuesta de satisfacción realizada de forma virtual

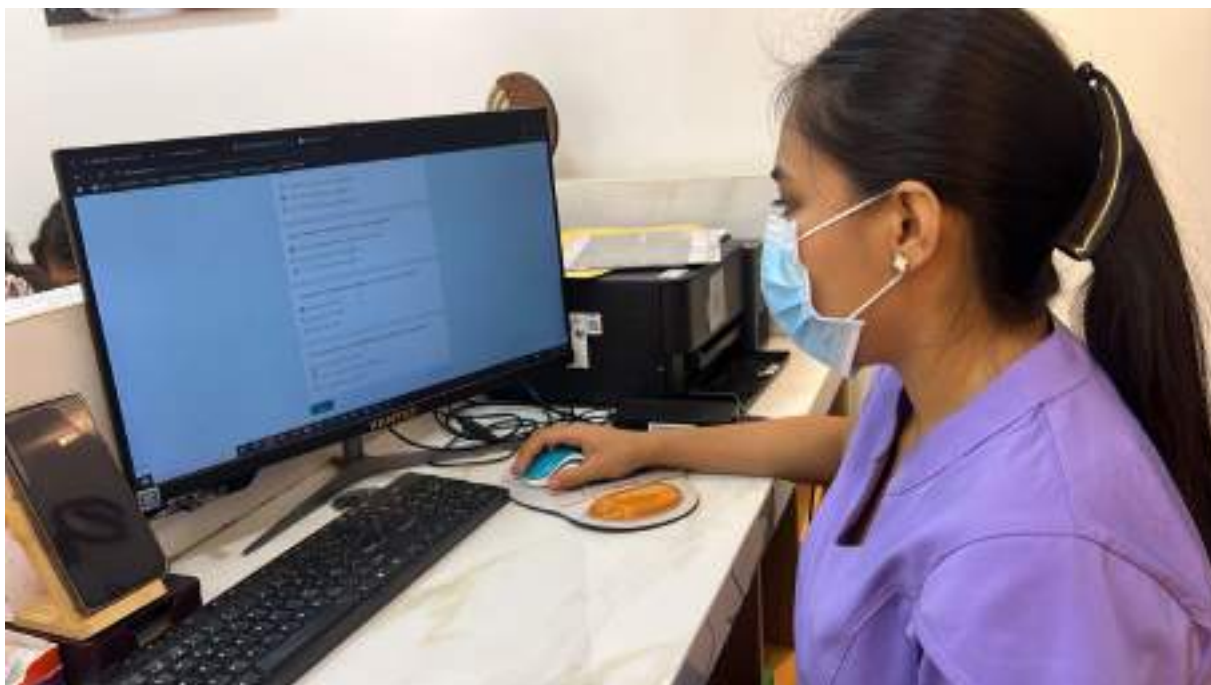
https://docs.google.com/forms/d/e/1FAIpQLSdC2YMxIO87sG4y8B54ZDEZNloW9n_v9GR7UrFQFHDWM7hW2A/viewform?usp=sharing&oid=117478922677810902807



The image shows a screenshot of a Google Form titled "Encuesta de Seguridad y Respaldo de Información en el Sector Salud de Machala". At the top left, there is a logo consisting of four squares (two brown, two blue) arranged in a larger square. To the right of this logo is the text "CS" in large blue letters, followed by "CIBERSEGURIDAD" and "TECNOLOGÍA SUPERIOR" in smaller blue letters. The main title of the form is "Encuesta de Seguridad y Respaldo de Información en el Sector Salud de Machala". Below the title, it says "Se ha registrado tu respuesta." and "Enviar otra respuesta.". At the bottom, there is a footer that reads "Este contenido no ha sido verificado ni aprobado por Google - Contactar con el propietario del formulario - Términos del Servicio - Política de Privacidad" and "¿Parece sospechoso este formulario? Informe". The Google Form logo is at the very bottom.

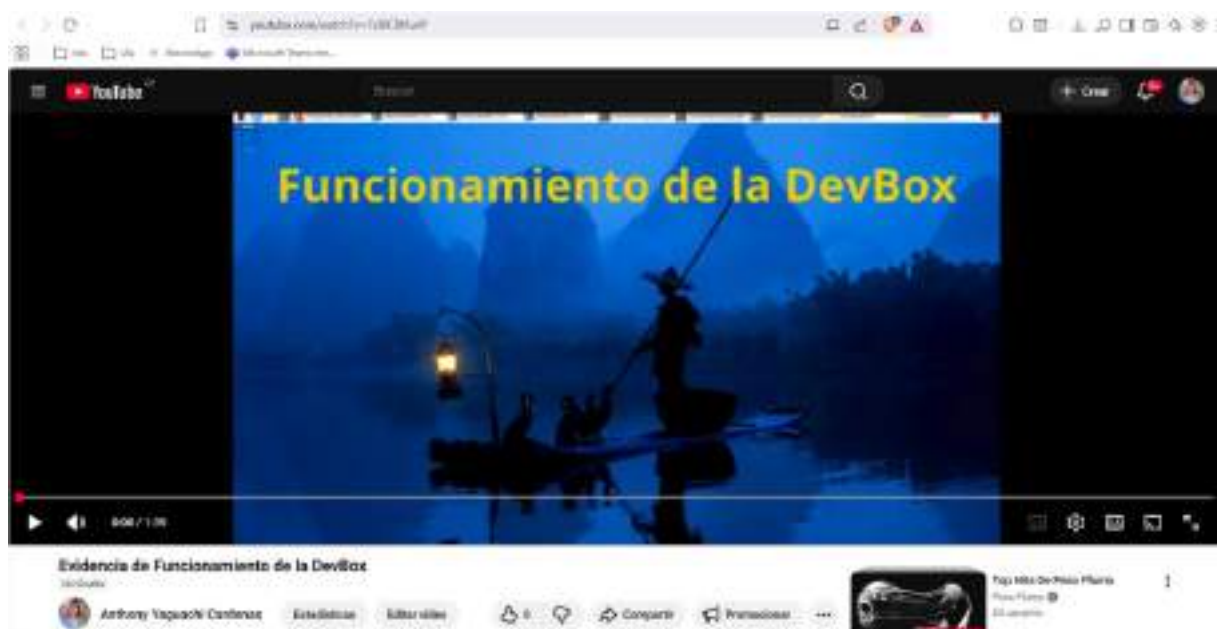
Anexo J: Base de datos

[illegible]

Anexo K: Evidencias fotográficas sobre la realización de encuestas y tabulación

Anexo N: Evidencias del funcionamiento de la aplicación

<https://youtu.be/7xBICBtFwIY>



Anexo Ñ: Solicitud de Aprobación del Tema de Titulación

ESPECIE VALORADA -Nº ITSS-



VALOR: \$2,00

Nº 001664

Machala, 09 de enero de 20 26

Señor(a)

RECTOR (A) DEL INSTITUTO TECNOLÓGICO SUPERIOR SUDAMERICANO

Ciudad:

De mis consideraciones:

Yo, Yaguachi Córdova Anthony Edinson, 0706528008,
Ciberseguridad solicito a Usted, muy atentamente se autorice
la aprobación del anteproyecto con el tema: Implementación de un
dispositivo de seguridad basado en raspberry pi para el respaldo inmutable
y mitigación de ransomware en clínicas y centros de especialidades privados de
Por la favorable atención, anticipo mi agradecimiento, la ciudad de machala.

Atentamente,

Firma de Peticionario

Vista la petición que antecede, _____

Firma Autorizada

Machala, ____ de ____ de 20 ____

Anexo O: Solicitud de Aprobación del Tema del Anteproyecto

Machala 09 de Enero de 2021



Estimada

Ing. María Verónica Paredes Mgs.

**COORDINADORA DEL INSTITUTO SUPERIOR TECNOLÓGICO
SUDAMERICANO - SEDE MACHALA,**

De mis consideraciones:

Saludo a usted cordialmente, por medio de la presente me dirijo a usted para solicitar la aprobación del tema de anteproyecto con el tema "Impacto de la implementación de Smart Grids en la Red de Distribución de Energía Eléctrica en la Zona Urbana de Machala, Páez, entre Sucre y Olmedo" para el desarrollo de la tesis de grado en Ingeniería Eléctrica, en la modalidad de Educación a Distancia, en la Sede Machala del Instituto Tecnológico Sudamericano.

Datos del estudiante

Apellidos y nombres: Roberto Rodríguez Jara
Número de cédula: 0705609857
Carrera: Electrónica
Ciclo: 5º
Modalidad: Presencial
Sección: Diurno () Nocturno A () Nocturno B (X)

Por su gentil atención, me suscribo.

Atentamente,

[Firma]
FIRMA DEL ESTUDIANTE
CL. 0705609857

Vista la petición que
antecede,

Firma: _____ Fecha: _____

Sede Machala: Machala, Páez, entre Sucre y Olmedo
WhatsApp: 0959286997
www.tecnologicosudamericano.edu.ec

Anexo P: Registro de Coordinación de Manera Virtual del Equipo de Investigación

