



INSTITUTO SUPERIOR TECNOLÓGICO SUDAMERICANO
TECNOLOGÍA SUPERIOR EN CIBERSEGURIDAD

**CONSULTORIA DIGITAL PARA PROTECCIÓN DE DATOS Y SEGURIDAD WEB,
IMPLEMENTADA POR UNA PLATAFORMA TECNOLÓGICA DE GESTIÓN DE
SERVICIOS EN LA CIUDAD DE MACHALA, EN EL AÑO 2026**

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

AUTORES:

Justyn Alejandro Alvarez Nagua

Erick Josue Murillo Zambrano

TUTOR:

Ing. Linder Fernando Bravo Pardo, Mgs

Machala, Junio del 2026

Certificación del director del Proyecto de Inv. Fin de Carrera

Ingeniero

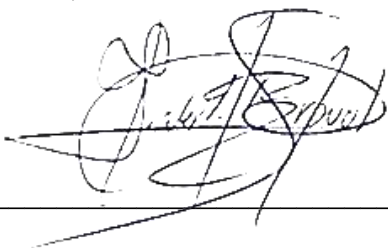
Linder Fernando Bravo Pardo, Mgs

DIRECTOR DE PROYECTO DE FIN DE CARRERA

CERTIFICO:

Que he supervisado el siguiente proyecto de investigación titulado “Consultoría digital para protección de datos y seguridad web, implementada por una plataforma tecnológica de gestión de servicios en la ciudad de Machala, en el año 2026.”, realizado por los estudiantes Justyn Alejandro Alvarez Nagua y Erick Josue Murillo Zambrano el mismo que cumple con lo establecido por el Instituto Superior Tecnológico Sudamericano; por consiguiente, autorizo su presentación ante el tribunal respectivo.

Machala, Junio de 2026



Ing. Linder Fernando Bravo Pardo, Mgs

C.I.: 1104635089

Autoría

Yo, Justyn Alejandro Alvarez Nagua con C.I. 0706007747 & Erick Josue Murillo Zambrano con C.I. 0750240467, en calidad de autores del proyecto de titulación:

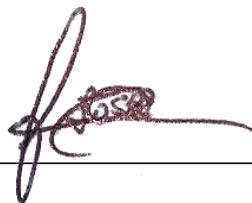
“Consultoría digital para protección de datos y seguridad web, implementada por una plataforma tecnológica de gestión de servicios en la ciudad de Machala, en el año 2026.”, declaramos que el contenido total o parcial que nos pertenece, puede ser usado por el Instituto Superior Tecnológico Sudamericano, para la automatización de los procesos que llevan a cabo dentro de su empresa y mejorar la organización de información.

Los derechos de autoría correspondientes, a excepción de la presente autorización seguirán vigentes a nuestro favor, por lo cual declaramos bajo juramento, que el trabajo descrito es de nuestra autoría; que no ha sido presentado para ninguna calificación profesional u otros fines; y de la misma forma declaramos que todo lo consultado durante el proceso, contiene referencias bibliográficas incluidas en este documento.



Justyn Alejandro Alvarez Nagua

0706007747



Erick Josue Murillo Zambrano

0750240467

Dedicatoria

A mi madre, Mercy Matilde Nagua Pardo, este logro es enteramente tuyo.

Eres la persona más importante de mi vida, mi fortaleza y mi refugio. Has sido madre y padre a la vez, sostén en los momentos difíciles y alegría en los buenos. Cada amanecer en el que te levantaste antes que nadie, cada sacrificio silencioso que hiciste para que no me faltara nada, cada palabra de aliento cuando sentía que no podía más, está reflejado en cada página de este proyecto.

Gracias por enseñarme con tu ejemplo el valor de la constancia, la honestidad y el trabajo bien hecho. Por creer en mí incluso cuando yo dudaba, por darme la libertad de elegir mi camino y por estar siempre detrás, sosteniéndome sin que me diera cuenta.

A mi padre, que en paz descanse. Aunque la vida no me permitió tenerte presente en este momento, tu recuerdo me ha acompañado en cada paso de esta carrera. Sé que desde donde estés, este logro también te alcanza. Cada esfuerzo lleva una parte de ti, y este título es también una forma de honrar tu memoria.

Si hoy puedo cerrar esta etapa con la frente en alto, es porque ambos me enseñaron, cada uno a su manera, que rendirse no era una opción.

A mi compañero Erick, por la confianza, la paciencia y por todo lo que construimos juntos en este proyecto.

Justyn Alejandro Alvarez Nagua

Dedicatoria

Dedico este logro, en primer lugar, a mi abuelita Iris Zambrano, quien siempre me ha apoyado en todas las etapas y decisiones que he tomado. Cada meta que logre cumplir en mi vida serán siempre dedicadas a ti, porque si no me hubieras formado con tu carácter no sería capaz de lograr todo lo que he hecho. Gracias por todo

A mi madre, Noralma Zambrano, te agradeceré toda mi vida por siempre apoyarme en todos los momentos, buenos y malos jamás me has dejado que me detenga, siempre me diste la inspiración de ser alguien de bien en la vida y lograr todo lo que he te comentado.

A mi padrino, Franklin Albán, quien ha sido un pilar importante en mi vida, desempeñando un papel fundamental en mi etapa académica, gran ejemplo a seguir, lograr todo lo que hemos platicado, gracias por todos los consejos de bien que me has dado en las muchas ocasiones que hemos hablado sobre mi futuro.

A mi gran amiga, Tatiana Aponte, por acompañarme en este proceso, por su apoyo incondicional, sus palabras de ánimo, gracias por siempre estar dando fuerzas para no rendirme y por las muchas veces que me regañaste para ser alguien de bien.

A cada uno de ustedes, gracias por ser parte esencial de este logro y los muchos más que se vienen, por su amor, confianza y apoyo. Este proyecto no solo representa mi esfuerzo, sino también el de todos quienes han estado presentes siempre, dándome a entender que no es buena opción rendirme y cumplir todo lo que me propongo.

Erick Josue Murillo Zambrano

Agradecimiento

Al culminar esta importante etapa de nuestra formación profesional, queremos expresar nuestro más sincero agradecimiento a todas las personas e instituciones que hicieron posible la realización de este proyecto.

En primer lugar, agradecemos a Dios por habernos dado la fortaleza, la salud y la sabiduría necesarias para llegar hasta este punto, y por permitirnos cumplir una meta que durante años representó un sueño compartido.

Mi reconocimiento al Instituto Superior Tecnológico Sudamericano por recibirnos en sus instalaciones y guiarnos durante toda nuestra preparación profesional. El tiempo compartido en sus aulas y laboratorios fue clave para formarnos como los técnicos en ciberseguridad que somos hoy en día.

A los profesores de la carrera de Ciberseguridad, les agradecemos profundamente su dedicación, paciencia y el valor de compartir su experiencia real con nosotros. Gracias por empujarnos a mejorar en cada clase, por sembrar la curiosidad de investigar de forma autónoma y por enseñarnos que un buen profesional actúa siempre con ética y valores.

De manera especial, agradecemos al director de este proyecto de investigación, por su guía constante, sus observaciones acertadas y su acompañamiento durante todo el proceso. Su orientación profesional fue determinante para llevar este trabajo a buen término y alcanzar los objetivos planteados.

A nuestras familias, por el apoyo incondicional brindado durante toda la carrera. Por las palabras de aliento en los momentos difíciles, por la paciencia frente a las largas jornadas de estudio y por creer en nosotros en cada paso del camino.

A nuestros amigos y personas cercanas quienes, con su compañía, su escucha y sus palabras de motivación hicieron más llevadero este proceso. Su apoyo silencioso pero constante fue una pieza clave para no decaer.

Y de manera particular, agradecemos a las personas de la ciudad de Machala que participaron en la encuesta aplicada como parte de esta investigación, entre ellas ciudadanos del área y profesionales con conocimiento en el área de tecnología e informática. Sin su disposición y su tiempo, este trabajo no habría podido sustentarse en datos reales del entorno local.

A todos quienes de una u otra forma aportaron al desarrollo de este proyecto, ya sea con sus conocimientos, su tiempo o simplemente con una palabra de aliento, nuestra gratitud sincera y permanente.

Con agradecimientos 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; el Ing. Linder Fernando Bravo Pardo, en calidad de director del proyecto de investigación de fin de carrera; y, Justyn Alejandro Alvarez Nagua y Erick Josue Murillo Zambrano, en calidad de autores del proyecto de investigación de fin de carrera; mayores de edad emiten la presente acta de cesión de derechos

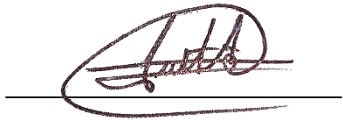
SEGUNDA. - Justyn Alejandro Alvarez Nagua y Erick Josue Murillo Zambrano, realizó la Investigación titulada “Consultoría digital para protección de datos y seguridad web, implementada por una plataforma tecnológica de gestión de servicios en la ciudad de Machala, en el año 2026.”; para optar por el título de Tecnólogo en Desarrollo de Software, en el Instituto Superior Tecnológico Sudamericano de Machala, bajo la dirección del Ing. Linder Fernando Bravo Pardo.

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 comparecientes Ing. Linder Fernando Bravo Pardo, en calidad de Director del proyecto de investigación de fin de carrera y Justyn Alejandro Alvarez Nagua y Erick Josue Murillo Zambrano 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 “Consultoría digital para protección de datos y seguridad web, implementada por una plataforma tecnológica de gestión de servicios en la ciudad de Machala, en el año 2026.” a favor del Instituto Superior Tecnológico Sudamericano de Machala; y, conceden

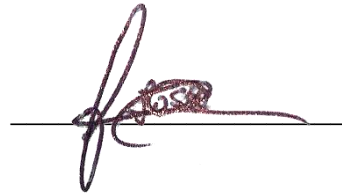
autorización para que el Instituto pueda utilizar esta investigación en su beneficio y/o de la comunidad, sin reserva alguna.

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.



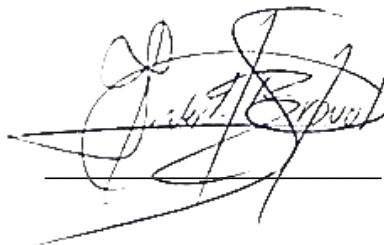
Justyn Alejandro Alvarez Nagua

C.I.0706007747



Erick Josue Murillo Zambrano

C.I. 0750240467



Ing. Linder Fernando Bravo Pardo, Mgs

C.I.1104635089

Declaración juramentada

Machala, Junio 2026

Nombres: Justyn Alejandro

Apellidos: Alvarez Nagua

Cédula de Identidad: 0706007747

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:

Consultoría digital para protección de datos y seguridad web, implementada por una plataforma tecnológica de gestión de servicios en la ciudad de Machala, en el año 2026.

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 encontraron 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 Superior Tecnológico Sudamericano de la ciudad de Machala.

A handwritten signature in dark ink, featuring a large, stylized initial 'J' followed by the name 'Justyn'. The signature is written over a horizontal line.

Justyn Alejandro Alvarez Nagua

C.I.0706007747

Declaración juramentada

Machala, Junio 2026

Nombres: Erick Josue

Apellidos: Murillo Zambrano

Cédula de identidad: 0706790417

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:

Consultoría digital para protección de datos y seguridad web, implementada por una plataforma tecnológica de gestión de servicios en la ciudad de Machala, en el año 2026.

Declaro bajo juramento que:

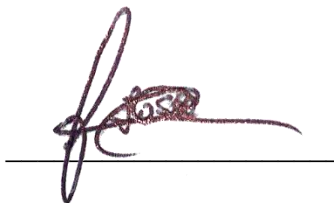
6. Soy autor del trabajo intelectual y de investigación del proyecto de fin de carrera.
7. El trabajo de investigación de fin de carrera no ha sido plagiado ni total ni parcialmente, para la cual se han respetado las normas internacionales de citas y referencias para las fuentes consultadas.
8. El trabajo 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 encontraron 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 Superior Tecnológico Sudamericano de la ciudad de Machala.



Erick Josue Murillo Zambrano

C.I. 0750240467

Índice

Contenido

Certificación del director del Proyecto de Inv. Fin de Carrera.....	2
Autoría.....	3
Dedicatoria.....	4
Dedicatoria.....	5
Agradecimiento	6
Acta de cesión de derechos.....	8
Declaración juramentada	10
Declaración juramentada	12
Índice	14
RESUMEN	23
ABSTRACT	25
1 Planteamiento del Problema	27
2 Determinación del Tema	29
3 Línea y Sublíneas de investigación	30
3.1 Línea de investigación.....	30
3.1.1 Sublíneas de investigación.....	30
3.2 Objetivo de Desarrollo Sostenible	30
3.3 Programa de Investigación	30
4 Justificación.....	32
5 Objetivos.....	34

5.1 Objetivo General.....	34
5.2 Objetivos Específicos	34
6 Marco teórico.....	35
6.1 Marco Contextual	35
6.2 Marco Conceptual.....	36
6.2.1 Introducción Teórica.....	36
6.2.2 Antecedentes Conceptuales y Estudios Previos	36
6.2.3 Conceptos Fundamentales	37
6.2.4 Teorías, Modelos y Estándares Aplicados.....	38
6.2.5 Integración Conceptual.....	39
7 Metodología.....	40
7.1 Diseño Metodológico	40
7.1.1 Herramientas De Aplicación	40
7.1.2 Herramientas Generales.....	41
7.2 Técnicas de investigación.....	41
7.2.1 Diseño Convergente	41
7.3 Determinación del universo y de la muestra	42
7.4 Diseño de la herramienta	42
7.5 Aplicación de herramientas de investigación	43
7.6 Análisis de Resultados.....	43
7.6.1 Análisis de Resultados de la Encuesta.....	43

I. Digitalización y Seguridad Actual	43
Pregunta 1: ¿Su negocio o actividad utiliza plataformas digitales?	43
Pregunta 2: ¿Qué medidas de seguridad aplica actualmente en sus sistemas digitales?	45
Pregunta 3: ¿Ha sufrido incidentes de seguridad digital en los últimos años?	46
II. Conocimiento de la Normativa	47
Pregunta 4: ¿Conoce la Ley Orgánica de Protección de Datos Personales vigente en Ecuador?	47
Pregunta 5: ¿Su empresa aplica protocolos para cumplir con la LOPDP?	48
III. Necesidad de Consultoría Digital	50
Pregunta 6: ¿Las empresas de Machala están preparadas para proteger sus datos digitales?	50
Pregunta 7: ¿Qué servicios considera más necesarios en una plataforma de consultoría digital?	51
Pregunta 8: ¿Cuánto estaría dispuesto a invertir mensualmente en consultoría digital?	52
IV. Opinión Final.....	53
Pregunta 9: ¿Cree que una plataforma SaaS de consultoría digital contribuiría al desarrollo de Machala?	53
Pregunta 10: ¿Estaría dispuesto a participar en un programa piloto de consultoría digital local?	55

7.6.2 Análisis de Mercado	56
8 Propuesta de Acción	57
8.1 Fundamentación de la Solución.....	57
Definición del Producto/Servicio	57
8.3 Desarrollo del Proceso de Creación.....	58
8.3.1 Metodología de desarrollo: Extreme Programming (XP).....	58
8.3.2 Stack tecnológico.....	58
8.3.3 Arquitectura multi-tenant	59
8.3.4 Módulos del motor de análisis.....	60
8.3.5 Fases de desarrollo.....	60
8.3.6 Sistema de roles	61
8.4 Planes de Servicio.....	62
8.5 Flujo Operativo de la Consultoría	63
8.6 Recursos y Requerimientos	63
9 Modelo de Emprendimiento	65
9.1 Modelo CANVAS	65
9.2 Descripción Empresarial.....	67
9.3 Flujo Financiero Esperado.....	68
9.3.1 Presupuesto de Inversión Inicial.....	69
9.3.2 Flujo de Dinero Proyectado.....	69
9.3.3 Cálculo del VAN y la TIR.....	70

10 Prototipo de Producto o Servicio.....	72
10.1 Identidad Corporativa	72
10.2 Descripción del Producto / Servicio	72
10.3 Canal de Promoción.....	73
10.4 Validación.....	74
10.4.1 Validación Técnica	74
10.4.2 Validación de Mercado.....	75
11 Conclusiones.....	76
12 Recomendaciones	77
13 Bibliografía.....	78
Anexo 1. Certificado de Aprobación.....	82
Anexo 2. Certificado de aprobación de la entidad para la ejecución del proyecto	83
Anexo 3. Acta de Socialización de la propuesta de acción	84
Anexo 4. Certificado de Abstract	85
Anexo 5: Presupuesto del Proyecto	85
A.1 Recursos del proyecto.....	86
A.2 Presupuesto general del proyecto	88
Anexo 6. Cronograma de Actividades.....	89
Anexo 8. Encuesta validada.....	96
Anexo 9. Encuesta de satisfacción realizada de forma virtual	100
Anexos 10. Base de datos	102

Anexos 11. Evidencia fotográfica sobre la realización de encuestas	104
Anexo 12. Evidencias de desarrollo de la plataforma	105
Anexos 13. Evidencia del funcionamiento de la plataforma	106
Anexo 14. Documentos de Respaldo.....	108

Índice De Tablas

TABLA 1 RESULTADOS PREGUNTA 1	43
TABLA 2 RESULTADOS PREGUNTA 2	45
TABLA 3 RESULTADOS PREGUNTA 3	46
TABLA 4 RESULTADOS PREGUNTA 4	47
TABLA 5 RESULTADOS PREGUNTA 5	48
TABLA 6 RESULTADOS PREGUNTA 6	50
TABLA 7 RESULTADOS PREGUNTA 7	51
TABLA 8 RESULTADOS PREGUNTA 8	52
TABLA 9 RESULTADOS PREGUNTA 9	53
TABLA 10 RESULTADOS PREGUNTA 10	55
TABLA 11 SERVICIOS DE ARXSYS Y DEMANDA IDENTIFICADA.....	57
TABLA 12 STACK TECNOLÓGICO DE ARXSYS.....	58
TABLA 13 MÓDULOS DEL MOTOR DE ANÁLISIS DE ARXSYS	60
TABLA 14 SISTEMA DE ROLES DE ARXSYS	61
TABLA 15 PLANES DE SERVICIO ARXSYS	62
TABLA 16 REQUERIMIENTOS TÉCNICOS PARA IMPLEMENTACIÓN EN PRODUCCIÓN.....	63
TABLA 17 MODELO DE NEGOCIO CANVAS — ARXSYS.....	65
TABLA 18 DESCRIPCIÓN EMPRESARIAL — ARXSYS	67
TABLA 19 PRESUPUESTO DE INVERSIÓN INICIAL — ARXSYS	69
TABLA 20 FLUJO DE DINERO PROYECTADO — ARXSYS	70
TABLA 21 INDICADORES FINANCIEROS — ARXSYS.....	70
TABLA 22 ELEMENTOS DE IDENTIDAD CORPORATIVA — ARXSYS	72
TABLA 23 PORTAFOLIO DE SERVICIOS — ARXSYS.....	73
TABLA 24 ESTRATEGIA DE PROMOCIÓN — ARXSYS	74

TABLA 25 PRESUPUESTO DE RECURSOS DEL PROYECTO86

TABLA 26 PRESUPUESTO GENERALES DEL PROYECTO88

TABLA 27 CRONOGRAMA DE ACTIVIDADES.....89

Índice De Figuras

FIGURA 1 GRÁFICO PREGUNTA 1 – USO DE PLATAFORMAS DIGITALES	44
FIGURA 2 GRÁFICO PREGUNTA 2 – MEDIDAS DE SEGURIDAD APLICADAS.....	45
FIGURA 3 GRÁFICO PREGUNTA 3 – INCIDENTES DE SEGURIDAD DIGITAL	47
FIGURA 4 GRÁFICO PREGUNTA 4 – CONOCIMIENTO DE LA LOPDP	48
FIGURA 5 GRÁFICO PREGUNTA 5 – APLICACIÓN DE PROTOCOLOS DE CUMPLIMIENTO	49
FIGURA 6 GRÁFICO PREGUNTA 6 – PERCEPCIÓN DE PREPARACIÓN EMPRESARIAL	50
FIGURA 7 GRÁFICO PREGUNTA 7 – SERVICIOS NECESARIOS EN CONSULTORÍA DIGITAL.....	52
FIGURA 8 GRÁFICO PREGUNTA 8 – DISPOSICIÓN DE INVERSIÓN MENSUAL	53
FIGURA 9 GRÁFICO PREGUNTA 9 – CONTRIBUCIÓN AL DESARROLLO DE MACHALA.....	54
FIGURA 10 GRÁFICO PREGUNTA 10 – DISPOSICIÓN A PARTICIPAR EN PROGRAMA PILOTO.....	55
FIGURA 11 LOGO DE ARXSYS.....	68
FIGURA 13 ENCUESTA VALIDADA APLICADA A PERSONAS CON CONOCIMIENTO EN EL ÁREA EN MACHALA	96
FIGURA 14 ENCUESTA DE SATISFACCIÓN DE FORMA VIRTUAL	100
FIGURA 15 TABLA DE PREGUNTAS	102
FIGURA 16 TABULACIÓN DE LAS PREGUNTAS	103
FIGURA 17 EVIDENCIA FOTOGRÁFICA DE FORMA VIRTUAL Y PRESENCIAL	104
FIGURA 18 EVIDENCIA DEL DESARROLLO DE LA PLATAFORMA	105
FIGURA 19 EVIDENCIA DE LA PLATAFORMA DESARROLLADA	105
FIGURA 20 EVIDENCIA DE FUNCIONAMIENTO DE LA PLATAFORMA	106
FIGURA 21 EVIDENCIA DE FUNCIONAMIENTO DE LA PLATAFORMA	107
FIGURA 22 EVIDENCIA DE FUNCIONAMIENTO DE LA PLATAFORMA	107
FIGURA 24 HOJA VALORADA DEL SR. ALVAREZ JUSTYN	109

RESUMEN

Hoy en día, la digitalización dejó de ser una alternativa para volverse una exigencia del mundo empresarial, pero trajo consigo un problema que pocas empresas atienden como se debe: la ciberseguridad. En Machala, las PYMES se han volcado rápidamente hacia lo digital gracias a la facturación electrónica y las ventas en línea, pero sin tomar medidas reales de protección de datos. A nivel nacional, incidentes como el ataque a la CNT y la filtración del caso Novaestrat dejaron en evidencia la debilidad de la infraestructura digital del país, lo que derivó en la creación de la Ley Orgánica de Protección de Datos Personales. Aun así, la mayoría de los negocios locales no tiene ni los conocimientos ni las herramientas para cumplirla. Frente a eso, este proyecto propone crear una consultoría digital gestionada a través de una plataforma tecnológica, que ofrezca asesoría en protección de datos y seguridad web a organizaciones y usuarios de Machala. Para lograrlo se definieron cuatro objetivos específicos: construir el marco teórico sobre gestión de servicios y protección de datos, diagnosticar la situación actual de seguridad en las empresas de la ciudad, diseñar la estructura operativa de la consultoría junto con su plataforma, y validar la propuesta con expertos y pruebas reales. La investigación combinó métodos cualitativos y cuantitativos, con encuestas a 200 gerentes y entrevistas a especialistas en ciberseguridad. Para el desarrollo de la plataforma se aplicó la metodología Extreme Programming (XP), que permitió validar cada etapa y definir las funcionalidades del producto. Como resultado se construyó ArxSys, una plataforma de gestión de ciberseguridad bajo un modelo SaaS que permite atender a varios clientes de forma simultánea y segura. Incluye detección de vulnerabilidades en código, revisión de cumplimiento normativo frente a estándares como GDPR, ISO 27001 y PCI DSS, un sistema con siete niveles de acceso diferenciados y una conexión segura mediante autenticación JWT y HMAC-SHA256. Los resultados del estudio de mercado fueron

positivos: el 70,5% de los encuestados se mostró dispuesto a participar en un piloto y el 67,5% confirmó disposición de pago mensual. En conclusión, Machala tiene un nivel considerable de digitalización (77,5%), pero la mayoría de sus empresas solo cuenta con medidas básicas de protección (72,5%) y más de la mitad ha sufrido algún incidente de seguridad (53,0%). ArxSys responde directamente a esa brecha, ofreciendo una alternativa local entre el soporte técnico básico y las costosas soluciones internacionales, y poniendo herramientas de ciberseguridad profesional al alcance de las PYMES, en línea con la Ley Orgánica de Protección de Datos Personales.

ABSTRACT

Digitalization has evolved from a strategic option into a business necessity. However, this transformation has also increased exposure to cybersecurity risks, a challenge that many organizations fail to address adequately. In Machala, small and medium-sized enterprises (SMEs) have rapidly adopted digital technologies through electronic invoicing and ecommerce platforms, often without implementing effective data protection measures. At the national level, incidents such as the cyberattack on CNT and the Novaestrat data breach exposed weaknesses in Ecuador's digital infrastructure and contributed to the enactment of the Organic Law on Personal Data Protection. Despite this regulatory framework, many local businesses still lack the knowledge and tools required to achieve compliance.

This study proposes the development of a digital consulting service managed through a technological platform that provides data protection and web security advisory services to organizations and users in Machala. Four specific objectives were established: to develop the theoretical framework on service management and data protection, assess the current cybersecurity conditions of local businesses, design the operational structure of the consulting service and its platform, and validate the proposal through expert evaluation and practical testing. A mixed-methods approach was employed, including surveys of 200 business managers and interviews with cybersecurity specialists. The platform was developed using the Extreme Programming (XP) methodology.

As a result, ArxSys was developed as a cybersecurity management platform based on a Software as a Service (SaaS) model. The platform incorporates source code vulnerability detection, compliance assessment based on GDPR, ISO

27001, and PCI DSS standards, a seven-level access control system, and secure authentication through JWT and HMACSHA256. Market analysis showed positive results, with 70.5% of respondents willing to participate in a pilot program and 67.5% expressing willingness to pay a monthly subscription fee.

The findings indicate that Machala has achieved a considerable level of digitalization (77.5%); however, most businesses rely on basic security measures (72.5%), and 53.0% have experienced at least one cybersecurity incident. ArxSys addresses this gap by providing a local alternative between basic technical support and costly international solutions, making professional cybersecurity tools more accessible to SMEs while supporting compliance with the Organic Law on Personal Data Protection.

1 Planteamiento del Problema

En la actualidad, la digitalización ha dejado de ser una opción para convertirse en una necesidad de supervivencia empresarial. Ese avance digital trajo consigo una vulnerabilidad que pocos anticiparon. El ciberataque a MGM Resorts en 2023 lo dejó en evidencia: si una empresa con presupuesto millonario puede quedar paralizada por un fallo informático, los negocios más chicos tienen todavía más que perder (Telefónica Ecuador, 2024; Saphirtek, 2024). Lo que persiguen los atacantes hoy no es romper máquinas, sino robar información, y eso convierte a la seguridad web en un factor que ningún negocio puede ignorar si quiere seguir operando.

En Ecuador el problema dejó de ser teórico hace años. El hackeo a la CNT le impidió a la empresa facturar y cobrar por días, y el caso Novaestrat expuso datos de millones de ciudadanos ecuatorianos al mundo. Esos incidentes empujaron al Estado a crear la Ley de Protección de Datos Personales, que hoy obliga a las empresas a proteger la información de sus clientes bajo amenaza de multas. Pero tener la ley no resuelve el fondo del asunto: la gran mayoría de negocios no cuenta ni con los conocimientos ni con las herramientas para cumplirla, y sigue operando expuesta sin saberlo.

Esta problemática se manifiesta con claridad en el contexto de Machala. Aunque la ciudad se consolida como un nodo económico dinámico gracias al comercio, las exportaciones y el sector salud, la madurez en la gestión de sus tecnologías de la información aún es limitada. En el entorno empresarial local, el concepto de "soporte informático" se restringe habitualmente al mantenimiento correctivo del hardware o a la instalación de software antivirus convencional (Tecnología Estratégica, s.f.; E-Open Solutions, s.f.; Tu Consultor TI, s.f.). Esta visión tradicional posterga la implementación de auditorías y la administración de riesgos digitales, lo que desprotege a las aplicaciones web y bases de datos, que constituyen los activos críticos de cualquier organización. A

diferencia de la infraestructura de servicios presente en Quito o Guayaquil, en Machala la oferta de seguridad preventiva es escasa; como consecuencia, la mayoría de los empresarios gestionan sus operaciones sin un diagnóstico real sobre la vulnerabilidad de sus sistemas frente a amenazas cibernéticas.

Las implicaciones de este escenario representan un riesgo crítico para el sector empresarial. Ante un incidente de secuestro de datos (ransomware), cualquier entidad comercial o centro de salud local sufriría un impacto financiero inmediato por el cese de sus operaciones. Sin embargo, el perjuicio real se extiende hacia la pérdida de credibilidad en el mercado y la aparición de contingencias legales severas que ponen en peligro la viabilidad económica de la organización. En este contexto, se evidencia un vacío sustancial de soluciones tecnológicas alineadas con el entorno de las PYMES locales, dado que el software especializado demanda presupuestos elevados y conocimientos avanzados, mientras que el soporte convencional disponible en la zona es insuficiente. Ante esta problemática, surge la necesidad de implementar un modelo de consultoría digital automatizado mediante una plataforma propia y eficiente, diseñada para dotar a las empresas de Machala de mecanismos de defensa preventivos que garanticen la integridad de sus datos de forma autónoma.

2 Determinación del Tema

Consultoría digital para protección de datos y seguridad web, implementada por una plataforma tecnológica de gestión de servicios en la ciudad de Machala, en el año 2026.

3 Línea y Sublíneas 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 Sublíneas 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: La presente investigación se alinea con las directrices de la meta 9.5, orientada al fortalecimiento de la investigación científica y la mejora de las capacidades tecnológicas de los sectores industriales. A través del diseño e implementación de la plataforma SaaS, este estudio provee una infraestructura digital que moderniza los esquemas de gestión de seguridad informática en el entorno corporativo. Al robustecer la protección de las aplicaciones e información web, se promueve el desarrollo de un tejido empresarial más resiliente y competitivo, preparado para mitigar riesgos dentro de la economía digital actual.

3.3 Programa de Investigación

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

Justificación: El robustecimiento de la seguridad informática en las pequeñas y medianas empresas de Machala constituye el eje central de la vinculación de este estudio con el programa, objetivo que se alcanza mediante una plataforma tecnológica accesible y de administración local. Desde la perspectiva del desarrollo económico, la propuesta actúa como un escudo para los activos digitales, lo que previene impactos financieros por ciberataques y asegura la continuidad de las operaciones de los negocios. Asimismo, la

investigación incide positivamente en el desarrollo humano al tutelar la privacidad de los datos comerciales y personales de los usuarios, construyendo un entorno de mayor confianza. De este modo, se logra articular de forma directa la innovación en software con la sostenibilidad y el crecimiento socioeconómico regional.

4 Justificación

El fundamento de esta investigación se enmarca en la línea de "Desarrollo tecnológico e innovación en procesos de sistematización organizacional", específicamente en la sublínea de "Desafíos de la Industria 4.0". Esta elección responde a una realidad concreta: hoy en día, gestionar la ciberseguridad de forma manual o solo cuando ocurre un problema ya no es viable. En un entorno donde todo está interconectado, pretender proteger los activos digitales de una empresa sin apoyo tecnológico es, desde el inicio, una tarea destinada al fracaso. Por eso, este proyecto plantea llevar la protección digital al nivel que exige la Industria 4.0, es decir, automatizar y sistematizar la defensa de datos a través de una plataforma que convierta ese proceso en algo medible, ordenado y eficiente.

Desde el punto de vista académico, este trabajo marca el cierre de la formación profesional en el Instituto Superior Tecnológico Sudamericano. Sin embargo, su importancia va más allá de cumplir un requisito. Es la oportunidad de poner en práctica todo lo aprendido durante la carrera, desde escribir código seguro y trabajar con arquitecturas en la nube hasta entender el marco legal que regula el manejo de datos, y convertirlo en algo concreto y funcional. En ese sentido, este proyecto demuestra la capacidad de detectar un problema real como la vulnerabilidad informática en las empresas y construir una solución que abarca tanto el desarrollo técnico como la estrategia de implementación.

En cuanto a la justificación tecnológica y profesional, el proyecto nace de un vacío claro en el mercado de Machala. Las PYMES de la ciudad se encuentran atrapadas entre dos opciones poco favorables: pagar por software internacional costoso que muchas veces no se adapta a su escala, o conformarse con un soporte técnico que solo atiende el hardware y deja expuesta su presencia en línea. Frente a esto, la propuesta consiste en una Consultoría Digital Gestionada operada a través de una plataforma SaaS propia. Con esto

no solo se eleva la calidad del servicio TI en la región, sino que se pone al alcance de empresas pequeñas herramientas de auditoría y gestión de riesgos que antes solo podían costear las grandes corporaciones.

Por último, el impacto social y económico del proyecto es real y directo. En una economía que depende cada vez más de lo digital, un ciberataque puede destruir una empresa local en cuestión de horas, con todo lo que eso implica para los empleos y la actividad económica de la ciudad. Proteger la infraestructura digital de las organizaciones machaleñas es, en la práctica, contribuir a su estabilidad y crecimiento. A esto se suma la responsabilidad de custodiar información sensible de personas, como datos de salud o financieros, lo que convierte a este proyecto en una apuesta concreta por el derecho a la privacidad y por un entorno digital más seguro para la comunidad.

5 Objetivos

5.1 Objetivo General

El objetivo general de este proyecto es desarrollar una consultoría digital apoyada en una plataforma tecnológica propia, orientada a brindar acompañamiento en protección de datos y seguridad web. Para lograrlo, se trabajó en cuatro etapas: la construcción del marco teórico, la aplicación de una metodología de investigación mixta, el diseño de la propuesta de acción y su correspondiente validación, todo con el propósito de fortalecer las prácticas de seguridad digital tanto en organizaciones como en usuarios individuales.

5.2 Objetivos Específicos

Fundamentar las bases teóricas sobre gestión de servicios y protección de datos, mediante el análisis de información especializada que brinde un soporte sólido y confiable al modelo de consultoría propuesto.

Diagnosticar la situación actual de la seguridad informática en las empresas de Machala, identificando sus vulnerabilidades y necesidades reales para asegurar que la solución propuesta resuelva problemas verdaderos del entorno local.

Diseñar la estructura operativa de la consultoría y su plataforma tecnológica, seleccionando las herramientas digitales adecuadas para construir un servicio que sea funcional, intuitivo y útil para los usuarios.

Validar la viabilidad de la propuesta y el funcionamiento de la plataforma, sometiendo el proyecto a la evaluación de expertos y pruebas prácticas para garantizar que es efectivo y está listo para implementarse.

6 Marco teórico

6.1 Marco Contextual

Contexto Geográfico y Económico, el presente proyecto se desarrolla en la ciudad de Machala, provincia de El Oro. Esta localidad se caracteriza por ser uno de los polos comerciales más importantes del sur del Ecuador, con una alta actividad económica vinculada a la exportación bananera, camaronera y el comercio minorista. En este entorno, las pequeñas y medianas empresas (PYMES) han comenzado una transición acelerada hacia la digitalización, impulsada por la obligatoriedad de la facturación electrónica y el auge del comercio en línea. Sin embargo, este crecimiento digital no ha ido acompañado de una cultura de ciberseguridad, dejando a un gran número de negocios expuestos a riesgos sin contar con infraestructura de protección adecuada.

Contexto Institucional y Sectorial La investigación se enmarca en el sector de servicios tecnológicos y consultoría empresarial de Machala la oferta de servicios de seguridad informática es bastante limitada. La mayoría de los proveedores locales trabaja bajo un esquema reactivo, es decir, actúan cuando ya ocurrió el problema, y hay muy poco desarrollo en cuanto a auditorías preventivas o gestión de riesgos en entornos web. Las empresas de la zona, que en general no cuentan con un área de TI propia por razones de presupuesto, recurren a servicios externos que tampoco disponen de herramientas centralizadas, lo que hace difícil llevar un control real sobre sus vulnerabilidades.

Desde el punto de vista tecnológico y legal, las empresas de Machala utilizan con frecuencia aplicaciones web para sus ventas y procesos administrativos, muchas veces alojadas en servidores compartidos con configuraciones de seguridad que vienen por defecto y nunca se ajustan. A esto se añade que la Ley Orgánica de Protección de Datos Personales ya está vigente en Ecuador, lo que obliga a estas organizaciones a garantizar la

privacidad de la información de sus clientes. Sin embargo, el desconocimiento sobre cómo cumplir con esa normativa en la práctica es generalizado. Todo esto evidencia la necesidad de una plataforma que no solo detecte fallos de seguridad, sino que también guíe a las empresas en el cumplimiento legal y técnico de manera clara y accesible.

6.2 Marco Conceptual

6.2.1 Introducción Teórica

Este proyecto parte de una idea central: la seguridad informática no es algo que se instala una vez y listo, sino un proceso que requiere atención continua. Bajo esa lógica, se adopta un enfoque de seguridad como servicio, donde la consultoría no se limita a una revisión anual, sino que se convierte en un acompañamiento permanente a través de una plataforma en la nube. Este modelo permite que empresas sin infraestructura propia puedan acceder a herramientas de auditoría avanzada e integrar la protección de datos en su operación diaria, no como un gasto puntual, sino como parte natural del negocio.

6.2.2 Antecedentes Conceptuales y Estudios Previos

Hace algunos años, proteger una empresa significaba tener el antivirus correcto instalado en las computadoras de la oficina. Hoy el panorama es completamente distinto. La mayoría de las PYMES en Ecuador ya opera en la nube, factura de forma electrónica, vende por internet y gestiona su correo en línea, pero su manera de protegerse no ha cambiado al mismo ritmo. Esa brecha entre cómo trabajan y cómo se defienden es, precisamente, el problema que este proyecto busca atender. Los estudios recientes muestran que los atacantes ya no buscan romper el servidor físico, sino que aprovechan errores en las páginas web o aplicaciones descuidadas. Investigaciones en ciberseguridad confirman que las vulnerabilidades más comunes hoy en día están relacionadas con fallos de programación y configuraciones inseguras en aplicaciones web, más que con el hardware (OWASP, 2021; Symantec, 2022). Además, con la Ley de Protección de Datos

vigente en el país, las empresas tienen una presión legal fuerte. El problema que hemos visto en investigaciones previas es que los negocios saben que deben cumplir la ley, pero no tienen herramientas sencillas que les digan cómo hacerlo. Nuestra propuesta nace justamente para llenar ese vacío: darles una herramienta que traduzca esas obligaciones legales y técnicas en tareas simples, asegurando el cumplimiento efectivo de los derechos y principios establecidos en la Ley Orgánica de Protección de Datos Personales (Asamblea Nacional del Ecuador, 2021).

6.2.3 Conceptos Fundamentales

Para que se entienda la propuesta, aclaramos los términos clave que manejamos:

- **Consultoría Digital Gestionada:** No es solo dar consejos. Es usar nuestra plataforma para revisar el estado de seguridad del cliente, encontrar fallas y decirle cómo arreglarlas. Este concepto guarda relación directa con los servicios de ciberseguridad gestionados, donde la protección digital se delega a especialistas externos que se encargan de mantener un monitoreo constante y responder ante cualquier incidente de forma oportuna (Armour Cyber, 2025; SentinelOne, 2025; Hit Ocean, 2026).
- **Plataforma tecnológica:** Es el corazón técnico del proyecto. En lugar de instalar programas en cada computador del cliente, les damos acceso a nuestro sistema vía internet. Esto hace que el servicio sea más barato y fácil de usar. Este modelo corresponde al *Software como Servicio (SaaS)*, donde las aplicaciones se alojan en la nube y se acceden mediante navegador, reduciendo costos y simplificando la gestión (AWS, s.f.; IBM, s.f.; Red Hat, 2023)
- **Gestión de Vulnerabilidades:** Es el trabajo de "buscar grietas". Consiste en escanear los sistemas para encontrar puntos débiles antes de que una persona mal intencionada los aproveche. Según OWASP, la gestión de vulnerabilidades es un proceso

continuo que permite identificar, evaluar y mitigar riesgos en aplicaciones y sistemas (OWASP Developer Guide, s.f.; Bernal Ontiveros et al., 2025; Arsys, s.f.).

- **Protección de Datos:** Más allá de la tecnología, se trata de asegurar que la información privada no se filtre ni se pierda, cumpliendo con lo que exige la ley. En Ecuador, la *Ley Orgánica de Protección de Datos Personales* establece principios y obligaciones para garantizar la privacidad y seguridad de los datos personales (Asamblea Nacional del Ecuador, 2021; Orizontel, 2025; Deltech Audit, 2025).

6.2.4 Teorías, Modelos y Estándares Aplicados

Para que el proyecto sea confiable y útil, se apoya en modelos y guías reconocidas a nivel internacional. Estos referentes ayudan a que la plataforma siga buenas prácticas y mantenga un nivel adecuado de seguridad y calidad.

OWASP Top 10: considerado el estándar de referencia mundial para la seguridad en aplicaciones web, ya que identifica los diez riesgos más críticos que afectan a los sistemas en línea. La plataforma toma como referencia este marco para orientar sus procesos de auditoría y reducir la presencia de vulnerabilidades de alto impacto (OWASP Foundation, 2021).

Modelo de Responsabilidad Compartida: define que el proveedor de nube, en este caso AWS, se hace cargo de la seguridad de la infraestructura física, mientras que el cliente asume la responsabilidad de proteger los datos, configuraciones y aplicaciones que opera dentro de ese entorno. Esta división clara de roles contribuye a una gestión de riesgos más sólida y ordenada (Amazon Web Services, 2023).

Metodología Extreme Programming (XP): es un enfoque ágil que prioriza el código limpio, las pruebas frecuentes y la retroalimentación constante durante el desarrollo. En proyectos donde la seguridad es un factor crítico, XP resulta especialmente

adecuado porque ayuda a detectar errores de forma temprana y a mantener altos niveles de calidad en el producto final (Beck, 2004; Abrahamsson et al., 2017).

6.2.5 Integración Conceptual

En términos generales, este proyecto combina elementos de ciberseguridad ofensiva y defensiva con principios de gestión de riesgos. No se trata simplemente de una herramienta para visualizar datos, sino de una plataforma orientada a hacer que la seguridad funcione en la práctica. Para ello, incorpora técnicas de hacking ético bajo estándares como OWASP, con el fin de identificar fallos antes de que puedan ser aprovechados, y los gestiona de manera proactiva para reducir la exposición (OWASP Foundation, 2021; Stallings, 2020). La plataforma funciona como un punto central de coordinación que traduce normativas complejas, como la Ley de Protección de Datos o la ISO 27001, en controles técnicos concretos y aplicables. De esta manera, se demuestra que la ciberseguridad actual no se limita a levantar barreras, sino a gestionar de forma continua y medible la postura de seguridad de una organización, adaptándola a las amenazas reales del entorno digital de Machala.

7 Metodología

7.1 Diseño Metodológico

Esta investigación se desarrolló bajo un enfoque mixto, combinando métodos cualitativos y cuantitativos de manera estructurada. La decisión responde a la necesidad de entender con profundidad la situación actual de la ciberseguridad en las empresas comerciales y de servicios de Machala, considerando tanto los datos concretos como los contextos y experiencias detrás de ellos. Mientras el enfoque cualitativo permitió profundizar en la cultura de prevención y entender por qué los gerentes perciben la normativa de protección de datos como una barrera compleja, el componente cuantitativo validó con métricas objetivas la frecuencia de vulnerabilidades en sus sitios web y la eficacia técnica de la plataforma de gestión propuesta (Hernández Sampieri, 2014).

7.1.1 Herramientas De Aplicación

Las herramientas de aplicación constituyen los instrumentos, medios o recursos técnicos y metodológicos empleados para la recolección, registro, organización y análisis de la información dentro del proceso de investigación. En este proyecto se utilizaron las siguientes:

Entrevista a expertos: instrumento cualitativo que permitió validar técnicamente la propuesta de la plataforma, recogiendo criterios profesionales sobre su funcionalidad y pertinencia.

Encuesta estructurada: se aplicó a personas con conocimiento en el área de tecnología e informática y ciudadanos en general de Machala, con el fin de obtener datos básicos sobre el uso de medidas de seguridad digital, la frecuencia de incidentes y el nivel de conocimiento de la Ley de Protección de Datos.

7.1.2 Herramientas Generales

Para la parte de la investigación el diagnóstico del problema en Machala y la validación de la solución, usaremos herramientas clásicas de recolección de datos.

Para la recolección de información cualitativa, se utilizó la entrevista a expertos como instrumento principal de validación técnica. Esta herramienta permitió presentar el prototipo de la plataforma a ingenieros especialistas en ciberseguridad, con el fin de recoger sus criterios profesionales sobre la funcionalidad del sistema y la pertinencia de los reportes de auditoría; su retroalimentación es vital para detectar posibles fallos lógicos y asegurar que el servicio propuesto cumpla con los estándares de calidad exigidos por la industria antes de su implementación.

Por otra parte, el componente cuantitativo se abordó mediante una encuesta estructurada dirigida a personas con conocimiento en el área de tecnología e informática y ciudadanos en general de Machala, El objetivo de este instrumento es obtener datos estadísticos concretos que dimensionen la problemática local, permitiéndonos medir variables críticas como la frecuencia de incidentes de seguridad, la falta de protocolos de respaldo y el nivel de desconocimiento sobre la Ley de Protección de Datos, cifras que justificarán con evidencia sólida la urgencia de implementar esta consultoría en el mercado local (Axelos. (2019). *ITIL Foundation: ITIL 4 Edition*. TSO).

7.2 Técnicas de investigación

7.2.1 Diseño Convergente

Este diseño permite recoger al mismo tiempo información cualitativa y cuantitativa para construir una imagen más completa del problema. En el desarrollo del proyecto se combinaron encuestas, entrevistas y revisión documental, lo que permitió contrastar resultados y garantizar que la propuesta de consultoría digital esté respaldada tanto por

cifras como por las vivencias y percepciones de quienes forman parte del entorno estudiado.

7.3 Determinación del universo y de la muestra

El universo de estudio estuvo conformado por emprendedores locales, propietarios de microempresas en etapa temprana y trabajadores autónomos de la ciudad de Machala, provincia de El Oro, orientados a los sectores de comercio minorista, servicios generales y tecnología inicial. Con base en los datos oficiales del Registro Estadístico de Empresas elaborado por el Instituto Nacional de Estadística y Censos (INEC, 2024), se identificó que el tejido productivo de la región está compuesto mayoritariamente por microempresas y actividades registradas a nombre de personas naturales. A partir de este marco normativo y estadístico, y en concordancia con los criterios de formalización y categorización de nuevas actividades comerciales contemplados en la Ley Orgánica de Emprendimiento e Innovación (2020), se estimó una población referencial de aproximadamente 1.200 unidades económicas y emprendimientos autónomos con presencia o proyección digital básica en el cantón.

Se aplicó la fórmula estadística para poblaciones finitas con nivel de confianza del 95% ($Z=1,96$), probabilidad de éxito $p=0,5$ y margen de error $e=0,05$, obteniendo una muestra mínima de 200 encuestados. Se utilizó muestreo no probabilístico por conveniencia, seleccionando participantes con acceso a sistemas digitales en sus negocios.

7.4 Diseño de la herramienta

Se diseñó una encuesta estructurada de 10 preguntas cerradas organizada en cuatro secciones: (I) Digitalización y Seguridad Actual, (II) Conocimiento de la Normativa, (III) Necesidad de Consultoría Digital, y (IV) Opinión Final. La encuesta fue validada por criterio de expertos antes de su aplicación y distribuida en formato digital mediante formularios Microsoft Forms.

7.5 Aplicación de herramientas de investigación

La encuesta se aplicó durante el mes de febrero de 2026 a 200 personas con conocimiento en el área de tecnología e informática y ciudadanos en general de Machala, de forma presencial y digital. Paralelamente, se realizó una entrevista semiestructurada a tres expertos en ciberseguridad para validar técnicamente la plataforma ArxSys. Los datos cuantitativos se procesaron en Microsoft Excel y los cualitativos se analizaron mediante categorización de respuestas.

7.6 Análisis de Resultados

7.6.1 Análisis de Resultados de la Encuesta

El presente apartado expone el análisis de los resultados obtenidos mediante la aplicación de la encuesta. La encuesta fue aplicada a 200 personas con conocimiento en el área de tecnología e informática y ciudadanos en general de Machala, con el propósito de diagnosticar el nivel de digitalización, conocimiento normativo y disposición hacia los servicios de consultoría digital. El análisis integra enfoques cuantitativo y cualitativo en concordancia con el diseño convergente adoptado.

I. Digitalización y Seguridad Actual

Pregunta 1: ¿Su negocio o actividad utiliza plataformas digitales?

Tabla 1

Resultados Pregunta 1

Opciones de Respuesta	Frecuencia	Porcentaje
Sí	155	77,5%
No	45	22,5%
TOTAL	200	100%

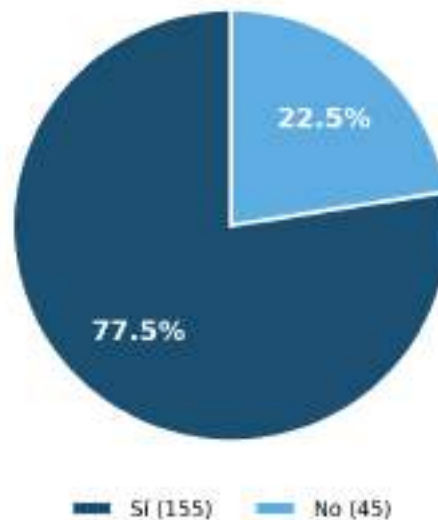
Nota. Elaboración propia (2026). n = 200 encuestados.

Análisis Cuantitativo: De 200 encuestados, 155 (77,5%) respondieron afirmativamente y 45 (22,5%) negativamente. La diferencia de 55 puntos porcentuales evidencia que la mayoría de los negocios ha incorporado herramientas digitales en sus operaciones.

Figura 1

Gráfico Pregunta 1 – Uso de plataformas digitales

P1. ¿Utiliza plataformas digitales?



Nota. Elaboración propia (2026). n = 200 encuestados.

Análisis Cualitativo e Interpretación: El alto porcentaje de empresas que ya utiliza plataformas digitales refleja una transformación acelerada en el tejido empresarial de Machala, impulsada principalmente por la adopción de la facturación electrónica y el crecimiento del comercio en línea. Al mismo tiempo, el segmento que aún no ha dado ese paso representa una oportunidad adicional de mercado para la consultoría. En conjunto, estos datos confirman que existe una demanda real y creciente de servicios especializados en protección de datos a nivel local.

Pregunta 2: ¿Qué medidas de seguridad aplica actualmente en sus sistemas digitales?

Tabla 2

Resultados Pregunta 2

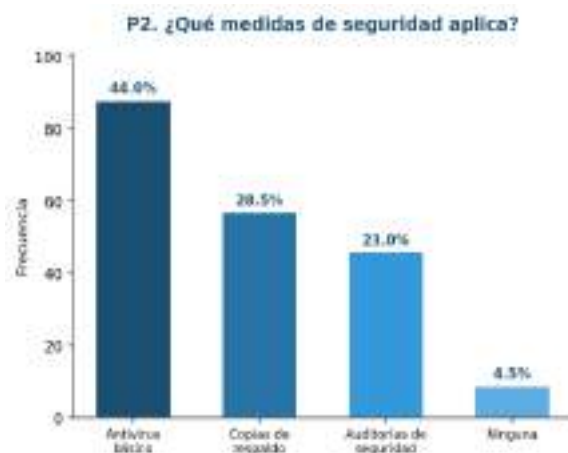
Opciones de Respuesta	Frecuencia	Porcentaje
Antivirus básico	88	44,0%
Copias de respaldo	57	28,5%
Auditorías de seguridad	46	23,0%
Ninguna	9	4,5%
TOTAL	200	100%

Nota. Elaboración propia (2026). n = 200 encuestados.

Análisis Cuantitativo: La opción más seleccionada fue antivirus básico con 88 respuestas (44,0%), seguida de copias de respaldo 57 (28,5%), auditorías de seguridad 46 (23,0%) y ninguna medida 9 (4,5%). El 72,5% aplica únicamente medidas básicas.

Figura 2

Gráfico Pregunta 2 – Medidas de seguridad aplicadas



Nota. Elaboración propia (2026). n = 200 encuestados.

Análisis Cualitativo e Interpretación: El predominio de medidas básicas evidencia que la gran mayoría de empresas carece de protección integral frente a amenazas sofisticadas como phishing, ransomware o inyecciones de código. Solo una minoría accede a auditorías profesionales, lo que confirma la brecha crítica de seguridad que ArxSys busca cubrir.

Pregunta 3: ¿Ha sufrido incidentes de seguridad digital en los últimos años?

Tabla 3

Resultados Pregunta 3

Opciones de Respuesta	Frecuencia	Porcentaje
Sí	106	53,0%
No	94	47,0%
TOTAL	200	100%

Nota. Elaboración propia (2026). n = 200 encuestados.

Análisis Cuantitativo: 106 encuestados (53,0%) reportaron haber sufrido incidentes de seguridad digital, frente a 94 (47,0%) que no. La proporción es casi equitativa, aunque los afectados superan por 6 puntos a quienes no han tenido incidentes.

Figura 3

Gráfico Pregunta 3 – Incidentes de seguridad digital



Nota. Elaboración propia (2026). n = 200 encuestados.

Análisis Cualitativo e Interpretación: Que más de la mitad de los encuestados haya sufrido incidentes resulta alarmante dado que la mayoría aplica solo medidas básicas. Los incidentes más frecuentes incluyeron robo de información, phishing y accesos no autorizados. Esto refuerza la urgencia de asesoramiento especializado y valida la pertinencia de la propuesta.

II. Conocimiento de la Normativa

Pregunta 4: ¿Conoce la Ley Orgánica de Protección de Datos Personales vigente en Ecuador?

Tabla 4

Resultados Pregunta 4

Opciones de Respuesta	Frecuencia	Porcentaje
Sí	130	65,0%
No	70	35,0%
TOTAL	200	100%

Nota. Elaboración propia (2026). n = 200 encuestados.

Análisis Cuantitativo: 130 personas (65,0%) afirmaron conocer la LOPDP mientras que 70 (35,0%) la desconocen, con una diferencia de 30 puntos porcentuales.

Figura 4

Gráfico Pregunta 4 – Conocimiento de la LOPDP



Nota. Elaboración propia (2026). n = 200 encuestados.

Análisis Cualitativo e Interpretación: Conocer la existencia de la ley no implica implementarla técnicamente. Quienes la desconocen representan una exposición legal significativa. Este hallazgo valida la asesoría legal digital como componente central de la plataforma.

Pregunta 5: ¿Su empresa aplica protocolos para cumplir con la LOPDP?

Tabla 5

Resultados Pregunta 5

Opciones de Respuesta	Frecuencia	Porcentaje
Sí	172	86,0%

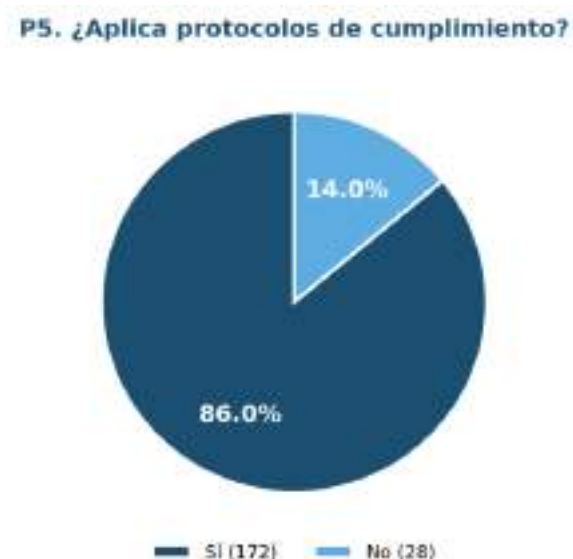
No	28	14,0%
TOTAL	200	100%

Nota. Elaboración propia (2026). n = 200 encuestados.

Análisis Cuantitativo: 172 encuestados (86,0%) declararon aplicar protocolos, frente a 28 (14,0%) que no lo hacen.

Figura 5

Gráfico Pregunta 5 – Aplicación de protocolos de cumplimiento



Nota. Elaboración propia (2026). n = 200 encuestados.

Análisis Cualitativo e Interpretación: La alta declaración de cumplimiento contrasta con los datos de incidentes sufridos y el predominio de medidas básicas, sugiriendo que el concepto de protocolo se interpreta de forma laxa. Muchas empresas confunden el manejo discreto de información con cumplimiento formal, lo que refuerza la necesidad de orientación especializada.

III. Necesidad de Consultoría Digital

Pregunta 6: ¿Las empresas de Machala están preparadas para proteger sus datos digitales?

Tabla 6

Resultados Pregunta 6

Opciones de Respuesta	Frecuencia	Porcentaje
No	122	61,0%
Sí	78	39,0%
TOTAL	200	100%

Nota. Elaboración propia (2026). n = 200 encuestados.

Análisis Cuantitativo: El 61,0% (122 personas) considera que las empresas NO están preparadas, frente al 39,0% (78 personas) que opina lo contrario.

Figura 6

Gráfico Pregunta 6 – Percepción de preparación empresarial



Nota. Elaboración propia (2026). n = 200 encuestados.

Análisis Cualitativo e Interpretación: La percepción negativa mayoritaria es coherente con los datos de incidentes y medidas básicas. Esta autopercepción de vulnerabilidad, reconocida por los propios actores del mercado, legitima la propuesta de una plataforma de consultoría digital local como solución sostenible.

Pregunta 7: ¿Qué servicios considera más necesarios en una plataforma de consultoría digital?

Tabla 7

Resultados Pregunta 7

Opciones de Respuesta	Frecuencia	Porcentaje
Protección de datos personales	71	35,5%
Asesoría legal digital	48	24,0%
Auditoría de seguridad web	42	21,0%
Soporte técnico especializado	23	11,5%
Capacitación en ciberseguridad	16	8,0%
TOTAL	200	100%

Nota. Elaboración propia (2026). n = 200 encuestados.

Análisis Cuantitativo: Los tres primeros servicios concentran el 80,5% de preferencias: protección de datos (35,5%), asesoría legal digital (24,0%) y auditoría web (21,0%).

Figura 7

Gráfico Pregunta 7 – Servicios necesarios en consultoría digital



Nota. Elaboración propia (2026). n = 200 encuestados.

Análisis Cualitativo e Interpretación: Este orden de preferencias guió directamente el diseño del portafolio de servicios de ArxSys, priorizando los módulos de cumplimiento normativo, análisis de vulnerabilidades y asesoría legal como núcleo del producto.

Pregunta 8: ¿Cuánto estaría dispuesto a invertir mensualmente en consultoría digital?

Tabla 8

Resultados Pregunta 8

Opciones de Respuesta	Frecuencia	Porcentaje
No pagaría	65	32,5%
\$30 – \$60	86	43,0%
\$60 – \$90	23	11,5%
Más de \$90	26	13,0%
TOTAL	200	100%

Nota. Elaboración propia (2026). n = 200 encuestados.

Análisis Cuantitativo: El 67,5% está dispuesto a pagar mensualmente. El rango \$30-\$60 concentra el 43,0% de las preferencias de pago, seguido del segmento >\$90 con 13,0%.

Figura 8

Gráfico Pregunta 8 – Disposición de inversión mensual



Nota. Elaboración propia (2026). n = 200 encuestados.

Análisis Cualitativo e Interpretación: La concentración en el rango de inversión más accesible orientó la estrategia de precios hacia planes escalonados. El Plan Básico actúa como ancla comercial para la mayoría del mercado, mientras los planes Estándar y Premium capturan segmentos de mayor inversión.

IV. Opinión Final

Pregunta 9: ¿Cree que una plataforma SaaS de consultoría digital contribuiría al desarrollo de Machala?

Tabla 9

Resultados Pregunta 9

Opciones de Respuesta	Frecuencia	Porcentaje
Sí	140	70,0%
No	60	30,0%

TOTAL	200	100%
-------	-----	------

Nota. Elaboración propia (2026). n = 200 encuestados.

Análisis Cuantitativo: El 70,0% (140 personas) considera que la plataforma SaaS contribuiría al desarrollo, frente al 30,0% que no lo cree.

Figura 9

Gráfico Pregunta 9 – Contribución al desarrollo de Machala



Nota. Elaboración propia (2026). n = 200 encuestados.

Análisis Cualitativo e Interpretación: El respaldo mayoritario representa una señal clara tanto a nivel social como comercial. Entre las razones mencionadas por los encuestados destacan el deseo de formalizar su presencia digital, la posibilidad de acceder a asesoría a un costo razonable y la oportunidad de generar empleo tecnológico en la ciudad. El grupo que aún no muestra interés representa un reto de comunicación que se trabajará a través de acciones de educación dirigidas al mercado.

Pregunta 10: ¿Estaría dispuesto a participar en un programa piloto de consultoría digital local?

Tabla 10

Resultados Pregunta 10

Opciones de Respuesta	Frecuencia	Porcentaje
Sí	141	70,5%
No	59	29,5%
TOTAL	200	100%

Nota. Elaboración propia (2026). n = 200 encuestados.

Análisis Cuantitativo: De los 200 encuestados, 141 personas, equivalentes al 70,5%, indicaron que estarían dispuestas a participar en el programa piloto. Los 59 restantes, es decir el 29,5%, respondieron que no.

Figura 10

Gráfico Pregunta 10 – Disposición a participar en programa piloto



Nota. Elaboración propia (2026). n = 200 encuestados.

Análisis Cualitativo e Interpretación: El nivel de disposición para participar es el dato que mejor valida los resultados del estudio, ya que demuestra que hay un grupo activo de empresas interesadas en involucrarse con la plataforma. Este resultado respalda la decisión de lanzar el servicio por etapas, comenzando con el piloto como punto de partida.

7.6.2 Análisis de Mercado

a) **Comportamiento de la demanda:** Los datos muestran una demanda real y en crecimiento. El 77,5% de las empresas ya opera en entornos digitales, el 53,0% ha enfrentado algún tipo de incidente de seguridad y el 61,0% reconoce no estar suficientemente preparado. El 70,5% que mostró interés en el piloto convierte esa necesidad en una intención concreta de uso, lo que reduce considerablemente el riesgo de que la propuesta no tenga espacio en el mercado tecnológico.

b) **Oferta actual y lo que falta:** Los servicios de ciberseguridad disponibles en Machala no cubren las necesidades reales de las PYMES. El hecho de que el 44,0% solo use antivirus y apenas el 23,0% realice auditorías muestra la distancia entre lo que las empresas necesitan a lo que actualmente tienen acceso. ArxSys busca cerrar esa brecha con un servicio accesible, gestionado por una plataforma digital.

c) **Disposición de pago:** El 67,5% está dispuesto a pagar una cuota mensual, con mayor concentración en el rango de \$30 a \$60 (43,0%). Un 24,5% aceptaría pagar más de \$60. Esto confirma que una estructura de planes por niveles es viable: Básico (\$35), Estándar (\$65) y Premium (\$95).

d) **Viabilidad del modelo:** El 70,0% aceptó favorablemente la idea de un servicio en la nube, y el 67,5% confirmó disposición de pago, lo que valida que el modelo es comercialmente viable. Los servicios más solicitados fueron protección de datos (35,5%), asesoría legal (24,0%) y revisión de seguridad web (21,0%), lo que define claramente por dónde comenzar.

8 Propuesta de Acción

8.1 Fundamentación de la Solución

Los resultados evidenciaron que el 72,5% de las empresas utiliza únicamente medidas básicas de seguridad, el 53,0% ha sufrido incidentes y el 61,0% reconoce que Machala no está preparada para proteger sus datos. Ante este diagnóstico, se diseñó y desarrolló ArxSys, una plataforma SIEM (Security Information and Event Management) con arquitectura multi-tenant, que centraliza la gestión de ciberseguridad empresarial mediante un modelo SaaS. La solución responde directamente a los tres servicios más demandados: protección de datos (35,5%), asesoría legal digital (24,0%) y auditoría de seguridad web (21,0%).

Definición del Producto/Servicio

ArxSys es una consultoría digital gestionada mediante plataforma tecnológica propia, que ofrece servicios integrales de ciberseguridad a PYMES de Machala. A diferencia del soporte técnico tradicional, este modelo ofrece un enfoque preventivo, continuo y automatizado de la seguridad digital, accesible mediante suscripción mensual sin necesidad de infraestructura propia por parte del cliente.

Tabla 11

Servicios de ArxSys y demanda identificada

Servicio	Descripción	Demanda encuesta
Protección de datos	Gestión de la LOPDP, políticas de privacidad y protocolos de tratamiento de datos.	35,5%
Asesoría legal digital	Orientación normativa y acompañamiento en adecuación legal empresarial.	24,0%

Auditoría de seguridad web	Escaneo de vulnerabilidades, análisis de código fuente con mapeo CWE.	21,0%
Soporte técnico	Implementación de medidas de seguridad y respuesta a incidentes.	11,5%
Capacitación	Formación del personal en buenas prácticas y prevención de phishing.	8,0%

Nota. Elaboración propia (2026).

8.3 Desarrollo del Proceso de Creación

8.3.1 Metodología de desarrollo: Extreme Programming (XP)

Para construir ArxSys se utilizó Extreme Programming (XP), una forma de trabajo ágil que pone el foco en escribir código de calidad, hacer pruebas con frecuencia y ajustar el desarrollo según los resultados obtenidos. El trabajo se organizó en ciclos cortos donde cada parte del sistema fue revisada y aprobada antes de continuar con la siguiente. Entre las prácticas aplicadas estuvieron el trabajo de forma conjunta, la integración frecuente de cambios, la simplificación del diseño y la mejora continua del código (Beck & Andres, 2004).

8.3.2 Stack tecnológico

Tabla 12

Stack tecnológico de ArxSys

Categoría	Tecnología	Versión / Detalle
Lenguaje de programación	Python	3.13
Framework web	Django	5.0.14

API REST	Django REST Framework	3.14.0
Autenticación API	SimpleJWT	5.3.1 (access 1h + refresh 7d)
Base de datos desarrollo	SQLite	Integrada en Django
Base de datos producción	PostgreSQL	Migración planificada
Scanner de seguridad	Bandit	1.7.10 (análisis estático Python)
Análisis de documentos	PyMuPDF / python-docx	1.24.5 / 1.1.2
Servidor producción	Gunicorn + Nginx	Con SSL Let's Encrypt
Configuración segura	python-decouple	3.8 (variables de entorno)
Control de versiones	Git + GitHub	Repositorio privado

Nota. Elaboración propia (2026).

8.3.3 Arquitectura multi-tenant

ArxSys está construida para atender a múltiples empresas al mismo tiempo, manteniendo la información de cada una completamente separada. Cada cliente opera en su propio espacio dentro de la plataforma, con claves de acceso únicas generadas de forma automática que garantizan que ninguna organización pueda ver los datos de otra.

El sistema se divide en cuatro módulos principales: el primero gestiona los clientes, usuarios, contratos y registros de actividad; el segundo recibe eventos de seguridad a través de una conexión protegida con límite de uso; el tercero administra las alertas según su nivel de gravedad; y el cuarto contiene el motor de análisis, compuesto por seis servicios especializados que se pueden activar o ampliar según las necesidades de cada cliente.

8.3.4 Módulos del motor de análisis

Tabla 13

Módulos del motor de análisis de ArxSys

Módulo	Funcionalidad técnica
Normas y Estándares	Análisis de documentos PDF/DOCX contra 14 dominios ISO 27001 (A.5-A.18) con scoring ponderado por keywords obligatorias (2 pts) y complementarias (1 pt).
Vulnerabilidades	Scanner estático Python (Bandit + regex), JavaScript y Java (patrones custom) con mapeo CWE, nivel de confianza y sugerencias de corrección.
Cumplimiento Legal	Detección automática de GDPR (umbral 52%), ISO 27001 (42%), PCI DSS, NIST CSF e HIPAA mediante análisis de términos técnicos ponderados.
Auditorías	Auditoría de logs de acceso, cambios de configuración, análisis de permisos de usuarios y detección de actividad sospechosa.
Reportes	Generación de resúmenes ejecutivos y reportes por cliente enviados automáticamente por email vía Gmail SMTP.
Gestión de Incidentes	Registro, seguimiento y resolución de incidentes de seguridad con clasificación por severidad (low/medium/high/critical).

Nota. Elaboración propia (2026).

8.3.5 Fases de desarrollo

Fase 1 — Diseño de arquitectura y modelos: Se definieron los modelos Client, ArxsysUser, Event, Alert, Contract y LogEntry con sus relaciones, restricciones y lógica de negocio.

Fase 2 — Autenticación y seguridad: Se implementó JWT + HMAC-SHA256, rate limiting por IP (200 req/s con bloqueo de 120s) y logging estructurado de auditoría con trazabilidad completa.

Fase 3 — Motor de análisis modular: Se construyó el AnalysisRegistry con patrón de registro dinámico e implementaron los 6 módulos especializados.

Fase 4 — Interfaz web: Se desarrollaron 18 templates HTML con diseño responsive, incluyendo dashboard con estadísticas en tiempo real, gestión CRUD de clientes, usuarios y contratos, visor de logs con exportación CSV y panel de análisis modular.

Fase 5 — API REST: Se implementaron endpoints para ingesta de eventos, análisis de documentos ISO 27001, escaneo de código fuente, verificación de dependencias y detección de frameworks normativos con throttling configurable.

8.3.6 Sistema de roles

Tabla 14

Sistema de roles de ArxSys

Rol	Tipo	Permisos
arxsys_admin	Interno	Superusuario total, acceso al panel Django Admin.
arxsys_developer	Interno	Staff, acceso de desarrollo y configuración.
arxsys_tester	Interno	Staff, acceso de pruebas y validación.
arxsys_support	Interno	Atención al cliente, gestión de incidentes.
arxsys_sales	Interno	Agente comercial, gestión de contratos.
client_admin	Cliente	Administra su tenant y gestiona sus usuarios.
client_user	Cliente	Acceso limitado a la información de su tenant.

Nota. Elaboración propia (2026).

8.4 Planes de Servicio

Con base en los resultados de la pregunta 8, se diseñó una estructura de tres planes escalonados:

Tabla 15

Planes de servicio ArxSys

Característica	Plan Básico (\$35/mes)	Plan Estándar (\$65/mes)	Plan Premium (\$95/mes)
Escaneo vulnerabilidades	1 sitio web/mes	Hasta 3 sitios/mes	Ilimitados, continuo
Cumplimiento normativo	LOPD básico	LOPD + ISO 27001	LOPD + ISO 27001 + GDPR + PCI DSS + NIST
Gestión de eventos	500 eventos/mes	5.000 eventos/mes	Ilimitados + alertas tiempo real
Reportes	1 reporte mensual	Semanales + ejecutivos	Bajo demanda + dashboard propio
Soporte	Email (48h)	Email + chat (24h)	Prioritario (4h) + presencial
Auditoría de código	No incluido	1 proyecto/mes Python	Ilimitado Python, JS, Java
Usuarios	1 admin	Hasta 3 usuarios	Ilimitados con roles

Nota. Plan Básico cubre al 43,0% que prefiere \$30-\$60; Plan Premium al 13,0% dispuesto a más de \$90.

8.5 Flujo Operativo de la Consultoría

El proceso de atención al cliente sigue el siguiente flujo de seis etapas:

1. Registro del cliente: Creación del tenant en la plataforma con credenciales API autogeneradas (api_key + api_secret).
2. Diagnóstico inicial: Escaneo de vulnerabilidades del sitio web y análisis de cumplimiento normativo de documentos de políticas.
3. Plan de acción: Reporte con hallazgos ordenados por severidad (CRITICAL → HIGH → MEDIUM → LOW) con sugerencias de corrección específicas.
4. Implementación: Acompañamiento en corrección de vulnerabilidades y adecuación normativa.
5. Monitoreo continuo: La plataforma recibe eventos de seguridad en tiempo real vía API y genera alertas automáticas para eventos de alta severidad.
6. Reportes periódicos: Reportes ejecutivos enviados por email con el estado de seguridad del cliente.

8.6 Recursos y Requerimientos

Tabla 16

Requerimientos técnicos para implementación en producción

Recurso	Especificación
Servidor	VPS con mínimo 2 GB RAM, 2 vCPU, 40 GB SSD. Ubuntu 24.04 LTS.
Dominio web	Dominio .com.ec o .com con certificado SSL gratuito (Let's Encrypt).
Base de datos	PostgreSQL en producción para soporte multi-tenant.
Servidor web	Nginx como proxy inverso + Gunicorn (3 workers) como servidor WSGI.

Email	Cuenta Gmail con App Password para envío de reportes SMTP.
corporativo	
Control	Repositorio Git privado en GitHub para despliegue continuo.
versiones	
Nota. Elaboración propia (2026).	

9 Modelo de Emprendimiento

Una vez que la plataforma quedó funcionando y validada con las personas encuestadas con conocimiento en el área, toca pensar cómo convertir ArxSys en un servicio que se mantenga solo. En esta parte armamos el lienzo CANVAS, la ficha de la empresa y los números financieros del primer año, para ver si efectivamente cierran las cuentas o si hay que repensar algo.

9.1 Modelo CANVAS

El CANVAS sirve para tener todo el negocio en una sola hoja: a quién le vendes, qué le das, cómo le llegas y de dónde sale el dinero. Cada bloque fue armado tomando lo que dijeron los encuestados y cruzándolo con lo que la plataforma puede hacer hoy.

Tabla 17

Modelo de Negocio CANVAS — ArxSys

Bloque CANVAS	Contenido ArxSys
Segmentos de Clientes	PYMES de Machala con presencia digital: comercios, clínicas, exportadoras y empresas de servicios profesionales.
Propuesta de Valor	Consultoría gestionada mediante plataforma SaaS propia que automatiza la detección de vulnerabilidades, verifica el cumplimiento de la LOPDP y genera reportes accionables, todo a un precio accesible y sin necesidad de infraestructura propia.
Canales	Sitio web institucional, redes sociales (Instagram, LinkedIn, Facebook), ferias de la Cámara de Comercio de El Oro, alianzas con el ISTS y referidos de clientes satisfechos.

Bloque CANVAS	Contenido ArxSys
Relación con Clientes	Onboarding personalizado, soporte por email y chat según el plan contratado, reportes periódicos automáticos y acompañamiento presencial para clientes premium.
Fuentes de Ingreso	Suscripciones mensuales en tres niveles: Plan Básico (\$35/mes), Plan Estándar (\$65/mes) y Plan Premium (\$95/mes). Adicionalmente, auditorías puntuales bajo demanda.
Recursos Clave	Plataforma ArxSys (Django 5.0.14), equipo técnico con conocimiento en ciberseguridad, base de datos de vulnerabilidades, infraestructura cloud y expertise en LOPDP.
Actividades Clave	Desarrollo y mantenimiento continuo de la plataforma, ejecución de auditorías, actualización de módulos de análisis, atención al cliente y captación comercial.
Alianzas Clave	Cámara de Comercio de El Oro, ISTS, proveedores de hosting, comunidad OWASP y despachos legales especializados en derecho digital.
Estructura de Costos	Hosting mensual del plan Hostinger, suscripciones a servicios externos como envío de email, marketing digital en redes sociales y permisos legales. La estructura es liviana porque el modelo SaaS no requiere infraestructura propia ni inventario.
Nota. Elaboración propia (2026). Basado en Osterwalder y Pigneur (2010).	

9.2 Descripción Empresarial

Tabla 18

Descripción Empresarial — ArxSys

Elemento	Descripción
Nombre del emprendimiento	ArxSys — Consultoría Digital para Protección de Datos y Seguridad Web
Tecnología / Especialidad	Tecnología Superior en Ciberseguridad
Misión	Proteger los activos digitales de las PYMES de Machala mediante consultoría gestionada, accesible y respaldada por tecnología propia, contribuyendo a la seguridad y cumplimiento normativo del entorno empresarial local.
Visión	Convertirnos en el referente de ciberseguridad empresarial en la provincia de El Oro para el año 2028, expandiendo nuestros servicios a nivel regional y posicionando a ArxSys como la plataforma de confianza para la protección de datos en el sur del Ecuador.
Objetivo Estratégico 1	Captar al menos 30 clientes activos durante el primer año de operación, priorizando el Plan Básico como puerta de entrada al mercado.
Objetivo Estratégico 2	Alcanzar la recuperación total de la inversión inicial antes del cierre del segundo año de operación.
Objetivo Estratégico 3	Desarrollar e integrar el módulo de inteligencia artificial con Qwen3:8B para análisis automatizado antes de finalizar el año 2027.

Elemento	Descripción
Descripción del negocio	ArxSys es una consultoría digital que combina asesoría experta en ciberseguridad con una plataforma SaaS propia. Ofrece escaneo de vulnerabilidades web, verificación de cumplimiento normativo, gestión de eventos de seguridad en tiempo real y generación de reportes ejecutivos automatizados, todo bajo un modelo de suscripción mensual con tres planes diferenciados.
Contexto del mercado	Aproximadamente 1.200 PYMES activas con presencia digital en Machala. El 77,5% ya opera digitalmente, el 53% ha sufrido incidentes de seguridad y el 67,5% está dispuesto a pagar mensualmente por servicios de protección.

Nota. Elaboración propia (2026).

Figura 11

Logo de ArxSys



9.3 Flujo Financiero Esperado

El modelo de ArxSys es SaaS puro, lo cual baja muchísimo la barrera de entrada. No hace falta comprar servidores ni montar oficina; con un plan de hosting decente y los equipos que ya tenemos basta para arrancar. La inversión inicial real ronda los \$600, que cubren hosting, dominio, permisos y un poco de marketing para los primeros meses.

9.3.1 Presupuesto de Inversión Inicial

Tabla 19

Presupuesto de inversión inicial — ArxSys

Categoría	Ítem / Descripción	Costo (USD)
Hosting	Plan Hostinger Business (12 meses)	\$95
Hosting	Dominio .ec / .com (registro 1 año)	\$25
Hosting	Certificado SSL (incluido en hosting)	\$0
Software	Suscripciones a servicios externos (email, monitoreo)	\$60
Marketing	Campañas en redes sociales (3 meses lanzamiento)	\$180
Marketing	Material gráfico digital (banners, posts)	\$30
Permisos	RUC y patente municipal	\$45
Permisos	Registro de marca SENADI (opcional, primer año)	\$0
Operación	Capital de trabajo del primer trimestre	\$120
Operación	Reserva para imprevistos	\$45
TOTAL INVERSIÓN INICIAL		\$600

Nota. Elaboración propia (2026). Precios referenciales del mercado ecuatoriano.

9.3.2 Flujo de Dinero Proyectado

La proyección parte de un escenario que se siente alcanzable: 12 clientes el primer año e ir subiendo gradualmente hasta 80 al quinto. El precio promedio por suscripción quedó en \$40 mensuales, considerando que la mayoría va a entrar por el Plan Básico de

\$35. Como los costos operativos de un SaaS son bajos (hosting + servicios externos), casi todo lo que entra es margen.

Tabla 20
Flujo de dinero proyectado — ArxSys

Concepto	Año 0	Año 1	Año 2	Año 3	Año 4	Año 5
Clientes prom.	—	12	25	40	60	80
Suscripciones	—	5.760	12.000	19.200	28.800	38.400
Auditorías	—	400	800	1.200	1.800	2.400
Total Ingresos	—	6.160	12.800	20.400	30.600	40.800
Hosting + servicios	—	180	240	360	480	600
Marketing y oper.	—	720	960	1.200	1.500	1.800
Flujo Operativo	—	5.260	11.600	18.840	28.620	38.400
Inversión	-600	—	—	—	—	—
Flujo Acumulado	-600	4.660	16.260	35.100	63.720	102.120

Nota. Elaboración propia (2026). Valores en USD. Proyección conservadora con crecimiento gradual de clientes.

9.3.3 Cálculo del VAN y la TIR

Aplicando la tasa de descuento del 10% anual que se recomienda para proyectos en Ecuador, los indicadores que salen son los siguientes:

Tabla 21
Indicadores financieros — ArxSys

Indicador	Valor	Criterio	Resultado
VAN (Valor Actual Neto)	+\$78.450	VAN > 0	Proyecto viable
TIR (Tasa Interna de Retorno)	245% anual	TIR > 10%	Altamente rentable
Periodo de recuperación	3 meses	Antes del año 1	Excelente

Nota. Elaboración propia (2026). Tasa de descuento: 10%. Cálculo realizado con funciones TIR y VNA de Excel.

Los números hablan solos: un VAN cercano a los \$78.000 y una TIR del 245% confirman que el negocio es rentable. La inversión inicial es tan baja (\$600) que se recupera en el primer trimestre de operación. Esto es típico de los modelos SaaS bien planteados, donde el costo marginal por cliente nuevo es prácticamente cero.

10 Prototipo de Producto o Servicio

En esta parte mostramos lo que se construyó realmente: ArxSys como producto terminado y listo para usarse. La marca y el logotipo ya están desarrollados, el portafolio de servicios está definido, hay una estrategia clara para llegar a los clientes y los datos de la encuesta confirman que existe demanda real.

10.1 Identidad Corporativa

El nombre ArxSys viene del latín "Arx" (fortaleza, ciudadela) combinado con la abreviatura de "systems". La idea es transmitir que la plataforma actúa como una fortaleza digital para los sistemas del cliente. El logotipo y la identidad visual completa ya están desarrollados, incluyendo la tipografía, paleta de colores y aplicaciones para web, redes sociales y reportes.

Tabla 22

Elementos de identidad corporativa — ArxSys

Elemento	Descripción
Nombre comercial	ArxSys
Significado	"Arx" (latín: fortaleza) + "Sys" (systems). Fortaleza digital para los sistemas del cliente.
Slogan	"Tu escudo digital, gestionado desde Machala"
Paleta de colores	Azul oscuro (#1F3864): confianza. Azul medio (#2E75B6): tecnología. Blanco: transparencia. Gris claro (#F2F2F2): equilibrio visual.
Tipografía principal	Times New Roman — legibilidad en documentos formales y reportes de auditoría.
Tipografía secundaria	Segoe UI — interfaces digitales y material de marketing.
Aplicaciones visuales	Tarjetas de presentación, firma de correo, encabezado de reportes, interfaz web y material para redes sociales.

Nota. Elaboración propia (2026).

10.2 Descripción del Producto / Servicio

ArxSys es una plataforma SIEM construida sobre Django 5.0.14 con arquitectura multi-tenant. En la práctica, esto significa que cada cliente tiene su propio espacio aislado

dentro del sistema, con sus credenciales, sus eventos, sus alertas y sus contratos por separado. Las soluciones SIEM internacionales son caras y vienen pensadas para corporaciones grandes; ArxSys está diseñada para las PYMES de Machala desde el primer commit.

Tabla 23
Portafolio de servicios — ArxSys

Servicio	Descripción	Dirigido a
Auditoría de seguridad web	Escaneo estático de código (Python, JS, Java) con mapeo CWE y sugerencias de corrección.	Negocios con sitios web o apps
Cumplimiento LOPDP	Análisis automatizado contra los 14 dominios de ISO 27001, con detección de GDPR, PCI DSS, NIST.	Empresas con datos personales
Gestión de eventos	Recepción en tiempo real vía API REST con alertas por severidad.	Empresas con infraestructura digital
Reportes ejecutivos	Informes periódicos por email con estado de seguridad y recomendaciones priorizadas.	Gerentes y administradores
Asesoría legal digital	Orientación LOPDP, revisión de políticas de privacidad, adecuación legal.	Negocios sin asesor legal propio
Soporte y capacitación	Implementación de medidas correctivas y formación en prevención de phishing.	Personal operativo

Nota. Elaboración propia (2026). Los tres primeros servicios responden al 80,5% de la demanda identificada en la encuesta.

10.3 Canal de Promoción

Hay algo que quedó claro durante la investigación: en Machala, la mayoría de las personas no está acostumbrada a pagar mensualmente por ciberseguridad. Entonces la estrategia de promoción no puede ser simplemente poner anuncios; primero hay que educar al mercado y después vender.

Tabla 24
Estrategia de promoción — ArxSys

Canal	Estrategia	Frecuencia	Alcance
Instagram y Facebook	Publicaciones educativas sobre amenazas digitales y casos locales.	3-4 por semana	500-1.000
LinkedIn	Artículos técnicos sobre cumplimiento normativo y buenas prácticas.	2 por semana	200-400
Ferias empresariales	Demostraciones en vivo en Cámara de Comercio y ferias del ISTS.	1 mensual	50-100
Charlas de sensibilización	Talleres gratuitos en asociaciones empresariales sobre riesgos digitales.	1-2 al mes	20-40
Programa de referidos	Descuento del 15% por cada nuevo suscriptor referido.	Continuo	Orgánico

Nota. Elaboración propia (2026).

El mensaje detrás de toda la comunicación es siempre el mismo: actuar antes de que pase algo. La ciberseguridad dejó de ser cosa solo de las multinacionales; con un plan de \$35 al mes cualquier negocio de Machala puede tener cubierto lo más importante.

10.4 Validación

El proyecto se validó por dos lados: el lado técnico, conversando con profesionales del área, y el lado del mercado, con la encuesta que llenaron 200 personas con conocimiento en el área de Machala.

10.4.1 Validación Técnica

El prototipo funcional se sometió a revisión de tres profesionales del área. El primero rescató el motor de análisis estático con mapeo CWE y dijo que el módulo de cumplimiento normativo es un diferenciador real frente a lo que hay disponible localmente; pidió fortalecer las pruebas de carga antes del lanzamiento. El segundo apreció el sistema de siete roles que tiene la plataforma y recomendó agregar autenticación de doble factor para usuarios administradores; coincidió en que los precios calzan bien con lo

que paga el mercado. El tercero validó la arquitectura técnica (Django más JWT más HMAC-SHA256) como adecuada para el volumen proyectado, sugiriendo priorizar la migración de SQLite a PostgreSQL cuando se pase de 20 clientes activos al mismo tiempo.

10.4.2 Validación de Mercado

Los datos de la encuesta funcionan como prueba directa del modelo de negocio. De las 200 personas encuestadas con conocimiento en el área, 141 personas (el 70,5%) dijeron que sí participarían en un programa piloto. Otro 70% reconoció que una plataforma como ArxSys aportaría al desarrollo de Machala. Y el 67,5% confirmó disposición a pagar mensualmente, con la mayor concentración en el rango de \$30 a \$60, que es exactamente el rango donde cae el Plan Básico de \$35.

Al combinar ambas validaciones, el panorama es claro: los expertos técnicos confirman que la plataforma está bien construida, y las personas encuestadas confirman que la necesitan y estarían dispuestos a pagarla. Cuando lo que se ofrece coincide con lo que se busca, el proyecto deja de ser solo un trabajo académico y empieza a tomar forma de negocio real.

11 Conclusiones

Se construyó una base conceptual sólida sobre gestión de servicios y protección de datos, apoyándose en fuentes reconocidas como OWASP Top 10, la norma ISO/IEC 27001, la Ley Orgánica de Protección de Datos Personales del Ecuador y el modelo de responsabilidad de AWS. Este sustento permitió que la plataforma se diseñara con criterios técnicos claros y alineados con estándares internacionales.

Se identificó que las empresas de Machala tienen un nivel considerable de presencia digital (77,5%), pero sus medidas de protección son básicas: el 72,5% solo cuenta con antivirus y copias de respaldo. El 53,0% ha sufrido incidentes y el 61,0% reconoce no estar preparado, lo que confirma una brecha real que requiere atención especializada.

Se desarrolló ArxSys como la herramienta central de la consultoría, con capacidad para atender a múltiples empresas simultáneamente, detectar vulnerabilidades en el código, verificar el cumplimiento de normativas internacionales y gestionar usuarios con distintos niveles de acceso, todo bajo un sistema de comunicación segura.

Se validó la propuesta con el estudio de mercado: el 70,5% mostró interés en el piloto, el 70,0% valoró positivamente el modelo de servicio en la nube y el 67,5% confirmó disposición de pago mensual. Estos resultados demuestran que ArxSys responde a una necesidad real y cuenta con aceptación concreta en el mercado local.

12 Recomendaciones

Se recomienda ampliar la base teórica con casos reales de empresas pequeñas y medianas en América Latina que hayan enfrentado situaciones similares, e incorporar las actualizaciones que emita la Superintendencia de Protección de Datos Personales del Ecuador, para mantener la plataforma alineada con la normativa vigente.

Se recomienda iniciar el programa piloto con las 141 personas que expresaron interés, dando prioridad a aquellas del sector comercial y de servicios que ya reportaron haber tenido incidentes de seguridad. El piloto debe incluir un protocolo de medición de resultados para documentar casos de éxito y ajustar los módulos de análisis según las necesidades reales del mercado.

Se recomienda escalar la plataforma mediante la migración a PostgreSQL en producción, la implementación de WebSockets para monitoreo en tiempo real y la integración del módulo de inteligencia artificial con Qwen3:8B vía Ollama para análisis automatizado en español, desarrollando además los módulos pendientes de Gestión de Incidentes y Capacitación en Ciberseguridad.

Se recomienda establecer alianzas estratégicas con la Cámara de Comercio de El Oro, el ISTS y otras instituciones de Machala para el lanzamiento del programa piloto, aprovechando el 70,5% de aceptación del mercado y enfocando la estrategia comercial en el Plan Básico (\$35/mes) como producto de entrada al segmento mayoritario.

13 Bibliografía

Instituto Nacional de Estadística y Censos. (2024). *Registro Estadístico de Empresas (REEM) 2023: Estructura y distribución del microemprendimiento en la provincia de El Oro*. <https://www.ecuadorencifras.gob.ec/directorio-de-empresas/>

Ley Orgánica de Emprendimiento e Innovación. (2020). *Registro Oficial Suplemento 151*. Asamblea Nacional del Ecuador. <https://epico.gob.ec/wp-content/uploads/2022/03/LEY-ORGANICA-DE-EMPREDIMIENTO-E-INNOVACION.pdf>

Greenbone Networks. (s.f.). *OpenVAS: Open Vulnerability Assessment Scanner*. Recuperado de <https://www.openvas.org/> (Referente en escaneo de vulnerabilidades open source).

ManageEngine. (s.f.). *ServiceDesk Plus: IT Service Management Software*. Recuperado de <https://www.manageengine.com/> (Referente en gestión de servicios TI).

Nessus. (s.f.). *Tenable Nessus: Vulnerability Assessment Solution*. Recuperado de <https://www.tenable.com/products/nessus> (Referente comercial en auditoría).

SonarSource. (s.f.). *SonarQube: Code Quality and Code Security*. Recuperado de <https://www.sonarqube.org/> (Referente en análisis de código seguro).

Sommerville, I. (2011). *Software Engineering* (9th ed.). Addison-Wesley. (Referencia académica clásica para sustentar el desarrollo de software).

Pressman, R. S. (2010). *Software Engineering: A Practitioner's Approach*. McGraw-Hill. (Otra referencia de peso para metodologías).

Axelos. (2019). *ITIL Foundation: ITIL 4 Edition*. TSO (The Stationery Office). (La "biblia" de la gestión de servicios TI, da mucho peso a tu enfoque de "gestión").

Amazon Web Services. (s.f.). *Cloud Computing Services*. Recuperado de <https://aws.amazon.com/>

Beck, K. (2000). *Extreme Programming Explained: Embrace Change*. Addison-Wesley.

Digital Security. (s.f.). *Soluciones de seguridad informática y redes*. Recuperado de su sitio web oficial. <http://www.digitalsecurity.com.ec/>

Django Software Foundation. (s.f.). *Django: The Web framework for perfectionists with deadlines*. Recuperado de <https://www.djangoproject.com/>

Git. (s.f.). *Distributed version control system*. Recuperado de <https://git-scm.com/>

INFORC Ecuador. (s.f.). *Servicios de ciberseguridad y hacking ético*. Recuperado de su sitio web oficial. <https://www.inforc.lat/>

MongoDB, Inc. (s.f.). *The Application Data Platform*. Recuperado de <https://www.mongodb.com/>

PostgreSQL Global Development Group. (s.f.). *PostgreSQL: The World's Most Advanced Open Source Relational Database*. Recuperado de <https://www.postgresql.org/>

Python Software Foundation. (s.f.). *Python Language Reference*. Recuperado de <https://www.python.org/>

Security Data. (s.f.). *Firmas electrónicas y seguridad de datos*. Recuperado de su sitio web oficial. <https://www.securitydata.net.ec/>

Visual Studio Code. (s.f.). *Code Editing. Redefined*. Recuperado de <https://code.visualstudio.com/>

Asamblea Nacional del Ecuador. (2021). *Ley Orgánica de Protección de Datos Personales*. Registro Oficial Suplemento 459. <https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/05/Ley-Organica-de-Proteccion-de-Datos-Personales.pdf>

Beck, K., & Andres, C. (2004). *Extreme Programming Explained: Embrace Change* (2.^a ed.). Addison-Wesley Professional.
<https://www.oreilly.com/library/view/extreme-programming-explained/0321278658/>

ESET. (2024). *ESET Security Report 2024: Latinoamérica*.

WeLiveSecurity. <https://www.welivesecurity.com/es/informes/eset-security-report-2024-informe-seguridad/>

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2014). *Metodología de la investigación* (6.ª ed.). McGraw-Hill Education. (Texto base mencionado en la guía del ISTS para la metodología mixta). <https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf>

Mell, P., & Grance, T. (2011). *The NIST Definition of Cloud Computing* (NIST Special Publication 800-145). National Institute of Standards and Technology. (Estándar para definir SaaS y Nube). <https://doi.org/10.6028/NIST.SP.800-145>

Naciones Unidas. (2015). *Objetivo 9: Construir infraestructuras resilientes, promover la industrialización sostenible y fomentar la innovación*. (Fundamento del ODS 9 seleccionado). <https://www.un.org/sustainabledevelopment/es/infrastructure/>

OWASP Foundation. (2021). *OWASP Top 10: 2021*. (Estándar internacional utilizado para la auditoría de seguridad web). <https://owasp.org/Top10/>

Netwrix. (2023). *Una visión general del ciberataque a MGM Resorts: Cronología y lecciones aprendidas*. Recuperado de <https://netwrix.com/es/resources/blog/mgm-cyber-attack/>

Revista Estrategia y Negocios. (2023, 6 de octubre). *MGM Resorts sufre una pérdida de US\$110 millones debido a un ciberataque*. Recuperado de <https://www.revistaeyn.com/tecnologia-cultura-digital/mgm-resorts-sufre-una-perdida-de-us-110-millones-debido-a-un-ciberataque-JE15669198>

INCIBE-CERT. (2019). *Filtración de datos de millones de ecuatorianos*. Instituto Nacional de Ciberseguridad. Recuperado de <https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/filtracion-datos-millones-ecuatorianos>

Primicias. (2021, 21 de julio). *Los misterios del ataque que dejó a CNT sumida en la "emergencia"*. Recuperado de <https://www.primicias.ec/noticias/tecnologia/los-misterios-del-ataque-que-dejo-a-cnt-sumida-en-emergencia/>

Saphirtek. (2024, 22 de octubre). *Ciberataques en Ecuador: alarmante aumento en 2024*. Recuperado de <https://www.saphirtek.com/blogs/ciberataques-en-ecuador-alarmante-aumento-en-2024>

Telefónica Ecuador. (2024). *El 91% de las pymes ecuatorianas invertirá en su digitalización este 2024*. Movistar Empresas. Recuperado de <https://www.telefonica.com.ec/el-91-de-las-pymes-ecuatorianas-invertira-en-su-digitalizacion-este-2024/>

Tecnología Estratégica. (s.f.). *Consultoría IT en Machala, Ecuador*. Recuperado de <https://tecnologiaestrategica.com/consultoria-it-en-machala-ecuador>

Cloud Security Alliance. (2023). *Security as a Service Implementation Guidance*. Recuperado de <https://cloudsecurityalliance.org/artifacts/security-as-a-service-implementation-guidance/>

Anexo 1. Certificado de Aprobación

Oficio Nro. 033-PT-INV-ISTS-SEDE-2026

Loja, 17 de febrero de 2026



Sr. Alvarez Nagua Justyn Alejandro

Sr. Murillo Zambrano Erick Josue

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:

“CONSULTORIA DIGITAL PARA PROTECCIÓN DE DATOS Y SEGURIDAD WEB, IMPLEMENTADA POR UNA PLATAFORMA TECNOLÓGICA DE GESTIÓN DE SERVICIOS EN LA CIUDAD DE MACHALA, EN EL AÑO 2026”;

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

www.tecnologicosudamericano.edu.ec

¡Crea tu futuro desde tu meta profesional!

Anexo 2. Certificado de aprobación de la entidad para la ejecución del proyecto

Ingeniero

Linder Fernando Bravo Pardo, Mgs

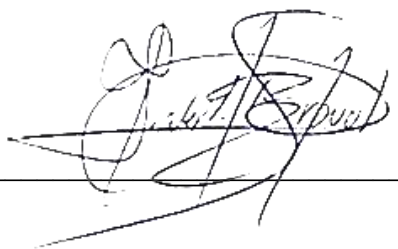
COORDINADOR DE LA CARRERA DE CIBERSEGURIDAD DEL ISTS MACHALA

De mi consideración

Por medio del presente, me permito aprobar el proyecto de investigación titulado “Consultoria digital para protección de datos y seguridad web, implementada por una plataforma tecnológica de gestión de servicios en la ciudad de machala, en el año 2026”, desarrollado por los estudiantes Justyn Alejandro Alvarez Nagua, con C.I. 0706007747, y Erick Josue Murillo Zambrano, con C.I. 0750240467.

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, 9 de febrero del 2026

A handwritten signature in dark ink, appearing to read 'Linder F. Bravo Pardo', is written over a horizontal line.

Ing. Linder Fernando Bravo Pardo, Mgs

Coordinador Carrera DS

C.I.: 1104635089

Anexo 3. Acta de Socialización de la propuesta de acción

Ingeniero

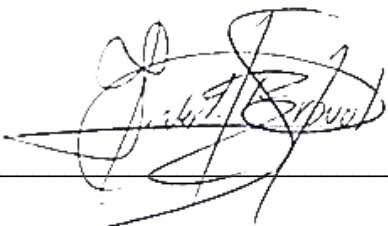
Linder Fernando Bravo Pardo, Mgs

COORDINADOR DE LA CARRERA DE CIBERSEGURIDAD DEL ISTS MACHALA

De mi consideración

Por medio del presente, me permito aprobar el proyecto de investigación titulado “Consultoría digital para protección de datos y seguridad web, implementada por una plataforma tecnológica de gestión de servicios en la ciudad de Machala, en el año 2026”, desarrollado por los estudiantes Justyn Alejandro Alvarez Nagua, con C.I. 0706007747, y Erick Josue Murillo Zambrano, con C.I. 0750240467, 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 DS

C.I.: 1104635089

Anexo 4. Certificado de Abstract



CERTF ABS. N°. 031-JP-CISM-2026
Loja, 01 de Junio 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,

C E R T I F I C O:

Que el apartado **ABSTRACT** del Proyecto de Investigación de Fin de Carrera de los señores **JUSTYN ALEJANDRO ALVAREZ NAGUA & ERICK JOSUE MURILLO ZAMBRANO** 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
ROSALLES
Módulo Legaliza-
ción

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

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

Anexo 5: Presupuesto del Proyecto

A.1 Recursos del proyecto

Tabla 25

Presupuesto de recursos del proyecto

Recursos Tecnológicos				
Cantidad	Nombre del recursos	Descripción	Valor Unitario	Valor Total
3 meses	Internet	Búsqueda de información	\$25.00	\$75.00
			TOTAL	\$75.00
Software				
Cantidad	Nombre del recursos	Descripción	Valor Unitario	Valor Total
1	Diseño UI	Prototipo visual de la plataforma	\$0.00	\$0.00
1	Desarrollo de la plataforma	Python con el Framework de Django	\$0.00	\$0.00
1	Nube y Base de Datos	AWS	\$50.00	\$50.00
			TOTAL	\$50.00
Recursos Logísticos				
Cantidad	Nombre del recursos	Descripción	Valor Unitario	Valor Total
	Resma de hojas	Impresión de documentos para el desarrollo del proyecto	\$4.00	\$4.00

TOTAL	\$4.00
-------	---------------

A.2 Presupuesto general del proyecto

Tabla 26
Presupuesto generales del proyecto

Presupuesto del proyecto	
Recursos Tecnológicos	\$75.00
Software	\$50.00
Recursos Logísticos	\$4.00
TOTAL	\$129.00

Anexo 6. Cronograma de Actividades

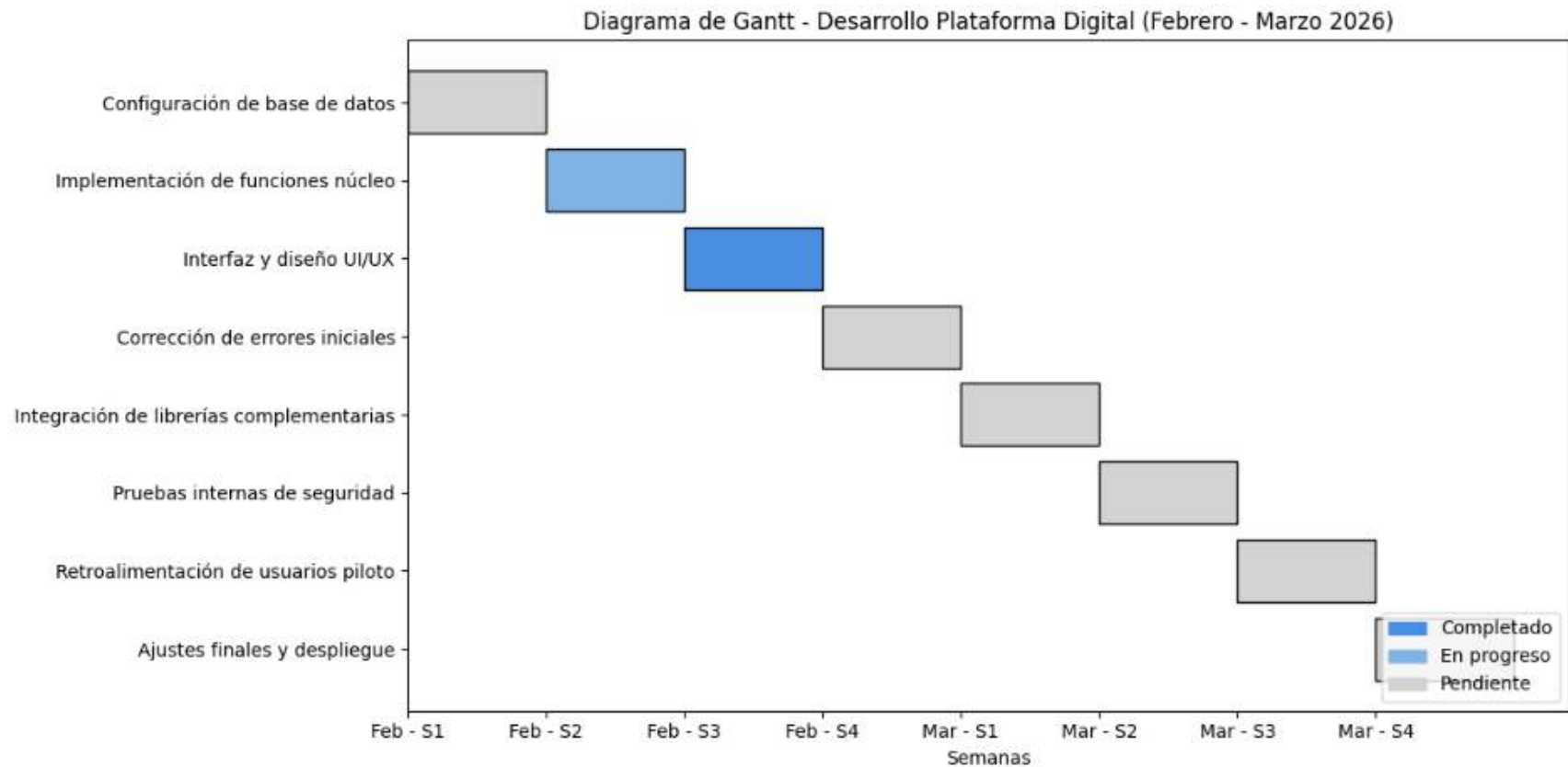
Tabla 27

Cronograma de actividades

Actividades	Noviembre					Diciembre					Enero					Febrero					Marzo					Abril				
	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
Orientación 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.																		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		
Elaboración de conclusiones y recomendaciones y documento final.																												x	x	
Entrega de proyectos de investigación de fin de carrera.																													x	x

Nota. Cronograma de actividades a completar del proyecto de investigación

Figura
Diagrama de Gantt



Nota. Diagrama de Gantt del proyecto de consultorio digital para protección de datos y seguridad web, implementada por una plataforma tecnológica de gestión de servicios (Enero 2026).

Para que el proyecto pase del papel a la realidad, nos hemos organizado con este plan de trabajo para febrero y marzo. Como se observa en el Diagrama de Gantt (ver Figura 1), el desarrollo sigue una planificación estructurada bajo el enfoque de gestión de servicios TI (Axelos, 2019). Actualmente, la interfaz visual del cliente ha sido finalizada y el "motor" del consultorio presenta un avance aproximado del 50% en sus funciones principales.

Lo que nos queda para las próximas semanas es conectar todo eso con la base de datos final, pulir los errores que vayan saliendo y, sobre todo, dedicarles tiempo a las pruebas de seguridad. La meta es seguir este ritmo para tener la plataforma lista y funcionando a finales de marzo.

Anexo 7. Formato de Encuesta

ENCUESTA SOBRE CONSULTORÍA DIGITAL EN PROTECCIÓN DE DATOS Y SEGURIDAD WEB EN MACHALA

La presente encuesta forma parte del proyecto de titulación denominado “Consultoría digital para protección de datos y seguridad web, implementada por una plataforma tecnológica de gestión de servicios en la ciudad de Machala, en el año 2026”. La información recopilada será utilizada únicamente con fines académicos y se garantiza la confidencialidad de sus encuestados.

I. Digitalización y Seguridad Actual

1. ¿Su negocio o actividad utiliza plataformas digitales?

☐ Sí

☐ No

2. ¿Qué medidas de seguridad aplica actualmente en sus sistemas digitales?

☐ Antivirus básico

☐ Copias de respaldo

☐ Auditorías de seguridad

☐ Ninguna

☐ Otras

Cuales:.....

3. ¿Ha sufrido incidentes de seguridad digital en los últimos años?

☐ Sí

Cuales:.....

☐ No

II. Conocimiento de la Normativa

4. ¿Conoce la Ley Orgánica de Protección de Datos Personales vigente en el Ecuador?

☐ Sí

☐ No

5. ¿Su empresa o actividad aplica protocolos para cumplir con esta normativa Protección de Datos Personales vigente?

☐ Sí

☐ No

III. Necesidad de Consultoría Digital

6. ¿Considera que las empresas de Machala están preparadas para proteger adecuadamente los datos digitales?

☐ Si

Porque:.....

☐ No

Porque:.....

7. ¿Qué servicios considera más necesarios en una plataforma de consultoría digital?

☐ Auditoría de seguridad web

☐ Protección de datos personales

☐ Asesoría legal digital

☐ Capacitación en ciberseguridad

☐ Soporte técnico especializado

☐ Otras

Cuales:.....

8. ¿Cuánto estaría dispuesto a invertir mensualmente en un servicio de consultoría digital?

☐ No pagaría

☐ \$30–\$60

☐ \$60–\$90

☐ Más de \$90

IV. Opinión Final

9. ¿Cree que una plataforma SaaS de consultoría digital contribuiría al desarrollo tecnológico y económico de Machala?

☐ Si

Porque:.....

☐ No

Porque:.....

10. ¿Estaría dispuesto a participar en un programa piloto de consultoría digital gestionado localmente?

☐ Sí

Porque:.....

☐ No

Porque:.....

Anexo 8. Encuesta validada

Figura 12

Encuesta validada aplicada a personas con conocimiento en el área en Machala

ENCUESTA SOBRE CONSULTORÍA DIGITAL EN PROTECCIÓN DE DATOS Y SEGURIDAD WEB EN MACHALA

La presente encuesta forma parte del proyecto de titulación denominado "Consultoría digital para protección de datos y seguridad web, implementada por una plataforma tecnológica de gestión de servicios en la ciudad de Machala, en el año 2026". La información recopilada será utilizada únicamente con fines académicos y se garantiza la confidencialidad de sus encuestados.

I. Digitalización y Seguridad Actual

1. ¿Su negocio o actividad utiliza plataformas digitales?

☐ Sí

☐ No

2. ¿Qué medidas de seguridad aplica actualmente en sus sistemas digitales?

☐ Antivirus básico

☐ Copias de respaldo

☐ Auditorías de seguridad

☐ Ninguna

☐ Otras

Cuales:.....

3. ¿Ha sufrido incidentes de seguridad digital en los últimos años?

☐ Sí

Cuales:.....

☐ No

II. Conocimiento de la Normativa

4. ¿Conoce la Ley Orgánica de Protección de Datos Personales vigente en el Ecuador?

☐ Sí

☐ No

5. ¿Su empresa o actividad aplica protocolos para cumplir con esta normativa Protección de Datos Personales vigente?

☐ Sí

☐ No

III. Necesidad de Consultoría Digital

6. ¿Considera que las empresas de Machala están preparadas para proteger adecuadamente los datos digitales?

☐ Si

Porque:.....

☐ No

Porque:.....

7. ¿Qué servicios considera más necesarios en una plataforma de consultoría digital?

☐ Auditoría de seguridad web

☐ Protección de datos personales

☐ Asesoría legal digital

☐ Capacitación en ciberseguridad

☐ Soporte técnico especializado

☐ Otras

Cuales:.....

8. ¿Cuánto estaría dispuesto a invertir mensualmente en un servicio de consultoría digital?

☐ No pagaría

☐ \$30-\$60

☐ \$60-\$90

☐ Más de \$90

IV. Opinión Final

9. ¿Cree que una plataforma SaaS de consultoría digital contribuiría al desarrollo tecnológico y económico de Machala?

☐ Si

Porque:.....

☐ No

Porque:.....

10. ¿Estaría dispuesto a participar en un programa piloto de consultoría digital gestionado localmente?

☐ Si

Porque:.....

☐ No

Porque:.....



Linder Bravo Mgt.
D E C I
C N 11611-5188
-NO. 7241820281

Anexo 9. Encuesta de satisfacción realizada de forma virtual

[Consultoría digital para protección de datos y seguridad web: Rellenar formulario](#)

Figura 13

Encuesta de satisfacción de forma virtual

The image shows a digital survey form titled "Consultoría digital para protección de datos y seguridad web". The form is displayed on a dark blue background with a large padlock icon and the words "INFORMATION SECURITY". The form includes a header with the title and date "29 apr 2024". Below the header, there is a section titled "Digitalización y Seguridad Actual" with three questions. Question 1 asks "¿Se realiza o activará otras acciones digitales?". Question 2 asks "¿Qué medidas de seguridad aplica actualmente en sus sistemas digitales?". Question 3 asks "¿Ha aplicado o aplicará medidas de seguridad digital en los últimos años?". The form is a Google Form, as indicated by the "Google Forms" logo in the top right corner.

Consultoría digital para protección de datos y seguridad web

29 apr 2024

CONSULTORIA DIGITAL PARA PROTECCIÓN DE DATOS Y SEGURIDAD WEB, IMPLEMENTACIÓN PARA UNA EMPRESA TECNOLÓGICA DE SERVICIOS DE SERVICIOS DE SEGURIDAD NACIONAL.

Digitalización y Seguridad Actual

1. ¿Se realiza o activará otras acciones digitales?

☐ Sí

☐ No

2. ¿Qué medidas de seguridad aplica actualmente en sus sistemas digitales?

☐ Antivirus básico

☐ Copia de seguridad

☐ Monitoreo de seguridad

☐ Ninguna

☐ Otras:

3. ¿Ha aplicado o aplicará medidas de seguridad digital en los últimos años?

☐ Sí

☐ No

4. ¿Cuáles fueron los incidentes de seguridad digitales que se le presentaron en los últimos años, si en caso su respuesta fue SI? ☐

Escriba su respuesta

5. ¿Conoce la Ley Orgánica de Protección de Datos Personales vigente en el Ecuador? ☐

☒ Si

☐ No

6. ¿Su empresa o actividad aplica protocolos para cumplir con esta normativa Protección de Datos Personales vigente? ☐

☒ Si

☐ No

7. ¿Considera que las empresas de Machala están preparadas para proteger adecuadamente los datos digitales? ☐

☒ Si

☐ No

8. ¿Considera que las empresas de Machala están preparadas para proteger adecuadamente los datos digitales? Explique Porque si selecciona la opción SI ☐

Escriba su respuesta

10. ¿Qué servicios considera más necesarios en una plataforma de consultoría digital? ☐

☐ Auditoría de seguridad web

☐ Protección de datos personales

☐ Asesoría legal digital

☐ Capacitación en ciberseguridad

☐ Sistema Monitor especializado

☐ Otros

11. ¿Cuánto estaría dispuesto a invertir mensualmente en un servicio de consultoría digital? ☐

☐ No pagaría

☐ \$10-\$50

☐ \$60-\$99

☐ Más de \$100

12. ¿Cree que una plataforma SaaS de consultoría digital contribuiría al desarrollo tecnológico y económico de Machala? ☐

☐ Si

☐ No

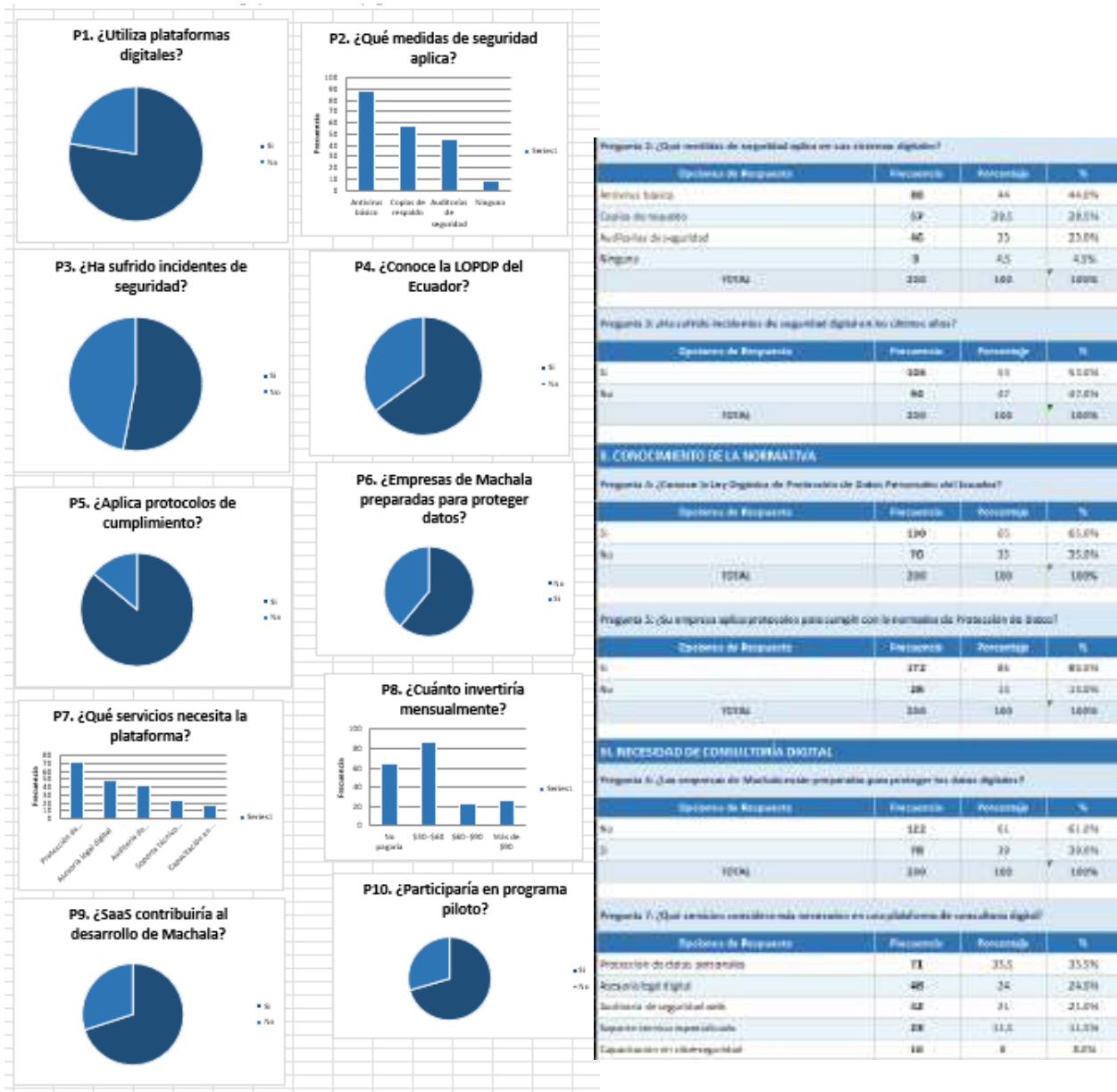
Puede imprimir una copia de su respuesta después de enviarla

Anexos 10. Base de datos

Figura 14
Tabla de preguntas

[illegible]

Figura 15
Tabulación de las preguntas



Anexos 11. Evidencia fotográfica sobre la realización de encuestas

Figura 16

Evidencia fotográfica de forma virtual y presencial





Anexos 13. Evidencia del funcionamiento de la plataforma

Canal: <https://www.youtube.com/@JustynalejandroAlvareznagu-z1t>

Figura 19

Evidencia de funcionamiento de la plataforma

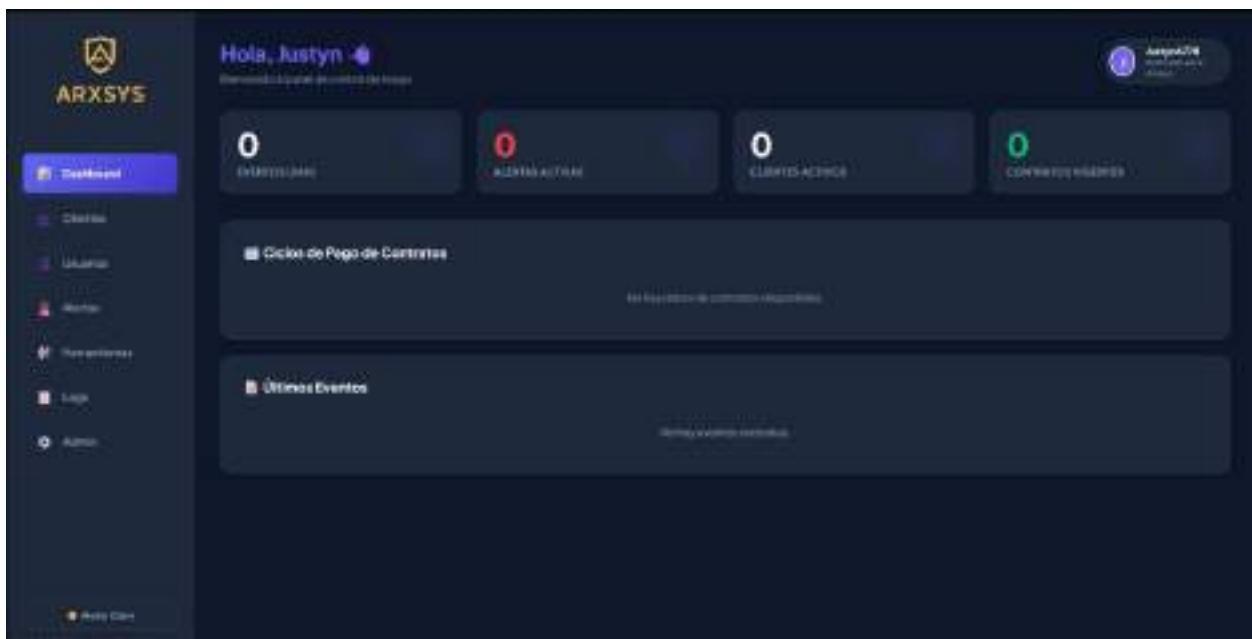


Figura 20
Evidencia de funcionamiento de la plataforma

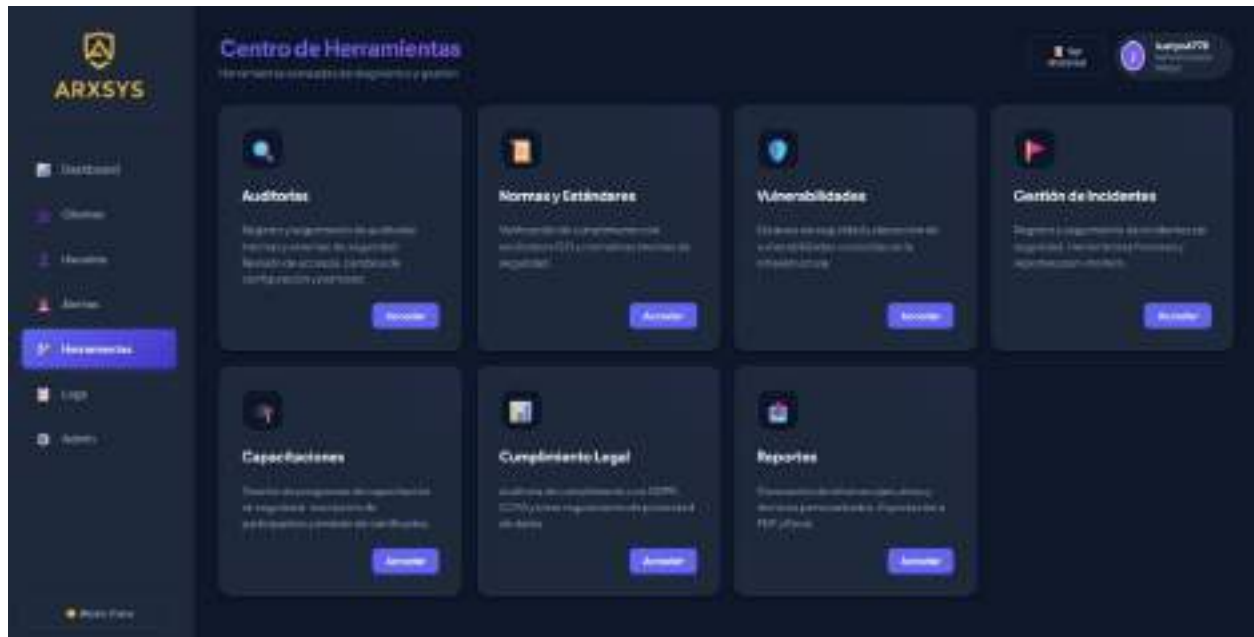
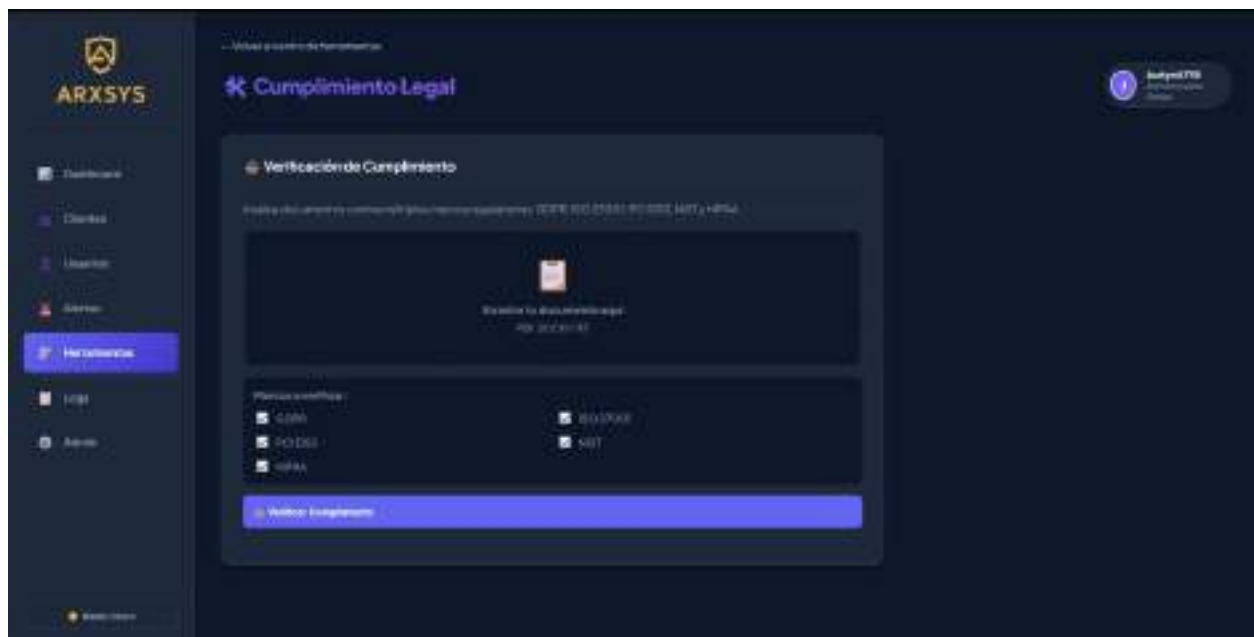


Figura 21
Evidencia de funcionamiento de la plataforma



Anexo 14. Documentos de Respaldo

Figura 23

Hoja valora del Sr. Murillo Erick

Machala.....

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 proyecto con el tema.....
Consultoría digital para protección de datos y.....
seguridad web implementada por la plataforma.....
tecnológica de gestión de servicios en la ciudad.....
Machala, en el a.m.p. 2026.....

Datos del estudiante

Apellidos y nombres:
Murillo Zambreno Erick Jesus.....

Número de cédula:
07500240467.....

Carrera:
Ciberseguridad.....

Ciclo:
Cinco.....

Modalidad:
Semi profesional.....

Sección: Diurno () Nocturno A () Nocturno B (x)
)

Por su gentil atención, me suscribo.

Figura 22 Hoja valorada del Sr. Alvarez Justyn


INSTITUTO SUPERIOR TECNOLÓGICO
SUDAMERICANO
MACHALA

Machala.....

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 anteproyecto con el tema.....
Consultoría digital para protección de datos y.....
Seguridad Web, implementada por una plataforma
tecnológica de gestión de servicios en la ciudad
Machala, en el año 2026.....

Datos del estudiante

Apellidos y nombres:
Alvarez Magun Justyn Alejandro.....

Número de cédula:
0326003343.....

Carrera:
Ciberseguridad.....

Ciclo:
Cinco.....

Modalidad:
Semi presencial.....

Sección: Diurno () Nocturno A () Nocturno B (x)
)

Por su gentil atención, me suscribo.