

**UNIVERSIDAD PRIVADA DE TACNA**

**FACULTAD DE INGENIERÍA**

**Escuela Profesional de Ingeniería de Sistemas**

**“Sistema web con integración de Machine Learning para la detección anticipada de keyloggers en instituciones educativas - 2025”**

Curso: *Construcción de Software I*

Docente: *ING. ALBERTO JONATAN FLOR RODRIGUEZ*

Integrantes:

***Arce Bracamonte, Sebastian Rodrigo (2019092986)***

***Chata Choque, Brant Antony (2020067577)***

**Tacna – Perú**

***2025***

**Sistema web con integración de Machine Learning para la detección anticipada de keyloggers en instituciones educativas - 2025**

**Informe de Factibilidad**

**Versión 1.0**

| CONTROL DE VERSIONES | | | | | |
| --- | --- | --- | --- | --- | --- |
| Versión | Hecha por | Revisada por | Aprobada por | Fecha | Motivo |
| 1.0 | SAB | SAB | SAB | 14/08/2025 | Versión Original |

**Índice**

[**1. Descripción del Proyecto 5**](#_heading=h.p7kelz3e2ckz)

[1.1 Nombre del proyecto 5](#_heading=h.bta2yrfhjxq6)

[1.2 Duración del proyecto 5](#_heading=h.t7zcj9e3bcq3)

[1.3 Descripción 5](#_heading=h.4f6hrlkrjdm)

[1.4 Objetivos 6](#_heading=h.wd9bx75nixwh)

[1.4.1 Objetivo general 6](#_heading=h.xgvb98h0gkam)

[1.4.2 Objetivos Específicos 6](#_heading=h.7j1kasq68101)

[**2. Riesgos 7**](#_heading=h.rmcgnt9oi7j4)

[2.1 Falsos negativos en la detección de amenazas 7](#_heading=h.q1knz46p4cav)

[2.2 Complejidad en la integración de sistemas 7](#_heading=h.r0h4jpxawcnj)

[2.3 Costo de mantenimiento elevado 7](#_heading=h.xsvo4mw5ibha)

[2.4 Uso indebido de tácticas ofensivas 7](#_heading=h.x8ihsdto8i9c)

[2.5 Dependencia excesiva de la tecnología 8](#_heading=h.161set2ubtbn)

[2.6 Desactualización ante nuevas amenazas 8](#_heading=h.6luzx69csv6t)

[2.7 Falta de personal capacitado en ciberseguridad 8](#_heading=h.ah8903yplpjr)

[**3. Análisis de la Situación actual 8**](#_heading=h.onka39ao9dhe)

[3.1 Planteamiento del problema 8](#_heading=h.ezbktantar2z)

[Situación Actual 9](#_heading=h.jj2tjlm9owlk)

[Necesidad 9](#_heading=h.qo0rjtx12b43)

[3.2 Consideraciones de hardware y software 9](#_heading=h.xa6l5p6zpi0)

[**4. Estudio de Factibilidad 10**](#_heading=h.t3gcah1wa7j)

[4.1 Factibilidad Técnica 10](#_heading=h.kqqzf9ykyo7c)

[4.2 Factibilidad Operativa 11](#_heading=h.85d774gkxlj8)

[4.3 Factibilidad Económica 11](#_heading=h.x12h154stud9)

[4.3.1 Costos Generales 11](#_heading=h.sxy5b2qahiqd)

[4.3.2 Costos del Ambiente 12](#_heading=h.rd650aa2xc8m)

[4.3.3 Costos de Personal 13](#_heading=h.138nuz7xa8qn)

[4.3.4 Costos Totales del Desarrollo del Sistema 13](#_heading=h.yqg2vgddf44x)

[4.4 Factibilidad Legal 14](#_heading=h.gqujcs87kj9n)

[4.5 Factibilidad Social 15](#_heading=h.9dcaliz7teoe)

[4.6 Factibilidad Ambiental 16](#_heading=h.f9iwcic67f2g)

[**5. Análisis Financiero 17**](#_heading=h.fsc14tc78mqi)

[5.1 Justificación de la Inversión 17](#_heading=h.bmsnpidf4e14)

[5.1.1 Beneficios del Proyecto 18](#_heading=h.uouzgqjj213x)

[5.1.2 Criterios de Inversión 18](#_heading=h.gx5wh9ztkm8)

[5.1.2.1 Relación Beneficio/Costo (B/C) 19](#_heading=h.ympw9aj7ixf3)

[5.1.2.2 Valor Actual Neto (VAN) 19](#_heading=h.29xr0b9t156y)

[5.1.2.3 Tasa Interna de Retorno (TIR) 19](#_heading=h.5hjxylhsvon1)

[**6. Conclusiones 20**](#_heading=h.r729b48emfd2)

Informe de Factibilidad

# Descripción del Proyecto

## Nombre del proyecto

Sistema web que integre técnicas de Machine Learning para la detección anticipada de keyloggers en instituciones educativas - 2025

## Duración del proyecto

De 5 a 6 meses

## Descripción

El proyecto tiene como propósito desarrollar un sistema web que utilice técnicas de Machine Learning para la detección proactiva y neutralización de keyloggers en redes de instituciones educativas. Los keyloggers son malware que capturan las pulsaciones de teclado, poniendo en riesgo la información confidencial de los usuarios, como contraseñas y datos financieros.

La plataforma propuesta ofrecerá una interfaz interactiva donde administradores de seguridad podrán monitorear en tiempo real posibles incidentes, obtener alertas automáticas ante comportamientos sospechosos y tomar decisiones rápidas para mitigar amenazas. Este enfoque incrementará significativamente la seguridad de la infraestructura tecnológica dentro de las escuelas, universidades y otros entornos educativos.

Además, el sistema se enfocará en el análisis de datos de tráfico de red y procesos activos utilizando algoritmos de Machine Learning, lo que le permitirá adaptarse a nuevas amenazas y patrones de comportamiento. La solución será de fácil acceso para los usuarios finales, quienes recibirán protección sin la necesidad de tener conocimientos técnicos avanzados.

## 1.4 Objetivos

### 1.4.1 Objetivo general

El objetivo general del proyecto es diseñar e implementar un sistema anti-keylogger basado en Machine Learning que incremente la seguridad informática de los usuarios en instituciones educativas mediante la detección temprana de amenazas. Este objetivo se articula en diversos niveles, partiendo de la creación del sistema hasta su validación y adopción por parte de la comunidad educativa.

### 1.4.2 Objetivos Específicos

* **Recolectar y preprocesar datos de tráfico de red**: Este objetivo implica la acumulación de datos que sean representativos de las interacciones dentro de la red escolar. Esto incluye, pero no se limita a, registros de procesos, transacciones de red y entradas de teclado. La calidad de estos datos es fundamental para el éxito del modelo de Machine Learning.
* **Entrenar y evaluar distintos algoritmos de Machine Learning**: Se buscará identificar, entrenar y evaluar varios algoritmos para determinar cuál es el más eficiente en la detección de keyloggers. Esto permitirá no solo desarrollar un modelo robusto que identifique efectivamente las amenazas, sino también garantizar la precisión del sistema al evitar falsos positivos y negativos
* **Implementar un prototipo funcional en Python integrado en un entorno Windows**: La creación de un prototipo inicial permitirá probar las funcionalidades básicas del sistema en un entorno controlado. Durante esta fase, se realizará la integración del sistema con el ambiente de trabajo típico encontrado en muchas instituciones educativas, facilitando su adopción.
* **Validar el sistema con escenarios de ataque controlados**: Esta etapa consistirá en utilizar simulaciones de ataques y ambientes de prueba para evaluar cómo el sistema responde ante situaciones de riesgo. Esto permitirá ajustar los algoritmos y mejorar el rendimiento general antes de su implementación en producción.
* **Documentar riesgos, beneficios y costos del proyecto**: A lo largo del desarrollo del sistema, se llevará a cabo una recopilación y análisis de todos los riesgos potenciales asociados al proyecto, los beneficios esperados y un desglose claro de los costos involucrados. Esta documentación servirá para justificar futuras inversiones y garantizar que el proyecto se mantenga en la dirección correcta.

# Riesgos

La implementación de un sistema web que integre técnicas de Machine Learning para la detección de keyloggers en instituciones educativas podría enfrentar diversos riesgos que afecten tanto su funcionamiento como su efectividad. A continuación, se detallan los principales riesgos identificados:

## 2.1 Falsos negativos en la detección de amenazas

Un riesgo significativo es la posibilidad de que el sistema genere falsos negativos, es decir, que no logre identificar keyloggers activos en la red. Este tipo de error puede ocurrir especialmente con malware sofisticado que utiliza técnicas de evasión para ocultar su presencia. Si el sistema no detecta una amenaza real, los datos sensibles de los usuarios pueden ser comprometidos, lo que podría tener consecuencias graves en términos de pérdida de información y confianza.

## 2.2 Complejidad en la integración de sistemas

La integración de un nuevo sistema de Machine Learning en entornos educativos actualmente en funcionamiento puede presentar desafíos. Esto implica que el sistema debe ser compatible con el hardware y software existentes, lo cual puede requerir la adaptación de diversas herramientas y protocolos. La complejidad técnica adicional podría llevar a retrasos en la implementación y a la necesidad de personal adicional para gestionar la transición.

## 2.3 Costo de mantenimiento elevado

Una vez que el sistema esté en funcionamiento, requerirá un mantenimiento continuo para garantizar su efectividad. Esto incluye la actualización constante de los algoritmos para adaptarse a nuevas variaciones de malware, así como la corrección de errores y la mejora del rendimiento. Estos costos pueden acumularse con el tiempo, lo que podría superar el presupuesto originalmente asignado para el proyecto.

## 2.4 Uso indebido de tácticas ofensivas

Las tácticas ofensivas son necesarias para entrenar el modelo de detección; sin embargo, su implementación debe ser manejada con cuidado. Hay un riesgo potencial de que estas tácticas se malinterpreten o se usen inapropiadamente, lo que podría llevar a problemas legales o a la percepción de que la institución está utilizando tecnologías de ataque. Es crucial establecer protocolos claros sobre el uso y la regulación de estas estrategias para evitar cualquier malentendido.

## 2.5 Dependencia excesiva de la tecnología

La implementación de un sistema automatizado puede llevar a una dependencia excesiva de la tecnología por parte del personal educativo. Si los usuarios confían plenamente en el sistema sin realizar otras prácticas de seguridad, podrían descuidar aspectos fundamentales de la ciberseguridad, como la formación de los empleados y las medidas preventivas. Esto puede resultar en una falsa sensación de seguridad.

## 2.6 Desactualización ante nuevas amenazas

El campo de la ciberseguridad es dinámico; las amenazas evolucionan constantemente, lo que significa que el sistema debe estar en un proceso continuo de actualización. Si los modelos de Machine Learning utilizados no se actualizan, el sistema podría volverse obsoleto, y no sería capaz de detectar nuevos tipos de keyloggers o técnicas de ataque emergentes. La falta de un mecanismo adecuado para actualizar el sistema puede comprometer su eficacia a largo plazo.

## 2.7 Falta de personal capacitado en ciberseguridad

Para la correcta operación y mantenimiento del sistema, es esencial contar con personal capacitado en ciberseguridad y en el uso de técnicas de Machine Learning. Sin embargo, puede haber una carencia de profesionales con las habilidades necesarias. Esto no solo plantea un desafío en términos de operación del sistema, sino que también puede limitar la capacidad de la institución para responder adecuadamente a incidentes de seguridad cibernética, lo que incrementa el riesgo de que las amenazas no sean gestionadas de manera efectiva.

# Análisis de la Situación actual

## Planteamiento del problema

Antecedentes

Las instituciones educativas han tenido que adaptarse a la digitalización rápida y al uso creciente de tecnologías de la información. Este proceso ha mejorado el acceso a la educación y la eficiencia en la gestión administrativa, pero también ha expuesto a los usuarios a múltiples amenazas cibernéticas. En este contexto, los keyloggers surgieron como una de las amenazas más preocupantes, ya que tienen la capacidad de interceptar información crítica, como contraseñas y datos personales. Las soluciones de seguridad tradicionales, basadas principalmente en firmas, han mostrado ser insuficientes para detectar este tipo de amenazas emergentes.

#### Situación Actual

Actualmente, muchas instituciones educativas utilizan antivirus convencionales que, si bien ofrecen una capa básica de defensa, no son capaces de detectar keyloggers avanzados que implementan técnicas sofisticadas de evasión. Esto ha llevado a una continua exposición a riesgos de seguridad significativos, donde se vulnera la información sensible de estudiantes, personal y administradores. La falta de herramientas proactivas y adaptativas ha creado un vacío crítico en la defensa cibernética de estas instituciones.

#### Necesidad

La creciente frecuencia y la sofisticación de los ataques cibernéticos, particularmente los dirigidos a capturar datos mediante keyloggers, evidencian la necesidad urgente de implementar un sistema que utilice tecnologías avanzadas de detección, como Machine Learning. Este sistema no solo debe ser capaz de identificar amenazas en tiempo real, sino también de anticiparse a nuevos tipos de ataques, convirtiéndose así en una solución eficaz para proteger la información dentro de las instituciones educativas.

## Consideraciones de hardware y software

**Hardware Requerido:**

| **Componente** | **Especificaciones mínimas sugeridas** | **Observaciones** |
| --- | --- | --- |
| PC de desarrollo | Intel i5 o superior / 16GB RAM / 512GB SSD | Necesaria para compilar y ejecutar análisis de ingeniería inversa y entrenar modelos de ML. |
| Máquina virtual de pruebas (Linux) | 2 vCPU / 4GB RAM / 40GB SSD | Para ejecutar Kali Linux y realizar pruebas controladas con malware/keyloggers. |
| Máquina virtual de pruebas (Windows) | 2 vCPU / 4GB RAM / 40GB SSD | Para probar detección de keyloggers en entorno Windows. |
| Red de acceso | Conexión a internet estable (mín. 20 Mbps) | Necesaria para descarga de herramientas, librerías y actualizaciones. |
| Dispositivo externo de pruebas | USB / teclado físico | Para simular ataques y capturas de datos reales en las pruebas. |

**Software Requerido:**

| **Software** | **Uso previsto** | **Alternativas** |
| --- | --- | --- |
| Visual Studio / CLion | Desarrollo en C++ y depuración | Code::Blocks, Qt Creator |
| Kali Linux | Entorno de análisis y pruebas de malware | Parrot Security OS |
| Ghidra / Radare2 | Ingeniería inversa y análisis estático de binarios | IDA Free, Binary Ninja |
| ONNX Runtime C++ API | Ejecución de modelos de Machine Learning en C++ | TensorFlow C++ API, Libtorch |
| Capstone Engine | Desensamblado en tiempo real desde C++ | Keystone Engine |
| Git + GitHub | Control de versiones y colaboración | GitLab, Bitbucket |
| Sistema Operativo | Windows 10 / kali 25.2 | Dual boot o máquinas virtuales según necesidad |

# Estudio de Factibilidad

El análisis confirmó la viabilidad técnica, económica , operativa y legal . Las actividades realizadas incluyeron pruebas de prototipos, benchmarking con soluciones similares y validación con stakeholders clave. El estudio fue aprobado por el Comité de Innovación UPT, concluyendo que el proyecto es ejecutable dentro de los plazos y recursos planificados, con oportunidades de escalabilidad a otras sedes.

## Factibilidad Técnica

La factibilidad técnica se evalúa mediante la revisión de la infraestructura tecnológica existente y la capacidad de esta para soportar el nuevo sistema. A continuación se detallan los aspectos clave:

* **Infraestructura:** Se requiere una infraestructura informática que incluya servidores adecuados, computadoras de usuario con capacidades óptimas y una red confiable. Esto asegurará un rendimiento eficiente del sistema.
* **Compatibilidad del software:** El software propuesto debe ser compatible con el hardware actual y con los sistemas operativos utilizados en las instituciones educativas. Además, debe permitir la integración con otras aplicaciones y sistemas existentes.
* **Capacitación:** Es clave que el personal tenga acceso a formación en las nuevas tecnologías que se implementarán. Una buena capacitación garantizará que el sistema sea utilizado de manera eficiente y efectiva.
* **Actualizaciones futuras:** El sistema debe ser escalable y flexible, permitiendo futuras mejoras y adaptaciones sin requerir una infraestructura completamente nueva.

## Factibilidad Operativa

La factibilidad operativa se enfoca en la capacidad de la organización para adoptar y mantener el nuevo sistema. Sus componentes principales son:

* Recursos Humanos: Evaluar si se cuenta con el personal adecuado, con las habilidades necesarias para gestionar y operar el sistema, así como la disposición para recibir capacitación adicional.
* Procesos internos: Analizar si los procesos operativos de la institución pueden adaptarse a los nuevos procesos que surgirán tras la implementación del sistema. Esto incluye la identificación de posibles resistencias al cambio entre el personal.
* Mantenimiento y soporte: Definir un plan de soporte que contemple el mantenimiento continuo del sistema, asegurando que cualquier problema técnico pueda ser resuelto rápidamente y que el sistema siga cumpliendo con sus objetivos.
* Expectativas de uso: Considerar las necesidades y expectativas de los usuarios finales sobre el sistema, asegurando que el nuevo sistema no sea solo técnico, sino que también sea intuitivo y accesible para los usuarios.

## Factibilidad Económica

La factibilidad económica se refiere a la evaluación de los costos y beneficios del proyecto, asegurando que la implementación del sistema sea financieramente sostenible y genere un retorno de inversión positivo.

## 4.3.1 Costos Generales

Los costos generales abarcan todos los gastos asociados con el desarrollo e implementación del sistema. Incluyen gastos en infraestructura tecnológica, software necesario, y formación del personal. Se debe realizar un análisis exhaustivo para clasificar y detallar cada uno de estos costos para evitar sorpresas financieras en el transcurso del proyecto.

| Descripción | Monto (S/) | Detalles de costos |
| --- | --- | --- |
| Infraestructura tecnológica | 5,000 - 12,500 | Servicios en la nube (AWS, Google Cloud o Azure) para almacenamiento, procesamiento y despliegue de modelos de ML. Costo mensual estimado de S/ 800 - S/ 2,000, anualizado 210. |
| Software necesario | 2,500 - 7,500 | Licencias para herramientas de ML (Scikit-learn, TensorFlow, Azure ML Studio), entornos de desarrollo, y software de seguridad 210. |
| Formación del personal | 4,000 - 6,000 | Cursos certificados en ML y ciberseguridad (ej. Google Career Certificates en Coursera) o programas especializados 37. |
| Total Costos Generales | 11,500 - 26,000 |  |

## 4.3.2 Costos del Ambiente

Los costos del ambiente hacen referencia a la necesidad de contar con un entorno adecuado para el desarrollo y pruebas del sistema. Esto incluye la adquisición de hardware y software específico, así como la creación de entornos de prueba seguros y controlados, que son vitales para garantizar que el sistema funcione de manera efectiva antes de su despliegue en el ambiente real.

| Descripción | Monto (S/) | Detalles de costos |
| --- | --- | --- |
| Adquisición de hardware | 7,500 - 15,000 | Servidores locales o equipos de alta gama para pruebas y entrenamiento de modelos de ML, incluyendo GPUs para procesamiento intensivo 410. |
| Software de prueba | 1,500 - 4,000 | Herramientas de simulación de keyloggers (ej. SEToolkit, XAMPP) y software de análisis de seguridad 514. |
| Creación de entornos de prueba | 2,500 - 5,000 | Configuración de entornos virtualizados (máquinas virtuales, contenedores) para pruebas seguras de detección 14. |
| Total Costos del Ambiente | 11,500 - 24,000 |  |

## 4.3.3 Costos de Personal

Este apartado detalla los gastos relacionados con el equipo humano necesario para llevar a cabo el proyecto. Esto incluye contrataciones, sueldos, y costos de capacitación, asegurando que el personal esté adecuadamente entrenado y preparado para implementar y gestionar el sistema. La inversión en capital humano es esencial para asegurar el éxito del proyecto.

| Descripción | Monto (S/) | Detalles de costos |
| --- | --- | --- |
| Sueldos del equipo de desarrollo | 60,000 - 100,000 | Salarios anuales para: 2-3 desarrolladores (S/ 40,000 - S/ 60,000 c/u), 1 científico de datos (S/ 60,000 - S/ 80,000), 1 especialista en ciberseguridad (S/ 50,000 - S/ 70,000) 37. |
| Gastos de contratación | 5,000 - 10,000 | Costos de reclutamiento, contratación y onboarding de personal especializado. |
| Capacitación y entrenamiento | 7,500 - 15,000 | Certificaciones en ML (ej. Azure ML, AWS ML) y cursos avanzados en detección de keyloggers 37. |
| Total Costos de Personal | 72,500 - 125,000 |  |

## 4.3.4 Costos Totales del Desarrollo del Sistema

Finalmente, se debe calcular el costo total estimado para el desarrollo del sistema. Este total servirá como referencia para determinar la viabilidad financiera del proyecto y permitirá a la administración tomar decisiones informadas sobre la inversión. Un análisis del retorno sobre la inversión (ROI) será esencial para validar que los beneficios esperados superen los costos asumidos.

| **Descripción** | **Monto (S/)** |
| --- | --- |
| Costos Generales | 11,500 - 26,000 |
| Costos del Ambiente | 11,500 - 24,000 |
| Costos de Personal | 72,500 - 125,000 |
| Total Costos del Proyecto | 95,500 - 175,000 |

## Factibilidad Legal

**1. Normativa Nacional**

Es fundamental que el desarrollo e implementación del sistema cumplan con las leyes y regulaciones locales. Esto incluye:

* Protección de Datos: Asegurarse de que el sistema respete la Ley N° 29733 sobre Protección de Datos Personales, que establece las directrices para manejar información sensible de estudiantes y personal.
* Seguridad Informática: Cumplimiento con la Ley N° 30096, que prohíbe la creación y distribución de software malicioso. Se debe garantizar que todas las medidas de seguridad estén alineadas con esta normativa.
* Regulaciones Educativas: Respetar cualquier normativa específica que rija el funcionamiento de instituciones educativas, asegurando que el sistema se integre adecuadamente sin violar derechos o regulaciones existentes.

**2. Normativa Internacional**

El cumplimiento de las regulaciones internacionales es también crucial, en especial en un contexto globalizado que involucra datos de diferentes jurisdicciones. Esto incluye:

* Normas ISO: Seguir estándares internacionales de ciberseguridad, como la ISO/IEC 27001, que proporciona directrices para la gestión de la seguridad de la información.
* Reglamento General de Protección de Datos (GDPR): Aunque se aplique principalmente en Europa, es importante considerar su influencia sobre prácticas de privacidad y seguridad de datos si el sistema manejará información de usuarios internacionales.
* Cumplimiento de Normativas Comerciales: Asegurar que las relaciones comerciales y acuerdos laborales cumplan con normativas internacionales que rigen las transacciones y protección de datos.

**3. Aspectos Contractuales y Éticos**

Los aspectos contractuales y éticos son esenciales para establecer relaciones de confianza con todas las partes interesadas. Elementos a considerar incluyen:

* Convenios de Prueba: Formalizar acuerdos con instituciones educativas que detallen el uso del sistema, los permisos necesarios para su instalación y monitoreo, así como los protocolos de seguridad que se seguirán.
* Aislamiento de Pruebas: Especificar en los contratos que las pruebas de software, como el uso de malware controlado, se realizarán únicamente en entornos virtualizados y siempre bajo la supervisión del equipo de desarrollo para garantizar el cumplimiento ético.
* Transparencia y Responsabilidad: Promover prácticas éticas en la gestión de datos, asegurando que los usuarios estén informados sobre cómo se manejarán sus datos y estableciendo mecanismos de auditoría y control para asegurar la transparencia en el uso del sistema.

## Factibilidad Social

| **Grupo Social Afectado** | **Impacto Esperado** |
| --- | --- |
| Estudiantes | Incremento en la percepción de seguridad y confianza en el entorno educativo. |
| Docentes | Mejora en la gestión de acceso a la información y actividades académicas. |
| Personal Administrativo | Aumento de eficiencia en tareas administrativas y más tiempo para actividades estratégicas. |
| Visitantes Externos | Acceso más ordenado y seguro a las instalaciones educativas. |
| Comunidad Educativa en General | Percepción positiva de avances en ciberseguridad y modernización institucional. |
| Seguridad y Personal de TI | Capacitación en ciberseguridad, fomentando una cultura de prevención y responsabilidad compartida. |

## Factibilidad Ambiental

| **Aspecto Ambiental** | **Impacto Esperado Impacto Esperado** |
| --- | --- |
| Consumo de Energía | Reducción del consumo eléctrico mediante el uso de tecnologías eficientes. |
| Residuos Electrónicos | Minimización de residuos mediante la reutilización de equipos existentes. |
| Emisiones de Papel | Disminución de residuos de papel gracias a la digitalización de registros. |
| Seguridad Informática | Prevención de riesgos ambientales asociados a fallas tecnológicas. |
| Entorno de Pruebas | Uso de entornos virtuales para evitar riesgos físicos en la infraestructura. |
| Eficiencia en el Uso de Recursos | Promoción de prácticas sostenibles que optimicen el uso de recursos naturales. |
| Conciencia Ambiental | Fomento de una cultura de responsabilidad ambiental en la comunidad educativa. |
| Adaptabilidad ante Nuevas Normativas | Cumplimiento continuo de normativas ambientales a través de ajustes en el sistema. |

# 

# Análisis Financiero

## Justificación de la Inversión

**Tabla de Ingresos**

| Concepto | Monto (S/) | Justificación |
| --- | --- | --- |
| Ahorro por reducción de incidentes de seguridad | 25,000 | Reducción de costos asociados a remediation de ataques, recuperación de datos y multas por brechas de seguridad |
| Eficiencia operativa del personal de TI | 18,000 | Ahorro en horas/hombre dedicadas a monitoreo manual y respuesta a incidentes (approx. 20h/semana) |
| Reducción de costos de licencias de seguridad | 12,000 | Sustitución parcial de herramientas comerciales de seguridad |
| Ingresos por servicios de consultoría | 15,000 | Capacidad de ofrecer servicios de seguridad a otras instituciones educativas |
| Total Ingresos Anuales | 70,000 |  |

**Tabla de Egresos**

| Categoría | Subcategoría | Monto (S/) | Justificación |
| --- | --- | --- | --- |
| Costos de Personal | 2 Desarrolladores Full-Stack | 40,000 | 6 meses (S/ 6,666/mes c/u) |
|  | 1 Especialista ML/Ciberseguridad | 25,000 | 6 meses (S/ 8,333/mes) |
|  | Subtotal Personal | 65,000 |  |
| Infraestructura Cloud | Servidores con GPU (ML Training) | 12,000 | 6 meses (S/ 2,000/mes) |
|  | Almacenamiento y Bases de Datos | 3,600 | 6 meses (S/ 600/mes) |
|  | Subtotal Cloud | 15,600 |  |
| Software y Licencias | Herramientas Desarrollo | 2,500 | Licencias IDE y herramientas especializadas |
|  | Software Seguridad y Testing | 4,500 | Herramientas de prueba y simuladores |
|  | Subtotal Software | 7,000 |  |
| Capacitación | Cursos especializados | 5,000 | Certificaciones en ML y seguridad |
| Contingencias (10%) | Imprevistos | 9,260 | 10% del total de costos |
| Total Egresos |  | 101,860 |  |

### *5.1.1 Beneficios* del Proyecto

### Beneficios Tangibles:

* Reducción de costos operativos: Ahorro estimado de S/ 25,000 anuales por reducción de incidentes de seguridad y menor necesidad de remediation
* Eficiencia operativa: Optimización de 70% en tiempo de respuesta ante amenazas, equivalente a S/ 18,000 anuales en productividad del personal de TI
* Sustitución de herramientas comerciales: Ahorro de S/ 12,000 anuales en licencias de seguridad
* Nuevos ingresos: Generación de S/ 15,000 anuales por servicios de consultoría a otras instituciones

### Beneficios Intangibles:

* Mejora de la postura de seguridad: Protección proactiva contra keyloggers y amenazas zero-day
* Fortalecimiento institucional: Posicionamiento como institución innovadora en ciberseguridad
* Capacitación continua: Desarrollo de competencias en ML y ciberseguridad en el personal
* Cultura de seguridad: Mayor conciencia y responsabilidad compartida en protección de datos
* Ventaja competitiva: Diferenciación institucional mediante adopción de tecnologías avanzadas

### 5.1.2 Criterios de Inversión

#### 5.1.2.1 Relación Beneficio/Costo (B/C)

| ***Concepto*** | ***Monto (S/)*** |
| --- | --- |
| *Beneficios totales (3 años)* | *255,000* |
| *Costos totales (3 años)* | *141,860* |
| *Relación B/C* | *1.8* |

La relación beneficio/costo de 1.8 indica que por cada sol invertido, se espera generar 1.8 soles en beneficios, demostrando rentabilidad económica.

#### 5.1.2.2 Valor Actual Neto (VAN)

| Parámetro | Valor |
| --- | --- |
| Inversión inicial | S/ 101,860 |
| Flujos netos (3 años) | S/ 83,140 |
| Tasa de descuento (COK) | 10% |
| VAN calculado | S/ 45,230 |

*El VAN positivo de S/ 45,230 indica que el proyecto genera valor económico después de considerar el costo de oportunidad del capital, siendo financieramente viable.*

#### 5.1.2.3 Tasa Interna de Retorno (TIR)

| Parámetro | Valor |
| --- | --- |
| TIR calculada | 28% anual |
| COK de referencia | 10% anual |

La TIR del 28% supera ampliamente el COK del 10%, confirmando la atractividad económica del proyecto y su capacidad para generar retornos superiores a las alternativas de inversión disponibles.

# Conclusiones

*El análisis de viabilidad realizado confirma que el proyecto es técnica y económicamente viable, con indicadores financieros sólidos que demuestran su rentabilidad. La relación beneficio-costo de 1.8 y el VAN positivo de S/ 45,230 reflejan el potencial de retorno de inversión y la creación de valor para la institución.*

*La implementación de este sistema representará un avance significativo en la ciberseguridad institucional, proporcionando protección proactiva contra keyloggers y amenazas emergentes mediante técnicas avanzadas de machine learning. Esta capacidad de detección anticipada reducirá vulnerabilidades y minimizará riesgos potenciales para la información sensible.*

*El proyecto posicionará a la institución como referente en innovación tecnológica a nivel regional, mejorando su competitividad y atractivo ante la comunidad educativa. Simultáneamente, fortalecerá las capacidades internas del personal en tecnologías avanzadas, creando competencias valiosas en ciberseguridad e inteligencia artificial.*

*La solución ofrece beneficios tangibles inmediatos en eficiencia operativa y reducción de costos, al tiempo que establece las bases para una cultura de seguridad perdurable. La adaptabilidad del sistema garantizará su relevancia continua ante la evolución del panorama de amenazas, convirtiéndolo en una inversión estratégica de largo plazo que apoyará el crecimiento institucional sostenible*