

**UNIVERSIDAD PRIVADA DE TACNA**

**FACULTAD DE INGENIERÍA**

**Escuela Profesional de Ingeniería de Sistemas**

**Sistema para la Gestión y Administración de la Configuración de Software**

# Curso: Construcción de Software I

# Docente: ING. ALBERTO JONATAN FLOR RODRIGUEZ

Integrante:

| **Brant Antony Chata Choque**  **Sebastian Arce Bracamonte** | **(2020067577)**  **(2019062886)** |
| --- | --- |

**Tacna – Perú**

**2025**

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

**Documento de Visión**

**Versión 1.0**

| **CONTROL DE VERSIONES** | | | | | |
| --- | --- | --- | --- | --- | --- |
| Versión | Hecha por | Revisada por | Aprobada por | Fecha | Motivo |
| 1.0 | SAB | SAB | SAB | 20/8/2025 | Primera Versión |

**ÍNDICE GENERAL**

**Curso: Construcción de Software I 1**

**Docente: ING. ALBERTO JONATAN FLOR RODRIGUEZ 1**

[1. Introducción 6](#_heading=h.n9j8td6zd08a)

[1.1 Propósito 6](#_heading=h.6qulj1r37d8s)

[1.2 Alcance 6](#_heading=h.y1p45wt58de1)

[1.3 Definiciones, Siglas y Abreviaturas 6](#_heading=h.acsp9nraxsfm)

[1.4 Referencias 7](#_heading=h.wd3rfx6kuib4)

[2. Visión General 7](#_heading=h.uaxj65fis7ms)

[2.1 Posicionamiento 7](#_heading=h.vwnd6vfdkggy)

[2.2 Oportunidad de Negocio 8](#_heading=h.vwkbay8rxrog)

[2.3 Definición del Problema 8](#_heading=h.f12lylfte7k)

[3. Descripción de los Interesados y Usuarios 9](#_heading=h.u21wowvctv19)

[3.1 Resumen de los Interesados 9](#_heading=h.qd1i6dyjyu5e)

[3.2 Resumen de los Usuarios 10](#_heading=h.icua0cd35sb4)

[3.3 Entorno del Usuario 10](#_heading=h.pwjsi2wc6z57)

[4. Vista General del Proyecto 11](#_heading=h.3e5tbni1lof8)

[4.1 Perspectiva del Producto 11](#_heading=h.nwi7w1v2hab4)

[4.2 Resumen de Capacidades 11](#_heading=h.zgjv8h9cwymc)

[4.3 Suposiciones y Dependencias 12](#_heading=h.qj0m178l26a1)

[5. Características del Proyecto 13](#_heading=h.uxh92dpomqjn)

[6. Restricciones 13](#_heading=h.p1hugv5f7y50)

[7. Satisfacción al Cliente 14](#_heading=h.izl0v2o990p2)

[8. Rangos de Calidad 14](#_heading=h.xo8r9ifnhw94)

[9. Precedencia y Prioridad 15](#_heading=h.jt9074snrr08)

[10. Otros Requerimientos del Producto 15](#_heading=h.h72cgqoanj14)

[11. Conclusiones 15](#_heading=h.9dq4a0i14xdy)

[12. Recomendaciones 16](#_heading=h.ggqsv0pbqbyj)

## **1. Introducción**

### **1.1 Propósito**

El propósito de este documento es proporcionar una visión detallada del sistema de detección de keyloggers que se está desarrollando. Esto incluye la justificación del proyecto, los objetivos a alcanzar y las expectativas de resultados. Se busca alinear los intereses de todas las partes involucradas, definir cómo funcionará el sistema y asegurar que satisfaga las necesidades de las instituciones educativas, mejorando su seguridad cibernética

### **1.2 Alcance**

**El sistema se enfocará en:**

* **Monitoreo en Tiempo Real**: Implementación de un sistema capaz de vigilar procesos y tráfico de teclado de manera continua, identificando comportamientos sospechosos que indiquen la presencia de keyloggers.
* **Detección Automática**: Desarrollo de algoritmos de Machine Learning que permitan identificar patrones asociados con keyloggers y, así, prevenir robos de información sensible.
* **Clasificación y Respuesta**: El sistema clasificaría automáticamente las amenazas y activaría respuestas defensivas, como la cuarentena de procesos sospechosos y generación de alertas para el personal de seguridad.
* **Interacción con Usuarios:** El sistema proporcionará interfaces amigables para los administradores y usuarios finales, garantizando que cualquier persona, independientemente de su nivel técnico, pueda disfrutar de las capacidades de protección ofrecidas.
* **Capacitación y Soporte**: Ofrecer sesiones de capacitación al personal de seguridad para garantizar el uso efectivo del sistema, así como soporte continuo para resolver dudas y problemas.

### **1.3 Definiciones, Siglas y Abreviaturas**

* **ML:** Machine Learning.
* **C++:** Lenguaje de programación de bajo nivel usado para módulos de monitoreo.
* **Python:** Lenguaje de programación de alto nivel para la implementación de modelos de ML.
* **Keylogger:** Software malicioso diseñado para registrar pulsaciones de teclado.
* **API Hook:** Técnica para interceptar funciones del sistema.

### **1.4 Referencias**

* CISA. (2020). "Guide to Keyloggers". Retrieved from CISA.
* Stojanovic, J. et al. (2021). "Machine Learning for Cybersecurity A Systematic Review". International Journal of Information Security, 20(5), 445-460.
* J. Smith. (2022). "Cybersecurity Best Practices for Educational Institutions". Educational Technology Magazine, 22(3), 34-39.
* NIST. (2018). "Framework for Improving Critical Infrastructure Cybersecurity". Retrieved from NIST.

## **2. Visión General**

### **2.1 Posicionamiento**

La posición de este sistema se define por su enfoque en la detección proactiva de keyloggers, a diferencia de las soluciones tradicionales que se basan principalmente en pautas de detección de firmas. El sistema será:

**Proactivo en la Detección:** Empleará algoritmos de ML que permitirán identificar comportamientos sospechosos y patrones de ataque en tiempo real, anticipándose a las intrusiones.

**Adaptativo y Aprendizaje Continuo**: Gracias a su capacidad para aprender de nuevos datos y adaptarse a amenazas emergentes, el sistema podrá mejorar su efectividad y precisión en la detección con el tiempo.

**Integrado con Infraestructura Educativa**: Diseñado para ser implementado fácilmente en infraestructuras tecnológicas existentes en instituciones educativas, sin necesidad de reemplazar sistemas operativos o hardware.

**Orientado a Usuarios No Técnicos:** La interfaz de usuario será intuitiva, permitiendo que personal no especializado comprenda y use la herramienta eficazmente.

### **2.2 Oportunidad de Negocio**

La creciente digitalización en el ámbito educativo ha generado un aumento en el uso de plataformas electrónicas y herramientas digitales, que a su vez son vulnerables a amenazas cibernéticas. La oportunidad de negocio para este sistema radica en:

**Demanda Creciente de Seguridad Cibernética:** A medida que aumenta la concienciación sobre la importancia de la ciberseguridad, las instituciones educativas buscan soluciones innovadoras que respondan a sus desafíos únicos. Este sistema aborda directamente la necesidad crítica de proteger información sensible.

**Mercado en Expansión:** Según estudios recientes, el mercado de la ciberseguridad en el sector educativo está proyectado para crecer significativamente en los próximos años, lo que sugiere que existe un nicho sin explotar para soluciones específicas como la detección de keyloggers.

**Alianzas Estratégicas:** Las colaboraciones con empresas de tecnología, proveedores de servicios educativos y organizaciones gubernamentales pueden facilitar la adopción y promoción del sistema, maximizando su impacto.

**Modelo de Suscripción:** Considerar un modelo de negocio basado en suscripción puede asegurar ingresos recurrentes para el mantenimiento y actualización del sistema, proporcionando a las instituciones un costo predecible y adecuando su presupuesto.

### **2.3 Definición del Problema**

La proliferación de keyloggers en ambientes educativos representa un desafío crítico. Los problemas vienen dados por:

**Robo de Información Sensible:** Los keyloggers pueden capturar contraseñas, números de tarjetas de crédito y otros datos sensoriales, resultando en violaciones de privacidad y robo de identidad.

**Falta de Conciencia y Capacitación:** Muchos usuarios en instituciones educativas no son plenamente conscientes de las amenazas existentes, lo que los hace vulnerables a ataques. Esto podría llevar a resultados devastadores para la integridad de la infraestructura informativa.

**Soluciones de Seguridad Insuficientes:** Las herramientas de seguridad convencionales a menudo son inadecuadas para detectar variaciones sofisticadas de keyloggers, lo que resalta la necesidad de un enfoque más moderno y adaptativo.

**Impacto en la Confianza Institucional:** Un ataque exitoso puede dañar gravemente la reputación de una institución educativa, disminuyendo la confianza de estudiantes y padres en la capacidad de la institución para proteger su información.

## **3. Descripción de los Interesados y Usuarios**

### **3.1 Resumen de los Interesados**

Los interesados son los individuos o grupos que tienen un interés en el proyecto, ya sea a través de su participación directa o indirecta. Incluyen:

* Administración de la Institución:
  + **Interés:** Proteger la integridad de los datos y mantener la confianza de estudiantes, padres y personal.
  + **Rol**: Aprobar la implementación del sistema, asignar recursos y supervisar la efectividad de las soluciones de seguridad.
* Docentes y Personal Académico:
  + **Interés**: Asegurarse de que la información relacionada con estudiantes y actividades académicas permanezca protegida.
  + **Rol**: Utilizar el sistema para comprender y cumplir con los protocolos de seguridad durante las actividades administrativas y de enseñanza.
* Personal de TI (Tecnologías de la Información):
  + **Interés**: Garantizar que la infraestructura tecnológica sea segura y eficiente, así como tener la capacidad de responder a incidentes.
  + **Rol**: Supervisar la instalación y mantenimiento del sistema, gestionar las actualizaciones y realizar auditorías de seguridad.
* Estudiantes:
  + **Interés**: Proteger su información personal y académica.
  + **Rol**: Utilizar las plataformas digitales de la institución sin preocuparse por la seguridad de sus datos.
* Proveedores de Tecnología:
  + **Interés**: Colaborar en el desarrollo, implementación y soporte del sistema.
  + **Rol**: Proporcionar las herramientas y la tecnología necesaria para el sistema, así como asistencia técnica.

### **3.2 Resumen de los Usuarios**

Los usuarios son aquellos que interactúan directamente con el sistema, y sus experiencias y retroalimentación son cruciales para el éxito del proyecto. Incluyen:

* Administrador de Seguridad:
  + **Responsabilidades**: Configurar el sistema, monitorizar su funcionamiento y responder a cualquier actividad sospechosa identificada. Deberá tener conocimientos técnicos para gestionar ajustes y actualizaciones.
* Usuarios Finales (Docentes y Personal Administrativo):
  + **Responsabilidades**: Utilizar el sistema para gestionar sus actividades diarias, hacer seguimiento de incidentes de seguridad y beneficiarse de la protección brindada sin la necesidad de conocimientos técnicos avanzados.
* Estudiantes:
  + **Responsabilidades**: Ser conscientes de las prácticas de seguridad y reportar cualquier actividad sospechosa que puedan notar.
  + **Interacción con el sistema**: La interacción directa podría ser mínima; sin embargo, son beneficiarios de un entorno más seguro.

### **3.3 Entorno del Usuario**

El entorno donde el sistema será utilizado se caracteriza por:

* Infraestructura Tecnológica:
  + **Componentes**: Consistirá en computadoras, redes internas, dispositivos móviles y servidores donde se alojará el sistema.
  + **Compatibilidad**: Debe ser capaz de integrarse con el hardware y software existente, asegurando que la implementación no interrumpa las operaciones diarias.
* Uso de Plataformas Digitales:
  + **Actividades**: Los usuarios interactuarán con plataformas de aprendizaje y gestión educativa que serán monitoreadas por el sistema de detección de keyloggers.
  + **Requerimientos** de Seguridad: Los estudiantes y docentes utilizan estas plataformas para intercambiar y almacenar información sensible, lo que hace crucial la seguridad en estos entornos.
* Cultura Institucional:
  + **Conciencia de Seguridad**: La cultura actual de la institución respecto a la ciberseguridad variará. Por lo tanto, es vital que se proporcionen capacitaciones y recursos para fomentar una conciencia adecuada entre todos los usuarios.
  + **Actitud hacia la Tecnología**: Un entorno que favorezca la adopción tecnológica facilitará la aceptación y el uso efectivo del nuevo sistema, rompiendo las barreras relacionadas con el cambio.

## **4. Vista General del Proyecto**

### **4.1 Perspectiva del Producto**

El sistema de detección de keyloggers se posiciona como una herramienta integral de ciberseguridad específicamente adaptada para instituciones educativas.

* **Funciones Principales:**
  + Monitoreo en Tiempo Real: Permite supervisar los procesos en el sistema y el tráfico de red, identificando comportamientos anómalos que pueden indicar la presencia de keyloggers.
  + Detección Automática: Utiliza algoritmos de Machine Learning que analizan continuamente los datos y generan alertas sobre posibles amenazas en tiempo real.
  + Interfaz de Usuario Intuitiva: Diseñada para ser accesible, permitiendo a los administradores y personal sin experiencia técnica manejar el sistema con facilidad.
* **Requisitos Extensibles:**
  + El producto debe ser escalable para adaptarse a las necesidades cambiantes de las instituciones y capaz de integrarse con otras herramientas de gestión de seguridad existentes.
  + Posibilidad de actualizaciones periódicas y mejoras continuas a medida que emergen nuevas amenazas.
* **Beneficios:**
  + Mejora la seguridad de la información y la confianza de estudiantes y padres.
  + Facilita la gestión de incidentes de seguridad mediante reportes automáticos y seguimiento de eventos.

### **4.2 Resumen de Capacidades**

| Capacidad | Descripción |
| --- | --- |
| Detección Proactiva | Identifica y neutraliza keyloggers antes de que causen daños, a través de análisis en tiempo real y aprendizaje continuo de patrones de comportamiento. |
| Automatización de Respuestas | Activa medidas automáticas como el aislamiento de procesos sospechosos y envía alertas al personal de seguridad para una intervención rápida. |
| Análisis de Datos | Recopila y analiza datos sobre incidentes previos, proporcionando insights para guiar futuras estrategias de mitigación. |
| Capacitaciones Integradas | Ofrece módulos de capacitación para familiarizar a los usuarios con el sistema y protocolos de seguridad necesarios. |
| Documentación y Soporte | Incluye manuales y asistencia técnica para resolver problemas y preguntas frecuentes, garantizando un uso eficiente del sistema. |

### **4.3 Suposiciones y Dependencias**

Para la implementación exitosa del sistema, se han considerado ciertas suposiciones y dependencias que determinarán su eficacia:

* **Suposiciones:**
  + Se asume que las instituciones tienen una infraestructura tecnológica mínima, incluyendo acceso a internet y dispositivos compatibles.
  + Se espera que el personal esté dispuesto a adoptar nuevas tecnologías y participar en programas de capacitación.
  + Se considera que los algoritmos de Machine Learning implementados tendrán un rendimiento suficiente para detectar keyloggers con alta precisión.
* **Dependencias:**
  + La efectividad del sistema dependerá de la continua actualización y mantenimiento de los algoritmos frente a nuevas variantes de keyloggers y otras amenazas cibernéticas.
  + Es fundamental una colaboración estrecha entre diferentes departamentos dentro de la institución (TI, seguridad, administración) para asegurar que el sistema se implemente adecuadamente y se mantenga.
  + La capacitación y sensibilización del personal son críticos; sin ellas, los usuarios pueden no aprovechar al máximo las capacidades del sistema.

## **5. Características del Proyecto**

El proyecto de detección de keyloggers incorpora diversas características que garantizan su efectividad y adaptabilidad a las necesidades de las instituciones educativas. Algunas de las características clave incluyen:

* **Monitoreo Continuo:** El sistema operará las 24 horas del día, proporcionando vigilancia constante sobre el tráfico de red y procesos del sistema para detectar actividad sospechosa.
* **Interfaz Amigable:** Diseñada para ser intuitiva, permitirá que tanto el personal de seguridad como los administradores gestionen el sistema con facilidad, sin necesitar formación técnica avanzada.
* **Adaptabilidad a Nuevas Amenazas:** La arquitectura del sistema es escalable y se actualizará regularmente para adaptarse a diferentes tipos de keyloggers y otras amenazas cibernéticas emergentes.
* **Reportes Personalizados:** Generación de informes que detallan las actividades sospechosas, la eficacia del sistema y recomendaciones para mejorar la seguridad.
* **Integración con otras herramientas:** El sistema se diseñará para trabajar en conjunto con otras plataformas de gestión de seguridad existentes en la institución, aumentando así su eficacia general.

## **6. Restricciones**

El desarrollo e implementación del proyecto se enfrenta a ciertas restricciones que deben ser consideradas para garantizar un enfoque eficiente:

* **Recursos Limitados**: La disponibilidad de infraestructura tecnológica adecuada puede ser una limitante, especialmente en instituciones con equipos antiguos o inadecuados.
* **Capacitación del Personal:** La necesidad de entrenar a los usuarios en el uso efectivo del sistema puede ser un obstáculo si no se cuenta con el tiempo o los recursos necesarios.
* **Restricciones Presupuestarias**: Los costos de mantenimiento y actualización del sistema deben ser contemplados dentro del presupuesto anual de la institución, lo que puede limitar la inversión inicial.
* **Cumplimiento de Normativas:** Deberá asegurarse que el sistema cumpla con las regulaciones de protección de datos y otras normativas pertinentes, lo que puede implicar ajustes en su diseño e implementación.
* **Dependencia de la Tecnología:** La efectividad del sistema dependerá del correcto funcionamiento de la infraestructura tecnológica subyacente, lo que puede representar un desafío en entornos con problemas de conectividad o estabilidad del hardware.

## **7. Satisfacción al Cliente**

La satisfacción del cliente es clave para el éxito del sistema de detección de keyloggers y se abordará a través de diversas estrategias:

* **Encuestas de Satisfacción:** Se realizarán encuestas periódicas entre los usuarios (docentes, personal administrativo y estudiantes) para evaluar su experiencia y el rendimiento del sistema.
* **Capacitación y Soporte**: Se proporcionará formación continua y soporte técnico para asegurar que los usuarios puedan aprovechar al máximo las funciones del sistema y resolver dudas o problemas que puedan surgir.
* **Retroalimentación Activa:** Se establecerán canales de comunicación donde los usuarios podrán expresar sus opiniones y sugerencias sobre el sistema, permitiendo realizar mejoras continuas basadas en su experiencia.
* **Compromiso con la Mejora Continua:** Se desarrollará un plan de acción para abordar cualquier problema o área de mejora que se identifique a través de la retroalimentación y las encuestas, asegurando que el sistema evolucione con las necesidades cambiantes de los usuarios.

## **8. Rangos de Calidad**

El proyecto establece rangos de calidad que deben cumplirse para garantizar su efectividad y satisfacción del cliente. Estos rangos son:

* **Confiabilidad**: Se espera que el sistema tenga una disponibilidad del 99%, lo que significa que deberá ser accesible y funcional casi todo el tiempo, minimizando el tiempo de inactividad.
* **Eficiencia**: La detección de amenazas debe realizarse en tiempo real sin sobrecargar el CPU, asegurando que el sistema opere de manera fluida y eficiente.
* **Seguridad**: Todos los logs y datos manejados por el sistema deberán estar cifrados, y el acceso a la información sensible debe estar restringido únicamente a personal autorizado.
* **Mantenibilidad**: El código del sistema debe ser modular y bien documentado, facilitando las actualizaciones y el mantenimiento a lo largo del tiempo.
* **Usabilidad**: La interfaz de usuario debe ser intuitiva y fácil de usar, permitiendo que los usuarios gestionen el sistema sin necesidad de conocimientos técnicos avanzados.

## **9. Precedencia y Prioridad**

| Código | Requerimiento | Prioridad |
| --- | --- | --- |
| RF01 | Captura de procesos activos | Alta |
| RF02 | Monitoreo de hooks de teclado | Muy Alta |
| RF03 | Análisis de tráfico de red | Alta |
| RF04 | Clasificación ML de procesos | Muy Alta |
| RF05 | Supresión automática de keyloggers | Muy Alta |
| RF06 | Reportes y métricas de detección | Alta |

## **10. Otros Requerimientos del Producto**

Los requerimientos adicionales del producto son fundamentales para asegurar su correcto funcionamiento y alineación con las normativas existentes. Algunos de estos incluyen:

* **Estándares Legales:** Cumplimiento con normativas de protección de datos para garantizar la privacidad y seguridad de la información de los usuarios.
* **Estándares de Comunicación:** Uso de API interna y formato de logs en JSON para facilitar la integración y el procesamiento de datos.
* **Plataforma**: Compatibilidad con sistemas operativos Windows 10/11 (64 bits) para asegurar su alcance en la infraestructura existente de las instituciones educativas.
* **Seguridad**: Implementación de autenticación para administradores y cifrado AES en los reportes generados para resguardar la información sensible.

## **11. Conclusiones**

El sistema híbrido en C++ y Python con técnicas de Machine Learning para la detección y supresión automática de keyloggers es una propuesta innovadora que ofrece una solución robusta frente a las crecientes amenazas cibernéticas en las instituciones educativas. Su enfoque proactivo de seguridad permitirá no solo proteger información sensible, sino también generar confianza en el uso de tecnologías digitales. Al cumplir con os requerimientos establecidos y priorizar la usabilidad, el sistema tiene el potencial de marcar una significativa mejora en la seguridad digital de las instituciones.

## **12. Recomendaciones**

Para asegurar el éxito del proyecto y la satisfacción del cliente, se recomiendan las siguientes acciones:

* Mantenimiento y Actualización Continua: Establecer un plan de mantenimiento que incluya la actualización periódica de los algoritmos de detección y la revisión de la infraestructura tecnológica.
* Capacitación Regular del Personal: Implementar un programa de capacitación continua para los usuarios finales y el personal de seguridad, asegurando que estén familiarizados con las nuevas actualizaciones y mejoras del sistema.
* Evaluaciones de Seguridad Periódicas: Realizar auditorías y pruebas de penetración recurrentes para identificar y corregir vulnerabilidades en el sistema.
* Fomento de una Cultura de Seguridad: Promover la concienciación sobre la ciberseguridad en toda la institución, incentivando a todos los miembros de la comunidad educativa a adoptar buenas prácticas de seguridad.