	<b>Asignatura: INGENIERIA DE SOFTWARE III</b>
	<b>Grupo: B</b>
	<b>Docente: Ing. Rodrigo Castro Caicedo</b>
	<b>Estudiantes: Santiago Monroy Quiazua – Diego Mauricio Paez Gonzalez</b>
	<b>Códigos: 076231132 - 076231135</b>


### **Cifrador Biometrico (KeyBS).**

Monroy Quiazua Santiago  
Paez Gonzalez Diego Mauricio

Universidad Libre – Sede Bosque

Ingenieria de software III  
ING 22032

Ing. Castro Caicedo Rodrigo  
Marzo 2025

	<b>Asignatura: INGENIERIA DE SOFTWARE III</b>
	<b>Grupo: B</b>
	<b>Docente: Ing. Rodrigo Castro Caicedo</b>
	<b>Estudiantes: Santiago Monroy Quiazua – Diego Mauricio Paez Gonzalez</b>
	<b>Códigos: 076231132 - 076231135</b>

## **CIFRADOR BIOMETRICO (KeyBS)**

**AUTORES:**


**MONROY QUIAZUA SANTIAGO  
PAEZ GONZALEZ DIEGO MAURICIO**

**DOCENTE:**

**INGENIERO CASTRO CAICEDO RODRIGO**

**UNIVERSIDAD LIBRE – SEDE BOSQUE  
FACULTAD INGENIERIA  
CARRERA DE INGENIERIA DE SISTEMAS  
BOGOTA D.C  
MARZO 2025**


**INTRODUCCION ..... 3**

	<b>Asignatura: INGENIERIA DE SOFTWARE III</b>
	<b>Grupo: B</b>
	<b>Docente: Ing. Rodrigo Castro Caicedo</b>
	<b>Estudiantes: Santiago Monroy Quiazua – Diego Mauricio Paez Gonzalez</b>
	<b>Códigos: 076231132 - 076231135</b>

PLANTEAMIENTO DEL PROYECTO .....	4
PLANTEAMIENTO DEL PROBLEMA:.....	4
JUSTIFICACION.....	5
IMPACTO DEL PROYECTO .....	5
OBJETIVOS .....	6
OBJETIVO GENERAL: .....	6
OBJETIVOS ESPECIFICOS: .....	6
MARCO TEÓRICO.....	6
ALGORITMOS DE CIFRADO:.....	6
Cifrado simétrico: .....	6
Cifrado asimétrico: .....	7
BIOMETRIA COMO METODO DE AUTENTICACIÓN .....	7
TIPOS DE AUTENTICACIÓN BIOMETRICA: .....	7
5.3.1 Reconocimiento dactilar: .....	7
Reconocimiento facial: .....	8
Escaneo de iris: .....	8
KEYLOGGING: .....	8
PHISHING: .....	8
MALWARE: .....	8
MATRIZ DE RIESGOS.....	8
REQUERIMIENTOS FUNCIONALES Y NO FUNCIONALES .....	9
REQUERIMIENTOS FUNCIONALES: .....	9
REQUERIMIENTOS NO FUNCIONALES: .....	13
DIAGRAMAS DE CASOS DE USO.....	14
HISTORIAS DE USUARIO.....	20
RF 1: AUTOMATIZACION DE PROCESOS. ....	20
RF 2: UNIVERSALIDAD Y COMPATIBILIDAD .....	20
RF 3: REGISTRO SEGURO. ....	21
RF 4: GESTION DE INICIOS DE SESION. ....	21
RF 5: MULTIPLATAFORMA.....	21
RF 6: INVITACION A CUENTAS.....	21

## **INTRODUCCION**

En la era digital, la seguridad de la información se ha convertido en una preocupación prioritaria tanto para individuos como para empresas. El acceso a plataformas digitales, servicios financieros, redes sociales y otras aplicaciones depende en gran medida del uso de contraseñas, lo que ha generado desafíos en términos de gestión, seguridad y usabilidad. Muchos usuarios optan por

	<b>Asignatura: INGENIERIA DE SOFTWARE III</b>
	<b>Grupo: B</b>
	<b>Docente: Ing. Rodrigo Castro Caicedo</b>
	<b>Estudiantes: Santiago Monroy Quiazua – Diego Mauricio Paez Gonzalez</b>
	<b>Códigos: 076231132 - 076231135</b>

contraseñas débiles o reutilizan las mismas credenciales en múltiples plataformas, aumentando el riesgo de exposición ante ataques cibernéticos.

Los métodos tradicionales de protección, como la autenticación de dos factores (2FA) y el almacenamiento cifrado de credenciales, han mejorado la seguridad, pero siguen presentando vulnerabilidades que pueden comprometer la integridad de los datos. Ante esta problemática, surge la necesidad de una solución más segura, eficiente y fácil de usar.

El presente proyecto propone el desarrollo de KeyBS, un sistema de encriptación de contraseñas basado en autenticación biométrica, que elimina la dependencia de claves convencionales y mejora la experiencia del usuario. Mediante el uso de tecnologías avanzadas de reconocimiento biométrico, KeyBS garantizará un acceso seguro a cualquier plataforma sin necesidad de recordar múltiples contraseñas, reduciendo significativamente los riesgos asociados al robo de credenciales y accesos no autorizados.

## ***PLANTEAMIENTO DEL PROYECTO***


### ***PLANTEAMIENTO DEL PROBLEMA:***

En la actualidad, la gestión segura de contraseñas representa uno de los desafíos más comunes en la vida cotidiana de las personas. Con la proliferación de aplicaciones y servicios en línea, los usuarios se ven obligados a recordar múltiples contraseñas seguras, lo que con frecuencia conduce al olvido de credenciales, el uso de combinaciones más débiles o la reutilización de claves en distintos servicios, incrementando así el riesgo de ataques cibernéticos.

Los métodos tradicionales de seguridad, como la autenticación de dos factores (2FA) y el almacenamiento cifrado de credenciales, han demostrado ser efectivos hasta cierto punto. Sin embargo, estos mecanismos aún presentan vulnerabilidades significativas si las credenciales son comprometidas a través de técnicas como phishing, keylogging, ataques de fuerza bruta o infecciones con malware. Además, la gestión de estos métodos suele implicar un esfuerzo adicional para los usuarios, quienes deben recordar múltiples códigos o utilizar aplicaciones externas para gestionar su seguridad.

Dada esta problemática, se hace necesario desarrollar una solución innovadora que ofrezca un nivel de seguridad superior sin comprometer la comodidad del usuario. En este contexto, surge KeyBS, un sistema de encriptación de contraseñas basado en tecnología biométrica que elimina la necesidad de recordar claves tradicionales. A través de huellas dactilares o reconocimiento facial, KeyBS permitirá a los usuarios acceder a sus credenciales de manera rápida, segura y sin riesgo de olvido o vulnerabilidad ante ataques externos.

El sistema propuesto busca proporcionar una solución universal que pueda ser implementada en múltiples plataformas y aplicaciones, asegurando su compatibilidad con distintos entornos digitales. De esta manera, KeyBS se posiciona como una alternativa revolucionaria para la gestión

	<b>Asignatura: INGENIERIA DE SOFTWARE III</b>
	<b>Grupo: B</b>
	<b>Docente: Ing. Rodrigo Castro Caicedo</b>
	<b>Estudiantes: Santiago Monroy Quiazua – Diego Mauricio Paez Gonzalez</b>
	<b>Códigos: 076231132 - 076231135</b>

de contraseñas, ofreciendo tanto a usuarios individuales como a empresas una herramienta confiable para la protección de información sensible.

### **JUSTIFICACION**


El desarrollo de sistemas de encriptación de contraseñas con autenticación biométrica representa un avance significativo en el ámbito de la ciberseguridad, ¿Por qué este es diferente?, gracias a la tecnología zero trust y el enfoque que le estamos dando a nuestro proyecto, este permitirá unan interfaz gráfica que se permita usar en todos los dispositivos, y aplicaciones, sin importar su sistema operativo, ¿Cómo?, la creación de este proyecto permitirá adaptarse a cualquier dispositivo y sin importar la marca, este usara alguno de nuestros escáneres biométricos (dactilar o facial). En la actualidad, los ataques cibernéticos como el phishing, el keylogging y el malware continúan evolucionando, afectando tanto a usuarios individuales como a organizaciones que manejan información sensible. Implementar una solución como KeyBS contribuye a mitigar estas amenazas al eliminar la necesidad de introducir manualmente contraseñas y sustituirlas por un sistema de autenticación basado en datos biométricos.

Una de las principales ventajas de KeyBS radica en su capacidad para reducir la filtración de credenciales, ya que la información almacenada estará cifrada y será inaccesible sin la correspondiente verificación biométrica. Esto hace que los intentos de robo de información sean significativamente más difíciles en comparación con los métodos tradicionales de autenticación.

Asimismo, esta solución no solo está dirigida a usuarios individuales que buscan mejorar la seguridad de sus cuentas personales, sino también a empresas y organizaciones que requieren métodos de autenticación más robustos para la protección de información corporativa. La implementación de un sistema de autenticación biométrica mejora la seguridad en el entorno empresarial al eliminar la dependencia de contraseñas estáticas y reducir el riesgo de accesos no autorizados a sistemas críticos.

### **IMPACTO DEL PROYECTO**

1. **Impacto Social:** La implementación de KeyBS contribuirá a una mayor conciencia sobre la importancia de la ciberseguridad en la vida cotidiana de las personas. Al ofrecer una solución segura y accesible, permitirá que los usuarios gestionen sus credenciales sin preocupaciones, reduciendo los incidentes de fraude y robo de identidad en la sociedad.
2. **Impacto Económico:** La seguridad digital es un factor clave en la economía actual, y la adopción de KeyBS en empresas y organizaciones ayudará a reducir las pérdidas económicas derivadas de ataques cibernéticos y filtraciones de datos. Además, su implementación fomentará el desarrollo del sector tecnológico y de ciberseguridad, impulsando la creación de empleos especializados.
3. **Impacto Ambiental:** Aunque los sistemas digitales dependen de infraestructuras físicas y energéticas, KeyBS puede contribuir a la reducción del uso de papel y otros métodos físicos de autenticación, promoviendo la transición hacia un entorno digital más sostenible.

	<b>Asignatura: INGENIERIA DE SOFTWARE III</b>
	<b>Grupo: B</b>
	<b>Docente: Ing. Rodrigo Castro Caicedo</b>
	<b>Estudiantes: Santiago Monroy Quiazua – Diego Mauricio Paez Gonzalez</b>
	<b>Códigos: 076231132 - 076231135</b>

4. **Impacto Tecnológico:** La implementación de KeyBS impulsará el desarrollo de nuevas tecnologías de autenticación biométrica, fomentando la investigación e innovación en este campo. Además, al ser un sistema multiplataforma, promoverá la compatibilidad y estandarización de tecnologías de seguridad en diferentes entornos digitales.

## **OBJETIVOS**

### **OBJETIVO GENERAL:**

Desarrollar un sistema de encriptación avanzada basado en autenticación biométrica que garantice la protección de credenciales en cualquier tipo de inicio de sesión.

### **OBJETIVOS ESPECIFICOS:**

1. Definir y ejecutar un plan de pruebas integral que evalúe la seguridad del cifrado de contraseñas, asegurando su resistencia ante ataques cibernéticos mediante pruebas de penetración y validaciones criptográficas.
2. Realizar pruebas de autenticación multifactorial, verificando la efectividad y usabilidad del reconocimiento biométrico (huella dactilar o reconocimiento facial) bajo distintos escenarios de uso.
3. Evaluar la compatibilidad multiplataforma mediante pruebas de integración en diversos sistemas operativos y aplicaciones, asegurando un rendimiento óptimo en cada entorno digital.
4. Garantizar la usabilidad y experiencia del usuario mediante pruebas de interfaz y funcionalidad, identificando mejoras en la eficiencia y accesibilidad del sistema.

## **MARCO TEÓRICO**

La criptografía es una disciplina que estudia los métodos para proteger la información mediante técnicas matemáticas, impidiendo que terceros no autorizados puedan acceder o modificar los datos transmitidos o almacenados. Esta se basa en los principios de confidencialidad, integridad, autenticación y no repudio. Evitando de esta manera ataques como el keylogging, el phishing y el malware.

### **ALGORITMOS DE CIFRADO:**

Se conoce por cifrado a la técnica criptográfica que transforma algunos datos para que se conviertan en una clave ilegible, hay dos tipos de cifrados: cifrado simétrico y cifrado asimétrico.

#### **Cifrado simétrico:**

Se denomina como cifrado simétrico cuando la misma clave que se usó desde un principio para cifrar la contraseña o el mensaje, será la misma que lo descifra, algunos tipos de cifrado simétrico son:



**Asignatura: INGENIERIA DE SOFTWARE III**

**Grupo: B**

**Docente: Ing. Rodrigo Castro Caicedo**

**Estudiantes: Santiago Monroy Quiazua – Diego Mauricio Paez Gonzalez**

**Códigos: 076231132 - 076231135**

1. **AES (Advanced Encryption Standard):** Utiliza claves de 128, 192 o 256 bits y es ampliamente utilizado en sistemas de seguridad.
2. **DES (Data Encryption Standard):** Antiguamente popular, pero ahora obsoleto debido a su vulnerabilidad a ataques de fuerza bruta.
3. **Blowfish y Twofish:** Algoritmos alternativos diseñados para ofrecer alta seguridad con baja complejidad computacional.

Siendo AES (Advanced Encryption Standard) el utilizado para encriptar y cifrar las claves junto con el escáner biométrico en este proyecto.

### **Cifrado asimétrico:**

A diferencia del cifrado simétrico, este tipo de cifrado usa 2 claves diferentes, una clave publica para cifrar y una clave privada para descifrar, este tipo de cifrado se suele usar en zonas de comunicación privada y segura y en firmas digitales, se conocen algunos tipos de cifrado asimétrico, pero al no usarse dentro del proyecto, no será importante definirlos de la anterior manera como se hizo con el tipo de cifrado simétrico.

### **BIOMETRIA COMO METODO DE AUTENTICACIÓN**

La biometría como método de autenticación tiene en cuenta una premisa importante, la cual define y se basa en que cada individuo y ser, posee características únicas y singulares, por ende, la biometría, es una tecnología que permite la identificación y autenticación a través de sus características físicas, como lo son, el reconocimiento facial, escaneo de huellas dactilares o el reconocimiento específico del iris o la retina del ojo humano.

Las características biométricas deben cumplir con ciertos criterios para ser efectivas:

4. **Universalidad:** Todos los individuos deben poseer la característica biométrica.
5. **Unicidad:** Debe ser única para cada persona.
6. **Permanencia:** No debe cambiar significativamente con el tiempo.
7. **Medibilidad:** Debe ser posible capturarla y analizarla con precisión.


### **TIPOS DE AUTENTICACIÓN BIOMETRICA:**

Como se viene mencionando en el documento, existen algunos tipos de autenticación biométrica, por ejemplo: reconocimiento dactilar, reconocimiento facial, y escaneo o reconocimiento de iris:

#### **5.3.1 Reconocimiento dactilar:**

La autenticación mediante huellas dactilares se basa en la detección de los patrones únicos de cada persona. Es ampliamente utilizada debido a su:

8. Alta precisión y rapidez.
9. Bajo costo de implementación.
10. Resistencia a ataques de suplantación mediante imágenes.

	<b>Asignatura: INGENIERIA DE SOFTWARE III</b>
	<b>Grupo: B</b>
	<b>Docente: Ing. Rodrigo Castro Caicedo</b>
	<b>Estudiantes: Santiago Monroy Quiazua – Diego Mauricio Paez Gonzalez</b>
	<b>Códigos: 076231132 - 076231135</b>

### **Reconocimiento facial:**

Utiliza algoritmos de visión computacional para analizar características geométricas del rostro, como la distancia entre los ojos, la forma de la nariz y la curvatura de la mandíbula. Este método es:

11. Cómodo y sin contacto físico.
12. Vulnerable a ataques de deepfakes si no se implementan contramedidas.
13. Mejorado con inteligencia artificial y detección de profundidad.

### **Escaneo de iris:**

(Se define de igual manera el escaneo de retina o iris, aunque este, no entrara en el proyecto; este se centrara solo en la autenticación por reconocimiento dactilar y por reconocimiento facial).

El escaneo del iris analiza los patrones únicos en la estructura del ojo. Sus ventajas incluyen:

14. Extremada seguridad debido a la complejidad del iris.
15. Alta resistencia a intentos de falsificación.
16. Costo elevado en comparación con otros métodos.

### **KEYLOGGING:**

Se conoce como keylogger o keylogging a un tipo de software o un dispositivo hardware específico el cual se encarga de registrar las pulsaciones recientes que se realizan en el teclado, para posteriormente almacenarlas en un fichero o enviarlas por medio de una red en la transferencia de datos y así proceder con el robo de datos.

### **PHISHING:**

El phishing se trata de un tipo de ciberataque que se suele realizar a través de correos electrónicos, mensajes de texto, llamadas telefónicas o sitios webs fraudulentos, en donde el objetivo es robar información confidencial, como lo puede ser, números de tarjetas de crédito, contraseñas, o incluso la instalación de malware en los dispositivos.

### **MALWARE:**


Es un programa informático malicioso que daña o altera el funcionamiento de un dispositivo, el malware puede propagarse por medio de: descargas inadvertidas, ataques a vulnerabilidades de seguridad, correo electrónico, mensajería instantánea y/o dispositivos USB.

### **MATRIZ DE RIESGOS**

TABLA 1: descripción de la matriz de riesgos:

<b>TIPO DE RIESGO</b>	<b>DESCRIPCION</b>	<b>IMPACTO POTENCIAL</b>	<b>PROBABILIDAD DE OCURRENCIA</b>
-----------------------	--------------------	--------------------------	-----------------------------------



	<b>Asignatura: INGENIERIA DE SOFTWARE III</b>
	<b>Grupo: B</b>
	<b>Docente: Ing. Rodrigo Castro Caicedo</b>
	<b>Estudiantes: Santiago Monroy Quiazua – Diego Mauricio Paez Gonzalez</b>
	<b>Códigos: 076231132 - 076231135</b>

Tecnológico.	Fallos en la integración con sistemas existentes o incompatibilidad con la infraestructura actual.	Puede generar interrupciones en la operatividad y/o retrasos en la implementación del sistema.	Moderado: La integración de nuevas tecnologías conlleva riesgos inherentes de compatibilidad.
Económico.	Costos imprevistos en el desarrollo, mantenimiento o capacitación del personal.	Puede afectar el presupuesto del proyecto y su viabilidad financiera.	Moderado: Es común que surjan costos adicionales en proyectos de tecnología como este.
Operativo.	Resistencia al cambio por parte de los usuarios finales.	Puede retrasar la adopción del nuevo y actualizado sistema y disminuir la eficiencia operativa.	Alto: La resistencia al cambio es un riesgo frecuente en la implementación de nuevos sistemas tecnológicos.
Seguridad.	Posibles vulnerabilidades en el sistema que comprometan la seguridad de los datos.	Puede ocasionar fuga de información y daños a la reputación de la empresa.	Moderado: La seguridad es un aspecto crítico que requiere monitoreo constante.


TABLA 2: Matriz de riesgos en función de probabilidad y gravedad.

IMPACTO	Insignificante I	Menor II	Significativo III	Mayor IV	Severo V
Casi segura V	<b>Medio</b>	<b>Alto</b>	<b>Muy alto</b>	<b>Extremo</b>	<b>Extremo</b>
Probabilidad IV	<b>Medio</b>	<b>Medio</b>	<b>Alto</b>	<b>Muy alto</b>	<b>Extremo</b>
<b>Moderado III</b>	<b>Bajo</b>	<b>Medio</b>	<b>Medio</b>	<b>Alto</b>	<b>Muy alto</b>
<b>Poco probable II</b>	<b>Muy bajo</b>	<b>Bajo</b>	<b>Medio</b>	<b>Medio</b>	<b>Alto</b>
<b>Raro I</b>	<b>Muy bajo</b>	<b>Muy bajo</b>	<b>Bajo</b>	<b>Medio</b>	<b>Medio</b>

## REQUERIMIENTOS FUNCIONALES Y NO FUNCIONALES

### REQUERIMIENTOS FUNCIONALES:


#### RF-1: automatización de procesos

	<b>Asignatura: INGENIERIA DE SOFTWARE III</b>
	<b>Grupo: B</b>
	<b>Docente: Ing. Rodrigo Castro Caicedo</b>
	<b>Estudiantes: Santiago Monroy Quiazua – Diego Mauricio Paez Gonzalez</b>
	<b>Códigos: 076231132 - 076231135</b>

Requerimiento	RF-1
Necesidad Relacionada	Gestión y automatización de procesos
Prioridad	Alta
Caso de uso/Evento relacionado	Permitir la definición y diseño de procesos específicos del sistema.
Descripcion	Automatizar la ejecución de los procesos biométricos con la mínima interacción de parte del usuario.
Justificacion	Optimizar el rapido acceso sin involucrar la constante atencion del usuario para realizar accesiones centrales del proceso.
Origen (Interesado)	Gestion de procesos
Criterio de aceptacion / Validacion	El sistema debe permitir definir procesos personalizados de autenticación biométrica y gestionar su ejecución de manera automática.

## RF-2: Universalidad y compatibilidad

Requerimiento	RF-2
Necesidad Relacionada	Universalidad y compatibilidad con cualquier aplicación.
Prioridad	Media
Caso de uso/Evento relacionado	Permitir un conector con el input de contraseñas en cualquier inicio de sesión sin comprometer la seguridad.
Descripcion	Proveer un conector con los inputs de contraseñas usados en los login de las aplicaciones.
Justificacion	El ser capaces de proveer un uso universal para todas las aplicaciones independientemente de si hayan sido pensadas o no con el propósito de ser usadas con KeyBS es un paso importante para generar un estándar y maximizar los posibles usuarios de la aplicación.
Origen (Interesado)	Gestión comercial, Gestión de seguridad, Usuario Final

	<b>Asignatura: INGENIERIA DE SOFTWARE III</b>
	<b>Grupo: B</b>
	<b>Docente: Ing. Rodrigo Castro Caicedo</b>
	<b>Estudiantes: Santiago Monroy Quiazua – Diego Mauricio Paez Gonzalez</b>
	<b>Códigos: 076231132 - 076231135</b>


Criterio de aceptacion / Validacion	Ante cualquier input de contraseña KeyBs sea capaz de detectarlo y abrir su sistema automáticamente
-------------------------------------	---

### RF-3: Registro Seguro

Requerimiento	RF-3
Necesidad Relacionada	Registro seguro de los datos
Prioridad	Alta
Caso de uso/Evento relacionado	Asegurar y proveer un camino directo y seguro para el transporte de los datos del cliente al servidor
Descripcion	El transporte de datos debe seguir métodos y practicas seguras que permitan tener la fiabilidad de que no haya data-breaches ni alguna posibilidad de interceptar los datos.
Justificacion	Para garantizar el éxito de una aplicación de informacion sensible tales como las contraseñas debemos de asegurar que sea totalmente inaccesible para terceros no deseados.
Origen (Interesado)	Seguridad y Usuarios Finales
Criterio de aceptacion / Validacion	Los datos deben de transportarse por un canal privado siguiendo protocolos de cifrado.

### RF-4: Gestion de inicios de sesion

Requerimiento	RF-4
Necesidad Relacionada	Tener control de los sitios y cuentas que han sido ingresados en KeyBS
Prioridad	Media
Caso de uso/Evento relacionado	Permitir la gestión y visualización de las cuentas ingresadas en KeyBS
Descripcion	El sistema debe permitir a los usuarios ver dispositivos conectados y cerrar sesiones en caso de actividad sospechosa.
Justificacion	Al conectar una cuenta en KeyBS esta debe de ser capaz de guardar su información de inicio de sesión junto con su estado en KeyBS, Permitiéndonos verificar en que servicios hemos iniciado sesion.

	<b>Asignatura: INGENIERIA DE SOFTWARE III</b>
	<b>Grupo: B</b>
	<b>Docente: Ing. Rodrigo Castro Caicedo</b>
	<b>Estudiantes: Santiago Monroy Quiazua – Diego Mauricio Paez Gonzalez</b>
	<b>Códigos: 076231132 - 076231135</b>


Origen (Interesado)	gestión de Seguridad y Usuario Final
Criterio de aceptacion / Validacion	El usuario debe ser capaz de tener un control frente a sus cuentas ingresadas en KeyBS

### **RF-5: Multiplataforma**

Requerimiento	RF-5
Necesidad Relacionada	Tener variedad en los dispositivos disponibles
Prioridad	Media
Caso de uso/Evento relacionado	Permitir el uso en dispositivos IOS y ANDROID
Descripcion	Debe de ser posible utilizar KeyBS en los diferentes sistemas operativos y dispositivos, teniendo siempre en cuenta sus características exclusivas.
Justificacion	Es importante proveer el sistema a la mayor cantidad de usuarios posibles, claro, siempre teniendo en cuenta las limitaciones de los dispositivos de los usuarios
Origen (Interesado)	Gestion comercial, Usuarios finales
Criterio de aceptacion / Validacion	Uso de KeyBS en dispositivos IOS y ANDROID

### **RF-6: INVITACION A CUENTAS**

Requerimiento	RF-6
Necesidad Relacionada	Compartir cuentas con usuarios en KeyBS
Prioridad	Baja
Caso de uso/Evento relacionado	Distribuir informacion de Inicio de Sesion
Descripcion	Compartir cuentas a traves de usuarios registrados en KeyBS durante un periodo indefinido o definido.
Justificacion	Compartir cuentas de ciertas aplicaciones es un hecho del dia a dia que pasa en aplicaciones de entretenimiento, La idea de KeyBS es que sea posible compartir cuentas sin necesidad de preocuparte porque otras personas no deseadas accedan a la misma.
Origen (Interesado)	Usuarios finales
Criterio de aceptacion / Validacion	Compartir cuentas a traves de KeyBS

	<b>Asignatura: INGENIERIA DE SOFTWARE III</b>
	<b>Grupo: B</b>
	<b>Docente: Ing. Rodrigo Castro Caicedo</b>
	<b>Estudiantes: Santiago Monroy Quiazua – Diego Mauricio Paez Gonzalez</b>
	<b>Códigos: 076231132 - 076231135</b>

## REQUERIMIENTOS NO FUNCIONALES:

### RNF-1: Documentabilidad


Requerimiento	RNF-1
Prioridad	Media
Descripcion	Proveer documentación del cómo funciona y como usar KeyBS
Justificacion	Es una obligación proveer una manera sencilla y comprensible para que nuestros programadores como nuestros usuarios entiendan y tengan una idea de que están haciendo y como lo están usando.
Origen (Interesado)	Usuarios finales y Desarrolladores
Criterio de aceptacion / Validacion	Documentación de los procesos elementales

### RNF-2: Rendimiento y escalabilidad

Requerimiento	RNF-2
Prioridad	Media
Descripcion	Garantizar un tiempo de respuesta inferior a 3 segundos en todas las transacciones.
Justificacion	El proveer un tiempo de respuesta corto y que transmita buenas sensaciones de fluidez al usuario es clave para dar la impresión de un software pulido y confiable.
Origen (Interesado)	Usuarios finales
Criterio de aceptacion / Validacion	Tiempos de respuesta inferiores a 3 segundos

### RNF-3: Disponibilidad

Requerimiento	RNF-3
Prioridad	Alta
Descripcion	Garantizar una disponibilidad del 99.5% para minimizar interrupciones del servicio.
Justificacion	Tener los menores tiempos fuera de actividad es una medida necesaria para aumentar disponibilidad y confiabilidad al usuario de que


	<b>Asignatura: INGENIERIA DE SOFTWARE III</b>
	<b>Grupo: B</b>
	<b>Docente: Ing. Rodrigo Castro Caicedo</b>
	<b>Estudiantes: Santiago Monroy Quiazua – Diego Mauricio Paez Gonzalez</b>
	<b>Códigos: 076231132 - 076231135</b>

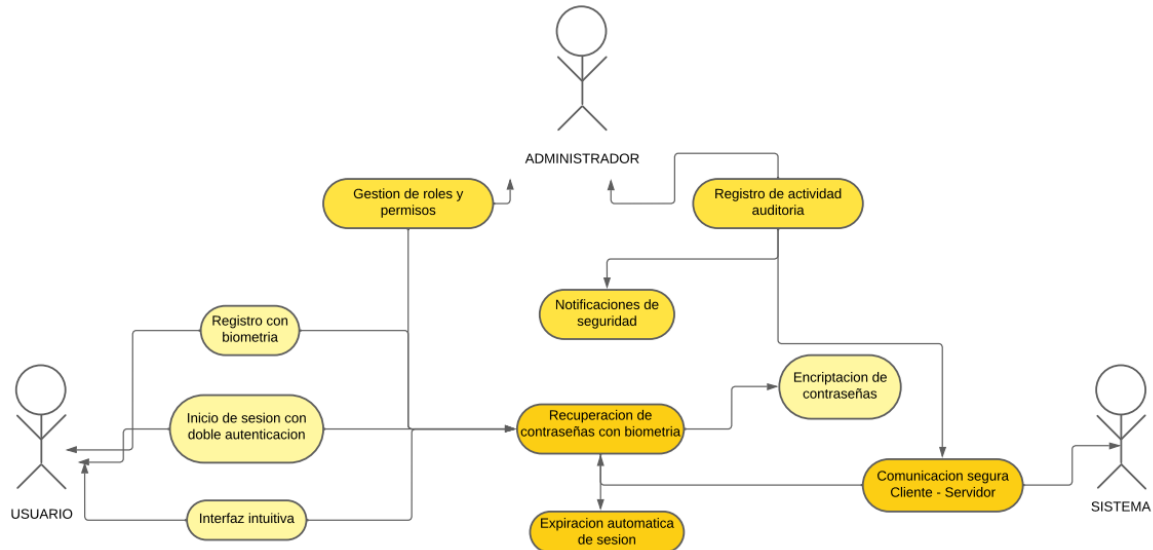
	sus contraseñas siempre estarán a disposición de él.
Origen (Interesado)	Usuarios finales
Criterio de aceptacion / Validacion	Acceso del 99.5% del tiempo a la aplicación

#### **RNF-4: Modularidad y escalabilidad**

Requerimiento	RNF-4
Prioridad	Baja
Descripcion	Crear un sistema modular que permita en un futuro una integración más completa en general, ya sea con sistemas operativos u otras aplicaciones.
Justificacion	Tener un sistema modular que sea capaz de crecer con los menores inconvenientes posibles es fundamental para permitir que la aplicación crezca sin tener que recurrir a rehacer trabajo de manera innecesaria.
Origen (Interesado)	Usuarios finales
Criterio de aceptacion / Validacion	Compatibilidad y modularidad casi total en la aplicacion.


#### **DIAGRAMAS DE CASOS DE USO.**

	<b>Asignatura: INGENIERIA DE SOFTWARE III</b>
	<b>Grupo: B</b>
	<b>Docente: Ing. Rodrigo Castro Caicedo</b>
	<b>Estudiantes: Santiago Monroy Quiazua – Diego Mauricio Paez Gonzalez</b>
	<b>Códigos: 076231132 - 076231135</b>



#### CU-01: Automatización de Procesos

Nombre	Automatización de Procesos
Autor	
Fecha	
Campo de prioridad	
Descripcion	Permitir la definición y automatización de procesos biométricos con mínima interacción del usuario.
Actores	Usuario
Precondiciones	<ol style="list-style-type: none"> <li>El usuario debe haber registrado previamente su biometría.</li> <li>El sistema debe contar con un módulo de automatización de autenticación.</li> </ol>
Flujo normal	<ol style="list-style-type: none"> <li>El usuario accede a la configuración de automatización en KeyBS.</li> <li>Define los procesos que desea automatizar.</li> <li>KeyBS registra los procesos y los activa en segundo plano.</li> <li>En futuras autenticaciones, el sistema ejecuta el proceso de manera automática sin intervención del usuario.</li> </ol>


	<b>Asignatura: INGENIERIA DE SOFTWARE III</b>
	<b>Grupo: B</b>
	<b>Docente: Ing. Rodrigo Castro Caicedo</b>
	<b>Estudiantes: Santiago Monroy Quiazua – Diego Mauricio Paez Gonzalez</b>
	<b>Códigos: 076231132 - 076231135</b>

Flujo alternativo	Si la configuración falla, el usuario recibe una notificación con opciones de ajuste manual.
Postcondiciones	11. Los procesos biométricos se ejecutan automáticamente sin intervención manual. 12. Se almacena la configuración personalizada del usuario. 13. El usuario recibe una confirmación de que la automatización está activa.

#### **CU-02: Universalidad y Compatibilidad**

Nombre	Universalidad y Compatibilidad
Autor	
Fecha	
Campo de prioridad	
Descripcion	Detectar cualquier input de contraseña en una aplicación y permitir autenticación biométrica con KeyBS.
Actores	Usuario
Precondiciones	14. KeyBS debe estar habilitado en el sistema del usuario. 15. La aplicación en la que se usa KeyBS debe permitir la entrada de contraseñas.
Flujo normal	16. El usuario intenta iniciar sesión en una aplicación. 17. KeyBS detecta el campo de contraseña. 18. Se solicita autenticación biométrica. 19. KeyBS verifica la identidad del usuario y completa el inicio de sesión.
Flujo alternativo	Si el usuario no tiene biometría registrada, se solicita ingresar la contraseña manualmente.
Postcondiciones	20. KeyBS detecta automáticamente los inputs de contraseña en cualquier aplicación compatible. 21. El usuario puede autenticarse sin necesidad de escribir su contraseña manualmente. 22. Se almacena un registro de la autenticación en KeyBS (si la privacidad lo permite).




	<b>Asignatura: INGENIERIA DE SOFTWARE III</b>
	<b>Grupo: B</b>
	<b>Docente: Ing. Rodrigo Castro Caicedo</b>
	<b>Estudiantes: Santiago Monroy Quiazua – Diego Mauricio Paez Gonzalez</b>
	<b>Códigos: 076231132 - 076231135</b>

### CU-03: Registro Seguro

Nombre	Registro Seguro
Autor	
Fecha	
Campo de prioridad	
Descripcion	Asegurar el transporte seguro de datos entre el cliente y el servidor.
Actores	Usuario
Precondiciones	23. El usuario debe estar registrado en KeyBS. 24. El sistema debe contar con un canal cifrado para el transporte de datos.
Flujo normal	25. El usuario ingresa datos de autenticación en KeyBS. 26. Los datos son cifrados con un protocolo seguro (Ej: AES-256, TLS). 27. Se envían al servidor a través de un canal seguro. 28. El servidor valida los datos y confirma el registro seguro.
Flujo alternativo	Si la conexión no es segura, el sistema alerta al usuario y bloquea el envío de datos.
Postcondiciones	29. Los datos han sido transportados y almacenados siguiendo protocolos de cifrado. 30. Se garantiza la seguridad y privacidad de la información del usuario. 31. Si el proceso falla, no se guarda ningún dato en el sistema y se notifica al usuario.

### CU-04: Gestión de Inicios de Sesión


Nombre	Gestión de Inicios de Sesión
Autor	
Fecha	
Campo de prioridad	

	<b>Asignatura: INGENIERIA DE SOFTWARE III</b>
	<b>Grupo: B</b>
	<b>Docente: Ing. Rodrigo Castro Caicedo</b>
	<b>Estudiantes: Santiago Monroy Quiazua – Diego Mauricio Paez Gonzalez</b>
	<b>Códigos: 076231132 - 076231135</b>

Descripción	Permitir la gestión y visualización de cuentas iniciadas en KeyBS.
Actores	Usuario
Precondiciones	32. El usuario debe haber autenticado al menos una cuenta con KeyBS. 33. El sistema debe almacenar información sobre los accesos realizados.
Flujo normal	34. El usuario accede al panel de gestión de cuentas en KeyBS. 35. Visualiza las cuentas donde ha iniciado sesión. 36. Puede cerrar sesión en dispositivos específicos o en todas las sesiones activas.
Flujo alternativo	Si el usuario detecta actividad sospechosa, puede reportarla al soporte de KeyBS.
Postcondiciones	37. El usuario puede ver todas las sesiones activas en KeyBS. 38. Si se cerró alguna sesión, la cuenta queda desvinculada del dispositivo en cuestión. 39. En caso de actividad sospechosa, se registra un evento de seguridad y se notifica al usuario.

#### CU-05: Uso Multiplataforma


Nombre	Uso Multiplataforma
Autor	
Fecha	
Campo de prioridad	

	<b>Asignatura: INGENIERIA DE SOFTWARE III</b>
	<b>Grupo: B</b>
	<b>Docente: Ing. Rodrigo Castro Caicedo</b>
	<b>Estudiantes: Santiago Monroy Quiazua – Diego Mauricio Paez Gonzalez</b>
	<b>Códigos: 076231132 - 076231135</b>

Descripción	Permitir el uso de KeyBS en dispositivos <b>iOS y Android.</b>
Actores	Usuario
Precondiciones	40. El usuario debe tener un dispositivo compatible con la aplicación.
Flujo normal	41. El usuario instala KeyBS en su dispositivo iOS o Android. 42. Configura su autenticación biométrica. 43. Puede utilizar KeyBS para autenticarse en cualquier plataforma compatible.
Flujo alternativo	Si el sistema operativo no admite un tipo de biometría, KeyBS ofrecerá una alternativa compatible.
Postcondiciones	44. KeyBS funciona correctamente en dispositivos iOS y Android. 45. El usuario puede autenticarse en cualquier plataforma sin problemas de compatibilidad. 46. Si un dispositivo no es compatible, se muestra una notificación con opciones alternativas.

#### CU-06: Invitación a Cuentas

Nombre	Invitación a Cuentas
Autor	
Fecha	
Campo de prioridad	
Descripción	Compartir credenciales de inicio de sesión a través de KeyBS con otros usuarios.
Actores	Usuario
Precondiciones	47. Ambos usuarios deben estar registrados en KeyBS. 48. El propietario de la cuenta debe habilitar el uso compartido.
Flujo normal	49. El usuario accede a la configuración de cuentas compartidas. 50. Selecciona la cuenta que desea compartir. 51. Ingresa el correo o ID de KeyBS del destinatario.

	<b>Asignatura: INGENIERIA DE SOFTWARE III</b>
	<b>Grupo: B</b>
	<b>Docente: Ing. Rodrigo Castro Caicedo</b>
	<b>Estudiantes: Santiago Monroy Quiazua – Diego Mauricio Paez Gonzalez</b>
	<b>Códigos: 076231132 - 076231135</b>

	<p>52. Define si la invitación será temporal o permanente.</p> <p>53. El destinatario recibe la invitación y puede acceder a la cuenta desde su propio dispositivo.</p>
Flujo alternativo	Si el usuario revoca el acceso, la cuenta compartida deja de estar disponible para el destinatario.
Postcondiciones	<p>54. La cuenta ha sido compartida exitosamente con otro usuario de KeyBS.</p> <p>55. Si la invitación tiene un tiempo definido, la cuenta se revocará automáticamente cuando expire.</p> <p>56. El usuario que compartió la cuenta puede ver y gestionar los accesos en cualquier momento.</p>

## ***HISTORIAS DE USUARIO.***

### ***RF 1: AUTOMATIZACION DE PROCESOS.***

- **¿Cómo?:** Usuario.
- **Quiero:** Que la autenticación biométrica se realice automáticamente con la mínima intervención.
- **Para:** De esta manera acceder a mis cuentas de manera rápida y segura.

#### ***CRITERIOS DE ACEPTACION.***


- El sistema debe permitir definir procesos personalizados de autenticación biométrica.
- La autenticación debe ejecutarse sin requerir múltiples interacciones del usuario.
- El sistema debe asegurar la correcta ejecución del proceso sin demoras.

### ***RF 2: UNIVERSALIDAD Y COMPATIBILIDAD***

- **¿Cómo?:** Usuario.
- **Quiero:** Que KeyBS detecte automáticamente los ampos de contraseña en cualquier ocasión.
- **Para:** Facilitar el inicio de sesión sin comprometer la seguridad.

#### ***CRITERIOS DE ACEPTACION.***

- El sistema debe detectar cualquier campo de contraseña de manera automática.
- La autenticación debe realizarse sin alterar el flujo de las aplicaciones.
- La implementación debe garantizar la seguridad de los datos al interactuar con otras aplicaciones.

	<b>Asignatura: INGENIERIA DE SOFTWARE III</b>
	<b>Grupo: B</b>
	<b>Docente: Ing. Rodrigo Castro Caicedo</b>
	<b>Estudiantes: Santiago Monroy Quiazua – Diego Mauricio Paez Gonzalez</b>
	<b>Códigos: 076231132 - 076231135</b>

### *RF 3: REGISTRO SEGURO.*

- **¿Cómo?:** Usuario.
- **Quiero:** Que mis datos de autenticación se envíen de manera muy segura hacia el servidor.
- **Para:** Evitar brechas de seguridad y accesos no autorizados.

#### *CRITERIOS DE ACEPTACION*

- El sistema debe cifrar los datos antes de transmitirlos.
- El canal de comunicación debe cumplir con estándares de seguridad (TLS/SSL).
- No debe ser posible interceptar ni modificar los datos en tránsito.

### *RF 4: GESTION DE INICIOS DE SESION.*

- **¿Cómo?:** Usuario.
- **Quiero:** Ver y gestionar los dispositivos en los que he iniciado sesión con KeyBS.
- **Para:** Monitorear mi actividad y cerrar inicios de sesión sospechosos.

#### *CRITERIOS DE ACEPTACION.*

- El sistema debe mostrar una lista de sesiones activas.
- Debe ser posible cerrar sesiones de manera remota.
- El usuario debe recibir alertas sobre accesos no reconocidos.

### *RF 5: MULTIPLATAFORMA*

- **¿Cómo?:** Usuario.
- **Quiero:** Usar KeyBS desde dispositivos IOS o Android.
- **Para:** Poder acceder a mis cuentas desde cualquier plataforma.

#### *CRITERIOS DE ACEPTACION.*

- La aplicación debe estar disponible en las tiendas oficiales de iOS y Android.
- La funcionalidad debe mantenerse consistente entre ambas plataformas.
- El sistema debe ajustarse a las diferencias de cada sistema operativo.

### *RF 6: INVITACION A CUENTAS.*

- **¿Cómo?:** Usuario.
- **Quiero:** Compartir mi cuenta de KeyBS con otros usuarios de manera totalmente segura.
- **Para:** Permitirles el acceso de mi cuenta sin necesidad de revelar mi contraseña.

#### *CRITERIOS DE ACEPTACION.*

- El sistema debe permitir compartir accesos de manera temporal o indefinida.
- Debe ser posible revocar el acceso en cualquier momento.
- El acceso compartido no debe exponer la contraseña original.