	<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**

### ***Tabla de contenido***


<b>1. INTRODUCCION .....</b>	<b>5</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>

2.	PLANTEAMIENTO DEL PROYECTO.....	5
2.1	PLANTEAMIENTO DEL PROBLEMA:.....	5
3.	JUSTIFICACION .....	6
3.1	IMPACTO DEL PROYECTO .....	6
4.	OBJETIVOS.....	7
4.1	OBJETIVO GENERAL: .....	7
4.2	OBJETIVOS ESPECIFICOS: .....	7
5.	MARCO TEÓRICO .....	7
5.1	ALGORITMOS DE CIFRADO: .....	7
5.1.1	Cifrado simétrico: .....	7
5.1.2	Cifrado asimétrico:.....	8
5.2	BIOMETRIA COMO METODO DE AUTENTICACIÓN .....	8
5.3	TIPOS DE AUTENTICACIÓN BIOMETRICA: .....	8
5.3.1	Reconocimiento dactilar: .....	8
5.3.2	Reconocimiento facial: .....	8
5.3.3	Escaneo de iris: .....	9
5.4	KEYLOGGING: .....	9
5.5	PHISHING: .....	9
5.6	MALWARE: .....	9
6.	MATRIZ DE RIESGOS .....	9
7.	REQUERIMIENTOS FUNCIONALES Y NO FUNCIONALES .....	10
7.1	REQUERIMIENTOS FUNCIONALES: .....	10
7.2	REQUERIMIENTOS NO FUNCIONALES: .....	13
8.	DIAGRAMAS DE CASOS DE USO.....	15
9.	PATRONES DE DISEÑO .....	23
10.	ARQUITECTURAS DE SOFTWARE: .....	23
10.1	¿QUÉ ES ZERO – TRUST Y COMO SE APLICA? .....	24
10.2	BENEFICIOS PARA EL PROYECTO .....	24
11.	HISTORIAS DE USUARIO.....	27
11.1	RF 1: AUTOMATIZACION DE PROCESOS. ....	28
11.2	RF 2: UNIVERSALIDAD Y COMPATIBILIDAD .....	28

	<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>

11.3 RF 3: REGISTRO SEGURO.....	28
11.4 RF 4: GESTION DE INICIOS DE SESION. ....	28
11.5 RF 5: MULTIPLATAFORMA .....	28
11.6 RF 6: INVITACION A CUENTAS. ....	29
12. PLAN DE PRUEBAS – CIFRADOR BIOMETRICO KeyBS .....	29
12.1 INTRODUCCION AL PLAN DE PRUEBAS.....	29
12.2 OBJETIVOS DEL PLAN DE PRUEBAS.....	29
12.3 ALCANCE DE LAS PRUEBAS. ....	29
12.3 CASOS DE PRUEBA. ....	30
CONCLUSIONES:.....	31
REFERENCIAS: .....	32

	<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>

## **1. 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 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.


## **2. PLANTEAMIENTO DEL PROYECTO**

### **2.1 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.

	<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>

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

### 3. 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 una 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 usará 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.

#### 3.1 IMPACTO DEL PROYECTO

- **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.
- **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.

	<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>

- **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.
- **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.

#### 4. OBJETIVOS

##### 4.1 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.

##### 4.2 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.

#### 5. 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.

##### 5.1 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.

##### 5.1.1 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:

	<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>

- **AES (Advanced Encryption Standard):** Utiliza claves de 128, 192 o 256 bits y es ampliamente utilizado en sistemas de seguridad.
- **DES (Data Encryption Standard):** Antiguamente popular, pero ahora obsoleto debido a su vulnerabilidad a ataques de fuerza bruta.
- **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.

### 5.1.2 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.

### 5.2 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:

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

### 5.3 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:

- Alta precisión y rapidez.
- Bajo costo de implementación.
- Resistencia a ataques de suplantación mediante imágenes.

#### 5.3.2 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:



	<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>

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

### 5.3.3 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:

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

### 5.4 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.

### 5.5 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.


### 5.6 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.

## 6. MATRIZ DE RIESGOS

TABLA 1: descripción de la matriz de riesgos:

TIPO DE RIESGO	DESCRIPCION	IMPACTO POTENCIAL	PROBABILIDAD DE OCURRENCIA
----------------	-------------	-------------------	----------------------------

	<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	Medio	Alto	Muy alto	Extremo	Extremo
Probabilidad IV	Medio	Medio	Alto	Muy alto	Extremo
Moderado III	Bajo	Medio	Medio	Alto	Muy alto
Poco probable II	Muy bajo	Bajo	Medio	Medio	Alto
Raro I	Muy bajo	Muy bajo	Bajo	Medio	Medio

## 7. REQUERIMIENTOS FUNCIONALES Y NO FUNCIONALES

### 7.1 REQUERIMIENTOS FUNCIONALES:

#### RF-1: automatización de procesos

Requerimiento	RF-1
---------------	------


	<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>

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

## RF-3: Registro Seguro

	<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-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.
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

	<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>

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

## 7.2 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

	<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>

	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 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

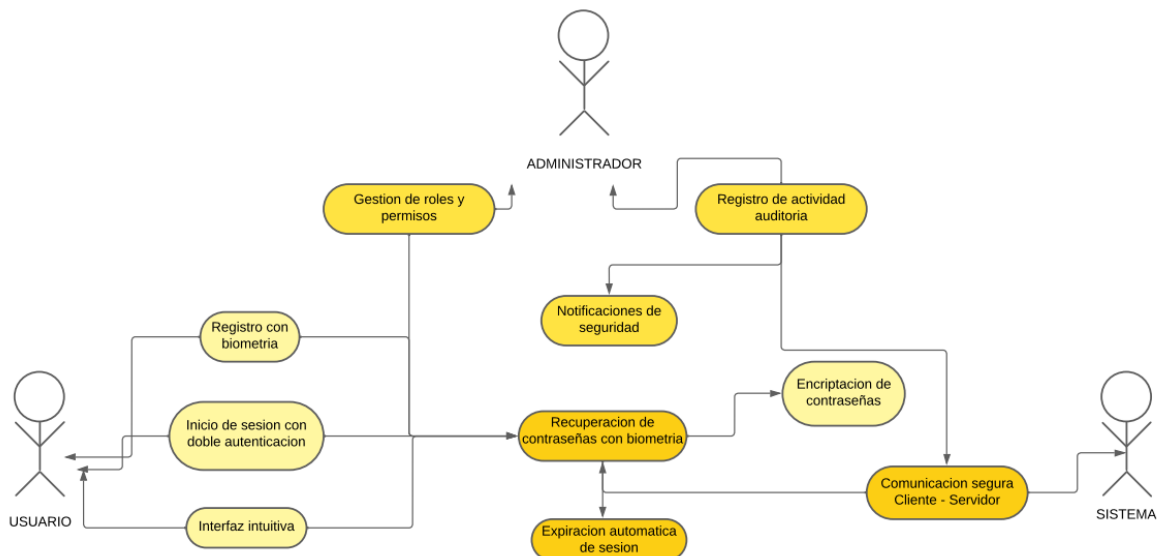
## RNF-4: Modularidad y escalabilidad

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.

	<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>	


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.

## 8. DIAGRAMAS DE CASOS DE USO.



### 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	<ul 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> </ul>


	<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 normal	<ul 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> </ul>
Flujo alternativo	Si la configuración falla, el usuario recibe una notificación con opciones de ajuste manual.
Postcondiciones	<ul style="list-style-type: none"> <li>- Los procesos biométricos se ejecutan automáticamente sin intervención manual.</li> <li>- Se almacena la configuración personalizada del usuario.</li> <li>- El usuario recibe una confirmación de que la automatización está activa.</li> </ul>

#### **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	<ul style="list-style-type: none"> <li>- KeyBS debe estar habilitado en el sistema del usuario.</li> <li>- La aplicación en la que se usa KeyBS debe permitir la entrada de contraseñas.</li> </ul>
Flujo normal	<ul style="list-style-type: none"> <li>- El usuario intenta iniciar sesión en una aplicación.</li> <li>- KeyBS detecta el campo de contraseña.</li> <li>- Se solicita autenticación biométrica.</li> <li>- KeyBS verifica la identidad del usuario y completa el inicio de sesión.</li> </ul>
Flujo alternativo	Si el usuario no tiene biometría registrada, se solicita ingresar la contraseña manualmente.



	<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>


Postcondiciones	<ul style="list-style-type: none"> <li>- KeyBS detecta automáticamente los inputs de contraseña en cualquier aplicación compatible.</li> <li>- El usuario puede autenticarse sin necesidad de escribir su contraseña manualmente.</li> <li>- Se almacena un registro de la autenticación en KeyBS (si la privacidad lo permite).</li> </ul>
-----------------	---

### 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	<ul style="list-style-type: none"> <li>- El usuario debe estar registrado en KeyBS.</li> <li>- El sistema debe contar con un canal cifrado para el transporte de datos.</li> </ul>
Flujo normal	<ul style="list-style-type: none"> <li>- El usuario ingresa datos de autenticación en KeyBS.</li> <li>- Los datos son cifrados con un protocolo seguro (Ej: AES-256, TLS).</li> <li>- Se envían al servidor a través de un canal seguro.</li> <li>- El servidor valida los datos y confirma el registro seguro.</li> </ul>
Flujo alternativo	Si la conexión no es segura, el sistema alerta al usuario y bloquea el envío de datos.
Postcondiciones	<ul style="list-style-type: none"> <li>- Los datos han sido transportados y almacenados siguiendo protocolos de cifrado.</li> <li>- Se garantiza la seguridad y privacidad de la información del usuario.</li> <li>- Si el proceso falla, no se guarda ningún dato en el sistema y se notifica al usuario.</li> </ul>

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


Nombre	Gestión de Inicios de Sesión
Autor	

	<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>

Fecha	
Campo de prioridad	
Descripción	Permitir la gestión y visualización de cuentas iniciadas en KeyBS.
Actores	Usuario
Precondiciones	<ul style="list-style-type: none"> <li>- El usuario debe haber autenticado al menos una cuenta con KeyBS.</li> <li>- El sistema debe almacenar información sobre los accesos realizados.</li> </ul>
Flujo normal	<ul style="list-style-type: none"> <li>- El usuario accede al panel de gestión de cuentas en KeyBS.</li> <li>- Visualiza las cuentas donde ha iniciado sesión.</li> <li>- Puede cerrar sesión en dispositivos específicos o en todas las sesiones activas.</li> </ul>
Flujo alternativo	Si el usuario detecta actividad sospechosa, puede reportarla al soporte de KeyBS.
Postcondiciones	<ul style="list-style-type: none"> <li>- El usuario puede ver todas las sesiones activas en KeyBS.</li> <li>- Si se cerró alguna sesión, la cuenta queda desvinculada del dispositivo en cuestión.</li> <li>- En caso de actividad sospechosa, se registra un evento de seguridad y se notifica al usuario.</li> </ul>

#### CU-05: Uso Multiplataforma


Nombre	Uso Multiplataforma
Autor	
Fecha	
Campo de prioridad	
Descripción	Permitir el uso de KeyBS en dispositivos <b>iOS y Android</b> .
Actores	Usuario
Precondiciones	<ul style="list-style-type: none"> <li>- El usuario debe tener un dispositivo compatible con la aplicación.</li> </ul>
Flujo normal	<ul style="list-style-type: none"> <li>- El usuario instala KeyBS en su dispositivo iOS o Android.</li> <li>- Configura su autenticación biométrica.</li> </ul>

	<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>

	<ul style="list-style-type: none"> <li>- Puede utilizar KeyBS para autenticarse en cualquier plataforma compatible.</li> </ul>
Flujo alternativo	Si el sistema operativo no admite un tipo de biometría, KeyBS ofrecerá una alternativa compatible.
Postcondiciones	<ul style="list-style-type: none"> <li>- KeyBS funciona correctamente en dispositivos iOS y Android.</li> <li>- El usuario puede autenticarse en cualquier plataforma sin problemas de compatibilidad.</li> <li>- Si un dispositivo no es compatible, se muestra una notificación con opciones alternativas.</li> </ul>

#### CU-06: Invitación a Cuentas

Nombre	Invitación a Cuentas
Autor	
Fecha	
Campo de prioridad	
Descripcion	Compartir credenciales de inicio de sesión a través de KeyBS con otros usuarios.
Actores	Usuario
Precondiciones	<ul style="list-style-type: none"> <li>- Ambos usuarios deben estar registrados en KeyBS.</li> <li>- El propietario de la cuenta debe habilitar el uso compartido.</li> </ul>
Flujo normal	<ul style="list-style-type: none"> <li>- El usuario accede a la configuración de cuentas compartidas.</li> <li>- Selecciona la cuenta que desea compartir.</li> <li>- Ingresa el correo o ID de KeyBS del destinatario.</li> <li>- Define si la invitación será temporal o permanente.</li> <li>- El destinatario recibe la invitación y puede acceder a la cuenta desde su propio dispositivo.</li> </ul>
Flujo alternativo	Si el usuario revoca el acceso, la cuenta compartida deja de estar disponible para el destinatario.
Postcondiciones	<ul style="list-style-type: none"> <li>- La cuenta ha sido compartida exitosamente con otro usuario de KeyBS.</li> </ul>

	<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>

	<ul style="list-style-type: none"> <li>- Si la invitación tiene un tiempo definido, la cuenta se revocará automáticamente cuando expire.</li> <li>- El usuario que compartió la cuenta puede ver y gestionar los accesos en cualquier momento.</li> </ul>
--	---

## 9. **MOCK UPS DEL PROYECTO.**



**Asignatura: INGENIERIA DE SOFTWARE III**

**Grupo: B**

**Docente: Ing. Rodrigo Castro Caicedo**

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

**Códigos: 076231132 - 076231135**





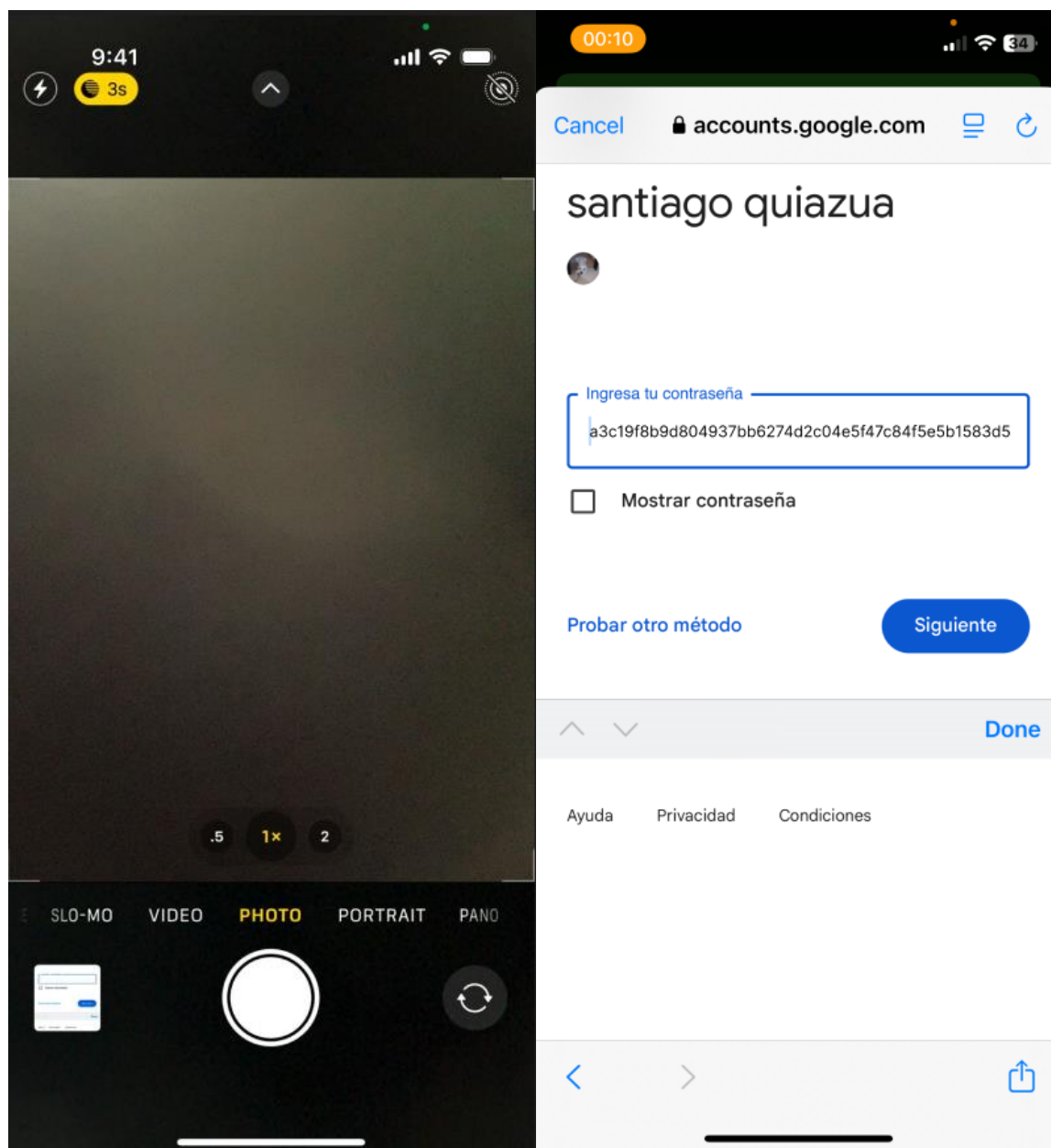
**Asignatura: INGENIERIA DE SOFTWARE III**


**Grupo: B**

**Docente: Ing. Rodrigo Castro Caicedo**

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

**Códigos: 076231132 - 076231135**



	<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>

## 10. PATRONES DE DISEÑO

El uso de un conjunto de patrones de diseño es un elemento clave para la organización, creación y seguridad del código, Por ende, el uso de los patrones FACADE y SINGLETON son de gran importancia al ser elementos que nos proveen de que solo haya una instancia del servicio de cifrado de contraseñas y claves biométricas en el caso de singleton.

A su vez reduce la complejidad, oculta la lógica interna de múltiples subsistemas y permitiendo múltiples accesos de los diferentes sistemas de biometría (Huella dactilar, Reconocimiento facial).

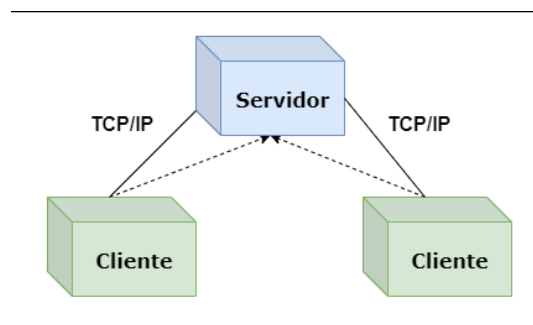
## 11. ARQUITECTURAS DE SOFTWARE:


Cuando nos referimos a “Arquitecturas de Software” estamos hablando de un concepto que se viene conociendo aproximadamente desde los años 60, menciona y establece que es una planificación basada en modelos, patrones y abstracciones teóricas las cuales se usan a la hora de realizar alguna pieza de software sin importar el nivel de complejidad y como paso previo a cualquier implementación dentro de este.

La arquitectura de software nos permite planificar a priori nuestro desarrollo y de esta manera elegir el mejor conjunto de herramientas y ayudas para llevar a cabo de la mejor manera el proyecto, por lo tanto, es uno de los pasos fundamentales antes de programar cualquier cosa relacionada ya que determinara a gran medida el ritmo del desarrollo, e incluso temas económicos dentro del proyecto. En base a esto, elegimos la arquitectura Cliente – servidor, la cual se adapta de la mejor manera para el desarrollo de nuestro cifrado biométrico.

### Arquitectura Cliente-Servidor

- Este modelo divide el sistema en dos partes:
- **Cliente:** La aplicación o dispositivo que solicita información o servicios (puede ser web, móvil o de escritorio).
- **Servidor:** El sistema que procesa las solicitudes, gestiona los datos y responde con la información necesaria.
- La ventaja principal es la **centralización**, lo que facilita la administración, seguridad y escalabilidad del sistema, permitiendo atender múltiples clientes sin comprometer el rendimiento.



	<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>

### *11.1 ¿QUÉ ES ZERO – TRUST Y COMO SE APLICA?*

- El modelo **Zero-Trust** se basa en la idea de "**nunca confiar, siempre verificar**", lo que significa que ningún usuario o dispositivo tiene acceso por defecto, sin importar si está dentro de la red corporativa.
- Para asegurar el sistema, se aplican las siguientes medidas:
- **Autenticación Multifactor (MFA):** Verificación constante de identidad con métodos seguros como OAuth 2.0 y OpenID Connect.
- **Acceso con menor privilegio:** Los usuarios solo pueden acceder a lo que realmente necesitan.
- **Monitoreo y detección de amenazas:** Uso de inteligencia artificial para identificar comportamientos sospechosos.
- **Cifrado de datos:** Se protege la información tanto en tránsito (TLS 1.3) como almacenada (AES-256).
- **Control de acceso adaptativo:** Se ajustan permisos según el usuario, su ubicación y el dispositivo que usa.

### *11.2 BENEFICIOS PARA EL PROYECTO*

- **Mayor seguridad:** Se reducen riesgos de ataques internos y externos.
- **Protección de datos:** Solo quienes realmente lo necesitan pueden acceder a la información.
- **Menor impacto en caso de ataques:** Si ocurre una brecha de seguridad, se limita el daño.
- **Cumplimiento de normativas:** Facilita la adaptación a regulaciones como GDPR y ISO 27001.
- **Escalabilidad sin riesgos:** Se pueden agregar nuevas funciones sin comprometer la seguridad.

## ***12. BASE DE DATOS, MODELOS ENTIDAD RELACION Y MODELO LOGICO.***





**Asignatura: INGENIERIA DE SOFTWARE III**

**Grupo: B**

**Docente: Ing. Rodrigo Castro Caicedo**

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

**Códigos: 076231132 - 076231135**

**MODELO LOGICO DE LA BASE DE DATOS:**

<b>USUARIOS</b>
Id (PK)
nombre
correo (UNIQUE)
contraseña_hash
salt
tipo_usuario
estado
fecha_creacion

<b>REGISTRO ACCESO</b>
Id (PK)
usuario_id (FK)
fecha_hora
metodo_autenticacion
estado
direccion_ip
dispositivo

<b>DATOS BIOMETRICOS</b>
Id (PK)
usuario_id (FK)
huella_hash
rostro_hash
fecha_registro

<b>DISPOSITIVOS AUTORIZADOS</b>
Id (PK)
usuario_id (FK)
dispositivo
ip
fecha_registro

<b>LOGS DE SEGURIDAD</b>
Id (PK)
usuario_id (FK)
accion
fecha
detalle



**Asignatura: INGENIERIA DE SOFTWARE III**

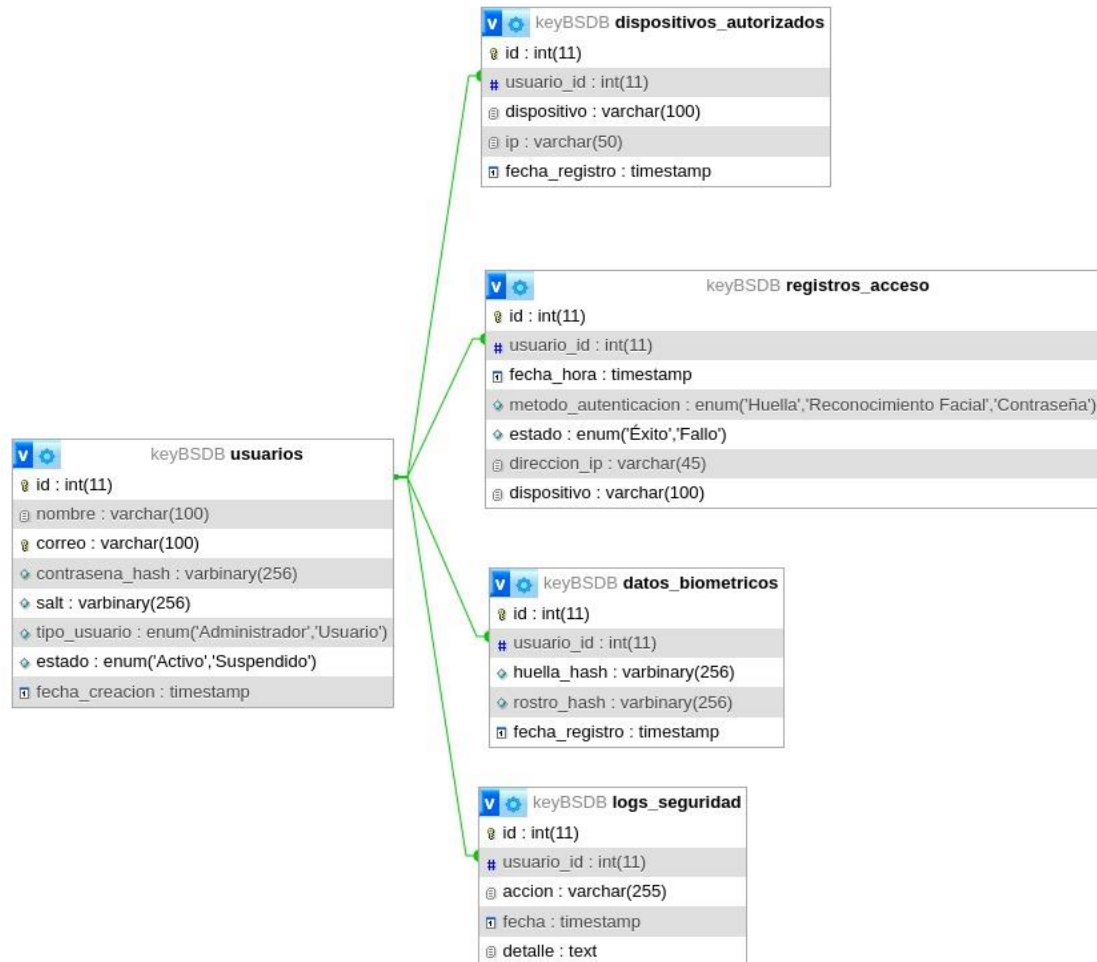
**Grupo: B**

**Docente: Ing. Rodrigo Castro Caicedo**

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

**Códigos: 076231132 - 076231135**

**MODELO ENTIDAD RELACION Y CARDINALIDAD:**





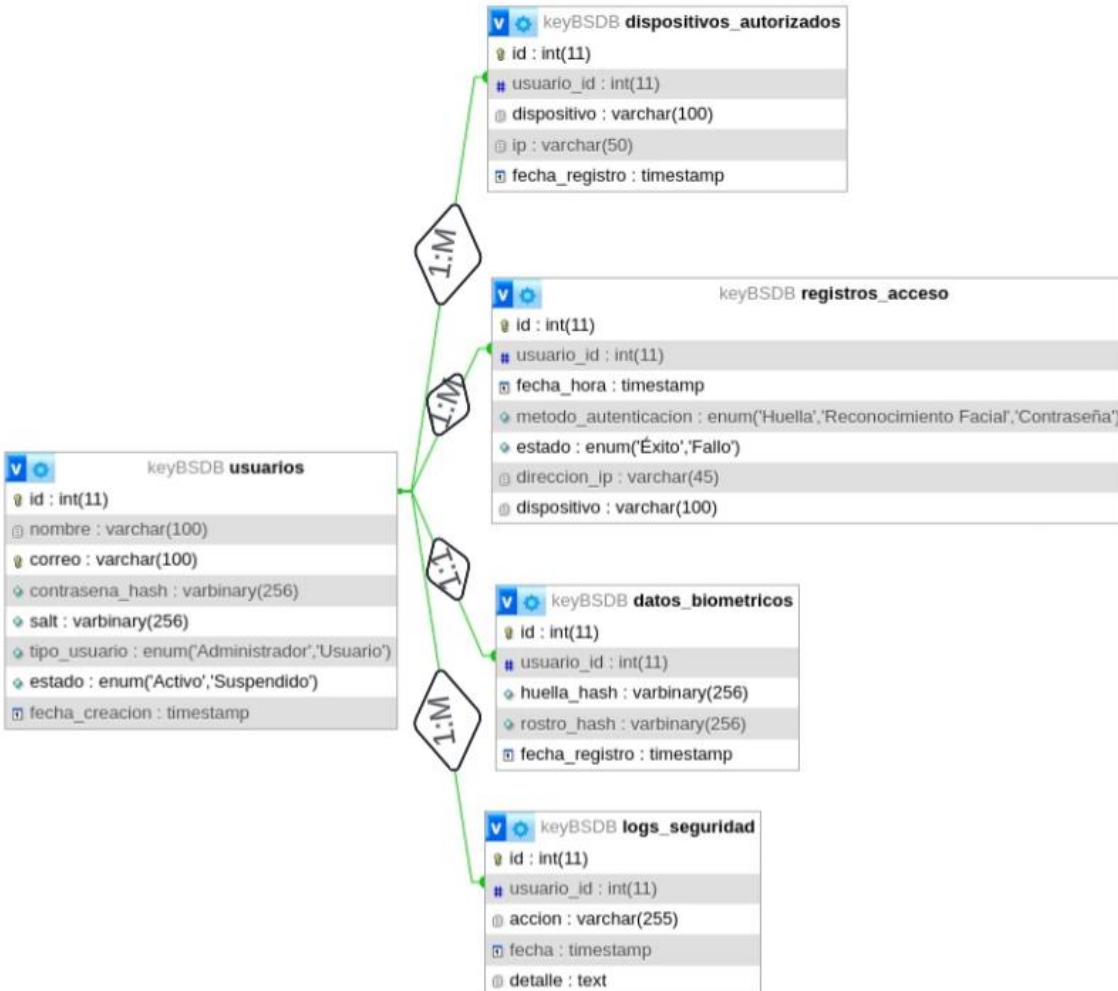
Asignatura: INGENIERIA DE SOFTWARE III

Grupo: B


Docente: Ing. Rodrigo Castro Caicedo

Estudiantes: Santiago Monroy Quiazua – Diego Mauricio Paez Gonzalez

Códigos: 076231132 - 076231135



### 13. HISTORIAS DE USUARIO.

	<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>

### 13.1 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.

### 13.2 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.

### 13.3 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.

### 13.4 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.

### 13.5 RF 5: MULTIPLATAFORMA

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

	<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>

### 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.

#### 13.6 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.

## 14. PLAN DE PRUEBAS – CIFRADOR BIOMETRICO KeyBS

### 14.1 INTRODUCCION AL PLAN DE PRUEBAS.


El plan de pruebas en este proyecto tiene como propósito asegurar la calidad y seguridad del sistema KeyBS, un cifrador biométrico que utiliza la autenticación facial y dactilar para la gestión de credenciales. Se evaluará el correcto funcionamiento de sus características principales, su seguridad, compatibilidad y experiencia de usuario.

### 14.2 OBJETIVOS DEL PLAN DE PRUEBAS.

1. Validar que nuestro sistema cumpla con los requisitos funcionales y no funcionales.
2. Asegurar la compatibilidad entre diferentes sistemas operativos y aplicaciones.
3. Detectar y corregir posibles fallos antes del lanzamiento.
4. Evaluar la seguridad del cifrado y la autenticación bioemtrica.

### 14.3 ALCANCE DE LAS PRUEBAS.

ALCANCE DE LAS PRUEBAS EN KeyBS	
Pruebas Funcionales.	Evaluar la autenticación biométrica, cifrado de contraseñas y la gestión de sesiones.
Pruebas de Seguridad.	Validar la protección contra ataques como lo son el keylogging, phishing y malware.
Pruebas de Compatibilidad.	Asegurar un buen rendimiento en las diferentes plataformas como lo son: Windows, macOS, Android e IOS.
Pruebas de Rendimiento.	Medir tiempos de respuesta y consumo de recursos.
Pruebas de Usabilidad.	Evaluar la experiencia del usuario en términos de interfaz y facilidad 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>

#### 14.4 CASOS DE PRUEBA.

##### PRUEBAS FUNCIONALES.


ID.	DESCRIPCION.	ENTRADA.	RESULTADO ESPERADO
CF-01	Registro de usuario con autenticación biométrica.	Datos personales, huella o rostro.	Usuario registrado correctamente.
CF-02	Inicio de sesión con autenticación biométrica.	Huella dactilar o reconocimiento facial.	Acceso concedido si coincide con los datos registrados.
CF-03	Cifrado y almacenamiento seguro de credenciales.	Credenciales ingresadas.	Las credenciales se almacenan cifradas correctamente.
CF-04	Recuperación de acceso con biometría.	Solicitud de recuperación.	Verificación biométrica exitosa permite acceso.

##### PRUEBAS DE SEGURIDAD.

ID.	DESCRIPCION.	ENTRADA.	RESULTADO ESPERADO
CS-01	Intento de acceso con una huella/rostro no registrado.	Biometría no autorizada.	Acceso denegado.
CS-02	Intento de acceder a credenciales sin autenticación.	Solicitud de visualización sin autenticación.	Bloqueo del acceso.
CS-03	Análisis de cifrado de datos almacenados.	Extracción de credenciales cifradas.	Datos ininteligibles sin la clave biométrica.
CS-04	Prueba de resistencia contra ataques de fuerza bruta.	Múltiples intentos de acceso.	Bloqueo del sistema tras intentos fallidos.

##### PRUEBAS DE COMPATIBILIDAD.

ID.	DESCRIPCION.	ENTORNO.	RESULTADO ESPERADO.
CC-01	Uso de Windows 10/11.	Windows.	Funcionalidad completa sin errores.
CC-02	Uso de macOS.	macOS.	Funcionalidad completa sin errores.
CC-03	Uso en Android.	Android 10+	Funcionalidad completa sin errores.

	<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>	

CC-04	Uso de IOS.	IOS 14+	Funcionalidad completa sin errores.
-------	-------------	---------	-------------------------------------

#### PRUEBAS DE RENDIMIENTO.

ID.	DESCRIPCION.	CONDICIONES.	RESULTADO ESPERADO.
PR-01	Tiempo de respuesta del sistema.	Inicio de sesión con biometría.	Acceso en menos de tres segundos.
PR-02	Consumo de memoria.	Uso prolongado.	No debe exceder el 10% de la RAM.

#### PRUEBAS DE USABILIDAD.

ID.	DESCRIPCION.	CONDICIONES.	RESULTADO ESPERADO.
PU-01	Facilidad de navegación en la interfaz.	Usuario sin experiencia previa.	Completa las tareas sin necesidad de ayuda.
PU-02	Claridad de mensajes de error.	Intento de acceso fallido.	Mensaje claro y comprensible.


#### 14.5 CRITERIOS DE ACEPTACION.

El sistema se considera listo para su implementación si:

- Se superan al menos el 95% de los casos de prueba.
- No se encuentran fallos críticos de seguridad o estabilidad.
- Se garantiza una respuesta inferior a 3 segundos en autenticaciones.
- La experiencia de usuario es positiva en al menos el 90% de las pruebas de usabilidad.

#### CONCLUSIONES:

- El desarrollo de KeyBS ha sido un proceso integral que combina ciberseguridad, criptografía, biometría y arquitectura de software para ofrecer una solución robusta y confiable en la gestión de accesos digitales. Su diseño está basado en seguridad, automatización, escalabilidad y usabilidad, asegurando una experiencia fluida sin comprometer la integridad de los datos.
- Uno de los principales logros del sistema es la autenticación biométrica con cifrado avanzado (AES y RSA), garantizando que las credenciales sean inaccesibles para terceros. La aplicación de protocolos seguros como TLS/SSL refuerza el enfoque Zero-Trust, donde cada acceso es verificado rigurosamente, minimizando riesgos de ataques como phishing o intercepciones.
- El enfoque en la automatización reduce la intervención del usuario, agilizando el acceso sin necesidad de recordar múltiples contraseñas. Además, la compatibilidad con diferentes aplicaciones y dispositivos refuerza la universalidad y escalabilidad de KeyBS, permitiendo su uso en entornos multiplataforma. La integración con cualquier campo de entrada de contraseñas ofrece una solución adaptable y accesible.

	<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>

- Desde el punto de vista del desarrollo, la aplicación de los patrones de diseño Singleton y Facade ha mejorado la estructuración, mantenibilidad y modularidad del sistema. Singleton asegura la existencia de una única instancia del sistema de autenticación, mientras que Facade permite una interfaz más simple y segura para la interacción con terceros.
- KeyBS no solo responde a la creciente preocupación por la seguridad digital, sino que también sienta las bases para futuras innovaciones en autenticación biométrica y criptografía. Su implementación en diferentes sectores podría consolidarlo como un estándar de seguridad digital, promoviendo un acceso más seguro, eficiente y confiable a los servicios digitales.

### **REFERENCIAS:**

Huet, P. Arquitectura de software: Qué es y qué tipos existen. *Openwebinars.net*.

<https://openwebinars.net/blog/arquitectura-de-software-que-es-y-que-tipos-existen/>

(N.d.). Computer.org. from <https://ieeecs-media.computer.org/media/education/swebok/swebok-v4.pdf>

Amalfitano, D., Faralli, S., Hauck, J. C. R., Matalonga, S., & Distant, D. (2024). Artificial intelligence applied to software testing: A tertiary study. *ACM Computing Surveys*, 56(3), 1–38. <https://doi.org/10.1145/3616372>

Niu, Y. (2020). Application of robust design in engineering software testing. *Proceedings of the 2nd International Conference on Industrial Control Network And System Engineering Research*.