



Asignatura: INGENIERIA DE SOFTWARE III

Grupo: B

Docente: Ing. Rodrigo Castro Caicedo

Estudiantes: Santiago Monroy Quiazua – Diego Mauricio Paez Gonzalez

Códigos: 076231132 - 076231135

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



Asignatura: INGENIERIA DE SOFTWARE III

Grupo: B

Docente: Ing. Rodrigo Castro Caicedo

Estudiantes: Santiago Monroy Quiazua – Diego Mauricio Paez Gonzalez

Códigos: 076231132 - 076231135

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**

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

PLAN DE PRUEBAS – CIFRADOR BIOMETRICO KeyBS	3
INTRODUCCION AL PLAN DE PRUEBAS.....	3
OBJETIVOS DEL PLAN DE PRUEBAS.....	3
ALCANCE DE LAS PRUEBAS.....	3
CASOS DE PRUEBA.	4

PLAN DE PRUEBAS – CIFRADOR BIOMETRICO KeyBS

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.

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.

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.

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

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.

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

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.


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 interceptaciones.

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

- 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.
- 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.