



**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**



<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>

PATRONES DE DISEÑO .....	4
ARQUITECTURAS DE SOFTWARE:.....	4
¿QUÉ ES ZERO – TRUST Y COMO SE APLICA? .....	5
BENEFICIOS PARA EL PROYECTO .....	5

	<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>

## 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).

## 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.



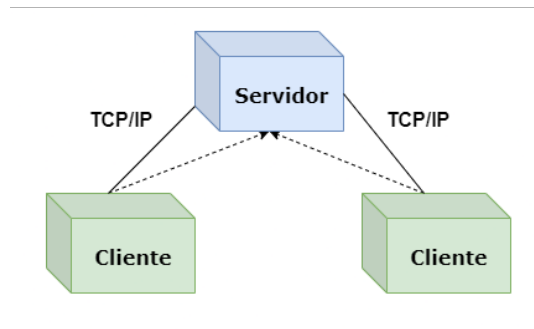
**Asignatura: INGENIERIA DE SOFTWARE III**

**Grupo: B**

**Docente: Ing. Rodrigo Castro Caicedo**

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

**Códigos: 076231132 - 076231135**



### *¿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.

### *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.



***Asignatura: INGENIERIA DE SOFTWARE III***

***Grupo: B***

***Docente: Ing. Rodrigo Castro Caicedo***

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

***Códigos: 076231132 - 076231135***