

# Pruebas no Funcionales

## Pruebas de Seguridad (Pentesting)

### Alerts (10)

- > Cloud Metadata Potentially Exposed
- > CSP: Wildcard Directive (31)
- > Content Security Policy (CSP) Header Not Set (3)
- > Missing Anti-clickjacking Header (3)
- > Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s) (49)
- > Server Leaks Version Information via "Server" HTTP Response Header Field (6)
- > Timestamp Disclosure - Unix (20)
- > X-Content-Type-Options Header Missing (13)
- > Information Disclosure - Suspicious Comments (7)
- > Modern Web Application (3)

### Cloud Metadata Potentially Exposed

**Vulnerabilidad:** Exposición de metadatos de la nube.

**Causa:** Configuración incorrecta del servidor NGINX, específicamente el uso de la variable \$host.

**Riesgo:** Acceso no autorizado a información confidencial de la instancia en la nube, como credenciales y configuración.

**Solución:** Evitar el uso de la variable \$host y no confiar en datos del usuario en la configuración de NGINX.

### CSP: Wildcard Directive

**Vulnerabilidad:** La configuración de la directiva Content Security Policy (CSP) permite cargar contenido de cualquier origen, lo que deja la aplicación vulnerable a ataques como Cross-Site Scripting (XSS) e inyección de datos.

**Causa:** La directiva CSP está configurada incorrectamente, permitiendo el uso de comodines o no definiendo correctamente las fuentes permitidas.

**Riesgo:** Un atacante podría aprovechar esta vulnerabilidad para inyectar código malicioso en la aplicación, robar datos confidenciales o tomar el control de esta.

**Solución:** Configurar correctamente la directiva CSP para especificar de forma precisa las fuentes permitidas de contenido.

### **Content Security Policy (CSP) Header Not Set**

**Vulnerabilidad:** Falta de encabezado Content Security Policy (CSP).

**Causa:** La aplicación web no está enviando el encabezado CSP en sus respuestas.

**Riesgo:** Exposición a una amplia gama de ataques como Cross-Site Scripting (XSS), inyección de contenido y otros tipos de ataques que comprometen la integridad y confidencialidad de la aplicación.

**Solución:** Implementar el encabezado CSP en todas las respuestas de la aplicación, definiendo de manera precisa las fuentes permitidas de contenido.

### **Missing Anti-clickjacking Header**

**Vulnerabilidad:** La aplicación web es vulnerable a ataques de clickjacking.

**Causa:** La falta de los encabezados HTTP Content-Security-Policy con la directiva frame-ancestors o X-Frame-Options.

**Riesgo:** Un atacante podría engañar a los usuarios para que hagan clic en elementos ocultos dentro de un iframe transparente, lo que podría resultar en acciones no autorizadas en nombre del usuario, como realizar transacciones financieras, cambiar contraseñas o revelar información sensible.

**Solución:** Implementar el encabezado X-Frame-Options o la directiva frame-ancestors del encabezado Content-Security-Policy en todas las respuestas de la aplicación.

### **Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)**

**Vulnerabilidad:** Exposición de Información Sensible a través del Encabezado "X-Powered-By"

**Causa:** Configuración incorrecta del servidor, revelando el framework utilizado (Express.js).

**Riesgo:** Ataques dirigidos basados en las vulnerabilidades conocidas del framework.

**Solución:** Eliminar o modificar el encabezado "X-Powered-By" para ocultar información sobre la tecnología utilizada.

## **Server Leaks Version Information via "Server" HTTP Response Header Field**

### **Timestamp Disclosure – Unix\**

**Vulnerabilidad:** Filtración de Información a través del Encabezado "Server"

**Causa:** El servidor web o la aplicación está configurando el encabezado HTTP "Server" con información específica sobre su versión (nginx/1.27.3 en este caso).

**Riesgo:** Al revelar esta información, los atacantes pueden:

- Identificar vulnerabilidades específicas asociadas a esa versión del servidor.
- Adaptar sus ataques a las debilidades conocidas de esa tecnología.
- Facilitar la explotación de la aplicación.

#### **Solución:**

- Eliminar el encabezado: Configurar el servidor para que no incluya el encabezado "Server" en las respuestas.
- Ocultar la versión: Si no es posible eliminar el encabezado, utilizar un valor genérico (por ejemplo, "Servidor web") para ocultar la versión específica.

## X-Content-Type-Options Header Missing

**Vulnerabilidad:** Divulgación de Tiempos

**Causa:** URLs muestran fechas exactas de creación o modificación.

**Riesgo:** Permite a atacantes rastrear cambios, estimar la edad del sistema y planificar ataques.

**Solución:**

- Eliminar fechas de las URLs.
- Usar nombres aleatorios o hash.
- Minimizar la información en las fechas.

## Information Disclosure - Suspicious Comments

**Vulnerabilidad:** Falta de encabezado X-Content-Type-Options

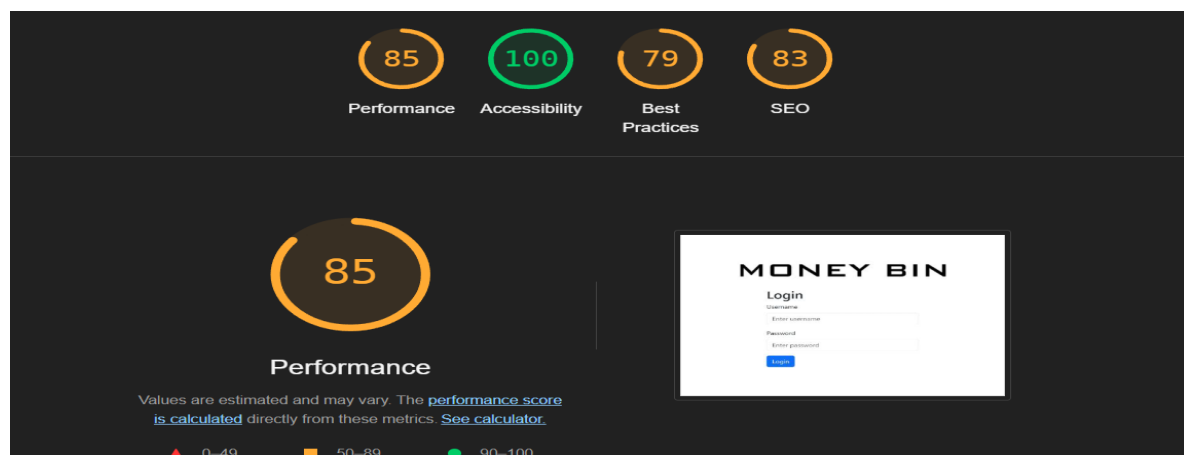
**Causa:** El servidor web no indica claramente el tipo de contenido de los archivos.

**Riesgo:** Los navegadores pueden interpretar mal los archivos, permitiendo ataques como XSS.

**Solución:**

- Agregar el encabezado X-Content-Type-Options con el valor "nosniff".
- Asegurar que el tipo de contenido (MIME) sea correcto.

## Pruebas de Rendimiento





■	Avoid serving legacy JavaScript to modern browsers	— Potential savings of 0 KiB	▼
○	Avoid large layout shifts	— 1 layout shift found	▼
○	Initial server response time was short	— Root document took 60 ms	▼
○	Avoids enormous network payloads	— Total size was 1,620 KiB	▼
○	Avoids an excessive DOM size	— 16 elements	▼
○	Avoid chaining critical requests	— 2 chains found	▼
○	JavaScript execution time	— 0.1 s	▼
○	Minimizes main-thread work	— 0.2 s	▼

100

## Accessibility

These checks highlight opportunities to [improve the accessibility of your web app](#). Automatic detection can only detect a subset of issues and does not guarantee the accessibility of your web app, so [manual testing](#) is also encouraged.

ADDITIONAL ITEMS TO MANUALLY CHECK (10)

Hide

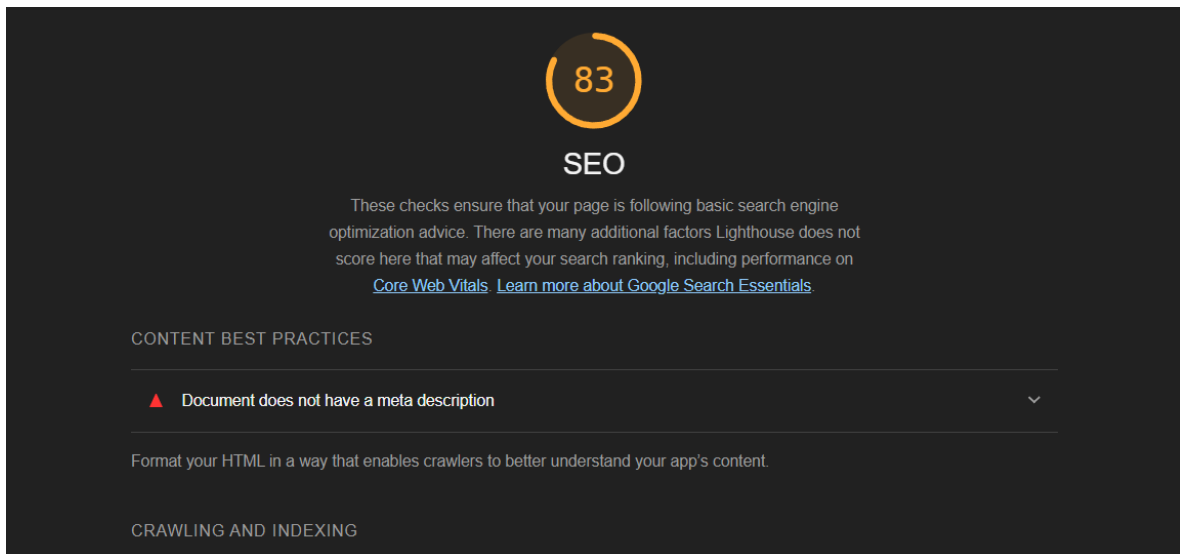
○	Interactive controls are keyboard focusable	▼
○	Interactive elements indicate their purpose and state	▼

79

## Best Practices

TRUST AND SAFETY

▲	Does not use HTTPS	— 5 insecure requests found	▼
▲	Does not redirect HTTP traffic to HTTPS		▼
○	Ensure CSP is effective against XSS attacks		▼



## Conclusiones:

- Buen desempeño general: La aplicación obtiene una puntuación de 85 en rendimiento, lo cual indica que carga de manera relativamente rápida y eficiente.
- Excelencia en accesibilidad: La puntuación de 100 en accesibilidad es destacable, lo que significa que la aplicación está diseñada para ser utilizada por personas con discapacidades, cumpliendo con los estándares de accesibilidad web.
- Potencial a mejorar en mejores prácticas: La puntuación de 79 en mejores prácticas sugiere que hay áreas en las que se podrían implementar mejoras para optimizar el código y la estructura de la aplicación.
- Buen posicionamiento SEO: La puntuación de 83 en SEO indica que la aplicación está bien optimizada para los motores de búsqueda, lo que puede ayudar a aumentar su visibilidad en línea.

## Recomendaciones:

- Profundizar en las mejores prácticas: Para alcanzar una puntuación perfecta, se recomienda analizar en detalle los aspectos en los que se ha obtenido una puntuación inferior a 100. Esto podría incluir la

optimización del código, la mejora de la estructura de la aplicación o la implementación de técnicas de desarrollo más modernas.

- **Mantener la accesibilidad:** Es fundamental continuar priorizando la accesibilidad para garantizar que la aplicación sea utilizable por el mayor número de personas posible.
- **Monitorear el rendimiento:** Es importante realizar un seguimiento continuo del rendimiento de la aplicación para identificar posibles cuellos de botella y realizar ajustes si es necesario.
- **Optimizar el SEO:** Aunque la puntuación de SEO es buena, siempre hay margen de mejora. Se pueden realizar ajustes en el contenido, las metaetiquetas y la estructura de los enlaces para mejorar el posicionamiento en los motores de búsqueda.
- **Considerar la opinión del usuario:** Además de las métricas técnicas, es importante tener en cuenta la experiencia del usuario. Realizar pruebas de usabilidad puede ayudar a identificar áreas de mejora en la interfaz y la funcionalidad de la aplicación.

## Pruebas de Inyección SQL

## Pruebas de Usabilidad

### Login

#### MONEY BIN

##### Login

Username

Enter username

Password

Enter password

Login

#### MONEY BIN

##### Login

Username

Enter username

Password

Enter password

Login

#### MONEY BIN

##### Login

Username

Enter username

Password

Enter password

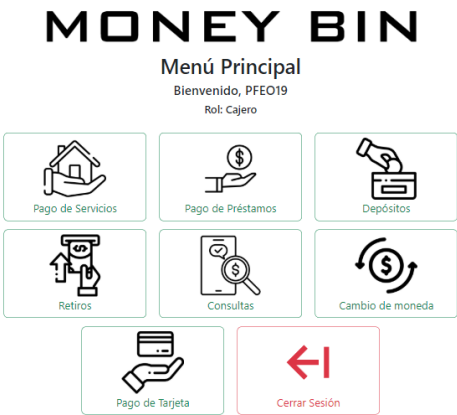
Login

## Display Desktop y Tablet



Cajero

Menú



Pago de Servicios

# MONEY BIN

## Tipo de Servicio

  
Luz

  
Agua

  
Teléfono


  
Internet


  
Cancelar


## Pago de Prestamos

# MONEY BIN

## Método de Pago

  
Parcial

  
Total

  
Cancelar

Depósitos

MONEY BIN

Deposito en Cuenta

Número de cuenta

Verificar

Cancelar

Cambio de moneda

Cambio de Moneda

CUI del Cliente

Monto en Quetzales

Precio de Venta del Dólar

Monto en Dólares

Realizar Cambio

Cancelar

Atención al cliente

Menú

MONEY BIN

Menú Principal

Bienvenido, PFE019

Rol: Atencion

Encuesta

Préstamos

Quejas

Cerrar Sesión

Bloqueo de tarjeta

MONEY BIN

Bloqueo de Tarjeta

Tipo de Tarjeta

Seleccione una opción

No. Tarjeta

No. Tarjeta

Motivo del Bloqueo

Seleccione un motivo

Titular

Titular

Respuesta a la Pregunta de Seguridad

Ingrese la respuesta

Bloquear Tarjeta

Cancelar

Actualización Cliente

# MONEY BIN

Actualización Cliente

Tipo de cuenta

Nombre

Apellido

Seleccione un cliente

Teléfono

Correo electrónico

Dirección

Pregunta de seguridad

Respuesta de seguridad

Finalizar Proceso

Cancelar

Nuevas tarjetas

# MONEY BIN

Solicitud de Nueva Tarjeta

Tipo de Tarjeta

Seleccione una opción

Enviar Solicitud

Cancelar

Nueva cuenta en dólares

# MONEY BIN

Solicitud de Nueva Cuenta en Dolares

CUI

Ingrese su CUI

Nombre

Ingrese su nombre

Apellido

Ingrese su apellido

Teléfono

Ingrese su teléfono

Correo electrónico

Ingrese su correo ele

Dirección

Ingrese su domicilio

Pregunta de seguridad

Ingrese su pregunta

Respuesta de seguridad

Ingrese su respuesta

Tipo de cuenta

Seleccione el tipo de

Monto Inicial (\$)

Ingrese el monto

Finalizar Proceso

Cancelar

## Administrador de sistemas

### Menú

# MONEY BIN

## Menú Principal

Bienvenido, admin

Rol: 1



Gestión de empleados



Registro de empleado

MONEY BIN

Registro de empleado

Nombre

Apellido

Edad

Número de teléfono

Numero de DPI

Correo electrónico

Papelería completa (PDF)

Choose File

No file chosen

Fotografía

Choose File

No file chosen

Estado Civil

Seleccione un estado

Genero

Seleccione un sexo

Rol

Seleccione un rol

Registrar

Cancelar

Asignación de roles

# MONEY BIN

**Rol de empleado**

Usuario Empleado

Rol actual

Nuevo Rol

Seleccione un empleado ▼

Seleccione un rol ▼

Guardar

Cancelar

## Eliminar empleado

# MONEY BIN

Empleados					
#	Nombre	Apellido	Usuario	Rol	Eliminar
1	John	Doe	admin	Administrador	
2	Lisa	Taylor	lisat	Administrador	
3	Alice	Smith	tiky	Cajero	
4	Jane	Doe	janed	Cajero	
5	Sam	Johnson	samj	Cajero	
6	Bob	Carter	bcarter	Supervisor	
7	Michael	Williams	mwill	Supervisor	
8	juan	gonzalez	JGONZAEZ24	Supervisor	
9	patito	feo	PFEO19	Supervisor	
10	Patrick	Star	ptrick	Servicio al Cliente	
<div>Cancelar</div>					

## Cambio de Contraseña



# MONEY BIN

Restablece la contraseña					
#	Nombre	Apellido	Usuario	Rol	Nueva Contraseña
1	John	Doe	admin	Administrador	...
2	Lisa	Taylor	lisat	Administrador	...
3	Alice	Smith	tkly	Cajero	...
4	Jane	Doe	janed	Cajero	...
5	Sam	Johnson	samj	Cajero	...
6	Bob	Carter	bcarter	Supervisor	...
7	Michael	Williams	mwill	Supervisor	...
8	Juan	gonzalez	JGONZAEZ24	Supervisor	...
9	patito	feo	PFE019	Supervisor	...
10	Patrick	Star	ptrick	Servicio al Cliente	...
Cancelar					

## Supervisor

### Menu

# MONEY BIN

## Menú Principal

Bienvenido, PFE019

Rol: Supervisor



Empleados



Solicitudes de Préstamos



Encuestas de Satisfacción



Registro de Quejas



Administradores



Monitoreo



Reportes



Gestión de Inventario Bancario



Solicitudes de Tarjetas



Cancelación de Servicios



Cerrar Sesión

## Registro de Quejas

[Inicio](#)

# MONEY BIN

## Quejas

ID	CUI	Cliente	Categoría	Descripción
> 1	5261956868514	Feliza Welden	Atención	La atención al cliente es pésima
> 2	5035286411254	Etty Jek	Producto	La tarjeta de crédito tiene cargos no
> 3	8552509080031	Trish Bontein	Servicio	El cajero automatico no me dio el di
> 4	2350670655803	Paige Balzen	Atención	La persona que me atendio no sabio
> 5	1317396730153	Clare Huckstepp	Producto	La cuenta de ahorro no da los intere

Rows per page: 10 1-5 of 6 |< < > >|

Administradores

[Inicio](#)

# MONEY BIN

## Administradores

Registrar

Usuario	CUI	Nombre	Correo	Telefono	Estado	Acciones
> admin	3026416610103	John Doe	jdoe@example.e...	12345678	Activo	Editar
> lsat	4445556667778	Lisa Taylor	ltaylor@example...	78945612	Activo	Editar

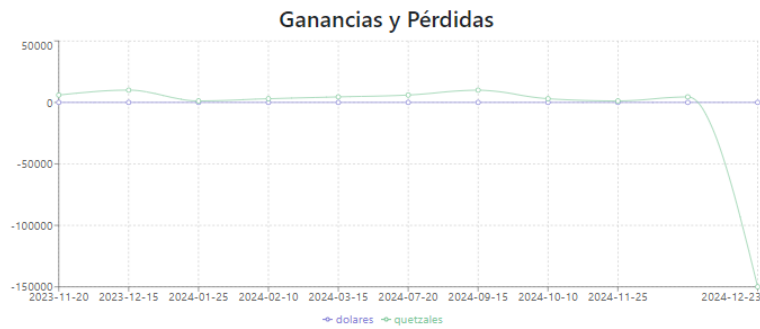
Rows per page: 10 1-2 of 2 |< < > >|

Monitoreo

[Inicio](#)      **Gestión de Inventarios Bancarios**

### Disponibilidad

Quetzales  
-100600.00 GTQ



Movimientos

Fecha	Movimientos	Empleado
> 2024-12-23 15:24:31	Se brindó un préstamo de 10000.00 al cliente con CUI 5261956868514	SYSTEM
> 2024-12-23 15:24:31	Se brindó un préstamo de 20000.00 al cliente con CUI 5035286411254	SYSTEM
> 2024-12-23 15:24:31	Se brindó un préstamo de 30000.00 al cliente con CUI 8552509080031	SYSTEM
> 2024-12-23 15:24:31	Se brindó un préstamo de 40000.00 al cliente con CUI 2350670655803	SYSTEM
> 2024-12-23 15:24:31	Se brindó un préstamo de 50000.00 al cliente con CUI 1337396730153	SYSTEM

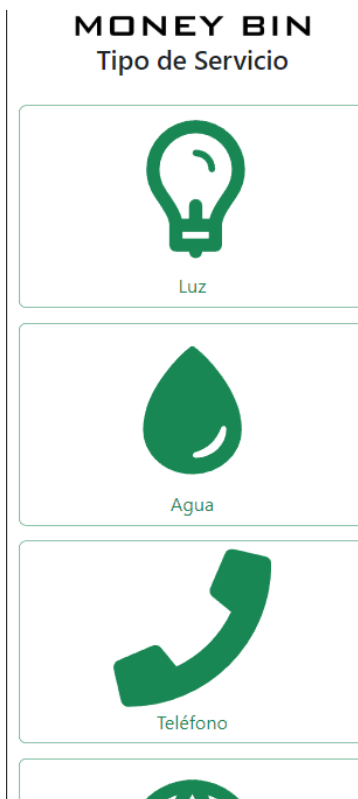
## Display Mobile

Cajero

Menú



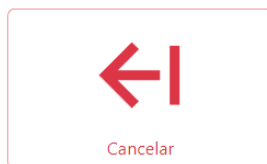
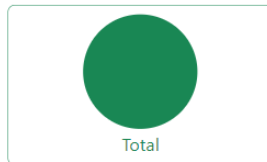
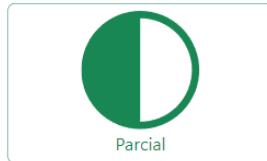
Pago de Servicios



Pago de Prestamos

## MONEY BIN

### Método de Pago



## Depósitos

## MONEY BIN

### Deposito en Cuenta

Número de cuenta

XXXXXXXX

Verificar

Cancelar

## Cambio de moneda

Cambio de Moneda

CUI del Cliente

Ingrese el CUI del cliente

Monto en Quetzales

Ingrese el monto en Quetzales

Precio de Venta del Dólar

Q 7.85

Monto en Dólares

\$ 0

Realizar Cambio

Cancelar

## Atención al cliente

### Menú

#### MONEY BIN

##### Menú Principal

Bienvenido, PFE019

Rol: Atencion



Nuevas Cuentas



Actualizaciones



Nuevas Tarjetas



### Bloqueo de tarjeta

## MONEY BIN

### Bloqueo de Tarjeta

Tipo de Tarjeta

Seleccione una opción

No. Tarjeta

No. Tarjeta

Titular

Titular

Motivo del Bloqueo

Seleccione un motivo

Respuesta a la Pregunta de Seguridad

Ingrese la respuesta

Bloquear Tarjeta

Cancelar

## Actualización Cliente

## MONEY BIN

### Actualización Cliente

Tipo de cuenta

Seleccione un cliente

Nombre

Apellido

Teléfono

Correo electrónico

Dirección

Pregunta de seguridad

Respuesta de seguridad

Nuevas tarjetas

MONEY BIN

Solicitud de Nueva Tarjeta

Tipo de Tarjeta

Seleccione una opción

Enviar Solicitud

Cancelar

Nueva cuenta en dólares

MONEY BIN

Solicitud de Nueva Cuenta en Dolares

CUI

Ingrese su CUI

Nombre

Ingrese su nombre

Apellido

Ingrese su apellido

Teléfono

Ingrese su teléfono

Correo electrónico

Ingrese su correo electró

Administrador de sistemas

Menú



## MONEY BIN

### Menú Principal

Bienvenido, admin

Rol: 1



Empleados



Copias de seguridad



Cerrar Sesión

## Registro de empleado

## MONEY BIN

### Registro de empleado

Nombre	Apellido	Edad
<input type="text"/>	<input type="text"/>	<input type="text"/>
Número de teléfono	Numero de DPI	Correo electrónico
<input type="text"/>	<input type="text"/>	<input type="text"/>
Papelería completa (PDF)	Fotografía	
<input type="button" value="Choose File"/>	<input type="button" value="Choose File"/>	
Estado	Genero	Rol
Civil	Se ▾	Se ▾
Se ▾		
<input type="button" value="Registrar"/>		
<input type="button" value="Cancelar"/>		

## Asignación de roles

MONEY BIN

Rol de empleado

Usuario  
Empleado

Rol  
actual

Nuevo  
Rol

Se ▾

Se ▾

Guardar

Cancelar

Eliminar empleado

MONEY

Empleados

#	Nombre	Apellido	Usuario
1	John	Doe	admin
2	Lisa	Taylor	lisat
3	calificacion	admin	cadmin
4	Alice	Smith	tiky
5	Jane	Doe	janed
6	Bob	Carter	bcarter
7	Michael	Williams	mwill
8	Patrick	Star	ptruck
9	Sam	Johnson	samj
10	calificacionp	cualquiera	CCUALQUIERA23

Cancelar

Cambio de Contraseña

# MONEY

Restablece la contraseña

#	Nombre	Apellido	Usuario
1	John	Doe	admin
2	Lisa	Taylor	lisat
3	calificacion	admin	cadmin
4	Alice	Smith	tiky
5	Jane	Doe	janed
6	Bob	Carter	bcarter
7	Michael	Williams	mwill
8	Patrick	Star	ptruck
9	Sam	Johnson	samj
10	calificacionp	cualquiera	CCUALQUIERA23

Cancelar

## Supervisor

### Menu

#### MONEY BIN

Menú Principal

Bienvenido, PFEO19

Rol: Supervisor



Empleados



Solicitudes de Préstamos



Encuestas de Satisfacción



## Registro de Quejas

Inicio

M

	ID	CUI	Client
>	1	5261956868514	Feliza
>	2	5035286411254	Etty J
>	3	8552509080031	Trish
>	4	2350670655803	Paige
>	5	1337396730153	Clare

|<

Administradores

Inicio

MON

Administra

	Usuario	CUI	Nombre
>	admin	3026416610...	John Doe
>	lisat	4445556667...	Lisa Taylor

|< <

Monitoreo

Inicio

	Fecha	Empleado
>	2024-12-26 22:08:24	admin
>	2024-12-23 15:24:31	SYSTEM
>	2024-12-23 15:24:31	SYSTEM
>	2024-12-23 15:24:31	SYSTEM
>	2024-12-23 15:24:31	SYSTEM
>	2024-12-23 15:24:31	SYSTEM
>	2024-12-23 15:24:31	SYSTEM
>	2024-12-23 15:24:31	SYSTEM
>	2024-12-23 15:24:31	SYSTEM

|<

Gestión de Inventario Bancario

Inicio

