

Informe de Auditoría de Sistemas - Examen de la Unidad I

Nombres y apellidos:

Jesús Eduardo Agreda Ramirez

Fecha:

10/09/2025

URL GitHub:

<https://github.com/mangoesafterplay/examen-u1>


1. Proyecto de Auditoría de Riesgos



Login

Evidencia:

Sistema de Auditoría de Riesgos

Ingresa tus credenciales para acceder

 Usuario

 Contraseña 

Iniciar Sesión

Usuario de demo: agreda

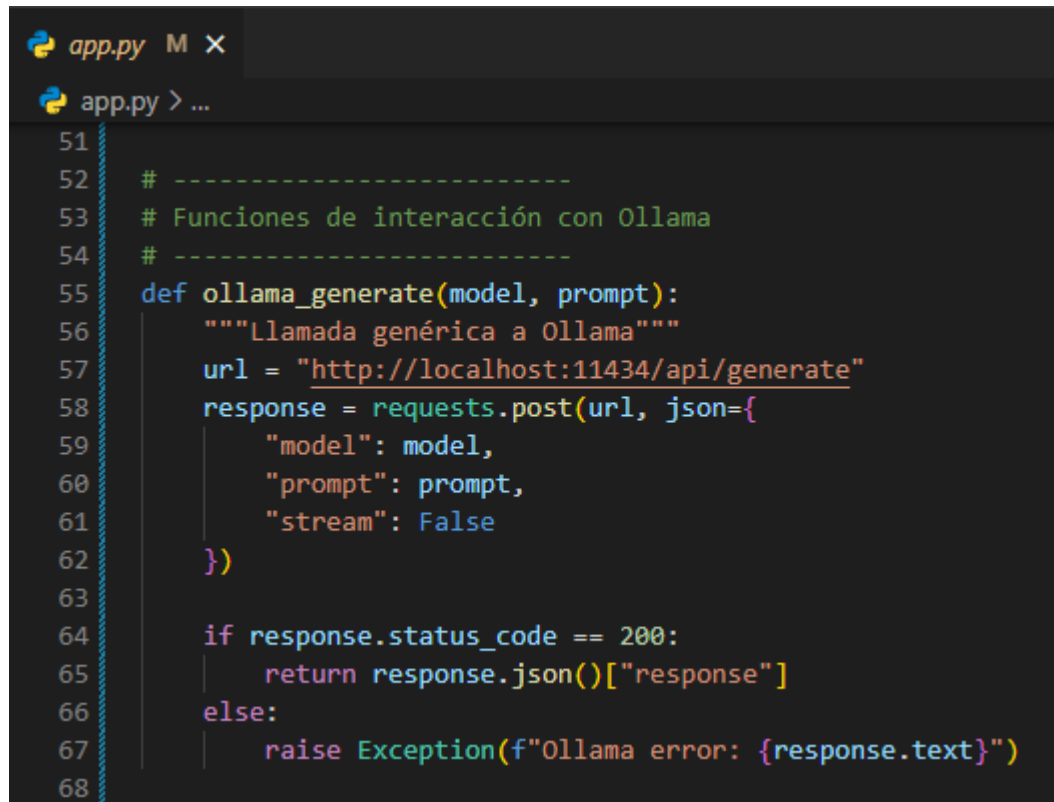
Contraseña: 123123

```
JS LoginService.js M X
src > services > JS LoginService.js > default
1 // Simple authentication service with hardcoded credentials
2 const credentials = {
3   username: "agreda",
4   password: "123123"
5 };
6
7 // Login function that returns a promise
8 export const login = (username, password) => {
9   return new Promise((resolve, reject) => {
10     // Simulate server delay
11     setTimeout(() => {
12       if (username === credentials.username && password === credentials.password) {
13         // Create a session token (could be more sophisticated in a real app)
14         const token = "mock-jwt-token-" + Math.random().toString(36).substr(2);
15         // Store token in localStorage
16         localStorage.setItem('authToken', token);
17         localStorage.setItem('user', username);
18         resolve({ success: true, user: username, token });
19       } else {
20         reject({ success: false, message: "Credenciales inválidas" });
21       }
22     }, 500); // 500ms delay to simulate network
23   });
24 };
25
```

Descripción:

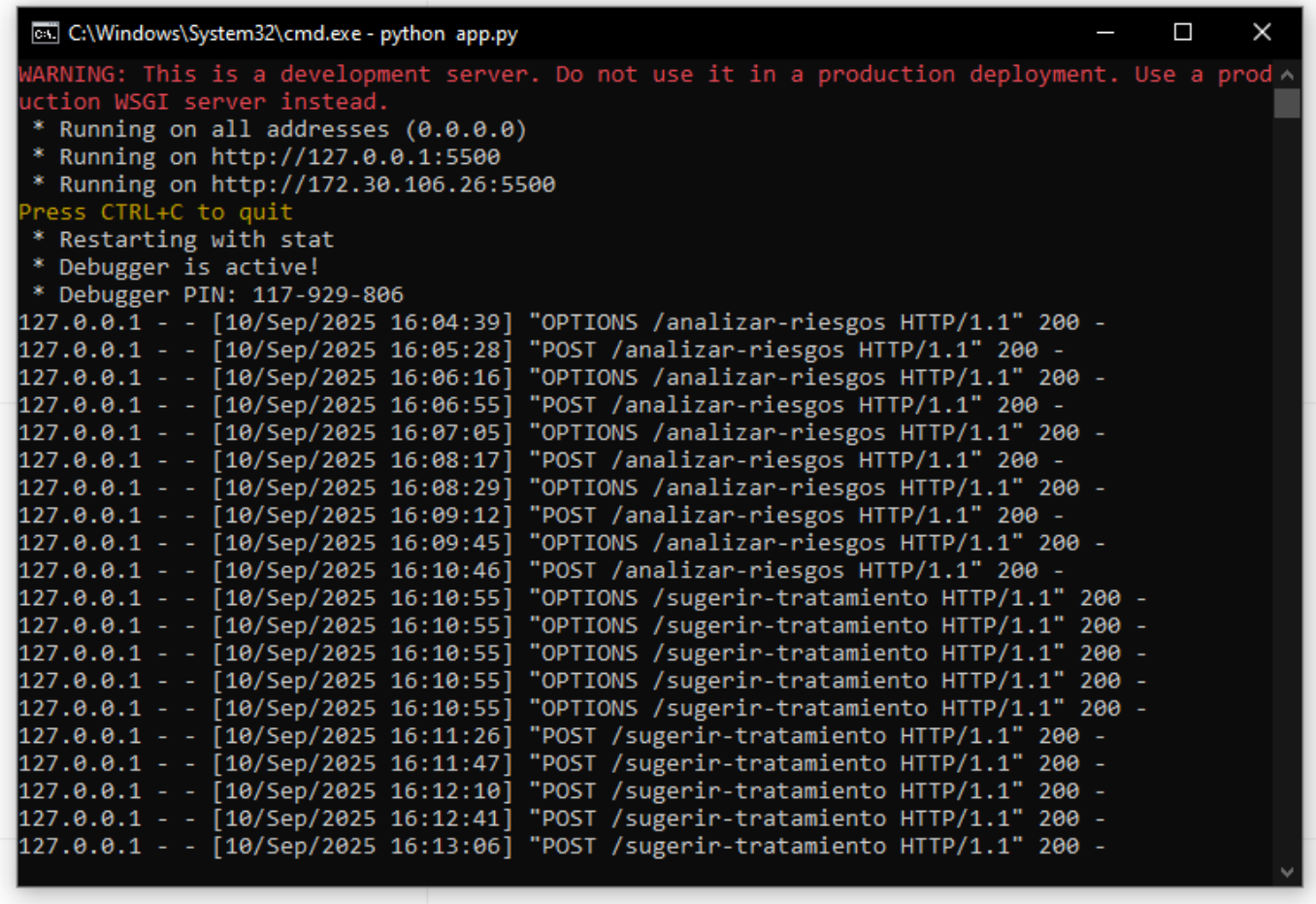
Se implementó un inicio de sesión ficticio sin base de datos, validando al usuario directamente desde el frontend con credenciales predefinidas en el código. Esto permite simular el acceso al sistema para pruebas sin exponer datos reales.

Motor de Inteligencia Artificial

Evidencia:

```
app.py M X
app.py > ...
51
52 # -----
53 # Funciones de interacción con Ollama
54 # -----
55 def ollama_generate(model, prompt):
56     """Llamada genérica a Ollama"""
57     url = "http://localhost:11434/api/generate"
58     response = requests.post(url, json={
59         "model": model,
60         "prompt": prompt,
61         "stream": False
62     })
63
64     if response.status_code == 200:
65         return response.json()["response"]
66     else:
67         raise Exception(f'Ollama error: {response.text}')
68
```

```
app.py M X
app.py > ...
69
70 def obtener_riesgos(activo):
71     prompt = f"""
72     Eres una herramienta de gestión de riesgos basada en ISO 27001.
73     El usuario te dará un activo tecnológico y debes responder con 5 riesgos en formato:
74     • **Riesgo**: Impacto.
75
76     Activo: {activo}
77     """
78     texto = ollama_generate("llama2:7b", prompt)
79
80     # Extraer riesgos e impactos con regex
81     patron = r'\*\*(.+?)\*\*:.*?(.+?)(?=\n|$)'
82     resultados = re.findall(patron, texto)
83
84     riesgos = [r[0].strip() for r in resultados]
85     impactos = [r[1].strip() for r in resultados]
86
87     return riesgos, impactos
88
89
90 def obtener_tratamiento(entrada):
91     prompt = f"""
92     Eres una herramienta de gestión de riesgos ISO 27001.
93     El usuario te dará un activo, un riesgo y un impacto.
94     Responde en máximo 200 caracteres con un tratamiento posible.
95
96     Entrada: {entrada}
97     """
98     texto = ollama_generate("llama2:7b", prompt)
99     return texto.strip()
100
101
102 if __name__ == '__main__':
103     app.run(debug=True, host="0.0.0.0", port=5500)
104
```



Descripción:

Se mejoró el motor de IA utilizando **Ollama con el modelo Llama2** integrado vía Flask. El sistema recibe un activo, genera riesgos e impactos asociados, y propone tratamientos de mitigación.

El código implementa funciones `obtener_riesgos()` y `obtener_tratamiento()` que interactúan con la API local de Ollama y devuelven resultados procesados en formato JSON.

2. Hallazgos

Activo 1: Servidor de base de datos

Evidencia:

Sistema de Auditoría de Riesgos				
+ Agregar activo		Recomendar tratamientos		
Activo	Riesgo	Impacto	Tratamiento	Operación
Servidor de base de datos	Riesgo	Fallas en la sistemática de seguridad del servidor de bases de datos.	Treatment possible: * Implementar medidas de gestión de riesgos para mitigar el impacto de las fallas en la sistemática de seguridad del servidor de base de datos, como la creación de un plan de contingencia y la implementación de tecnologías de redundancia y replicación de bases de datos. * Realizar pruebas y evaluaciones periódicas para detectar posibles vulnerabilidades en la sistemática de seguridad del servidor de base de datos y corregirlas antes de que puedan ser explotadas por atacantes malintencionados. * Proporcionar capacitación y sensibilización a los usuarios sobre la importancia de la seguridad en el uso del servidor de bases de datos y cómo minimizar el riesgo de fallas en la sistemática de seguridad.	Eliminar

Condición: Se detectaron posibles fallas en la sistemática de seguridad del servidor de bases de datos.

Recomendación:

- Implementar un plan de contingencia y tecnologías de redundancia/replicación de bases de datos.

- Realizar pruebas y evaluaciones periódicas de seguridad.
- Capacitar a usuarios en buenas prácticas de seguridad.

Riesgo: Alta

Activo 2: API Transacciones

Evidencia:

API Transacciones	Riesgo	Intrusión maliciosa. Los atacantes podrían intentar infiltrarse en la API para obtener información confidencial o realizar transacciones fraudulentas.	<p>* Control de acceso: Implementar un sistema de autenticación y autorización seguro para limitar el acceso a la API solo a los usuarios autorizados. *</p> <p>Monitoreo: Realizar un monitoreo constante del tráfico de red y las actividades en la API para detectar posibles intentos de infiltración o actividades sospechosas. *</p> <p>Protección de datos: Implementar medidas de protección de datos confidenciales, como cifrado de datos en transit y en repositorios, para evitar la exposición de información sensible. *</p> <p>Reducción de impacto: Definir un plan de respuesta a incidentes de infiltración o actividades sospechosas, incluyendo el restablecimiento rápido de servicios críticos y la limpieza de la red después de un incidente.</p>	Eliminar
-------------------	--------	--	---	--------------------------

Condición: La API está expuesta a intentos de intrusión maliciosa para obtener información confidencial o realizar transacciones fraudulentas.

Recomendación:

- Implementar autenticación y autorización seguras.
- Monitorear constantemente el tráfico y actividades sospechosas.
- Cifrar datos en tránsito y en reposo.
- Definir un plan de respuesta a incidentes.

Riesgo: Alta

Activo 3: Aplicación Web de Banca

Evidencia:

Aplicación Web de Banca	Riesgo	Pérdida de datos sensibles. La aplicación web de banca puede almacenar información sensible como nombres de usuarios, direcciones de correo electrónico, números de tarjeta de crédito, etc. Si este activo tecnológico cayera en manos malintencionadas, podría haber una pérdida significativa de datos sensibles que podrían ser utilizados para obtener beneficios ilícitos.	<p>Treatment possible: 1. Implementar medidas de seguridad adicionales para proteger la información sensible almacenada en la aplicación web de banca, como el uso de tecnologías de cifrado avanzadas y la creación de controles de acceso rigurosos para los usuarios. 2. Realizar pruebas de penetración periódicas para identificar posibles vulnerabilidades en la aplicación web y garantizar que se estén protegiendo adecuadamente los datos sensibles. 3. Establecer un plan de respuesta a incidentes para manejar cualquier infracción o amenaza que pueda afectar la seguridad de la información almacenada en la aplicación web de banca. 4. Brindar capacitación y educación a los usuarios sobre la importancia de proteger los datos sensibles y cómo pueden contribuir a la seguridad de la información almacenada en la aplicación web de banca.</p>	Eliminar
-------------------------	--------	--	--	--------------------------

Condición: Riesgo de pérdida de datos sensibles como credenciales, correos electrónicos o números de tarjeta.

Recomendación:

- Aplicar cifrado avanzado y controles de acceso rigurosos.
- Realizar pruebas de penetración periódicas.
- Establecer un plan de respuesta a incidentes.
- Capacitar a los usuarios en protección de datos sensibles.

Riesgo: Alta

Activo 4: Firewall Perimetral

Evidencia:

Firewall Perimetral	Impacto	Falta de seguridad en la configuración del firewall, lo que podría permitir accesos no autorizados a sistemas críticos o datos sensibles.	Posible tratamiento: 1. Implementar un procedimiento de revisión y verificación periódica de la configuración del firewall para garantizar que esté actualizada y segura. 2. Realizar un auditoría de seguridad regular para identificar posibles vulnerabilidades en la configuración del firewall y otros sistemas críticos. 3. Proporcionar entrenamiento y educación a los usuarios sobre el uso seguro del firewall y la importancia de mantener su configuración actualizada. 4. Implementar un sistema de seguimiento y monitoreo de actividades de acceso no autorizado para detectar posibles incidentes de infracción de seguridad.	Eliminar
---------------------	---------	---	---	--------------------------

Condición: Configuración insegura que podría permitir accesos no autorizados.
Recomendación:

- Revisar y verificar periódicamente la configuración del firewall.
- Realizar auditorías de seguridad regulares.
- Capacitar al personal en uso y gestión segura del firewall.
- Implementar monitoreo de intentos de acceso no autorizados.

Riesgo: Media

Activo 5: Backup en NAS

Evidencia:

Backup en NAS	Riesgo	Pérdida de datos críticos. Si el backup no se realiza adecuadamente o si la copia de seguridad en NAS se daña o se pierde, puede haber una pérdida de datos críticos que afecten significativamente a la empresa.	Treatment possible: 1. Implementar un calendarización y programación automatizada para el backup en NAS, para garantizar su realización diaria y evitar posibles errores o omitirla. 2. Monitorear regularmente la integridad de la copia de seguridad en NAS y realizar una recuperación de datos críticos en caso de daños o pérdida accidental. 3. Proporcionar capacitación y educación a los usuarios sobre el uso adecuado de la copia de seguridad y la importancia de mantenerla actualizada y segura. 4. Revisar y actualizar regularmente los procedimientos de backup y recuperación para garantizar su efectividad y adaptabilidad a las necesidades de la empresa.	Eliminar
---------------	--------	---	---	--------------------------

Condición: Riesgo de pérdida de datos críticos por errores en la copia o daños en el almacenamiento.
Recomendación:

- Automatizar la calendarización de backups.
- Monitorear la integridad de las copias y probar restauraciones.
- Capacitar al personal sobre uso adecuado del sistema de respaldo.
- Revisar y actualizar periódicamente los procedimientos de backup.

Riesgo: Media

Anexo 1: Activos de información

Anexo 1: Activos de información

Nº	Activo	Tipo
1	Servidor de base de datos	Base de Datos
2	API Transacciones	Servicio Web
3	Aplicación Web de Banca	Aplicación
4	Servidor de Correo	Infraestructura
5	Firewall Perimetral	Seguridad
6	Autenticación MFA	Seguridad

Nº	Activo	Tipo
7	Registros de Auditoría	Información
8	Backup en NAS	Almacenamiento
9	Servidor DNS Interno	Red
10	Plataforma de Pagos Móviles	Aplicación
11	VPN Corporativa	Infraestructura
12	Red de Cajeros Automáticos	Infraestructura
13	Servidor FTP	Red
14	CRM Bancario	Aplicación
15	ERP Financiero	Aplicación
16	Base de Datos Clientes	Información
17	Logs de Seguridad	Información
18	Servidor Web Apache	Infraestructura
19	Consola de Gestión de Incidentes	Seguridad
20	Políticas de Seguridad Documentadas	Documentación
21	Módulo KYC (Know Your Customer)	Aplicación
22	Contraseñas de Usuarios	Información
23	Dispositivo HSM	Seguridad
24	Certificados Digitales SSL	Seguridad
25	Panel de Administración de Usuarios	Aplicación
26	Red Wi-Fi Interna	Red
27	Sistema de Control de Acceso Físico	Infraestructura
28	Sistema de Video Vigilancia	Infraestructura
29	Bot de Atención al Cliente	Servicio Web
30	Código Fuente del Core Bancario	Información
31	Tabla de Usuarios y Roles	Información
32	Documentación Técnica	Documentación
33	Manuales de Usuario	Documentación
34	Script de Backups Automáticos	Seguridad
35	Datos de Transacciones Diarias	Información
36	Herramienta SIEM	Seguridad

Nº	Activo	Tipo
37	Switches y Routers	Red
38	Plan de Recuperación ante Desastres	Documentación
39	Contratos Digitales	Información Legal
40	Archivos de Configuración de Servidores	Información
41	Infraestructura en la Nube	Infraestructura
42	Correo Electrónico Ejecutivo	Información
43	Panel de Supervisión Financiera	Aplicación
44	App Móvil para Clientes	Aplicación
45	Token de Acceso a APIs	Seguridad
46	Base de Datos Histórica	Información
47	Entorno de Desarrollo	Infraestructura
48	Sistema de Alertas de Seguridad	Seguridad
49	Configuración del Cortafuegos	Seguridad
50	Redundancia de Servidores	Infraestructura

Anexo 2: Rúbrica de Evaluación

Criterio	0 pts	5 pts	Puntaje
Login	No presenta evidencia o está incorrecto	Login ficticio completo, funcional y con evidencia clara	5
IA	No presenta IA o está incorrecta	IA implementada, funcionando y con evidencia clara	5
Evaluación de 5 Activos	Menos de 5 activos evaluados o sin hallazgos válidos	5 activos evaluados con hallazgos claros y evidencias	5
Informe claro y completo	Informe ausente, incompleto o poco entendible	Informe bien estructurado y completo según lo requerido	5

Puntaje Final: 20/20