

# AT5 Audit Platform: Manual de Usuario para Auditoria de Software

## Guia Completa para Auditores

### Procedimientos de Verificacion y Validacion de Software

**Version:** 1.0.0 **Fecha:** Enero 2026 **Clasificacion:** Manual Operativo de Usuario **Audiencia:** Auditores de Software, Lead Auditors, Reviewers **Estandares:** ISO/IEC/IEEE 29119, ISTQB Foundation Level

## Indice de Contenidos

1. [Introduccion al Sistema](#)
2. [Requisitos y Acceso al Sistema](#)
3. [Autenticacion y Roles de Usuario](#)
4. [Panel de Control \(Dashboard\)](#)
5. [Gestion de Sesiones de Auditoria](#)
6. [Ejecucion de Casos de Prueba](#)
7. [Gestion de Evidencias](#)
8. [Proceso de Firma y Aprobacion](#)
9. [Generacion de Reportes](#)
10. [Consulta del Log de Auditoria](#)
11. [Flujo Completo de Auditoria: Caso Practico](#)
12. [Resolucion de Problemas Comunes](#)
13. [Glosario de Terminos](#)
14. [Anexos](#)

## 1. Introduccion al Sistema

### 1.1 Proposito de AT5 Audit Platform

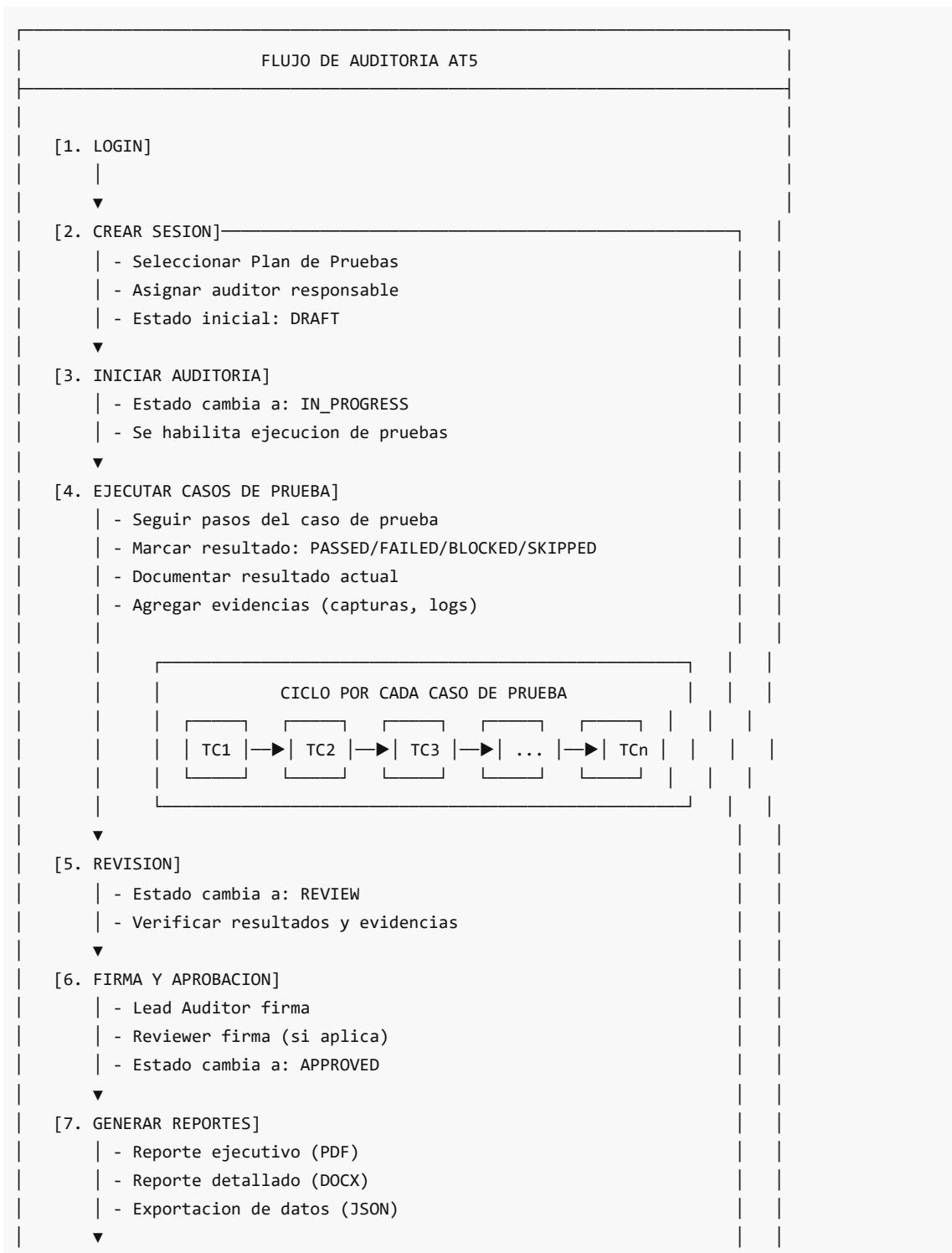
AT5 Audit Platform es un sistema empresarial de auditoria de software disenado para facilitar la ejecucion, documentacion y trazabilidad de pruebas de software de acuerdo con los estandares internacionales ISO/IEC/IEEE 29119 (Software Testing) e ISTQB (International Software Testing Qualifications Board).

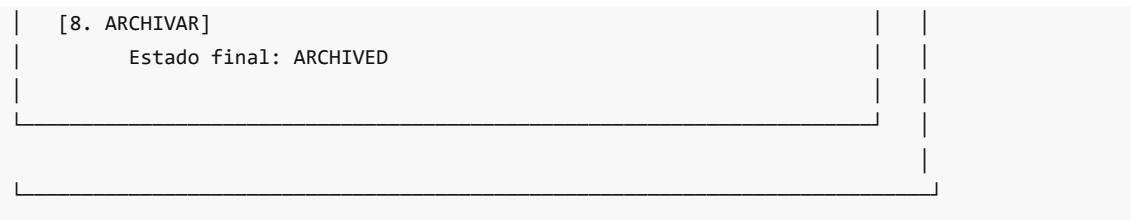
### 1.2 Caracteristicas Principales

Caracteristica	Descripcion	Beneficio para el Auditor
Ejecucion Interactiva	Interfaz paso a paso para ejecutar casos de prueba	Guia clara del proceso de testing
Gestion de Evidencias	Subida y almacenamiento de capturas, logs y documentos	Documentacion completa para reportes
Firmas Digitales	Certificados SHA-256 para aprobacion de sesiones	No repudio y validez legal
Audit Log Inmutable	Registro cronologico con hash encadenado	Trazabilidad total de acciones

<b>Reportes Automaticos</b>	Generacion de informes en multiples formatos	Ahorro de tiempo en documentacion
<b>Metricas en Tiempo Real</b>	Dashboards con KPIs de auditoria	Visibilidad del progreso

### 1.3 Flujo General de Trabajo





## 2. Requisitos y Acceso al Sistema

### 2.1 Requisitos de Hardware

Componente	Mínimo	Recomendado
Procesador	Dual Core 2.0 GHz	Quad Core 2.5 GHz+
Memoria RAM	4 GB	8 GB+
Almacenamiento	500 MB libre	2 GB+ libre
Pantalla	1280x720	1920x1080+
Conexión	1 Mbps	10 Mbps+

### 2.2 Requisitos de Software

Software	Versión Mínima	Notas
Navegador Web	Chrome 90+, Firefox 88+, Edge 90+, Safari 14+	Se recomienda Chrome
JavaScript	Habilitado	Requerido para funcionamiento
Cookies	Habilitadas	Necesario para sesión
PDF Reader	Integrado en navegador	Para visualizar reportes

### 2.3 URL de Acceso

Producción: <https://at5-audit.axongroup.com>

Desarrollo: <http://localhost:3000>

## 3. Autenticación y Roles de Usuario

### 3.1 Proceso de Inicio de Sesión

#### Paso 1: Acceder a la Página de Login

1. Abra su navegador web preferido
2. Ingrese la URL del sistema: <http://localhost:3000/login>
3. Aparecerá la pantalla de inicio de sesión con el logo de AT5 Audit Platform

#### Paso 2: Ingresar Credenciales

1. En el campo "**Correo Electrónico**", ingrese su email corporativo
2. En el campo "**Contrasena**", ingrese su contraseña

3. Opcionalmente, haga clic en el icono del ojo para ver/ocultar la contraseña

### Paso 3: Autenticar

1. Haga clic en el botón "Ingresar"
2. Si las credenciales son correctas, será redirigido al Dashboard
3. Si son incorrectas, verá un mensaje de error en rojo

The screenshot shows the login interface for the AT5 Audit Platform. At the top, it displays the platform's name: "AT5 Audit Platform" and "Sistema de Auditoria Interactiva". Below this, the title "Iniciar Sesión" is centered, followed by the instruction "Ingrese sus credenciales para acceder al sistema". There are two input fields: "Correo Electronico" containing "usuario@axongroup.com" and "Contraseña" containing "\*\*\*\*\*". To the right of the password field is a small square checkbox labeled "o". Below these fields is a large rectangular button labeled "Ingresar". At the bottom of the page, there is a section titled "Credenciales de Prueba:" listing four sets of credentials:

Lead Auditor:	garcia@axongroup.com
Auditor:	lopez@axongroup.com
Reviewer:	martinez@axongroup.com
Contraseña:	audit2026

### 3.2 Credenciales de Prueba (Ambiente de Desarrollo)

Para propósitos de prueba y demostración, el sistema incluye los siguientes usuarios pre-configurados:

Rol	Email	Contraseña	Permisos
<b>Lead Auditor</b>	<a href="mailto:garcia@axongroup.com">garcia@axongroup.com</a>	audit2026	Crear sesiones, ejecutar pruebas, firmar
<b>Auditor</b>	<a href="mailto:lopez@axongroup.com">lopez@axongroup.com</a>	audit2026	Ejecutar pruebas, agregar evidencias
<b>Reviewer</b>	<a href="mailto:martinez@axongroup.com">martinez@axongroup.com</a>	audit2026	Revisión y firma de aprobación

### **3.3 Roles y Permisos Detallados**

#### **ADMIN (Administrador)**

- Acceso total al sistema
- Gestión de usuarios y organizaciones
- Configuración del sistema
- Visualización de todos los logs

#### **LEAD\_AUDITOR (Auditor Líder)**

- Crear y gestionar sesiones de auditoría
- Ejecutar todos los casos de prueba
- Agregar y eliminar evidencias
- Firmar sesiones para aprobación
- Acceso a configuración básica
- Ver logs de auditoría

#### **AUDITOR (Auditor)**

- Ejecutar casos de prueba asignados
- Agregar evidencias a ejecuciones
- Documentar resultados
- No puede firmar sesiones

#### **REVIEWER (Revisor)**

- Solo lectura de sesiones y resultados
- Puede firmar para aprobar sesiones
- Acceso a logs de auditoría
- No puede ejecutar pruebas

#### **VIEWER (Observador)**

- Solo lectura
- Puede ver dashboard y sesiones
- Puede descargar reportes
- Sin capacidad de modificación

### **3.4 Seguridad de la Cuenta**

#### **Sistema de Bloqueo Automático:**

- Despues de **5 intentos fallidos** de login, la cuenta se bloquea por **15 minutos**
- El sistema registra todos los intentos de login en el audit log
- Las contrasenas se almacenan encriptadas con bcrypt (10 rounds)

#### **Duración de Sesión:**

- La sesión de usuario expira automáticamente despues de **8 horas** de inactividad
- Al cerrar el navegador, se mantiene la sesión (cookie persistente)

---

## **4. Panel de Control (Dashboard)**

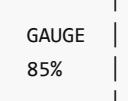
### **4.1 Vista General del Dashboard**

Al iniciar sesión exitosamente, el auditor es dirigido al Dashboard principal, que presenta una vista consolidada del estado de las auditorías.

AT5 Audit Platform [User] [Logout]

Dashboard [+ Nueva Auditoria]  
Bienvenido, Maria Garcia. Sistema de auditoria AT5 MCP

Sesiones Activas  3	Tasa de Exito  85%	En Revision  2	Completadas  8
--	---	---	--

Estado de Ejecuciones 	Tasa de Exito Global  85%
<ul style="list-style-type: none"><li>• Aprobadas: 21</li><li>• Fallidas: 2</li><li>• Bloqueadas: 1</li><li>• Pendientes: 9</li></ul>	Aprobadas: 21 Fallidas: 2

Sesiones Recientes [Ver todas]

Auditoria Sistema Login v2.1 Maria Garcia	En Progreso   75% 18/24 casos
Auditoria API REST Backend Juan Lopez	En Revision   100% 12/12 casos

Actividad Reciente [Ver logs]

LOGIN	Usuario garcia inicio sesion	Hace 5m
TEST_PASSED	TC-001 marcado como PASSED	Hace 12m
SIGNATURE	Firma agregada por martinez	Hace 1h

## 4.2 Componentes del Dashboard

### 4.2.1 Tarjetas de Estadísticas Principales

Tarjeta	Descripcion	Color
<b>Sesiones Activas</b>	Auditorias en estado IN_PROGRESS	Azul
<b>Tasa de Exito</b>	% de pruebas PASSED vs FAILED	Verde
<b>En Revision</b>	Sesiones esperando firmas	Amarillo
<b>Completadas</b>	Sesiones APPROVED + ARCHIVED	Verde Teal

### 4.2.2 Graficos Interactivos

1. **Grafico de Torta (Pie Chart)**: Distribucion de estados de ejecucion

- Verde: Aprobadas (PASSED)
- Rojo: Fallidas (FAILED)
- Amarillo: Bloqueadas (BLOCKED)
- Gris: Omitidas (SKIPPED)
- Gris claro: Pendientes (NOT\_STARTED)

2. **Indicador de Exito (Gauge)**: Tasa de exito global como velocimetro visual

3. **Grafico de Tendencia (Line Chart)**: Evolucion de ejecuciones en ultimos 7 dias

4. **Grafico de Barras**: Progreso de sesiones activas

## 4.3 Acciones Rapidas

Desde el Dashboard, el auditor puede:

1. **Crear Nueva Auditoria**: Boton superior derecho "[+ Nueva Auditoria]"
2. **Continuar Auditoria**: Tarjeta "Continuar Auditoria" - retoma la ultima sesion
3. **Revisar Defectos**: Acceso directo a casos FAILED
4. **Aprobar Sesion**: Acceso a sesiones pendientes de firma

## 5. Gestión de Sesiones de Auditoria

### 5.1 Crear Nueva Sesión de Auditoria

#### Paso 1: Acceder al Formulario de Creacion

1. Desde el Dashboard, haga clic en "[+ Nueva Auditoria]"
2. O navegue a: **Sesiones > Nueva Sesión** desde el menu lateral

#### Paso 2: Completar Información de la Sesión

Nueva Sesión de Auditoria

Nombre de la Sesion *	<input type="text" value="Auditoria Sistema de Facturacion v3.0"/>
Descripcion	<input type="text" value="Auditoria completa del modulo de facturacion electronica incluyendo integracion con SII y generacion de DTE."/>
Plan de Pruebas *	<input type="text" value="Plan de Pruebas - Sistema Facturacion v3.0 (33 casos) [▼]"/>
Auditor Responsable *	<input type="text" value="Maria Garcia (Lead Auditor) [▼]"/>
<input type="button" value="Cancelar"/> <input type="button" value="Crear"/>	

#### Campos del Formulario:

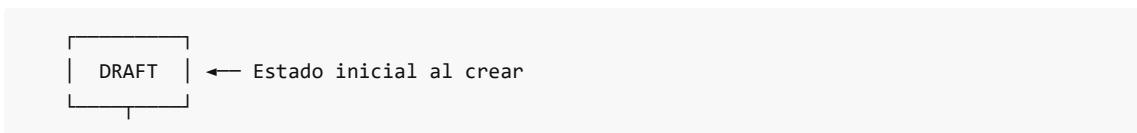
Campo	Obligatorio	Descripcion
<b>Nombre de la Sesion</b>	Si	Identificador descriptivo de la auditoria
<b>Descripcion</b>	No	Detalle del alcance y objetivos
<b>Plan de Pruebas</b>	Si	Seleccionar plan con casos de prueba
<b>Auditor Responsable</b>	Si	Usuario que ejecutara las pruebas

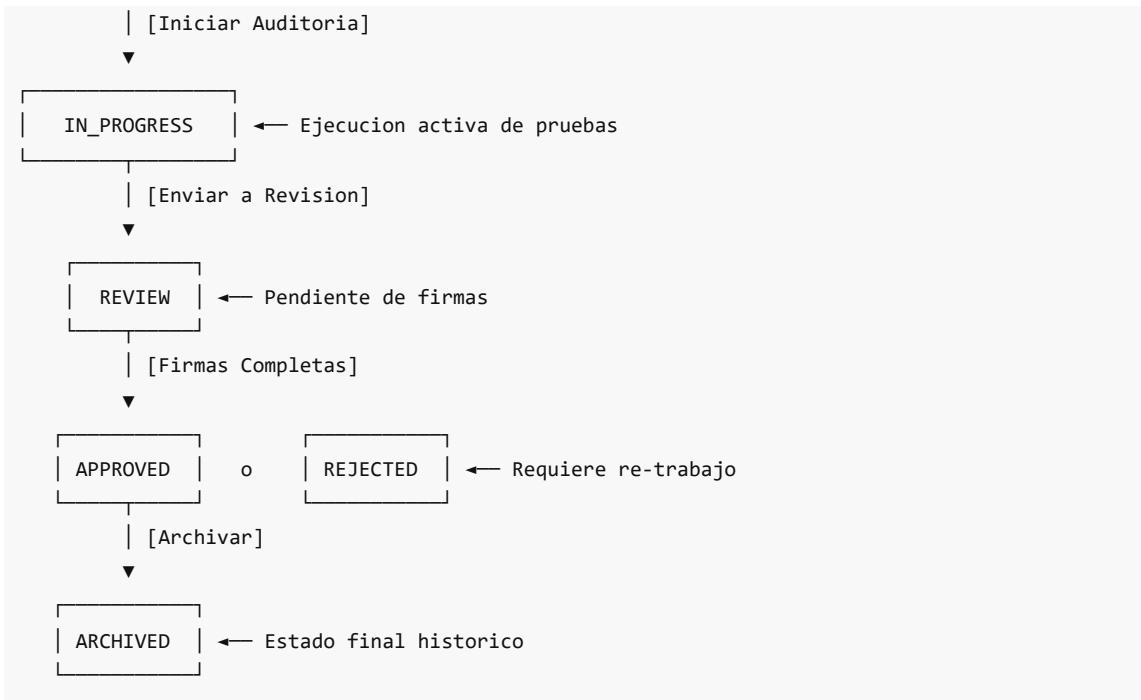
#### Paso 3: Confirmar Creacion

1. Verifique que todos los campos obligatorios esten completos
2. Haga clic en "**Crear**"
3. El sistema mostrara un mensaje de confirmacion
4. La sesion se crea en estado **DRAFT** (Borrador)

#### 5.2 Estados de una Sesion

Una sesion de auditoria pasa por los siguientes estados durante su ciclo de vida:





## 5.3 Ver Lista de Sesiones

1. Navegue a **Sesiones** desde el menu lateral
  2. Verá una tabla con todas las sesiones disponibles

Sesiones de Auditoria					[+ Nueva Sesión]	
Filtros: [Todos ▼] [Fecha ▼] [Auditor ▼]					[Buscar...]	
Nombre	Auditor	Estado	Progreso	Fecha		
Auditoria Sistema Login	M. Garcia	En Progreso	<div style="width: 75%; background-color: #ccc;"></div> 75%	15/01		
Auditoria API Backend	J. Lopez	En Revision	<div style="width: 100%; background-color: #ccc;"></div> 100%	14/01		
Auditoria Reportes PDF	M. Garcia	Borrador	<div style="width: 0%; background-color: #ccc;"></div> 0%	13/01		
Auditoria Modulo Pagos	P.Martinez	Aprobada	<div style="width: 100%; background-color: #ccc;"></div> 100%	10/01		

## 5.4 Ver Detalle de Sesión

1. Haga clic en una sesion de la lista
  2. Verá la pantalla de detalle con toda la información

### **Informacion mostrada:**

- Nombre y descripción de la sesión

- Estado actual y progreso
  - Estadísticas: Aprobados, Fallidos, Bloqueados, Omitidos
  - Lista de casos de prueba con sus estados
  - Firmas requeridas y completadas
  - Botones de acción según el estado
- 

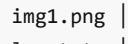
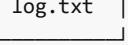
## 6. Ejecución de Casos de Prueba

### 6.1 Acceder al Modo de Ejecución

1. Desde el detalle de una sesión, haga clic en "**Ejecutar Pruebas**"
2. O desde una sesión en estado IN\_PROGRESS, haga clic en "**Continuar**"

### 6.2 Interfaz de Ejecución Interactiva

La pantalla de ejecución se divide en tres columnas:

← Auditoria Sistema Login v2.1		Progreso:  33%
Casos de Prueba	Detalle del Caso de Prueba	Cronómetro
[Suite: Login]	TC-LOG-001 [CRITICAL] Validar Login con Credenciales Validas • TC-LOG-001 ○ TC-LOG-002 ○ TC-LOG-003 ○ TC-LOG-004	00:00:00 [▶] [⌚]
	Descripción: Verificar que el usuario puede ingresar al sistema con credenciales validas.	Estadísticas
		• Aprobados: 4 • Fallidos: 0 ○ Pendientes:
[Suite: 2FA]	Precondiciones: - Usuario registrado en el sistema - Cuenta activa y no bloqueada	Evidencias
	Resultado Esperado: El usuario es redirigido al Dashboard y se muestra su nombre en el header.	[↑] Subir  
	Pasos de Ejecución: <input checked="" type="checkbox"/> Paso 1: Navegar a /login <input type="checkbox"/> Paso 2: Ingresar email válido <input type="checkbox"/> Paso 3: Ingresar contraseña <input type="checkbox"/> Paso 4: Clic en "Ingresar" <input type="checkbox"/> Paso 5: Verificar redirección	
	Resultado Actual:	

		Describa el resultado observado...		
		<input type="checkbox"/> Aprobado <input type="checkbox"/> Fallido <input type="checkbox"/> Bloqueado <input type="checkbox"/> Omit		

## **6.3 Procedimiento de Ejecucion Paso a Paso**

## Paso 1: Seleccionar Caso de Prueba

1. En el panel izquierdo, los casos aparecen agrupados por **Suite de Pruebas**
  2. Los iconos indican el estado:
    - Gris: No ejecutado
    - Verde: Aprobado (PASSED)
    - Rojo: Fallido (FAILED)
    - Amarillo: Bloqueado (BLOCKED)
    - Gris oscuro: Omitido (SKIPPED)
  3. Haga clic en un caso para seleccionarlo
  4. El sistema automaticamente selecciona el primer caso pendiente

## Paso 2: Revisar Información del Caso

Antes de ejecutar, revise cuidadosamente:

1. **Código del Caso:** Identificador único (ej: TC-LOG-001)
  2. **Prioridad:** CRITICAL, HIGH, MEDIUM, LOW
  3. **Descripción:** Objetivo de la prueba
  4. **Precondiciones:** Requisitos previos que deben cumplirse
  5. **Resultado Esperado:** Comportamiento correcto del sistema

### **Paso 3: Iniciar Cronómetro (Opcional)**

1. Haga clic en el botón **[▶]** para iniciar el cronómetro
  2. Use **[↻]** para reiniciar si es necesario
  3. El tiempo se registra automáticamente al guardar el resultado

## Paso 4: Ejecutar los Pasos

1. Siga cada paso indicado en la lista de "Pasos de Ejecución"
  2. Marque cada paso completado haciendo clic en el checkbox
  3. Los pasos marcados cambian de color para indicar progreso

## Ejemplo de Pasos:

- Paso 1: Navegar a la pagina de login (/login)
  - Paso 2: Ingresar email valido en el campo correspondiente
  - Paso 3: Ingresar contraseña correcta
  - Paso 4: Hacer clic en el botón "Ingresar"
  - Paso 5: Verificar redirección al Dashboard

#### **Paso 5: Documentar Resultado Actual**

1. En el campo "**Resultado Actual**", describa lo que observo
  2. Sea específico y objetivo

3. Si hay errores, incluya mensajes de error exactos

#### Ejemplo de documentacion:

Correcto: "El usuario fue redirigido exitosamente al Dashboard.  
El nombre 'Maria Garcia' aparece en el header."

Incorrecto: "Funciona bien" (demasiado vago)

Para FAILED: "Se mostro error 'Credenciales invalidas' a pesar de usar credenciales correctas. Codigo de error HTTP 401."

#### Paso 6: Agregar Notas Adicionales (Opcional)

1. Use el campo "**Notas adicionales**" para informacion complementaria
2. Puede incluir: observaciones, sugerencias, contexto adicional

#### Paso 7: Registrar Resultado

Seleccione el resultado apropiado haciendo clic en el boton correspondiente:

Resultado	Cuando Usarlo	Color
<b>Aprobado</b>	El sistema se comporto segun lo esperado	Verde
<b>Fallido</b>	Se detecto un defecto o comportamiento incorrecto	Rojo
<b>Bloqueado</b>	No se pudo ejecutar por dependencias no satisfechas	Amarillo
<b>Omitir</b>	El caso esta fuera del alcance actual	Gris

#### Criterios para cada resultado:

##### PASSED (Aprobado):

- Todos los pasos se completaron exitosamente
- El resultado observado coincide con el esperado
- No hay desviaciones del comportamiento definido

##### FAILED (Fallido):

- Al menos un paso no se completo correctamente
- El resultado observado difiere del esperado
- Se detecto un defecto, error o comportamiento inesperado
- **IMPORTANTE:** Siempre agregue evidencia (captura de pantalla, log de error)

##### BLOCKED (Bloqueado):

- No fue posible ejecutar la prueba
- Existe una dependencia que impide la ejecucion
- Ejemplos: servidor caido, datos de prueba no disponibles, permisos faltantes
- **IMPORTANTE:** Documente la razon del bloqueo

##### SKIPPED (Omitido):

- El caso de prueba no aplica en este ciclo
- Esta fuera del alcance acordado

- Razon valida para no ejecutar

#### **Paso 8: Avanzar al Siguiente Caso**

1. Despues de registrar el resultado, el sistema automaticamente avanza al siguiente caso pendiente
2. O puede seleccionar manualmente otro caso del panel izquierdo

#### **6.4 Tipos de Casos de Prueba**

El sistema soporta diferentes tipos de pruebas segun ISO/IEC/IEEE 29119-4:

Tipo	Descripcion	Ejemplo
<b>FUNCTIONAL</b>	Verifican funcionalidad del sistema	Login, CRUD de datos
<b>INTEGRATION</b>	Verifican comunicacion entre componentes	API + Base de datos
<b>PERFORMANCE</b>	Miden tiempos de respuesta	Carga de pagina < 3s
<b>SECURITY</b>	Verifican vulnerabilidades	SQL Injection, XSS
<b>USABILITY</b>	Evaluau experiencia de usuario	Navegacion intuitiva
<b>REGRESSION</b>	Verifican que cambios no rompan funcionalidad	Despues de deploy

### **7. Gestión de Evidencias**

#### **7.1 Tipos de Evidencia Soportados**

Tipo	Extensiones	Uso Recomendado
<b>Screenshot</b>	.png, .jpg, .jpeg, .gif, .webp	Capturas de pantalla
<b>Log</b>	.txt, .log	Archivos de log del sistema
<b>PDF</b>	.pdf	Documentos, reportes
<b>Video</b>	.mp4, .webm	Grabaciones de ejecucion
<b>JSON</b>	.json	Respuestas de API, datos
<b>Other</b>	Otros	Cualquier archivo relevante

#### **7.2 Subir Evidencia**

##### **Metodo 1: Arrastrar y Soltar (Drag & Drop)**

1. Ubique el panel de "**Evidencias**" en la columna derecha
2. Arrastre el archivo desde su explorador de archivos
3. Suelte el archivo en el area indicada
4. El archivo se sube automaticamente

##### **Metodo 2: Boton de Seleccion**

1. Haga clic en "**Seleccionar Archivos**"
2. En el dialogo, navegue hasta el archivo
3. Seleccione uno o mas archivos

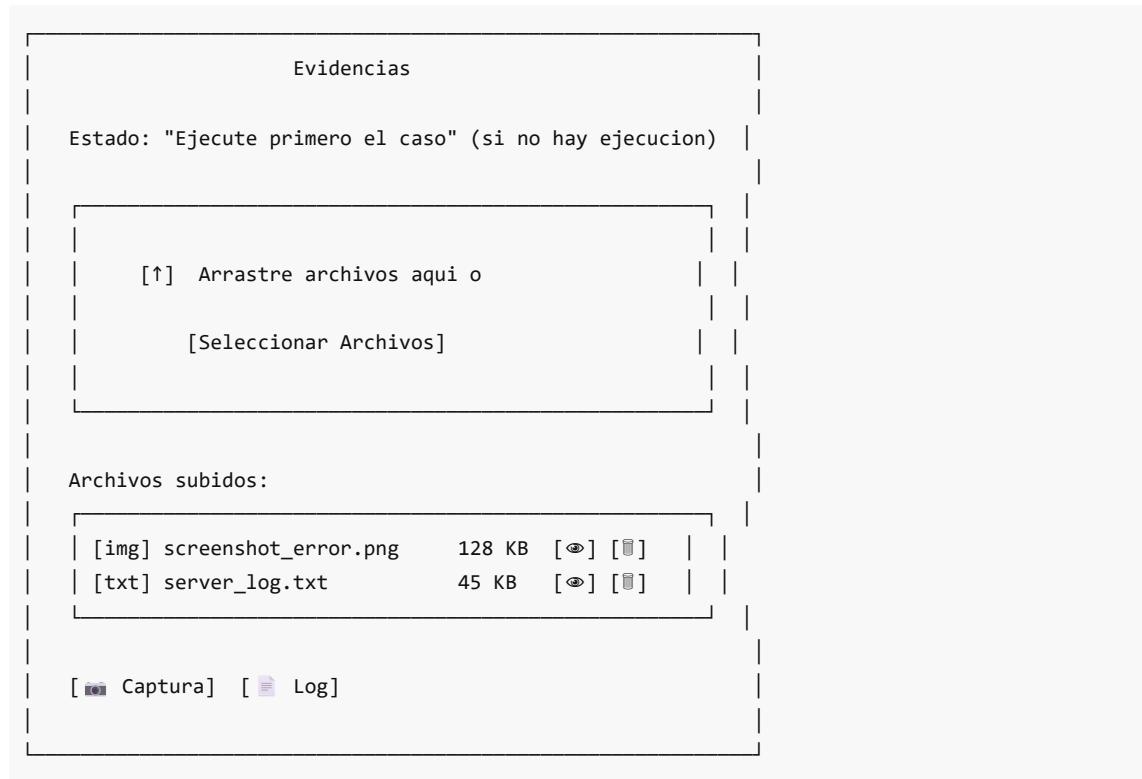
4. Haga clic en "Abrir"

#### Metodo 3: Botones Rapidos

- "**Captura**": Abre selector solo para imagenes
- "**Log**

### 7.3 Requisitos para Subir Evidencia

**IMPORTANTE:** Solo puede subir evidencia despues de que el caso de prueba tenga al menos un resultado registrado. El sistema requiere una "ejecucion" existente para asociar la evidencia.



### 7.4 Visualizar Evidencia

1. Haga clic en el icono [👁] (ojito) junto al archivo
2. Se abrirá un dialogo de vista previa
3. Para imágenes: muestra la imagen completa
4. Para PDF: muestra el documento embebido
5. Para otros: ofrece botón de descarga

### 7.5 Eliminar Evidencia

1. Haga clic en el icono [📄] (papelera) junto al archivo
2. Confirme la eliminación en el diálogo
3. **ADVERTENCIA:** Esta acción queda registrada en el audit log

### 7.6 Integridad de Evidencias

Cada evidencia subida genera automáticamente:

- **Hash SHA-256:** Garantiza que el archivo no ha sido modificado
- **Timestamp:** Fecha y hora exacta de subida

- **Metadatos:** Tamano, tipo MIME, nombre original

Esta informacion aparece al ver el detalle de la evidencia:

Hash SHA-256: a1b2c3d4e5f6...  
Subido: 15/01/2026 14:32:45

## 8. Proceso de Firma y Aprobacion

### 8.1 Requisitos para Firmar

Una sesion puede ser firmada cuando:

1. El estado es **REVIEW** (en revision)
2. El usuario tiene rol **LEAD\_AUDITOR**, **REVIEWER**, o **ADMIN**
3. El usuario no ha firmado previamente esta sesion

### 8.2 Firmas Requeridas

Para que una sesion sea aprobada, se requieren las siguientes firmas:

Rol	Obligatorio	Proposito
<b>LEAD_AUDITOR</b>	Si	Certifica la ejecucion correcta
<b>REVIEWER</b>	Si	Certifica la revision de resultados

### 8.3 Procedimiento de Firma

#### Paso 1: Acceder a la Sesión en Revision

1. Navegue a la sesion con estado **REVIEW**
2. Vera la seccion de "Firmas y Aprobaciones"

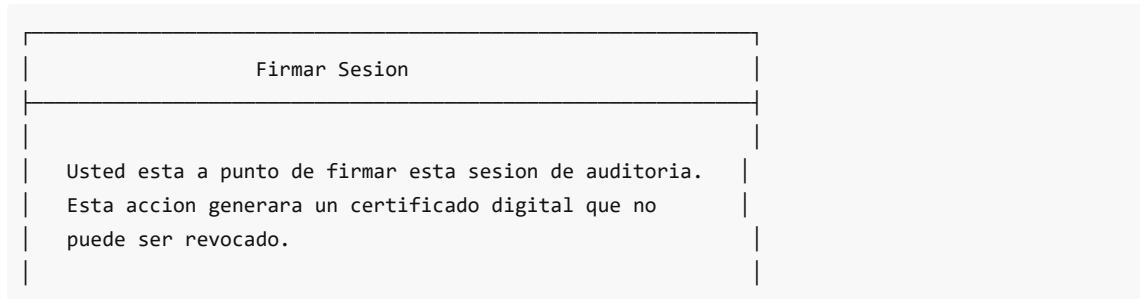
#### Paso 2: Revisar Resultados

Antes de firmar, verifique:

- Todos los casos de prueba tienen resultado
- Las evidencias estan completas
- Los resultados estan correctamente documentados

#### Paso 3: Agregar Firma

1. Haga clic en "**Agregar Firma**"
2. Opcionalmente, dibuje su firma en el canvas
3. Haga clic en "**Firmar**"



Firma Visual (opcional):	
[Canvas para dibujar firma]	
Al firmar, certifico que:	
<ul style="list-style-type: none"> <li>- He revisado los resultados de esta auditoria</li> <li>- Los resultados son precisos y completos</li> <li>- Las evidencias son autenticas</li> </ul>	
<input type="button" value="Cancelar"/>	<input type="button" value="Firmar"/>

#### 8.4 Certificado Digital

Al firmar, el sistema genera un certificado digital que incluye:

Campo	Descripcion
<b>ID de Firma</b>	Identificador unico
<b>Usuario</b>	Nombre y email del firmante
<b>Rol</b>	Rol del firmante al momento de firmar
<b>Fecha/Hora</b>	Timestamp exacto de la firma
<b>IP Address</b>	Direccion IP desde donde se firmo
<b>Certificado SHA-256</b>	Hash criptografico del estado de la sesion

#### 8.5 Verificacion de Firma

Para verificar la autenticidad de una firma:

1. En la seccion de firmas, haga clic en "**Verificar**" junto a una firma
2. El sistema recalculara el hash y comparara
3. Resultado:
  - **VALIDA:** El hash coincide, datos no alterados
  - **INVALIDA:** El hash no coincide, posible alteracion

Resultado de Verificacion
✓ FIRMA VALIDA

Firmante: Maria Garcia	
Rol: Lead Auditor	
Fecha: 15/01/2026 16:45:32	
Certificado: a1b2c3d4e5f6g7h8i9j0k1l2m3n4o5p6...	
Los datos de la sesion no han sido modificados desde que se agrego esta firma.	
<a href="#">Cerrar</a>	

## 8.6 Aprobacion Automatica

Cuando todas las firmas requeridas estan presentes:

1. El estado de la sesion cambia automaticamente a **APPROVED**
  2. Se genera un registro en el audit log
  3. La sesion queda lista para archivar y generar reportes finales
- 

## 9. Generacion de Reportes

### 9.1 Tipos de Reportes Disponibles

Tipo	Descripcion	Formato
<b>Resumen Ejecutivo</b>	Vista de alto nivel para gerencia	PDF
<b>Reporte Detallado</b>	Informacion completa de todas las pruebas	DOCX
<b>Reporte de Defectos</b>	Solo casos FAILED con evidencias	PDF
<b>Metricas</b>	Estadisticas y KPIs	JSON

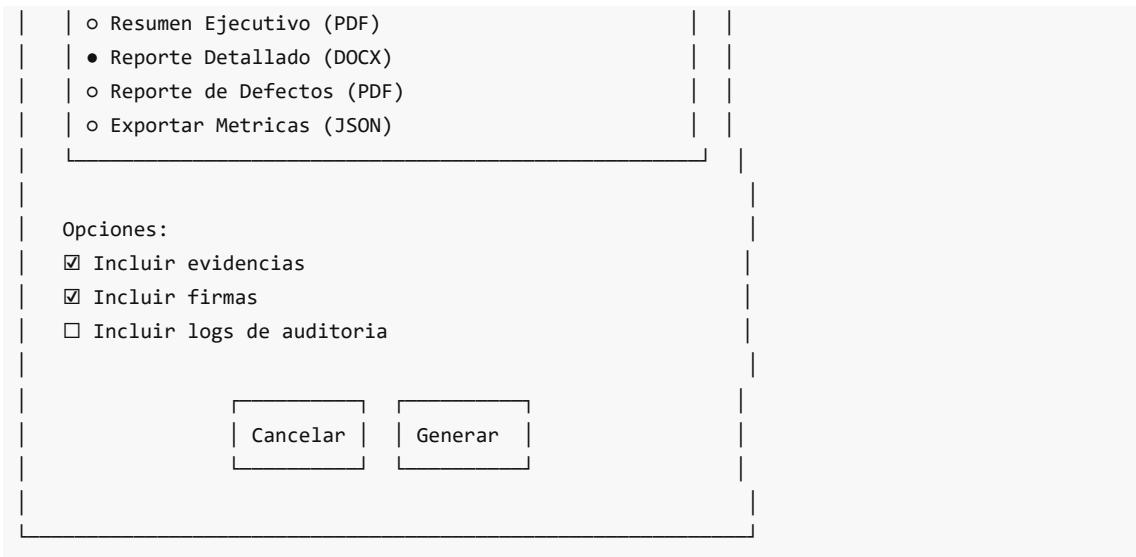
### 9.2 Generar Reporte

#### Paso 1: Acceder a Generacion de Reportes

1. Desde el detalle de una sesion, haga clic en "**Generar Reporte**"
2. O navegue a **Reportes** desde el menu lateral

#### Paso 2: Seleccionar Tipo de Reporte

<a href="#">Generar Reporte</a>
Sesion: Auditoria Sistema Login v2.1
Tipo de Reporte:



### Paso 3: Descargar Reporte

1. Haga clic en "**Generar**"
2. Espere mientras el sistema procesa
3. El archivo se descargara automaticamente
4. O haga clic en el enlace de descarga si no inicia

### 9.3 Contenido del Reporte Detallado

El reporte detallado incluye las siguientes secciones:

#### 1. Portada

- Nombre de la sesion
- Fecha de ejecucion
- Auditor responsable
- Estado final

#### 2. Resumen Ejecutivo

- Total de casos ejecutados
- Tasa de exito
- Defectos detectados
- Recomendaciones

#### 3. Detalle de Ejecuciones

- Por cada caso de prueba:
  - Codigo y nombre
  - Resultado y duracion
  - Resultado esperado vs actual
  - Evidencias adjuntas

#### 4. Registro de Firmas

- Lista de firmantes
- Certificados de firma

#### 5. Anexos

- Evidencias en alta resolucion
- Logs relevantes

## 10. Consulta del Log de Auditoria

### 10.1 Acceso al Audit Log

1. Navegue a **Audit Log** desde el menu lateral
2. **Requisito:** Rol ADMIN, LEAD\_AUDITOR, o REVIEWER

### 10.2 Interfaz del Audit Log

**Log de Auditoria**

Filtros:

[Usuario ▼] [Acción ▼] [Entidad ▼] [Desde: \_\_\_/\_\_\_/\_\_\_] [Hasta: \_\_\_/\_\_\_/\_\_\_]

Fecha/Hora	Usuario	Acción	Entidad	Detalle
15/01 16:45:32	M. Garcia	SIGNATURE_ADD	Signature	Firma...
15/01 16:30:15	M. Garcia	TEST_PASSED	Execution	TC-001...
15/01 16:25:08	M. Garcia	TEST_FAILED	Execution	TC-002...
15/01 14:00:00	M. Garcia	LOGIN	User	Usuario...
14/01 18:30:22	J. Lopez	EVIDENCE_UP	Evidence	Subida...

Mostrando 1-50 de 234 registros      [< 1 2 3 4 >]

[Verificar Integridad]

### 10.3 Filtros Disponibles

Filtro	Descripción
<b>Usuario</b>	Filtrar por usuario que realizó la acción
<b>Acción</b>	Tipo de acción (LOGIN, TEST_PASSED, etc.)
<b>Entidad</b>	Tipo de objeto afectado (User, Session, etc.)
<b>Fecha Desde</b>	Inicio del rango de fechas
<b>Fecha Hasta</b>	Fin del rango de fechas

### 10.4 Acciones Registradas

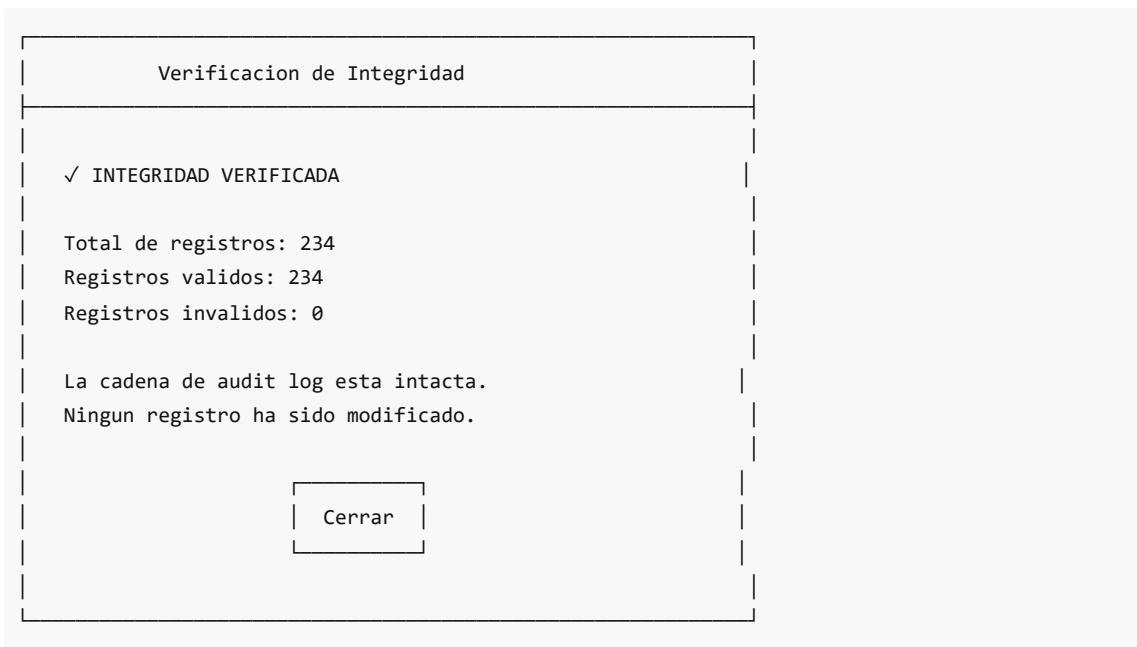
Acción	Descripción
LOGIN	Inicio de sesión exitoso

LOGOUT	Cierre de sesion
LOGIN_FAILED	Intento de login fallido
SESSION_CREATED	Creacion de sesion de auditoria
SESSION_UPDATED	Modificacion de sesion
TEST_EXECUTED	Caso de prueba ejecutado
TEST_PASSED	Caso marcado como aprobado
TEST_FAILED	Caso marcado como fallido
EVIDENCE_UPLOADED	Evidencia subida
EVIDENCE_DELETED	Evidencia eliminada
SIGNATURE_ADDED	Firma agregada
SIGNATURE_VERIFIED	Firma verificada
REPORT_GENERATED	Reporte generado

## 10.5 Verificar Integridad del Audit Log

El botón "**Verificar Integridad**" permite comprobar que ningún registro ha sido alterado:

1. Haga clic en "**Verificar Integridad**"
  2. El sistema recalcula todos los hashes secuencialmente
  3. Resultado:
    - o **INTEGRIDAD OK:** Todos los registros son validos
    - o **INTEGRIDAD COMPROMETIDA:** Se detectaron registros alterados



## 11. Flujo Completo de Auditoria: Caso Practico

### Escenario: Auditoria del Modulo de Login de un Sistema Web

A continuacion se presenta un ejemplo completo de como realizar una auditoria desde inicio a fin.

#### Fase 1: Preparacion (Lead Auditor)

##### 1.1 Iniciar Sesion

1. Acceder a <http://localhost:3000/login>
2. Ingresar: garcia@axongroup.com / audit2026
3. Hacer clic en "Ingresar"

##### 1.2 Crear Sesion de Auditoria

1. Clic en "+ Nueva Auditoria" en el Dashboard
2. Completar formulario:
  - Nombre: "Auditoria Modulo Login v2.1"
  - Descripcion: "Verificacion de funcionalidad de autenticacion"
  - Plan de Pruebas: "Plan de Pruebas - Modulo Login"
  - Auditor: "Maria Garcia"
3. Clic en "Crear"

##### 1.3 Iniciar Auditoria

1. Desde el detalle de la sesion, clic en "Iniciar Auditoria"
2. El estado cambia de DRAFT a IN\_PROGRESS
3. Clic en "Ejecutar Pruebas"

#### Fase 2: Ejecucion (Auditor)

##### 2.1 Ejecutar Caso TC-LOG-001: Login con Credenciales Validas

Informacion del Caso:

- Codigo: TC-LOG-001
- Prioridad: CRITICAL
- Tipo: FUNCTIONAL

Pasos:

1. [✓] Navegar a /login  
→ Accion: Abrir navegador e ir a <http://sistema.com/login>
2. [✓] Ingresar email valido  
→ Accion: Escribir "usuario@empresa.com" en campo email
3. [✓] Ingresar contrasena correcta  
→ Accion: Escribir "Password123" en campo contrasena
4. [✓] Clic en "Ingresar"  
→ Accion: Presionar boton de login

5. [✓] Verificar redireccion al Dashboard  
→ Resultado: URL cambio a /dashboard, nombre de usuario visible

Resultado Actual:

"El usuario fue autenticado exitosamente y redirigido al Dashboard.  
El nombre 'Usuario Demo' aparece en el encabezado.  
Tiempo de respuesta: 0.8 segundos."

Decision: [APROBADO ✓]

## 2.2 Ejecutar Caso TC-LOG-002: Login con Credenciales Invalidas

Informacion del Caso:

- Código: TC-LOG-002
- Prioridad: HIGH
- Tipo: SECURITY

Pasos:

1. [✓] Navegar a /login
2. [✓] Ingresar email valido
3. [✓] Ingresar contraseña incorrecta
4. [✓] Clic en "Ingresar"
5. [✓] Verificar mensaje de error

Resultado Esperado:

"Se muestra mensaje 'Credenciales invalidas' y el usuario permanece en la pagina de login."

Resultado Actual:

"Se mostro el mensaje 'Credenciales invalidas' correctamente.  
El usuario no fue autenticado y permanecio en /login.  
El campo de contraseña se limpio automaticamente."

Decision: [APROBADO ✓]

## 2.3 Ejecutar Caso TC-LOG-003: Bloqueo por Intentos Fallidos

Informacion del Caso:

- Código: TC-LOG-003
- Prioridad: CRITICAL
- Tipo: SECURITY

Pasos:

1. [✓] Navegar a /login
2. [✓] Intentar login con contraseña incorrecta 5 veces
3. [ ] Verificar bloqueo de cuenta

Resultado Esperado:

"Despues de 5 intentos fallidos, la cuenta se bloquea por 15 minutos con mensaje 'Cuenta bloqueada. Intente en X minutos'."

Resultado Actual:  
"Se realizaron 6 intentos fallidos pero la cuenta nunca se bloqueo.  
El usuario pudo seguir intentando indefinidamente.  
DEFECTO: El mecanismo de bloqueo no esta funcionando."

Evidencia Agregada:  
- captura\_6\_intentos.png (muestra contador no funcionando)  
- server\_log.txt (no hay registro de bloqueo)

Decision: [FALLIDO X]

## 2.4 Ejecutar Caso TC-LOG-004: Login con 2FA Habilitado

Informacion del Caso:

- Código: TC-LOG-004
- Prioridad: HIGH
- Tipo: SECURITY

Pasos:

1. [✓] Navegar a /login con usuario 2FA habilitado
2. [ ] Ingresar credenciales
3. [ ] Verificar solicitud de codigo 2FA

Resultado Actual:

"No fue posible ejecutar esta prueba. El ambiente de pruebas no tiene configurado el servidor de 2FA. Se requiere coordinacion con el equipo de infraestructura."

Decision: [BLOQUEADO △]

## Fase 3: Revision (Lead Auditor)

### 3.1 Revisar Resultados

1. Navegar al detalle de la sesion
2. Verificar estadisticas:
  - Total: 4 casos
  - Aprobados: 2
  - Fallidos: 1 (TC-LOG-003)
  - Bloqueados: 1 (TC-LOG-004)
  - Tasa de Exito: 66.7%
3. Revisar evidencias del caso fallido
4. Verificar documentacion completa

### 3.2 Enviar a Revision

1. Clic en "Enviar a Revision"
2. El estado cambia de IN\_PROGRESS a REVIEW
3. Se notifica al Reviewer

## Fase 4: Aprobacion (Lead Auditor + Reviewer)

### 4.1 Firma del Lead Auditor

1. Acceder a la sesion ([garcia@axongroup.com](mailto:garcia@axongroup.com))
2. En seccion "Firmas", clic en "Agregar Firma"
3. Confirmar firma
4. Resultado: Firma de LEAD\_AUDITOR registrada

### 4.2 Firma del Reviewer

1. Acceder con reviewer ([martinez@axongroup.com](mailto:martinez@axongroup.com))
2. Revisar toda la sesion
3. En seccion "Firmas", clic en "Agregar Firma"
4. Confirmar firma
5. Resultado: Firma de REVIEWER registrada
6. Estado cambia automaticamente a APPROVED

## Fase 5: Documentacion Final

### 5.1 Generar Reporte Ejecutivo

1. Clic en "Generar Reporte"
2. Seleccionar: Resumen Ejecutivo (PDF)
3. Opciones: Incluir evidencias, Incluir firmas
4. Clic en "Generar"
5. Descargar: "Auditoria\_Login\_v2.1\_Ejecutivo.pdf"

### 5.2 Generar Reporte de Defectos

1. Clic en "Generar Reporte"
2. Seleccionar: Reporte de Defectos (PDF)
3. Clic en "Generar"
4. Descargar: "Auditoria\_Login\_v2.1\_Defectos.pdf"

Contenido del reporte:

- TC-LOG-003: Bloqueo por intentos fallidos no funciona
  - Severidad: CRITICAL
  - Evidencias: 2 archivos adjuntos
  - Recomendacion: Corregir antes de produccion

## Resumen de la Auditoria

Metrica	Valor
Total Casos	4
Aprobados	2 (50%)
Fallidos	1 (25%)
Bloqueados	1 (25%)

Omitidos	0 (0%)
Tasa de Exito	66.7%
Duracion Total	2h 15m
Firmantes	2
Evidencias	3 archivos

## 12. Resolucion de Problemas Comunes

### 12.1 Problemas de Autenticacion

Problema	Causa Probable	Solucion
"Credenciales invalidas"	Contrasena incorrecta	Verificar mayusculas/minusculas
"Cuenta bloqueada"	5+ intentos fallidos	Esperar 15 minutos
"La cuenta esta desactivada"	Usuario inactivo	Contactar administrador
Pagina de login no carga	Error de red	Verificar conexion, limpiar cache

### 12.2 Problemas de Ejecucion

Problema	Causa Probable	Solucion
No puedo ejecutar pruebas	Sesion en estado DRAFT	Iniciar la auditoria primero
No aparecen casos de prueba	Plan sin casos	Verificar plan de pruebas asignado
Cronometro no funciona	JavaScript deshabilitado	Habilitar JS en navegador
Resultados no se guardan	Sesion expirada	Refrescar pagina, re-autenticar

### 12.3 Problemas de Evidencias

Problema	Causa Probable	Solucion
No puedo subir archivos	Sin ejecucion previa	Registrar resultado primero
"Archivo muy grande"	Lmite excedido	Comprimir archivo o dividir
Error al visualizar	Formato no soportado	Convertir a formato compatible
Evidencia no aparece	Cache del navegador	Limpiar cache o refrescar

### 12.4 Problemas de Firma

Problema	Causa Probable	Solucion
No puedo firmar	Rol sin permisos	Solo LEAD_AUDITOR/REVIEWER pueden firmar
"Ya firmaste"	Firma duplicada	Solo una firma por rol/usuario

Firma invalida	Datos modificados	Los datos cambiaron post-firma
----------------	-------------------	--------------------------------

## 13. Glosario de Terminos

Termino	Definicion
<b>Auditoria de Software</b>	Proceso de evaluacion independiente de productos o procesos de software
<b>Caso de Prueba</b>	Conjunto de condiciones y pasos para verificar un requisito especifico
<b>Certificado Digital</b>	Hash criptografico que garantiza la autenticidad de una firma
<b>Evidencia</b>	Archivo que documenta el resultado de una prueba
<b>Hash SHA-256</b>	Funcion criptografica que genera un resumen unico de datos
<b>Plan de Pruebas</b>	Documento que describe el alcance, enfoque y recursos de testing
<b>RBAC</b>	Control de Acceso Basado en Roles
<b>Sesion de Auditoria</b>	Instancia de ejecucion de un plan de pruebas
<b>Suite de Pruebas</b>	Agrupacion logica de casos de prueba relacionados
<b>Trazabilidad</b>	Capacidad de rastrear cada accion a su origen

## 14. Anexos

### Anexo A: Atajos de Teclado

Atajo	Accion
Ctrl + Enter	Guardar resultado actual
Espacio	Marcar/desmarcar paso actual
↑ / ↓	Navegar entre casos de prueba
P	Marcar como PASSED
F	Marcar como FAILED

### Anexo B: Formatos de Reporte

#### Reporte Ejecutivo (PDF)

- 2-3 paginas
- Graficos de resumen
- Para: Gerencia, stakeholders

#### Reporte Detallado (DOCX)

- 10+ paginas
- Cada caso documentado

- Para: Equipo tecnico, QA

#### **Reporte de Defectos (PDF)**

- Solo casos FAILED
- Evidencias adjuntas
- Para: Desarrolladores

#### **Anexo C: Contacto de Soporte**

Para asistencia tecnica:

- Email: [soporte@axongroup.com](mailto:soporte@axongroup.com)
  - Telefono: +56 2 1234 5678
  - Horario: Lunes a Viernes, 9:00 - 18:00 (Hora Chile)
- 

#### **Fin del Manual de Usuario**

*Documento generado para AT5 Audit Platform Version 1.0.0 - Enero 2026 Todos los derechos reservados*