

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

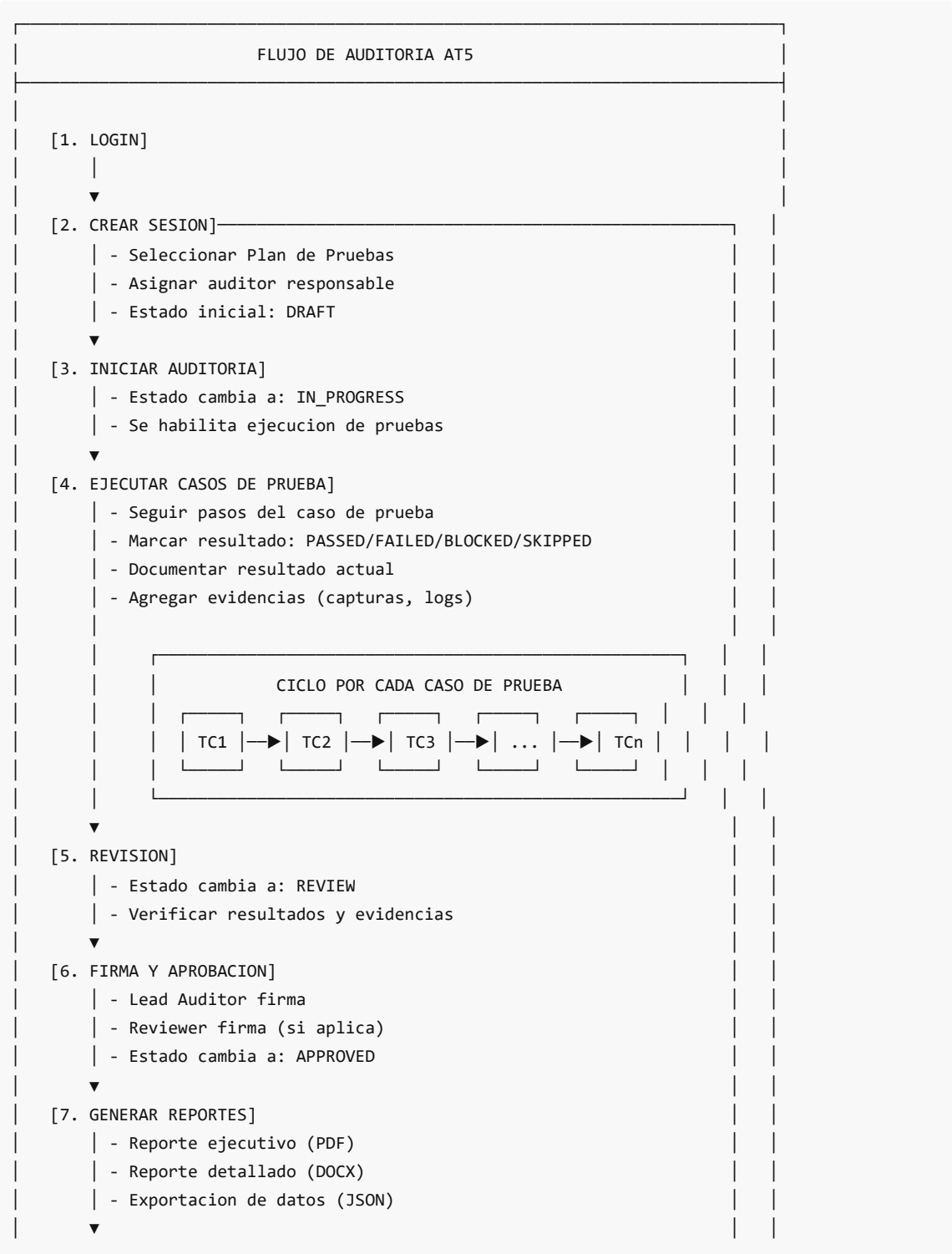
AT5 Audit Platform es un sistema empresarial de auditoria de software disenado para facilitar la ejecucion, documentacion y trazabilidad de pruebas de software de acuerdo con los estandares internacionales ISO/IEC/IEEE 29119 (Software Testing) e ISTQB (International Software Testing Qualifications Board).

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

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

1.3 Flujo General de Trabajo



[8. ARCHIVAR]

Estado final: ARCHIVED

2. Requisitos y Acceso al Sistema

2.1 Requisitos de Hardware

Componente	Minimo	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+
Conexion	1 Mbps	10 Mbps+

2.2 Requisitos de Software

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

2.3 URL de Acceso

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

Desarrollo: <http://localhost:3000>

3. Autenticacion y Roles de Usuario

3.1 Proceso de Inicio de Sesión

Paso 1: Acceder a la Pagina de Login

- Abra su navegador web preferido
- Ingrese la URL del sistema: <http://localhost:3000/login>
- Aparecera la pantalla de inicio de sesion con el logo de AT5 Audit Platform

Paso 2: Ingresar Credenciales

- En el campo "**Correo Electronico**", ingrese su email corporativo
- En el campo "**Contrasena**", ingrese su contrasena

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

Paso 3: Autenticar

- 1. Haga clic en el boton **"Ingresar"**
- 2. Si las credenciales son correctas, sera redirigido al Dashboard
- 3. Si son incorrectas, vera un mensaje de error en rojo

AT5 Audit Platform

Sistema de Auditoria Interactiva

Iniciar Sesion

Ingrese sus credenciales para acceder al sistema

Correo Electronico

usuario@axongroup.com

Contraseña

*****o

Ingresar

Credenciales de Prueba:

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
Lead Auditor	garcia@axongroup.com	audit2026	Crear sesiones, ejecutar pruebas, firmar
Auditor	lopez@axongroup.com	audit2026	Ejecutar pruebas, agregar evidencias
Reviewer	martinez@axongroup.com	audit2026	Revisión y firma de aprobación

3.3 Roles y Permisos Detallados

ADMIN (Administrador)

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

LEAD_AUDITOR (Auditor Lider)

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

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 auditoria
- 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:

- Después 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 contraseñas se almacenan encriptadas con bcrypt (10 rounds)

Duración de Sesión:

- La sesión de usuario expira automáticamente después 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

PIE CHART

Aprobadas: 21

Fallidas: 2

Bloqueadas: 1

Pendientes: 9

Tasa de Exito Global

GAUGE

85%

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
Sesiones Activas	Auditorías en estado IN_PROGRESS	Azul
Tasa de Exito	% de pruebas PASSED vs FAILED	Verde
En Revision	Sesiones esperando firmas	Amarillo
Completadas	Sesiones APPROVED + ARCHIVED	Verde Teal

4.2.2 Graficos Interactivos

- 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)
- Indicador de Exito (Gauge):** Tasa de exito global como velocimetro visual
- Grafico de Tendencia (Line Chart):** Evolucion de ejecuciones en ultimos 7 dias
- Grafico de Barras:** Progreso de sesiones activas

4.3 Acciones Rapidas

Desde el Dashboard, el auditor puede:

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

5. Gestion de Sesiones de Auditoria

5.1 Crear Nueva Sesion de Auditoria

Paso 1: Acceder al Formulario de Creacion

- Desde el Dashboard, haga clic en "[+ Nueva Auditoria]"
- O navegue a: **Sesiones > Nueva Sesion** desde el menu lateral

Paso 2: Completar Informacion de la Sesion

Nueva Sesion de Auditoria

Nombre de la Sesion *

Auditoria Sistema de Facturacion v3.0

Descripcion

Auditoria completa del modulo de facturacion electronica incluyendo integracion con SII y generacion de DTE.

Plan de Pruebas *

Plan de Pruebas - Sistema Facturacion v3.0 (33 casos) [▼]

Auditor Responsable *

Maria Garcia (Lead Auditor) [▼]

Cancelar

Crear

Campos del Formulario:

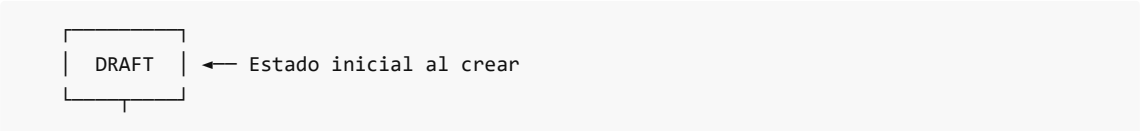
Campo	Obligatorio	Descripcion
Nombre de la Sesion	Si	Identificador descriptivo de la auditoria
Descripcion	No	Detalle del alcance y objetivos
Plan de Pruebas	Si	Seleccionar plan con casos de prueba
Auditor Responsable	Si	Usuario que ejecutara las pruebas

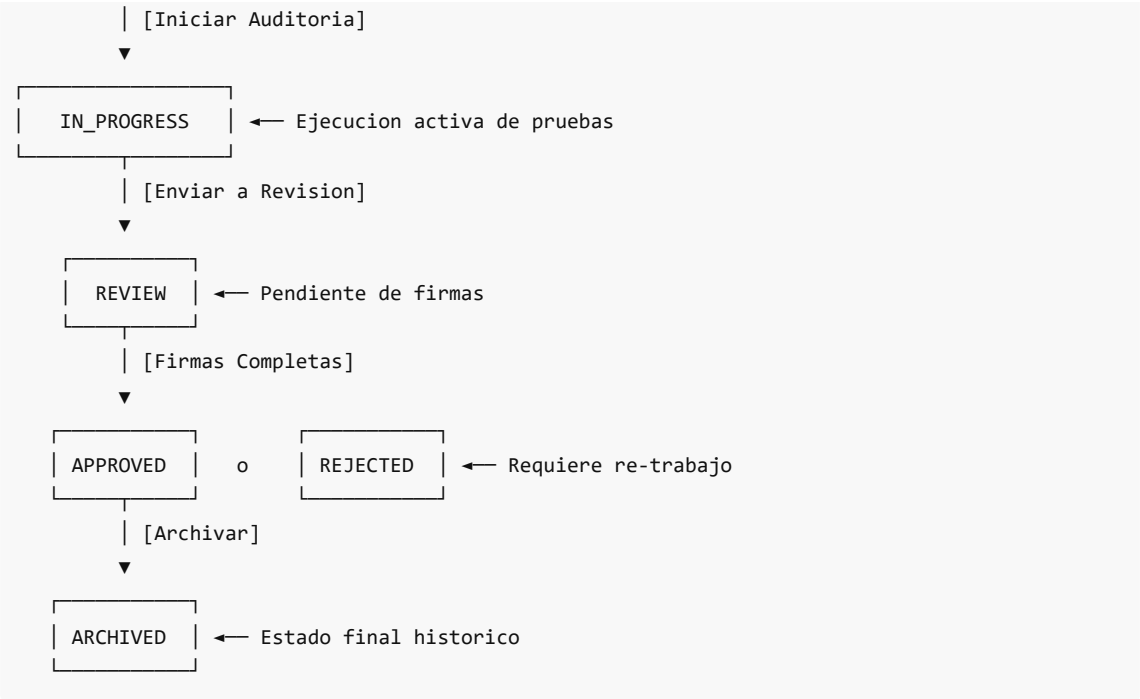
Paso 3: Confirmar Creacion

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. Vera una tabla con todas las sesiones disponibles

Sesiones de Auditoria

[+ Nueva Sesion]

Filtros: [Todos ▼] [Fecha ▼] [Auditor ▼]

[Buscar...]

Nombre	Auditor	Estado	Progreso	Fecha
Auditoria Sistema Login	M. Garcia	En Progreso	<div><div></div></div> 75%	15/01
Auditoria API Backend	J. Lopez	En Revision	<div><div></div></div> 100%	14/01
Auditoria Reportes PDF	M. Garcia	Borrador	<div><div></div></div> 0%	13/01
Auditoria Modulo Pagos	P.Martinez	Aprobada	<div><div></div></div> 100%	10/01

Mostrando 1-4 de 4 sesiones

[< 1 >]

5.4 Ver Detalle de Sesion

- 1. Haga clic en una sesion de la lista
- 2. Vera la pantalla de detalle con toda la informacion

Informacion mostrada:

- Nombre y descripcion de la sesion

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

6. Ejecucion de Casos de Prueba

6.1 Acceder al Modo de Ejecucion

1. Desde el detalle de una sesion, haga clic en **"Ejecutar Pruebas"**
2. O desde una sesion en estado IN_PROGRESS, haga clic en **"Continuar"**

6.2 Interfaz de Ejecucion Interactiva

La pantalla de ejecucion se divide en tres columnas:

← Auditoria Sistema Login v2.1		Progreso: <div><div></div></div> 33%
Casos de Prueba	Detalle del Caso de Prueba	Cronometro
[Suite: Login]	TC-LOG-001 [CRITICAL] Validar Login con Credenciales Validas	00:00:00 [▶] [↺]
<ul style="list-style-type: none">• TC-LOG-001◦ TC-LOG-002◦ TC-LOG-003◦ TC-LOG-004	Descripcion: Verificar que el usuario puede ingresar al sistema con credenciales validas.	Estadisticas
[Suite: 2FA]	Precondiciones: - Usuario registrado en el sistema - Cuenta activa y no bloqueada	<ul style="list-style-type: none">• Aprobados: 4• Fallidos: 0• Bloqueados:◦ Pendientes:
<ul style="list-style-type: none">◦ TC-2FA-001◦ TC-2FA-002	Resultado Esperado: El usuario es redirigido al Dashboard y se muestra su nombre en el header.	Evidencias
		[↑] Subir
		<div>img1.png</div> <div>log.txt</div>
	Pasos de Ejecucion:	
	<div><div><input checked="" type="checkbox"/> Paso 1: Navegar a /login</div><div><input type="checkbox"/> Paso 2: Ingresar email valido</div><div><input type="checkbox"/> Paso 3: Ingresar contrasena</div><div><input type="checkbox"/> Paso 4: Clic en "Ingresar"</div><div><input type="checkbox"/> Paso 5: Verificar redireccion</div></div>	
	Resultado Actual:	

	<div>Describe el resultado observado...</div>	
	<div>Aprobado</div> <div>Fallido</div> <div>Bloqueado</div> <div>Omit</div>	

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 Informacion del Caso

Antes de ejecutar, revise cuidadosamente:

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

Paso 3: Iniciar Cronometro (Opcional)

1. Haga clic en el boton **[▶]** para iniciar el cronometro
2. Use **[⌂]** para reiniciar si es necesario
3. El tiempo se registra automaticamente al guardar el resultado

Paso 4: Ejecutar los Pasos

1. Siga cada paso indicado en la lista de "Pasos de Ejecucion"
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 contrasena correcta
- ☐ Paso 4: Hacer clic en el boton "Ingresar"
- ☐ Paso 5: Verificar redireccion al Dashboard

Paso 5: Documentar Resultado Actual

1. En el campo **"Resultado Actual"**, describa lo que observo
2. Sea especifico 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: "Funciono 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
Aprobado	El sistema se comporto segun lo esperado	Verde
Fallido	Se detecto un defecto o comportamiento incorrecto	Rojo
Bloqueado	No se pudo ejecutar por dependencias no satisfechas	Amarillo
Omitir	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
FUNCTIONAL	Verifican funcionalidad del sistema	Login, CRUD de datos
INTEGRATION	Verifican comunicacion entre componentes	API + Base de datos
PERFORMANCE	Miden tiempos de respuesta	Carga de pagina < 3s
SECURITY	Verifican vulnerabilidades	SQL Injection, XSS
USABILITY	Evaluan experiencia de usuario	Navegacion intuitiva
REGRESSION	Verifican que cambios no rompan funcionalidad	Despues de deploy

7. Gestion de Evidencias

7.1 Tipos de Evidencia Soportados

Tipo	Extensiones	Uso Recomendado
Screenshot	.png, .jpg, .jpeg, .gif, .webp	Capturas de pantalla
Log	.txt, .log	Archivos de log del sistema
PDF	.pdf	Documentos, reportes
Video	.mp4, .webm	Grabaciones de ejecucion
JSON	.json	Respuestas de API, datos
Other	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"**: Abre selector solo para archivos de texto/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.

Evidencias

Estado: "Ejecute primero el caso" (si no hay ejecucion)

[↑] Arrastre archivos aqui o
[Seleccionar Archivos]

Archivos subidos:

[img]	screenshot_error.png	128 KB	[👁]	[🗑]
[txt]	server_log.txt	45 KB	[👁]	[🗑]

[📷] Captura

[📄] Log

7.4 Visualizar Evidencia

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

7.5 Eliminar Evidencia

1. Haga clic en el icono [🗑] (papelera) junto al archivo
2. Confirme la eliminacion en el dialogo
3. **ADVERTENCIA:** Esta accion queda registrada en el audit log

7.6 Integridad de Evidencias

Cada evidencia subida genera automaticamente:

- **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
LEAD_AUDITOR	Si	Certifica la ejecucion correcta
REVIEWER	Si	Certifica la revision de resultados

8.3 Procedimiento de Firma

Paso 1: Acceder a la Sesion 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**"

Firmar Sesion

Usted esta a punto de firmar esta sesion de auditoria.
Esta accion generara un certificado digital que no
puede ser revocado.

Firma Visual (opcional):

[Canvas para dibujar firma]

Al firmar, certifico que:

- He revisado los resultados de esta auditoria

- Los resultados son precisos y completos

- Las evidencias son autenticas

Cancelar

Firmar

8.4 Certificado Digital

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

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

Cerrar

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
Resumen Ejecutivo	Vista de alto nivel para gerencia	PDF
Reporte Detallado	Informacion completa de todas las pruebas	DOCX
Reporte de Defectos	Solo casos FAILED con evidencias	PDF
Metricas	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

Generar Reporte

Sesion: Auditoria Sistema Login v2.1

Tipo de Reporte:

○ Resumen Ejecutivo (PDF)

● Reporte Detallado (DOCX)

○ Reporte de Defectos (PDF)

○ Exportar Metricas (JSON)

Opciones:

☒ Incluir evidencias

☒ Incluir firmas

☐ Incluir logs de auditoria

Cancelar

Generar

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 ▼] [Accion ▼] [Entidad ▼] [Desde: __/__/__] [Hasta: __/__/__]

Fecha/Hora	Usuario	Accion	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	Descripcion
Usuario	Filtrar por usuario que realizo la accion
Accion	Tipo de accion (LOGIN, TEST_PASSED, etc.)
Entidad	Tipo de objeto afectado (User, Session, etc.)
Fecha Desde	Inicio del rango de fechas
Fecha Hasta	Fin del rango de fechas

10.4 Acciones Registradas

Accion	Descripcion
LOGIN	Inicio de sesion 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 boton "**Verificar Integridad**" permite comprobar que ningun registro ha sido alterado:

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

Verificacion de Integridad

✓ INTEGRIDAD VERIFICADA

Total de registros: 234
Registros validos: 234
Registros invalidos: 0

La cadena de audit log esta intacta.
Ningun registro ha sido modificado.

Cerrar

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 redirección 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

Información del Caso:

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

Pasos:

1. [✓] Navegar a /login
2. [✓] Ingresar email válido
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 página 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

Información 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:

"Después 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 está 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

Información 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 código 2FA

Resultado Actual:

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

Decision: [BLOQUEADO ⚠]

Fase 3: Revision (Lead Auditor)

3.1 Revisar Resultados

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

3.2 Enviar a Revision

1. Clic en "Enviar a Revisión"
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)
- 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)
- 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"	Limite 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
Auditoria de Software	Proceso de evaluacion independiente de productos o procesos de software
Caso de Prueba	Conjunto de condiciones y pasos para verificar un requisito especifico
Certificado Digital	Hash criptografico que garantiza la autenticidad de una firma
Evidencia	Archivo que documenta el resultado de una prueba
Hash SHA-256	Funcion criptografica que genera un resumen unico de datos
Plan de Pruebas	Documento que describe el alcance, enfoque y recursos de testing
RBAC	Control de Acceso Basado en Roles
Sesion de Auditoria	Instancia de ejecucion de un plan de pruebas
Suite de Pruebas	Agrupacion logica de casos de prueba relacionados
Trazabilidad	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
- 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