ESPECIFICACIÓN DE CASO DE USO

Sistema: Sistema de Control y Planificación de Mano de Obra Agroindustrial
Caso de Uso: CU-001 - Autenticar Usuario
Versión: 1.0
Fecha: Diciembre 2024

---

1. INFORMACIÓN GENERAL

1.1 Identificación

- **ID:** CU-001
- **Nombre:** Autenticar Usuario
- **Actor Principal:** Usuario del Sistema
- **Nivel:** Objetivo del Usuario
- **Estado:** Activo

1.2 Resumen

Este caso de uso describe el proceso mediante el cual un usuario del sistema ingresa sus credenciales para acceder a las funcionalidades del Sistema de Gestión Agrícola, obteniendo los permisos correspondientes según su rol asignado.

1.3 Actores

- **Actor Principal:** Usuario del Sistema (Admin, Gerente RRHH, Supervisor Campo, Supervisor RRHH, Empleado, Visual)
- **Actores Secundarios:** Sistema de Autenticación, Base de Datos

---

2. ESPECIFICACIÓN DEL CASO DE USO

2.1 Precondiciones

- El usuario debe tener credenciales válidas (email y contraseña) registradas en el sistema
- El sistema debe estar operativo y accesible
- La base de datos debe estar disponible
- El usuario no debe tener una sesión activa previa

2.2 Garantía de Éxito (Postcondiciones)

- El usuario queda autenticado en el sistema
- Se genera un token JWT válido con información del rol
- Se redirige al usuario a la página principal según su rol
- Se registra el acceso en los logs del sistema
- La sesión queda activa por el tiempo configurado (8 horas)

2.3 Garantía Mínima

- Se mantiene la seguridad del sistema
- Los intentos fallidos se registran en logs
- No se expone información sensible en caso de error

---

3. FLUJO PRINCIPAL DE EVENTOS

3.1 Escenario Exitoso

1. **Usuario** accede a la página de login del sistema
2. **Sistema** presenta el formulario de autenticación con campos:
    - Email
    - Contraseña
    - Botón "Iniciar Sesión"
    - Enlace "¿Olvidaste tu contraseña?"
3. **Usuario** ingresa su email en el campo correspondiente
4. **Usuario** ingresa su contraseña en el campo correspondiente
5. **Usuario** hace clic en el botón "Iniciar Sesión"
6. **Sistema** valida que los campos no estén vacíos
7. **Sistema** valida el formato del email
8. **Sistema** encripta la contraseña ingresada
9. **Sistema** consulta en la base de datos las credenciales
10. **Sistema** verifica que las credenciales sean correctas
11. **Sistema** verifica que la cuenta esté activa
12. **Sistema** genera un token JWT con información del usuario:
    - ID del usuario
    - Email
    - Rol asignado
    - Timestamp de generación
    - Tiempo de expiración
13. **Sistema** registra el acceso exitoso en los logs
14. **Sistema** actualiza la fecha de último acceso del usuario
15. **Sistema** redirige al usuario al dashboard principal según su rol:
    - Admin → Dashboard administrativo completo
    - Gerente RRHH → Dashboard de recursos humanos
    - Supervisor Campo → Dashboard operacional de campo
    - Supervisor RRHH → Dashboard de supervisión RRHH
    - Empleado → Dashboard personal limitado
    - Visual → Dashboard de solo lectura
16. **Sistema** muestra mensaje de bienvenida personalizado

---

4. FLUJOS ALTERNATIVOS

4.1 Credenciales Inválidas (A1)

Punto de Extensión: Después del paso 10 del flujo principal

1. **Sistema** detecta que las credenciales no coinciden
2. **Sistema** incrementa el contador de intentos fallidos para esa cuenta
3. **Sistema** registra el intento fallido en los logs de seguridad
4. **Sistema** muestra mensaje de error: "Email o contraseña incorrectos"
5. **Sistema** mantiene el formulario visible para nuevo intento
6. Si los intentos fallidos superan 5 en 15 minutos: a. **Sistema** bloquea temporalmente la cuenta por 30 minutos b. **Sistema** envía notificación al administrador c. **Sistema** muestra mensaje: "Cuenta bloqueada temporalmente"
7. Regresa al paso 2 del flujo principal

4.2 Cuenta Inactiva (A2)

Punto de Extensión: Después del paso 11 del flujo principal

1. **Sistema** detecta que la cuenta está marcada como inactiva
2. **Sistema** registra el intento de acceso a cuenta inactiva
3. **Sistema** muestra mensaje: "Su cuenta ha sido desactivada. Contacte al administrador"
4. **Sistema** no permite el acceso
5. Regresa al paso 2 del flujo principal

4.3 Campos Vacíos (A3)

Punto de Extensión: Después del paso 6 del flujo principal

1. **Sistema** detecta que uno o ambos campos están vacíos
2. **Sistema** resalta en rojo los campos faltantes
3. **Sistema** muestra mensaje de validación: "Todos los campos son obligatorios"
4. Regresa al paso 3 del flujo principal

4.4 Formato de Email Inválido (A4)

Punto de Extensión: Después del paso 7 del flujo principal

1. **Sistema** detecta formato de email inválido
2. **Sistema** resalta el campo email en rojo
3. **Sistema** muestra mensaje: "Ingrese un email válido"
4. Regresa al paso 3 del flujo principal

4.5 Error del Sistema (A5)

Punto de Extensión: En cualquier momento del flujo principal

1. **Sistema** detecta un error interno (BD no disponible, servidor sobrecargado, etc.)
2. **Sistema** registra el error en los logs del sistema
3. **Sistema** muestra mensaje genérico: "Error temporal del sistema. Intente nuevamente"
4. **Sistema** envía alerta al equipo técnico
5. Regresa al paso 2 del flujo principal

---

5. REQUERIMIENTOS ESPECIALES

5.1 Requerimientos de Rendimiento

- El proceso de autenticación debe completarse en menos de 2 segundos
- El sistema debe soportar hasta 100 intentos de login concurrentes
- La validación de credenciales no debe exceder 500ms

5.2 Requerimientos de Seguridad

- Las contraseñas deben transmitirse encriptadas (HTTPS)
- Los tokens JWT deben usar algoritmo HS256
- Se debe implementar protección contra ataques de fuerza bruta
- Los logs de seguridad deben ser inmutables
- Las sesiones deben expirar automáticamente después de 8 horas

5.3 Requerimientos de Usabilidad

- El formulario debe ser responsive para dispositivos móviles
- Debe mostrar indicadores visuales claros de errores
- Debe incluir funcionalidad "Recordar usuario" (opcional)
- Los mensajes de error deben ser claros y orientativos

5.4 Requerimientos de Confiabilidad

- El sistema debe manejar gracefully las fallas de conexión
- Debe implementar retry automático en caso de errores temporales
- Los logs deben persistir incluso en caso de fallos del sistema

---

6. INFORMACIÓN ADICIONAL

6.1 Frecuencia de Uso

- **Alta:** Se estima 200-300 logins diarios
- **Picos:** Inicio de jornada laboral (6:00-8:00 AM)
- **Usuarios concurrentes:** Hasta 50 usuarios simultáneos

6.2 Reglas de Negocio

- **RN-001:** Solo usuarios activos pueden autenticarse
- **RN-002:** Máximo 5 intentos fallidos antes del bloqueo temporal
- **RN-003:** Las sesiones deben expirar automáticamente
- **RN-004:** Los administradores pueden desbloquear cuentas
- **RN-005:** Se debe mantener auditoría de todos los accesos

6.3 Supuestos y Dependencias

- **Supuesto:** Los usuarios tienen navegadores modernos con JavaScript habilitado
- **Supuesto:** La conexión a internet es estable

- **Dependencia:** Base de datos MySQL operativa
- **Dependencia:** Servicio de Redis para gestión de sesiones
- **Dependencia:** Servicio de logs (Winston) funcionando

6.4 Problemas Abiertos

- Definir política de expiración de contraseñas
- Implementar autenticación de dos factores (2FA) en fases futuras
- Evaluar integración con Active Directory empresarial

---

7. TRAZABILIDAD

7.1 Relación con Requerimientos

- **RF-026:** Login de usuario
- **RF-027:** Logout de usuario
- **RF-030:** Control de acceso por roles
- **RNF-001:** Seguridad de autenticación
- **RNF-002:** Tiempo de respuesta < 2 segundos

7.2 Relación con Azure DevOps

- **Feature:** Autenticación Básica (Pendiente de creación)
- **User Stories:** HU-026, HU-027
- **Epic:** Gestión de Identidad y Acceso

Elaborado por: Equipo de Desarrollo
Revisado por: Product Owner
Aprobado por: Stakeholder de Negocio
Estado: Aprobado para Implementación