Elaboración de Cuestionario con Fundamentación

Alumnos: Luciano Esteban, Camila Codina.

Ejercicio 1: Caso de uso Ingresar al sistema

- **Nombre:** CU01 – Ingresar al sistema
- **Actor principal:** Usuario (Alumno/Docente)
- **Objetivo:** Permitir que un usuario válido acceda al sistema de manera segura.
- **Disparador:** El usuario abre la pantalla de inicio e intenta autenticarse.
- **Precondiciones:**
  - El usuario está previamente registrado.
  - El sistema y la base de datos están disponibles.
- **Postcondiciones (éxito):**
  - Sesión iniciada
    - El usuario accede a la pantalla principal con opciones según su perfil.
  - Se registra el inicio de sesión (timestamp) para auditoría.
- **Reglas/Restricciones:**
  - Tras **3 intentos fallidos consecutivos**, la cuenta queda **bloqueada** hasta la gestión del administrador.
  - Contraseña comparada mediante hash seguro.
    - Nunca se persiste ni se muestra en claro.

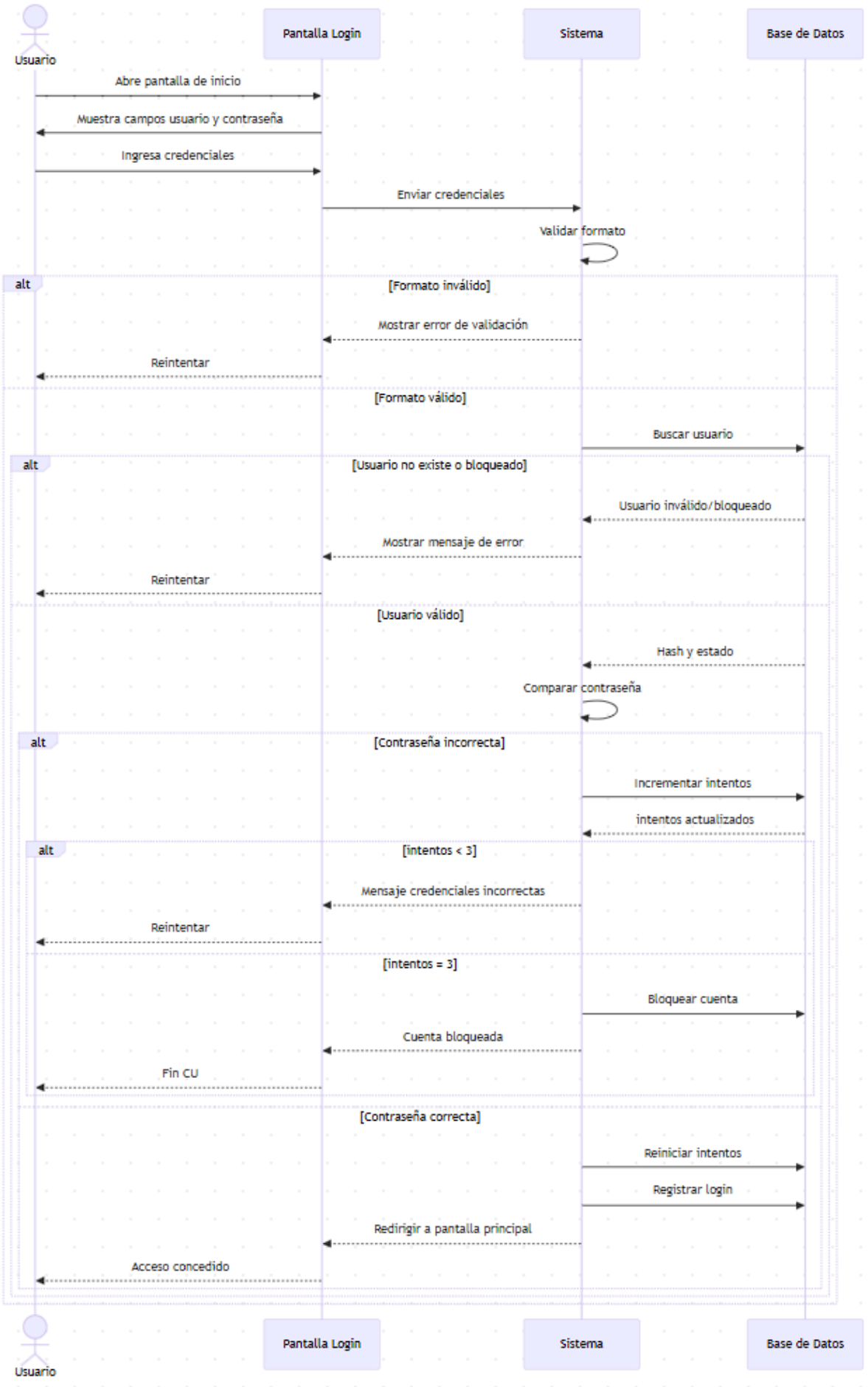
Flujo principal (camino de éxito)

1. El sistema muestra la pantalla “Iniciar sesión” con campos **nombreUsuario** y **contraseña**.
2. El usuario ingresa **nombreUsuario** y **contraseña** y presiona **Ingresar**.
3. El sistema valida formato básico (no vacíos; longitud permitida).
4. El sistema busca **nombreUsuario** en BD y verifica que la cuenta **no esté bloqueada**.
5. El sistema compara la **contraseña** ingresada contra el **hash** almacenado.
6. Las credenciales son correctas ⇒ reinicia **intentosFallidos** a 0.
7. El sistema determina el **perfil** (Alumno/Docente) y construye el contexto de sesión.
8. El sistema redirige a la **pantalla principal** mostrando opciones según el perfil.
9. Se registra **evento de login** (usuario, timestamp, IP opcional para auditoría).

Flujos alternativos (mínimo 2)

- **A1 – Credenciales inválidas (reintento):**
    - Si el usuario no existe o está bloqueado → mostrar mensaje (“Usuario inexistente o bloqueado. Contacte al administrador si persiste”).
    - Si la contraseña no coincide ⇒ incrementar **intentosFallidos**
        - Mostrar “Credenciales incorrectas. Intente nuevamente.”
            - Volver al paso 1.

- **A2 – Bloqueo por intentos fallidos:**
    - Si **intentosFallidos** alcanza 3 → marcar **bloqueado = true**.
        - Informar “Cuenta bloqueada por intentos fallidos. Contacte al administrador.”; finalizar CU.


Usuario
Pantalla Login
Sistema
Base de Datos
Abre pantalla de inicio
Muestra campos usuario y contraseña
Ingresa credenciales
Enviar credenciales
Validar formato
alt
[Formato inválido]
Mostrar error de validación
Reintentar
[Formato válido]
Buscar usuario
alt
[Usuario no existe o bloqueado]
Usuario inválido/bloqueado
Mostrar mensaje de error
Reintentar
[Usuario válido]
Hash y estado
Comparar contraseña
alt
[Contraseña incorrecta]
Incrementar intentos
intentos actualizados
alt
[intentos < 3]
Mensaje credenciales incorrectas
Reintentar
[intentos = 3]
Bloquear cuenta
Cuenta bloqueada
Fin CU
[Contraseña correcta]
Reiniciar intentos
Registrar login
Redirigir a pantalla principal
Acceso concedido
Usuario
Pantalla Login
Sistema
Base de Datos

Ejercicio 2: Recuperar Contraseña

- **Nombre:** CU02 – Recuperar contraseña
- **Actor principal:** Usuario (Alumno/Docente)
- **Objetivo:** Permitir que un usuario restablezca su contraseña olvidada.
- **Disparador:** El usuario selecciona “¿Olvidaste tu contraseña?” en la pantalla de login.
- **Precondiciones:**
  - El usuario cuenta con un email registrado en el sistema.
  - Servicio de emails funciona
- **Postcondiciones (éxito):**
  - Se **envía un email** con un enlace/token de restablecimiento de un solo uso y vencimiento.
  - Queda **registrada la solicitud** (timestamp).
- **Relaciones/Extensiones:**
  - Si el email no existe ⇒ **Extiende a CU “Registrar Usuario”** (o mostrar mensaje sin filtrar existencia).

Flujo principal (solicitud + envío)

1. En la pantalla de login, el usuario selecciona **“¿Olvidaste tu contraseña?”**.
2. El sistema muestra formulario para ingresar **email**.
3. El usuario ingresa su **email** y envía la solicitud.
4. El sistema valida formato de email y busca existencia en BD.
5. Si el email existe, el sistema genera **tokenRecupero** con **vencimientoToken** y lo guarda.
6. El sistema envía un **correo** al email con un **enlace de restablecimiento** (incluye token).
7. El sistema muestra mensaje de confirmación genérico: “Si el email existe, recibirás un enlace para restablecer tu contraseña.”
8. Se registra la solicitud (timestamp).

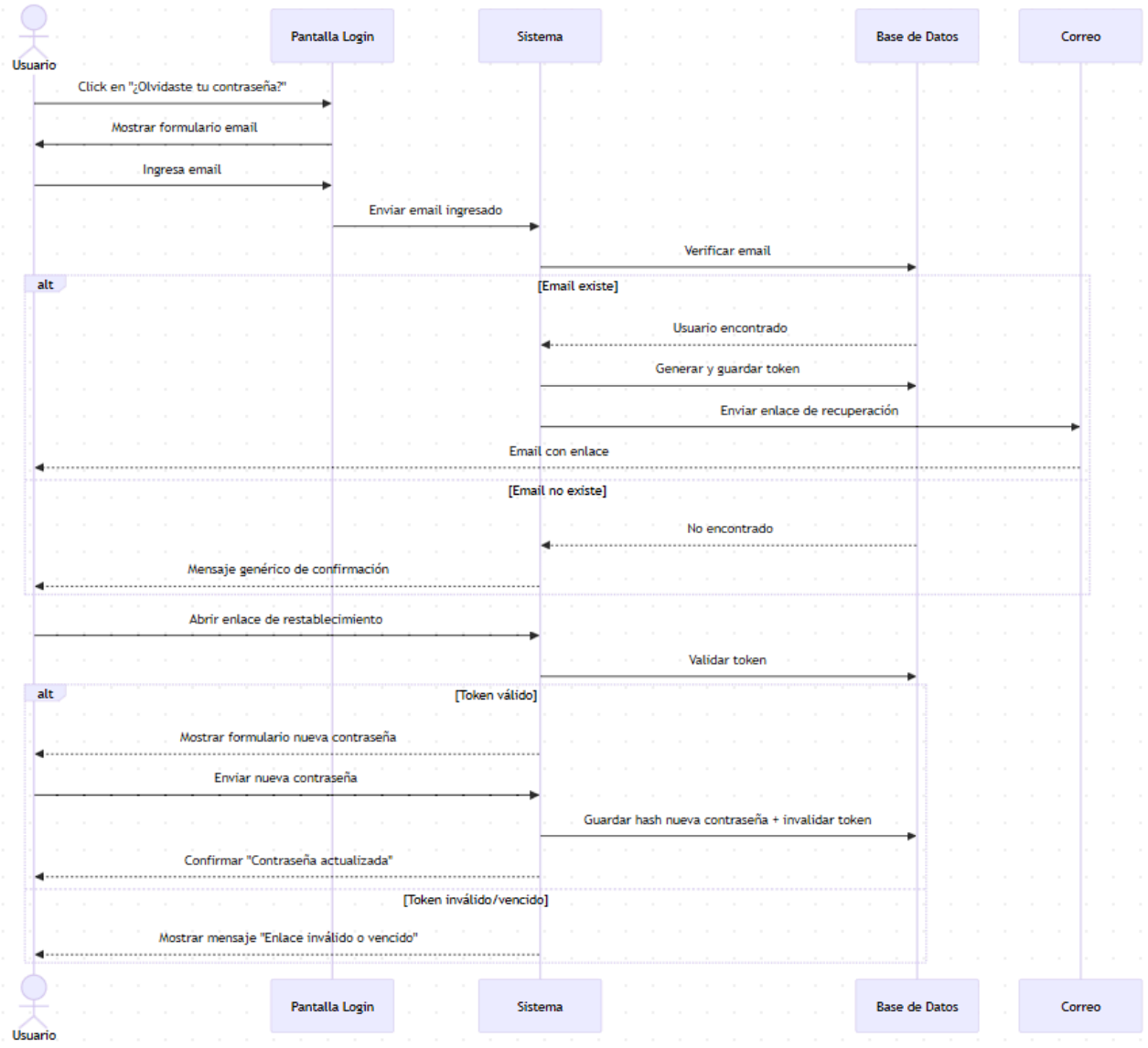
Completa del lado del enlace:

9. El usuario hace clic en el enlace recibido.
10. El sistema valida **tokenRecupero** (vigencia y estado).
11. El sistema muestra formulario para **nuevaContraseña** y **confirmarContraseña**.
12. El usuario envía el formulario.
13. El sistema valida política de contraseña y coincidencia.
14. Se guarda **hash** de la nueva contraseña; se **invalida** el token.
15. El sistema confirma “Contraseña actualizada” y sugiere volver a **Ingresar al sistema**.

Flujos alternativos

- **B1 – Email no existe (extensión a Registrar Usuario):** Si el email no existe…
  - **opción 1**: mostrar mensaje genérico (para no revelar existencia) y proceder igual al paso 7.
  - **Opción 2 (según consigna):** derivar a **CU "Registrar Usuario"** para alta.

- **B2 – Token inválido o vencido:**
  - Si el token no es válido o está vencido ⇒ mostrar "Enlace inválido o vencido"; ofrecer reenviar el correo de recuperación (volver a paso 1).



Ejercicio 3: Cargar Usuario