## 📄 Documento de Caso de Uso: UC001 - Login

### 1. Identificação

* **Nome:** UC001 - Login
* **Resumo:** Este caso de uso permite que o usuário acesse o sistema utilizando a autenticação via Google OAuth, vinculada à conta institucional.

### 2. Atores

* **Primário:** Usuário não logado
* **Secundário:** Google OAuth

### 3. Pré-condições

* O usuário deve possuir uma conta institucional válida vinculada ao provedor OAuth da universidade (Google).
* O sistema deve estar integrado ao serviço OAuth e com conexão ativa.

### 4. Pós-condições

* O usuário é autenticado com sucesso e redirecionado ao ambiente do sistema, com acesso restrito às funcionalidades compatíveis com os papéis atribuídos.
* Caso o usuário não possua perfil aprovado, será redirecionado para a tela de cadastro de perfil.

### 5. Fluxo Básico de Eventos

1. O usuário acessa a aplicação e seleciona a opção "Login com Google".
2. O sistema redireciona para o serviço Google OAuth.
3. O usuário insere suas credenciais no serviço OAuth.
4. O serviço OAuth autentica o usuário e redireciona de volta para o sistema com o token de autenticação.
5. O sistema valida o token e recupera os dados do usuário (nome, email institucional).
6. O sistema verifica se o perfil do usuário já está cadastrado e aprovado.
   * Se sim: redireciona o usuário para o painel correspondente aos seus papéis.
   * Se não: redireciona o usuário para o fluxo de UC004 - Cadastrar Perfil.

### 6. Fluxos Alternativos

**6A - Autenticação falhou**

* O serviço OAuth informa falha de autenticação (ex.: credenciais inválidas, permissão negada).
* O sistema exibe mensagem de erro e permite nova tentativa de login.

**6B - Conta institucional inválida**

* O sistema identifica que o domínio do email não pertence à universidade.
* O sistema informa que a conta não é permitida para acesso.

### 7. Requisitos Especiais

* Integração segura com Google OAuth (protocolo OAuth 2.0).
* Armazenamento seguro do token de sessão.
* Garantir que o domínio da conta autenticada seja da universidade (ex.: @upe.br).

### 8. Regras de Negócio Associadas

* **RN001:** O acesso ao sistema só pode ser realizado com uma conta institucional verificada.
* **RN002:** Um usuário sem perfil aprovado não pode acessar funcionalidades além do cadastro de perfil.
* **RN003:** A autenticação deve seguir os protocolos de segurança do Google OAuth 2.0.

### 9. Pontos de Extensão

* **UC004 - Cadastrar Perfil**: extensão caso o usuário logado ainda não possua perfil aprovado.