**Use Case — Login & Authentication (UC-SEG-001)**

**Acceptance Criteria**

* **AC-SEG-001-01 (Valid login)**
  + **Given** an active client with correct login and password
  + **When** I send POST /api/auth/login
  + **Then** the system returns 200 OK with an accessToken (15 min) and a refreshToken (7 days).
* **AC-SEG-001-02 (Missing required fields)**
  + **Given** the request omits login or password
  + **When** I send the login request
  + **Then** the system returns 400 Bad Request with error CAMPOS\_OBRIGATORIOS.
* **AC-SEG-001-03 (Invalid login format)**
  + **Given** login is neither a valid email nor a valid CPF
  + **When** I send the login request
  + **Then** the system returns 422 Unprocessable Entity with error LOGIN\_INVALIDO.
* **AC-SEG-001-04 (Invalid credentials)**
  + **Given** an incorrect password for an existing user
  + **When** I attempt login
  + **Then** the system returns 401 Unauthorized with error CREDENCIAIS\_INVALIDAS and increments failed attempts.
* **AC-SEG-001-05 (Blocked or inactive user)**
  + **Given** the user is Inativo or Bloqueado
  + **When** I attempt login
  + **Then** the system returns 423 Locked (USUARIO\_BLOQUEADO) or 403 Forbidden (USUARIO\_INATIVO).
* **AC-SEG-001-06 (Too many attempts / rate limit)**
  + **Given** 5 consecutive failed attempts or IP exceeds threshold
  + **When** I attempt login
  + **Then** the system returns 429 Too Many Requests with error MUITAS\_TENTATIVAS or 423 USUARIO\_BLOQUEADO.
* **AC-SEG-001-07 (Valid refresh — rotating)**
  + **Given** a valid refreshToken
  + **When** I send POST /api/auth/refresh
  + **Then** the system returns 200 OK with a new accessToken and a new refreshToken, revoking the previous one.
* **AC-SEG-001-08 (Refresh reuse detection)**
  + **Given** a refreshToken that has already been exchanged
  + **When** I attempt to reuse it
  + **Then** the system returns 401 Unauthorized with error REFRESH\_REUTILIZADO and revokes related sessions.
* **AC-SEG-001-09 (Logout current session)**
  + **Given** a valid accessToken
  + **When** I send POST /api/auth/logout
  + **Then** the system invalidates the current session and returns 200 OK.
* **AC-SEG-001-10 (Logout all sessions)**
  + **Given** a valid accessToken
  + **When** I send POST /api/auth/logout-all
  + **Then** the system revokes all active sessions for the user and returns 200 OK.
* **AC-SEG-001-11 (Internal authentication failure)**
  + **Given** a system error occurs during authentication
  + **When** I send the login request
  + **Then** the system returns 500 Internal Server Error with error ERRO\_AUTENTICACAO.