

|  |
| --- |
| **Sistema IA – Portal Web**  Documento de Requisitos  (Submódulo Logs de Acesso) |
|  |
| Versão 1.0 |

|  |
| --- |
| Clovis Ap. Moratta  18/9/2025 |

|  |  |  |  |
| --- | --- | --- | --- |
| **HISTÓRICO DE REVISÕES** | | | |
| Data | Versão | Descrição | Autor |
| 18/09/2025 | 1.0 | Criação do documento de requisitos “Submódulo Logs de Acesso” | Clovis Ap. Moratta |
|  |  |  |  |
|  |  |  |  |

**SUMÁRIO**

[1) Informações do Projeto 3](#_Toc209083803)

[2. Objetivo e Escopo 3](#_Toc209083804)

[3. Atores e Permissões 3](#_Toc209083805)

[4. Visão Geral Funcional 3](#_Toc209083806)

[5. Requisitos Funcionais (RF) 4](#_Toc209083807)

[6. Requisitos Não Funcionais (RNF) 4](#_Toc209083808)

[7. Regras de Negócio e Invariantes 4](#_Toc209083809)

[8. Casos de Uso (Descritivo) 5](#_Toc209083810)

[**Caso de Uso UC01** – Registrar Login Sucesso 5](#_Toc209083811)

[**Caso de Uso UC02** – Registrar Login Falha 5](#_Toc209083812)

[**Caso de Uso UC03** – Consultar Logs 5](#_Toc209083813)

[**Caso de Uso UC04** – Detalhar Log 6](#_Toc209083814)

[9. Interface do Usuário (referência) 6](#_Toc209083815)

[10. Dados e Integrações 7](#_Toc209083816)

[11. Mensagens do Sistema 8](#_Toc209083817)

[12. Considerações de LGPD e Segurança 8](#_Toc209083818)

[13. Estrutura de Dados (Proposta) 8](#_Toc209083819)

[14. Referências do Projeto 8](#_Toc209083820)

[15. Mapa de Integrações 9](#_Toc209083821)

[16. Integração com o Projeto Existente (Resumo) 9](#_Toc209083822)

# 1) Informações do Projeto

* **Projeto:** IA - Portal Web - Protótipo
* **Módulo:** Segurança
* **Submódulo:** Logs de Acesso

**Descrição:** Registro, armazenamento e consulta de eventos de acesso (login/logout, falhas de autenticação, timeouts) para fins de segurança, auditoria e conformidade.

# 2. Objetivo e Escopo

**Objetivo**

Disponibilizar mecanismos de registro e consulta de logs de acesso; fornecer endpoints/contratos para consumo por outros submódulos; garantir rastreabilidade e imutabilidade dos registros.

**Escopo – Incluído**

* Registro automático de eventos de login, logout, falhas e timeout.
* Consulta paginada e filtrada de logs.
* Exibição detalhada de log em modal read-only.
* Endpoints REST para listagem, filtro e detalhe.
* Integração obrigatória com submódulo de Permissões.

**Escopo – Excluído**

* Alteração ou exclusão de logs (imutáveis).
* Relatórios estatísticos analíticos (serão tratados em outro módulo).

# 3. Atores e Permissões

**Ator Principal:** Administrador de Segurança / Auditor (permissão: visualizar logs).

**Permissões do ator:** listar, filtrar e detalhar registros de acesso.

# 4. Visão Geral Funcional

Tela de consulta em grid paginado (20 registros/página, ordenação por data decrescente).

Filtros por usuário, data, tipo de evento e status. Modal read-only exibe detalhes (IP, dispositivo, data/hora, resultado).

Validação obrigatória de permissões via guards no Front-End e policies no Back-End.

# 5. Requisitos Funcionais (RF)

|  |  |  |  |
| --- | --- | --- | --- |
| **ID** | **Título** | **Descrição** | **Critérios de Aceite** |
| RF01 | Registrar Login Sucesso | Registro automático de login bem-sucedido. | Evento gravado com usuário, IP, user agent, data/hora. |
| RF02 | Registrar Login Falha | Registro automático de tentativas de login malsucedidas. | Evento gravado com causa (ex.: senha inválida). |
| RF03 | Registrar Logout | Registro de logout explícito do usuário. | Evento gravado com data/hora e IP. |
| RF04 | Registrar Timeout | Registro de encerramento automático de sessão por inatividade. | Evento gravado com data/hora, motivo timeout. |
| RF05 | Listar Logs | Consulta paginada (20 por página) ordenada por data/hora desc. | Exibir X–Y de Z; suportar paginação anterior/próxima. |
| RF06 | Filtrar Logs | Filtro por usuário, intervalo de datas, tipo de evento e status. | Filtros case-insensitive; resetam paginação para página 1. |
| RF07 | Detalhar Log | Exibir dados completos do log em modal read-only. | Campos ausentes exibem “—”. |
| RF08 | API REST Consulta | Disponibilizar endpoints para listagem, filtro e detalhe. | Documentados no A-integration\_guide.md. |
| RF09 | API REST Registro | Disponibilizar endpoint interno para registro automático. | Consumido pelo submódulo de Login. |

# 6. Requisitos Não Funcionais (RNF)

|  |  |  |
| --- | --- | --- |
| **ID** | **Categoria** | **Requisito** |
| RNF01 | Performance | P95 ≤ 3000 ms em consultas; registro ≤ 500 ms. |
| RNF02 | Disponibilidade | Meta ≥ 99,5% mensal para serviço de logs. |
| RNF03 | Usabilidade | UI consistente com outros submódulos (grid, modal, tooltips). |
| RNF04 | Segurança | Logs imutáveis; acesso restrito a perfis autorizados; auditoria. |

# 7. Regras de Negócio e Invariantes

|  |  |  |
| --- | --- | --- |
| **ID da Regra (RN)** | **Descrição** | **Aplica a** |
| RN01 | Logs são imutáveis (sem edição/exclusão). | RF01, RF02, RF03, RF04, RF09 |
| RN02 | Filtros são case-insensitive e resetam para página 1. | RF06 |
| RN03 | Sempre 20 registros por página (fixo). | RF05 |
| RN04 | Campos sem valor exibem “—”. | RF07 |

# 8. Casos de Uso (Descritivo)

## **Caso de Uso UC01** – Registrar Login Sucesso

**Descrição:** Gravar log de login bem-sucedido.

* **Ator Primário:** Sistema
* **Pré-condições:** Autenticação bem-sucedida.
* **Fluxo Principal:**
  + Usuário informa credenciais corretas.
  + Sistema valida com sucesso.
  + Sistema chama API interna de logs.
  + Evento é registrado com usuário, IP, dispositivo e data/hora.
* **Fluxo Alternativo:**
  + Falha na gravação → retorna erro para fila de retry.
* **Pós-condições:** Log persistido e imutável.
* **Integração:** IN01 – POST /api/logs

## **Caso de Uso UC02** – Registrar Login Falha

**Descrição:** Gravar log de tentativa inválida.

* **Ator Primário:** Sistema
* **Pré-condições:** Tentativa de autenticação.
* **Fluxo Principal:**
  + Usuário informa credenciais incorretas.
  + Sistema identifica falha.
  + Sistema chama API interna de logs.
  + Evento é registrado com causa da falha, IP e data/hora.
* **Fluxo Alternativo:**
  + Falha na gravação → log deve ser reenviado em batch posterior.
  + Pós-condições: Tentativa de login registrada.
* **Integração:** IN01 – POST /api/logs

## **Caso de Uso UC03** – Consultar Logs

**Descrição:** Listar registros com paginação e filtros.

* **Ator Primário:** Administrador de Segurança / Auditor
* **Pré-condições:** Usuário autenticado e autorizado.
* **Fluxo Principal:**
  + Usuário abre tela de logs.
  + Sistema exibe grid paginado com últimos registros.
  + Usuário aplica filtros (usuário, data, evento, status).
  + Sistema atualiza grid conforme filtro.
* **Fluxo Alternativo:**
  + Nenhum resultado encontrado → mensagem “Nenhum registro encontrado”.
  + Falha API → mensagem “Erro de comunicação com servidor”.
* **Pós-condições:** Logs visualizados conforme critérios.
* **Integração:** IN02 – GET /api/logs

## **Caso de Uso UC04** – Detalhar Log

**Descrição:** Exibir dados completos do log em modal read-only.

* **Ator Primário:** Administrador / Auditor
* **Pré-condições:** Usuário autenticado e autorizado; log selecionado no grid.
* **Fluxo Principal:**
  + Usuário clica em um registro.
  + Sistema abre modal com detalhes do log.
  + Sistema exibe todos os campos disponíveis.
* **Fluxo Alternativo:**
  + Dados incompletos → campos exibem “—”.
  + Falha API → mensagem “Erro de comunicação com servidor”.
* **Pós-condições:** Log detalhado visualizado.
* **Integração:** IN03 – GET /api/logs/{id}

# 9. Interface do Usuário (referência)

**9.1 Estrutura Geral da Tela**

* Grid central com listagem de registros de logs.
* Barra superior com filtros: Usuário, Data Inicial, Data Final, Tipo de Evento, Status.
* Barra inferior com paginação fixa (20 registros por página), botões **Anterior** e **Próximo**.
* Ações via modal (detalhamento).
* Mensagens padrão para vazio, erro e sucesso.

**9.2 Grid de Logs**

* Colunas padrão: **Data/Hora**, **Usuário**, **Evento**, **Status**, **IP de Origem**.
* Ordenação padrão: **Data/Hora decrescente**.
* Tooltip para valores truncados (ex.: user agent longo).
* Mensagem de vazio: “Nenhum log encontrado para os critérios selecionados”.

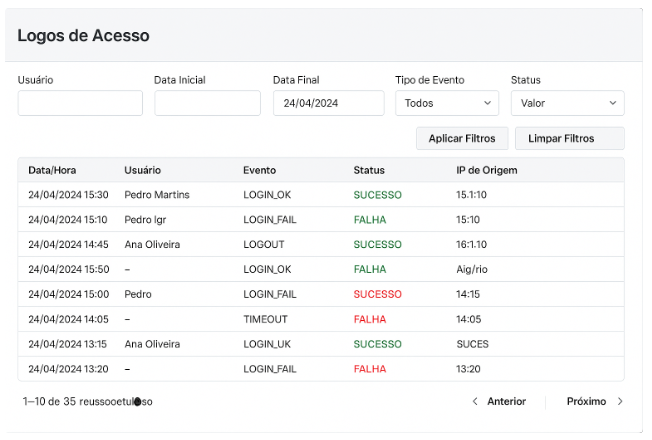
**9.3 Filtros**

* **Usuário**: pesquisa por nome/ID (case-insensitive, contains).
* **Período**: Data Inicial e Data Final (obrigatório quando preenchido em par).
* **Evento**: seleção múltipla (LOGIN\_OK, LOGIN\_FAIL, LOGOUT, TIMEOUT).
* **Status**: seleção única (SUCESSO, FALHA).
* Botão **Aplicar Filtros**: reinicia paginação para página 1.
* Botão **Limpar Filtros**: restaura listagem padrão (últimos registros).

**9.4 Modal de Detalhes**

* Abertura ao clicar em linha do grid.
* Campos exibidos:
  + Usuário (nome e ID, se disponível)
  + Evento (LOGIN\_OK, LOGIN\_FAIL, LOGOUT, TIMEOUT)
  + Status (SUCESSO/FALHA)
  + Data/Hora do evento
  + IP de Origem
  + Dispositivo/Navegador (user agent)
  + Mensagem adicional (quando existir)
* Campos sem valor exibem **“—”**.
* Botão **Fechar** retorna ao grid.

Exemplo:



# 10. Dados e Integrações

Principais rotas:  
• IN01 – POST /api/logs (registro de evento)  
• IN02 – GET /api/logs?usuario=&evento=&status=&dataIni=&dataFim=&page=  
• IN03 – GET /api/logs/{id}

# 11. Mensagens do Sistema

* “Log registrado com sucesso”
* “Nenhum registro encontrado”
* “Operação não permitida”
* “Erro de comunicação com servidor”

# 12. Considerações de LGPD e Segurança

Acesso restrito a administradores. Auditoria nas operações de escrita. Não há tratamento de dados pessoais sensíveis neste submódulo. Anonimizar IP de logs após 180 dias.

# 13. Estrutura de Dados (Proposta)

**Tabela: seguranca\_logs\_acesso**  
• id BIGSERIAL PK  
• usuario\_id BIGINT FK(usuarios.id)  
• nome\_usuario VARCHAR(150)  
• evento VARCHAR(50)  
• status VARCHAR(20)  
• ip\_origem VARCHAR(45)  
• user\_agent TEXT  
• data\_evento TIMESTAMPTZ NOT NULL  
• mensagem TEXT  
  
Índices:  
• IX\_logs\_usuario\_data  
• IX\_logs\_evento\_status

# 14. Referências do Projeto

*Os arquivos abaixo são os guias oficiais deste projeto e servem como referência normativa para front‑end, back‑end, integração e nomenclatura. A implementação deve observar estritamente estes materiais.*

|  |  |
| --- | --- |
| **Arquivo** | **Descrição** |
| A-react\_guide.md | Guia de front‑end (padrões de componentes, UX, grid, modal, tooltip, truncamento visual, acessibilidade). |
| A-guia\_fastapi.md | Guia de back‑end (FastAPI): estrutura de rotas, validação, handlers de erro, observabilidade. |
| NomenclatureGuide.md | Padrões de nomenclatura: DDD, nomes de módulos, rotas, DTOs e eventos. |
| A-integration\_guide.md | Integrações externas e internas: contratos, autenticação, timeouts, políticas de retry e mensagens de erro. |

# 15. Mapa de Integrações

|  |  |  |  |
| --- | --- | --- | --- |
| ID | Título | Escopo | Documento |
| **IN01** | **Registrar Log** | **POST /api/logs** | **A-integration\_guide.md (§IN01)** |
| **IN02** | **Listar Logs** | **GET /api/logs?filters** | **A-integration\_guide.md (§IN02)** |
| **IN03** | **Detalhar Log** | **GET /api/logs/{id}** | **A-integration\_guide.md (§IN03)** |

# 16. Integração com o Projeto Existente (Resumo)

⚠️ IMPACTO OBRIGATÓRIO NO CÓDIGO DOS DEMAIS SUBMÓDULOS.  
  
Os submódulos já existentes (Usuários, Grupos, Grupos X Usuários, Permissões) DEVEM ser ajustados para registrar e consultar logs de acesso.  
• Front-end: inclusão de chamadas automáticas para registrar eventos.  
• Back-end: inclusão de chamadas à API POST /api/logs.  
• Perfis não autorizados devem ser bloqueados pelo submódulo de Permissões.