**Plano de Segurança**

**Sistema de Controle de Documentos Internos**

| **Empresa:** | SecureData TI |
| --- | --- |
| **Sistema:** | Sistema de Controle de Documentos Internos |
| **Data de Elaboração:** | 21 de agosto de 2025 |
| **Versão do Documento:** | 1.0 |
| **Autor:** | Rafael Gustavo Kuhnen |

**Histórico de Revisões**

| **Versão** | **Data** | **Descrição da Alteração** | **Autor** |
| --- | --- | --- | --- |
| 1.0 | 21/08/2025 | Versão inicial do Plano de Segurança. | Rafael Gustavo Kuhnen |

**1. Introdução**

Este documento estabelece o Plano de Segurança para o **Sistema de Controle de Documentos Internos** da SecureData TI. O seu principal objetivo é definir e formalizar as regras, os procedimentos e as configurações de segurança aplicadas ao sistema para garantir a proteção das informações corporativas.

O plano aborda a política de controle de acesso, a definição de perfis de usuário, a lógica de autorização implementada e a validação dos mecanismos de segurança por meio de simulações. A aplicação destas diretrizes visa mitigar riscos de acesso não autorizado, assegurando a **confidencialidade**, **integridade** e **disponibilidade** dos documentos gerenciados pela plataforma.

**2. Política de Controle de Acesso**

A política de acesso do sistema é fundamentada no princípio do **menor privilégio**. Cada usuário terá acesso apenas aos recursos e funcionalidades estritamente necessários para a execução de suas tarefas

**3. Lista de Usuários e Permissões**

Foram definidos três perfis de acesso para o sistema. A tabela abaixo detalha as permissões de cada perfil e exemplifica sua atribuição a usuários fictícios.

| **Nome Fictício** | **Login** | **Perfil** | **Permissões Concedidas** |
| --- | --- | --- | --- |
| Rafael Kuhnen | rafael.kuhnen@adm.com | **Administrador** | **Acesso Total:** Visualizar, criar, editar e excluir todos os documentos. Gerenciar contas de usuários (criar, editar perfis, desativar). Acessar logs de auditoria do sistema. |
| João Silva | joao.silva@editor.com | **Editor** | **Acesso para Colaboração:** Visualizar todos os documentos. Editar o conteúdo de documentos existentes. Não pode excluir documentos ou gerenciar usuários. |
| Ana Souza | ana.souza@visu.com | **Leitor** | **Acesso para Consulta:** Apenas visualizar .Não possui permissão para criar, editar ou excluir qualquer conteúdo. |

**4. Lógica de Controle Implementada**

O controle de acesso do sistema segue um fluxo rigoroso para garantir que as permissões sejam aplicadas corretamente em todas as interações do usuário com a plataforma.

1. **Autenticação do Usuário:**
   * O usuário acessa a tela de login e informa suas credenciais (email e senha).
   * O sistema verifica as credenciais.
   * Em caso de sucesso, uma sessão segura é criada para o usuário. Em caso de falha, o acesso é negado.
2. **Autorização Baseada em Perfil (RBAC):**
   * Após a autenticação bem-sucedida, o sistema recupera o perfil associado ao usuário (Administrador, Editor ou Leitor).
   * Para cada requisição que o usuário faz (ex: editar um documento, visualizar um documento), o sistema intercepta a ação e verifica se o perfil do usuário possui a permissão necessária para executá-la.
   * Se a permissão for concedida, a ação é executada.
   * Se a permissão for negada, o usuário é redirecionado para uma recebe uma mensagem informando que a operação não é permitida.

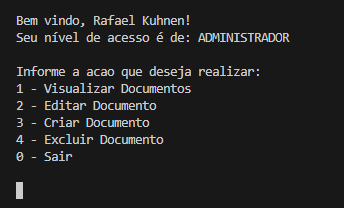
**5. Simulação de Tentativas de Acesso Inválido**

Para validar a eficácia dos controles implementados, foram realizados testes simulando tentativas de contornar as regras de segurança.

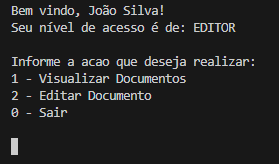
| Cenário de Teste | Ação Simulada | Resultado Esperado | Resultado Obtido (Status) |
| --- | --- | --- | --- |
| **1. Login com Credenciais Inválidas** | Um usuário tenta acessar o sistema com a senha senha1234 para o login joao.silva. | O sistema deve bloquear o acesso e exibir a mensagem "Usuário ou senha inválidos." | **Sucesso** |
| **2. Tentativa de Edição por um Leitor** | O usuário ana.souza (Leitor) tenta enviar uma requisição de edição de um documento, burlando seu nível de acesso. | O sistema deve validar a permissão do usuário antes de processar a requisição e retornar um erro de "Não autorizado", sem alterar o documento. | **Sucesso** |
| **3. Tentativa de Exclusão por um Editor** | O usuário joao.silva (Editor) tenta acessar a funcionalidade de exclusão de um documento, que é restrita ao Administrador. | A interface não deve exibir o botão de exclusão. Se o usuário tentar forçar o acesso, o sistema deve bloquear a ação com uma mensagem de erro. | **Sucesso** |

**6. Prints de Tela das Permissões Funcionando (Evidências)**

Nesta seção são apresentadas as evidências visuais do correto funcionamento do controle de acesso no sistema.

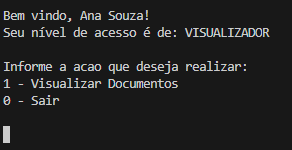
Figura 1 – Visão do Perfil Administrador

Legenda: A interface do Administrador exibe todas as opções de gerenciamento,  
incluindo a opção “Criar Documento” e “Excluir Documento”.

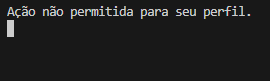
Figura 2 – Visão do Perfil Editor

Legenda: O perfil Editor tem acesso às funcionalidades de criação e edição de documentos, mas as opções administrativas não estão visíveis.

Figura 3 – Visão do Perfil Leitor



Legenda: A interface do Leitor é restrita à visualização. Todos os botões que permitem a modificação de conteúdo estão ocultos.

Figura 4 – Tela de Acesso Negado

Legenda: Mensagem de erro exibida quando o usuário ana.souza (Leitor) tentou acessar uma ação ao qual não tem acesso.

Este documento foi aprovado e deve ser seguido como padrão para a operação segura do Sistema de Controle de Documentos Internos.