### **Documento 1: Plano de Segurança**

**Plano de Segurança – Sistema de Controle de Documentos (SCD)**

* **Empresa:** SecureData TI
* **Data:** 27 de agosto de 2025
* **Versão:** 1.0
* **Responsável:** [Nome do Responsável pela Segurança da Informação]

**1. Introdução e Objetivos**

Este Plano de Segurança estabelece as diretrizes, responsabilidades e procedimentos para garantir a confidencialidade, integridade e disponibilidade dos documentos gerenciados pelo Sistema de Controle de Documentos (SCD) da SecureData TI.

O objetivo principal é proteger os ativos de informação da empresa contra acesso, modificação, destruição ou divulgação não autorizada, em conformidade com as políticas internas e regulamentações aplicáveis, como a LGPD.

**2. Ativos de Informação a Serem Protegidos**

O principal ativo protegido por este plano são os **documentos internos** da SecureData TI, que incluem, mas não se limitam a:

* Contratos com clientes e fornecedores
* Propostas comerciais e estratégias de negócio
* Documentação técnica e código-fonte de projetos
* Relatórios financeiros e dados contábeis
* Documentos de Recursos Humanos (dados de funcionários)

**3. Classificação da Informação e Níveis de Acesso**

Todos os documentos no SCD devem ser classificados no momento do upload. O acesso é controlado por um sistema de Role-Based Access Control (RBAC), definido em três perfis principais:

* **Nível 1: Visualização (Leitor)**
  + **Permissões:** Apenas visualizar e baixar o conteúdo dos documentos aos quais tem acesso.
  + **Proibido:** Editar, excluir, compartilhar ou alterar permissões.
  + **Caso de Uso:** Colaboradores que precisam consultar informações, como políticas internas ou relatórios finalizados.
* **Nível 2: Edição (Colaborador)**
  + **Permissões:** Todas as permissões do Nível 1, mais a capacidade de editar, salvar novas versões e fazer upload de documentos em pastas designadas.
  + **Proibido:** Excluir documentos de outros usuários (exceto os seus próprios), gerenciar usuários ou alterar a estrutura de pastas do sistema.
  + **Caso de Uso:** Equipes de projeto que trabalham colaborativamente em documentos, como desenvolvedores e analistas.
* **Nível 3: Administração (Administrador)**
  + **Permissões:** Acesso total ao sistema. Pode visualizar, editar, excluir e gerenciar qualquer documento ou pasta. É o único perfil que pode gerenciar contas de usuários (criar, editar perfis, resetar senhas) e configurar as regras de acesso do sistema.
  + **Proibido:** Nenhuma restrição técnica, mas deve seguir as políticas de governança da empresa.
  + **Caso de Uso:** Gestores de TI, líderes de departamento e o responsável pela segurança da informação.

**4. Políticas de Controle de Acesso**

* **Autenticação:** O acesso ao SCD exigirá autenticação via login (e-mail corporativo) e senha. Recomenda-se a implementação de Autenticação de Múltiplos Fatores (MFA) para perfis de Administração.
* **Política de Senhas:**
  + Mínimo de 12 caracteres.
  + Uso obrigatório de letras maiúsculas, minúsculas, números e símbolos.
  + Troca obrigatória a cada 90 dias.
  + Bloqueio de conta após 5 tentativas de login sem sucesso.
* **Concessão de Acesso:** O acesso será concedido com base no princípio do "menor privilégio". Um usuário receberá apenas o nível de acesso estritamente necessário para desempenhar suas funções. A criação de novos usuários e a atribuição de perfis são de responsabilidade exclusiva dos Administradores.
* **Revisão de Acesso:** A cada 6 meses, os Administradores deverão realizar uma auditoria completa dos perfis e permissões, revogando acessos que não são mais necessários.

**5. Segurança do Ambiente**

* **Criptografia:** Todos os documentos armazenados no servidor devem ser criptografados em repouso (AES-256). A comunicação entre o usuário e o servidor deve ser protegida com criptografia em trânsito (HTTPS/TLS 1.2 ou superior).
* **Logs e Monitoramento:** O sistema deve registrar todas as atividades relevantes, incluindo: logins (sucesso e falha), visualização, upload, edição e exclusão de documentos. Esses logs devem ser revisados periodicamente.
* **Backup:** Rotinas de backup automatizadas e diárias devem ser configuradas para os dados do sistema. Testes de restauração devem ser realizados trimestralmente para garantir a integridade dos backups.

**6. Simulação e Validação (Plano de Testes de Segurança)**

Antes da entrada em produção, uma simulação de uso será conduzida para validar os controles de permissão:

1. **Criação de Usuários de Teste:** Criar um usuário para cada perfil (Leitor, editor, admin).
2. **Cenário 1 (Leitor):**
   * Login com reader
   * Tentar acessar um documento permitido (deve funcionar).
   * Tentar editar o mesmo documento (deve ser bloqueado).
   * Tentar fazer upload de um novo arquivo (deve ser bloqueado).
   * Tentar acessar a área de administração de usuários (deve ser bloqueado).
3. **Cenário 2 (Colaborador):**
   * Login com editor
   * Acessar e editar um documento permitido (deve funcionar).
   * Fazer upload de um novo documento em sua pasta (deve funcionar).
   * Tentar excluir um documento de outro usuário (deve ser bloqueado).
   * Tentar resetar a senha de outro usuário (deve ser bloqueado).
4. **Cenário 3 (Administrador):**
   * Login com admin
   * Executar todas as ações acima com sucesso.
   * Criar um novo usuário e atribuir-lhe o perfil de Leitor.
   * Verificar os logs de atividades dos outros usuários de teste.

A entrada em produção só será autorizada após a conclusão bem-sucedida de todos os cenários de teste, com documentação dos resultados.