**Questionário de Avaliação de Integração AD**

**2. Requisitos Funcionais**

**2.1 Autenticação e Controle de Acesso**

1. O sistema garante que somente usuários autorizados consigam acessá-lo por meio de um processo seguro de autenticação?

Sim, o sistema possui autenticação com controle de acesso seguro, SSO.

1. O sistema permite autenticação via LDAP, SAML, OIDC ou outro protocolo seguro?

Autenticação via SAML

1. Se não houver suporte ao AD, o sistema possui mecanismos robustos de autenticação (banco de usuários próprio com MFA obrigatório)?

Possui suporte ao AD

1. A autorização de usuários é baseada em grupos do AD ou perfis internos do sistema?

Perfis internos do sistema.

1. O sistema permite atribuir e remover permissões de forma centralizada?

Sim

1. O sistema suporta MFA (ex.: Google Authenticator, Microsoft Authenticator, Yubikey)?

Sim

1. O MFA é exigido para acessos administrativos ou de alto privilégio?

Será exigido a todos os usuários

1. O sistema impede múltiplas sessões simultâneas com a mesma credencial?

Sim

1. É possível configurar tempo máximo de inatividade antes do logout automático?

Não é possível

1. O número de tentativas inválidas de login é configurável para bloquear o usuário após um limite definido?

3 tentativas, não configurável

1. O sistema permite a recuperação de conta com fluxo seguro de redefinição de senha?

Sim

1. A redefinição de senha exige autenticação secundária (ex.: e-mail verificado, MFA)?

Sim

**2.2 Gestão de Senhas**

1. O sistema permite envio automático de senhas por canal seguro (e-mail criptografado, SMS seguro)?

Permite via e-mail

1. As senhas iniciais são aleatórias e temporárias, exigindo troca no primeiro acesso?

Sim

1. O sistema suporta configuração personalizada de senhas, incluindo:
   * Mínimo de 8 caracteres;
   * Uso obrigatório de letras maiúsculas, minúsculas, números e caracteres especiais;
   * Expiração periódica de senhas (parametrizável)?

Permite personalizar a política de senhas, e expiração periódica.

1. O sistema obriga a troca de senha no primeiro acesso?

Sim

1. O sistema notifica o usuário sempre que sua senha for alterada?

Sim

**2.3 Controle de Permissões e Perfis**

1. O sistema permite criação e gerenciamento de perfis de acesso com permissões predefinidas?

Sim

1. Perfis são baseados em funções de negócio, evitando atribuição direta de permissões a usuários individuais?

Sim

1. O sistema impede que um único usuário tenha acessos conflitantes (ex.: criar e aprovar transações financeiras)?

É possível configurar as permissões dos usuários

1. O sistema oferece um painel ou relatório que permite visualizar e auditar acessos atribuídos a cada usuário?

Sim

**3. Requisitos de Segurança e Auditoria**

**3.1 Logs e Rastreabilidade**

1. O sistema armazena logs detalhados de:
   * Tentativas de login (sucesso e falha);
   * Alterações de senha (usuário, data, IP de origem);
   * Criação, remoção e modificação de usuários e permissões;
   * Alterações administrativas (configurações críticas do sistema)?

Sim

1. O sistema permite exportação dos logs para ferramentas de auditoria e SIEMs?

Não é possível exportar

1. Logs são retidos por no mínimo 6 meses e estão acessíveis para consulta?

Sim

**4. Requisitos de Automação e Provisionamento**

1. O sistema permite importação e sincronização de usuários com o AD?

Via AD apenas autenticação.

1. A criação e remoção de usuários é automatizada conforme regras de governança?

É possível automatizar através de API

1. O sistema permite extração de relatório de dados de usuários, incluindo:
   * Login, nome, status, perfil, data de criação, último login, última modificação?

Sim, exceto informações de último login

1. O sistema oferece APIs que permitem integração com ferramentas de gestão de identidades e acessos?

Sim. Documentação disponível através do link: <https://lemontechinfo.atlassian.net/wiki/spaces/DW/overview>

**5. Conformidade e Manutenção**

1. O sistema segue padrões reconhecidos, como:
   * ISO 27001 (Gestão de Segurança da Informação);
   * NIST SP 800-63 (Autenticação Digital);
   * LGPD / GDPR (Proteção de Dados Pessoais)?

Possuímos certificação PCI-DSS

1. O fornecedor garante atualizações regulares e suporte técnico contínuo?

Sim

1. Vulnerabilidades de segurança são corrigidas com SLAs claros?

Sim

1. O sistema permite auditorias para verificar conformidade com os requisitos estabelecidos?

Sim

1. Logs e acessos são revisados regularmente para identificação de anomalias?

Sim