**Documento Consolidado: Arquitetura e Requisitos do BGS IDP Connect**

**1. Introdução**

O presente documento consolida todas as informações relacionadas ao projeto **BGS IDP Connect**, desenvolvido para a integração e autenticação unificada dos sistemas da BGS Corporate. Ele inclui a arquitetura técnica, fluxos de autenticação, modelo de dados, requisitos de compliance e resultados de validação.

**2. Arquitetura Geral**

1. **Componentes Principais:**
   * **IDP:** Centraliza a autenticação e gera tokens JWT/SAML para integração.
   * **SSO:** Permite acesso unificado a todos os sistemas.
   * **MFA:** Adiciona uma camada extra de segurança.
   * **API Gateway:** Roteia as solicitações de autenticação e autorização.
   * **Banco de Dados de Usuários:** Armazena credenciais e perfis de forma criptografada.
   * **Sistema de Logs:** Garante rastreabilidade e conformidade com a LGPD.
2. **Diagrama de Arquitetura:**
   * Representação visual dos módulos e integrações.
   * Inclui os sistemas legados (CRM, ERP, BGS Club) e modernos (Marketplace, BGS Pay).

**3. Integração dos Sistemas**

1. **Sistemas Modernos:**
   * Protocolos Utilizados: **OpenID Connect**.
   * Detalhes de Integração:
     + Registro do Client ID no IDP.
     + Configuração de URLs de redirecionamento.
     + Mapear atributos como email e roles.
2. **Sistemas Legados:**
   * Protocolos Utilizados: **SAML**.
   * Ajustes Realizados:
     + Mapeamento de atributos personalizados.
     + Configuração de endpoints de login e logout.
     + Importação de certificados digitais para validação.

**4. Modelo de Dados**

1. **Tabelas Principais:**
   * **Usuários:** ID, nome, email, senha (criptografada).
   * **Perfis:** Definem os tipos de acesso atribuídos.
   * **Permissões:** Ações permitidas por perfil.
   * **Logs de Acessos:** Histórico de atividades de login.
2. **Diagrama Entidade-Relacionamento (ERD):**
   * Representação visual das relações entre as tabelas.

**5. Requisitos de Compliance**

1. **LGPD:**
   * **Segurança de Dados:** Credenciais criptografadas e transmissão via TLS.
   * **Auditoria:** Logs detalhados de acessos para rastreabilidade.
   * **Consentimento:** Configuração para obtenção e registro de consentimento de usuários.
2. **Outras Medidas de Segurança:**
   * MFA implementado para acessos sensíveis.
   * Certificados digitais X.509 configurados para garantir autenticidade.

**6. Resultados e Validação**

1. **Relatório de Testes:**
   * Cenários Testados:
     + Autenticação bem-sucedida em sistemas legados e modernos.
     + Logout propagado entre sistemas.
     + Falhas controladas em credenciais inválidas.
2. **Evidências:**
   * Capturas de tela mostrando autenticações bem-sucedidas.
   * Logs detalhados de acessos.

**7. Checklist Final**

1. Configuração do IDP concluída.
2. Certificados digitais instalados.
3. Integração validada com sistemas modernos e legados.
4. Logs e evidências registrados para auditoria.

Este documento consolidado reflete o sucesso da implementação do **BGS IDP Connect** e está alinhado aos requisitos técnicos e de compliance da BGS Corporate. Ele serve como referência para operação, manutenção e futuras expansões.

deixe esse documento mais completo com os gráficos