**BRUNO GONZAGA TEIXEIRA CORREA**

Documentação Consolidada:

Arquitetura e Requisitos do BGS IDP Connect

**São Paulo  
06/01/2025**

**Sumário**

1. **Introdução**
2. **Canvas do Projeto Aplicado**
   * Matriz CSD para análise do desafio
   * POEMS para o projeto BGS IDP Connect
   * Personas e mapa de empatia
   * Blueprint do projeto
   * CANVAS de proposta de valor
   * Hipóteses e matriz de priorização
3. **Evidências do planejamento, execução e resultados**
   * **Sprint 1: Planejamento da Arquitetura**
     + Tarefa 1: Estrutura geral do IDP
     + Tarefa 2: Escolha dos protocolos de segurança
     + Tarefa 3: Mapeamento dos sistemas existentes
     + Resultados Alcançados na Sprint 1
   * **Sprint 2: Desenvolvimento da Integração**
     + Tarefa 1: Fluxo de autenticação SSO
     + Tarefa 2: Modelo de banco de dados
     + Tarefa 3: Integração com sistemas legados
     + Resultados Alcançados na Sprint 2
   * **Sprint 3: Validação e Consolidação**
     + Tarefa 1: Validação de sistemas legados
     + Tarefa 2: Guia de implementação
     + Tarefa 3: Consolidação da documentação
     + Resultados Alcançados na Sprint 3
4. **Arquitetura Geral**
   * Componentes principais
   * Fluxo de conexão
5. **Integração dos Sistemas**
   * Sistemas modernos (OpenID Connect)
   * Sistemas legados (SAML)
6. **Modelo de Dados**
   * Estrutura de tabelas principais (ERD)
7. **Requisitos de Compliance**
   * LGPD e medidas de segurança
8. **Resultados e Validação**
   * Relatório de testes
   * Evidências de autenticação
9. **Checklist Final**
   * Itens de configuração validados
10. **Considerações Finais**
    * Resultados alcançados
    * Contribuições do projeto
    * Próximos passos

**Documentação Consolidada:**

**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, servindo como referência para operação, manutenção e futuras expansões.

**2. Canvas do Projeto Aplicado**



**2.2. Matriz CSD para Análise do Desafio**

| **Certezas** | **Suposições** | **Dúvidas** |
| --- | --- | --- |
| 1. Cada sistema da BGS Corporate possui seu próprio login, exigindo autenticações separadas para o marketplace, BGS Pay, BGS Club, CRM e ERP. | 1. Usuários preferem uma experiência de login unificada para reduzir o tempo gasto em autenticações múltiplas. | 1. Qual é a aceitação dos usuários finais para autenticação multifatorial (MFA) para sistemas sensíveis? |
| 2. A fragmentação dos logins aumenta os chamados de suporte técnico relacionados a problemas de acesso. | 2. A unificação do login via um IDP (Identity Provider) reduzirá o tempo de resposta do suporte e a carga operacional. | 2. Como será o impacto na experiência de usuário ao implementar um IDP com SSO? |
| 3. A falta de um sistema de autenticação centralizado dificulta a aplicação de políticas de segurança consistentes. | 3. Implementar uma autenticação multifatorial (MFA) integrada ao IDP aumentará a segurança em sistemas críticos, como o BGS Pay. | 3. Quais barreiras tecnológicas poderemos encontrar ao integrar o IDP com os sistemas legados, como o marketplace em PHP? |
| 4. Conformidade com a LGPD e proteção de dados exige controle centralizado de autenticação e permissões. | 4. Uma solução IDP em nuvem facilitará o escalonamento para futuras integrações com novos serviços ou parcerias. | 4. Qual a aceitação e familiaridade da equipe interna com a nova solução de autenticação centralizada? |

**2.3 POEMS para o Projeto BGS IDP Connect**

**P**essoas diretamente envolvidas no uso dos sistemas da BGS Corporate:

* Clientes Finais: usuários do marketplace e do BGS Club que desejam uma experiência de navegação fluida com acesso simplificado a todos os serviços.
* Equipe Interna: colaboradores das áreas de marketing, vendas e atendimento ao cliente que utilizam os sistemas de CRM e ERP.
* Equipe de Suporte Técnico: colaboradores da área de TI que atendem os chamados relacionados a problemas de acesso e login.

**O**bjetos utilizados para acessar os serviços e sistemas da BGS Corporate:

* Interfaces de Login: cada sistema possui uma interface de login separada, o que gera uma experiência fragmentada.
* Dispositivos de Autenticação: telefones celulares e desktops para autenticação multifatorial (MFA) quando disponível.
* Portais de Suporte: ferramentas de suporte usadas pela equipe técnica para ajudar na recuperação de acessos e reset de senhas.

**A**mbientes onde os sistemas da BGS Corporate são utilizados:

* Ambiente Corporativo: acesso para os colaboradores via conexão à internet do escritório ou VPN.
* Ambiente Digital: acesso para os clientes finais de qualquer dispositivo com conexão à internet.
* Ambiente de Suporte: acesso para a equipe de suporte aos sistemas de atendimento e chamados dos colaboradores.

**M**ensagens que os usuários recebem durante a navegação nos sistemas:

* Notificações de Login e Autenticação: as mensagens de autenticação e verificação de login são separadas para cada sistema, e não há uma mensagem centralizada ou personalizada.
* Alertas de Segurança: faltam alertas de segurança consistentes entre os sistemas, como notificações de login em locais não reconhecidos ou tentativas de login suspeitas.
* Mensagens de Suporte: os usuários recebem respostas padronizadas e muitas vezes repetitivas, o que não resolve efetivamente a maioria dos problemas relacionados ao login.

**S**erviços disponibilizados para usuários internos e clientes finais:

* Single Sign-On (SSO) Proposto: o serviço de autenticação unificada que o BGS IDP Connect pretende oferecer, permitindo acesso centralizado a todos os sistemas com uma única credencial.
* Suporte ao Cliente: o suporte técnico e a assistência de TI para recuperação de senhas e problemas de login, que atualmente demandam bastante tempo.
* Autenticação Multifatorial (MFA): o uso de MFA para aumentar a segurança, especialmente para o BGS Pay e outras áreas sensíveis.
* Painel de Gestão de Acessos: serviço interno que permitirá a gestão dos acessos e perfis de usuários, facilitando a administração e controle de permissões.

**2.4. Personas e Mapa de Empatia**

**Bruno, Arquiteto de Software e Soluções**

**Características Pessoais**: 35 anos, casado, pai de uma filha. Apaixonado por tecnologia e inovação, Bruno dedica seu tempo livre a hobbies como leitura de ficção científica e viagens em família.

**Características Sociais**: Introvertido, porém excelente comunicador em reuniões técnicas e apresentações de projetos. Participa de conferências de tecnologia e é respeitado no setor por seu conhecimento profundo em arquiteturas modernas.

**Características Intelectuais**: Formado em Engenharia de Computação, com especialização em Arquitetura de Sistemas. Possui certificações em metodologias ágeis, SSO (Single Sign-On) e segurança da informação. Bruno é altamente analítico e possui forte foco em soluções escaláveis e seguras.

**Características Profissionais**: Trabalha na BGS Corporate há 3 anos, liderando projetos de arquitetura e soluções digitais. Com experiência em transições para arquiteturas baseadas em microsserviços e integração de sistemas complexos, Bruno é responsável pelo desenho da arquitetura do BGS IDP Connect. Seu objetivo é criar um sistema que permita autenticação unificada e segura, compatível com os protocolos modernos e que seja facilmente escalável. Ele prioriza a segurança e a conformidade com a LGPD e busca uma solução que garanta uma experiência integrada e simplificada para usuários internos e externos, enquanto reduz as demandas de suporte técnico.

Diagrama

Descrição gerada automaticamente

**Carla, Gerente de TI da BGS Corporate**

**Características Pessoais**: 45 anos, casada, mãe de dois filhos. Gosta de resolver problemas complexos e é entusiasta da inovação tecnológica.

**Características Sociais**: Comunicativa e colaborativa, valoriza o trabalho em equipe e participa ativamente de conferências de TI.

**Características Intelectuais**: Graduada em Ciência da Computação com MBA em Gestão de Tecnologia. É orientada para resultados e possui experiência em implementação de soluções corporativas de TI.

**Características Profissionais**: Atua na BGS Corporate há 10 anos e é responsável pela implementação e manutenção de soluções tecnológicas na empresa. Ela busca um sistema de autenticação unificada que facilite o acesso e traga mais segurança para os dados corporativos, simplificando a gestão de acessos.

Diagrama, Site

Descrição gerada automaticamente

**Roberto, Analista de Segurança da Informação**

**Características Pessoais**: 37 anos, solteiro, apaixonado por cibersegurança e leitura sobre novas ameaças digitais.

**Características Sociais**: Reservado, mas ativo em fóruns de segurança online, onde compartilha práticas de proteção de dados.

**Características Intelectuais**: Formado em Engenharia de Redes com especialização em Segurança da Informação. Tem forte atenção aos detalhes e é motivado por desafios técnicos.

**Características Profissionais**: Trabalha na BGS Corporate há 5 anos, sendo responsável pela segurança dos sistemas e pela proteção dos dados corporativos. Ele considera a criação de uma arquitetura IDP robusta essencial para garantir a conformidade com a LGPD e minimizar vulnerabilidades.

Diagrama, Site

Descrição gerada automaticamente

**Fernanda, Designer e Especialista em UX**

**Características Pessoais**: 31 anos, solteira, apaixonada por design de interfaces intuitivas e centradas no usuário. Nas horas vagas, gosta de estudar psicologia cognitiva aplicada ao design e é entusiasta de práticas de meditação.

**Características Sociais**: Extrovertida e comunicativa, adora colaborar com equipes multifuncionais e participa de eventos e conferências sobre UX/UI. É conhecida por ser uma excelente ouvinte, sempre aberta ao feedback de usuários e colegas para aprimorar o design.

**Características Intelectuais**: Formada em Design Gráfico, com especialização em UX e certificação em Design Thinking. Fernanda é criativa e analítica, sempre em busca de entender as necessidades dos usuários e de oferecer a melhor experiência possível.

**Características Profissionais**: Trabalha na BGS Corporate há 2 anos, dedicando-se a criar interfaces claras e eficazes para os produtos da empresa. No projeto BGS IDP Connect, Fernanda é responsável por desenhar a interface de login unificado, garantindo que o sistema seja simples e intuitivo tanto para clientes quanto para colaboradores. Ela se preocupa em oferecer uma experiência de login segura, rápida e acessível, considerando a diversidade de usuários. Para Fernanda, a satisfação do usuário e a eficiência da interface são prioridades, e buscando constantemente melhorar a usabilidade e acessibilidade.

Diagrama

Descrição gerada automaticamente

**2.5. Blueprint**

O blueprint detalhado do projeto BGS IDP Connect oferece uma visão completa de todo o processo, desde o planejamento inicial até as interações com os usuários e o suporte contínuo. Com essa estrutura, fica mais fácil acompanhar cada fase do projeto de forma organizada, permitindo que todos os envolvidos entendam suas responsabilidades e saibam exatamente o que precisa ser feito em cada etapa.

| **Seção** | **Etapa** | **Ações do Usuário** | **Interações Internas** | **Processos de Suporte** |
| --- | --- | --- | --- | --- |
| **Planejamento** | 1. Definição de Requisitos | - | Equipe de TI e de segurança definem requisitos de autenticação e SSO | Consultoria com especialistas em segurança e conformidade |
|  | 2. Mapeamento dos Sistemas | - | Identificação de sistemas que serão integrados (Marketplace, BGS Pay, etc.) | Criação de um plano de integração para compatibilidade |
|  | 3. Design da Arquitetura | - | Arquiteto de soluções define a estrutura técnica do IDP | Validação da arquitetura com revisões de conformidade e segurança |
| **Implementação** | 4. Desenvolvimento do IDP | - | Equipe de desenvolvimento constrói o sistema de autenticação | Testes iniciais de integração e segurança |
|  | 5. Configuração de SSO e MFA | - | Implementação de SSO e autenticação multifatorial | Teste de funcionalidade para acesso unificado e segurança adicional |
|  | 6. Teste e Validação | - | Equipe de QA realiza testes de usabilidade e segurança | Identificação e resolução de problemas antes do lançamento |
| **Etapas do Usuário** | 7. Acesso Inicial ao Sistema | Usuário acessa o portal da BGS Corporate | Configuração de autenticação para todos os sistemas | Suporte técnico para problemas de login |
|  | 8. Login Único (SSO) | Usuário faz login com credenciais únicas | Verificação de credenciais e aplicação de MFA se necessário | Atendimento para dúvidas e problemas com MFA |
|  | 9. Navegação Integrada entre Sistemas | Usuário navega entre sistemas sem login adicional | Sincronização de permissões entre o IDP e sistemas conectados | Monitoramento de acessos e detecção de comportamentos anômalos |
| **Interações Internas** | 10. Gestão de Acessos e Permissões | - | TI define níveis de acesso e permissões para clientes e colaboradores | Auditorias periódicas para garantir conformidade com políticas de acesso |
|  | 11. Monitoramento de Segurança | - | Equipe de segurança monitora acessos suspeitos e aplica políticas de segurança | Suporte para redefinição de senha e análise de incidentes |
|  | 12. Gestão de Conformidade | - | Equipe de conformidade verifica aderência às normas da LGPD | Relatórios de compliance e revisão de práticas de proteção de dados |
| **Processos de Suporte** | 13. Manutenção e Atualizações do IDP | - | TI realiza manutenção e aplica correções de segurança | Documentação de melhorias e otimizações na plataforma |
|  | 14. Análise de Dados e Geração de Relatórios | - | Geração de relatórios sobre uso do sistema e análise de incidentes | Insights para otimizar o sistema e reduzir incidentes |
|  | 15. Coleta de Feedback e Melhoria Contínua | - | Coleta de feedback de usuários e análise de sugestões | Implementação de melhorias com base nas necessidades dos usuários |

**2.6. CANVAS de Proposta de Valor**

Diagrama

Descrição gerada automaticamente

**2.7. Hipóteses**

**1) A unificação dos logins (SSO) melhorará a experiência do usuário**

* Hipótese: A complexidade atual dos múltiplos logins causa frustração para os usuários, e um sistema de autenticação unificada (SSO) reduzirá essa frustração e aumentará a satisfação dos clientes e colaboradores.

**2) A implementação de autenticação multifatorial (MFA) reduzirá incidentes de segurança**

* Hipótese: A ausência de uma camada adicional de segurança no login torna os sistemas da BGS Corporate mais vulneráveis a acessos indevidos. Ao incorporar MFA, o projeto irá mitigar os riscos de segurança e proteger melhor os dados dos usuários.

**3) A centralização da gestão de acessos aumentará a eficiência operacional**

* Hipótese: A necessidade de gerenciar acessos separadamente em cada sistema aumenta a carga de trabalho da equipe de TI. Com o BGS IDP Connect, a centralização das permissões reduzirá o tempo e o esforço necessários para administração de acessos.

**4) A conformidade com a LGPD fortalecerá a confiança dos usuários**

* Hipótese: A falta de um sistema centralizado de autenticação dificulta a aplicação de políticas de conformidade com a LGPD, o que gera preocupações entre os usuários quanto à segurança dos seus dados. O IDP com conformidade garantida melhorará a percepção de segurança e a confiança dos usuários.

**5) A redução de chamados ao suporte técnico relacionados a problemas de login**

* Hipótese: O suporte técnico atualmente gasta tempo e recursos com chamados relacionados a problemas de login. Com um sistema de SSO centralizado e simplificado, espera-se uma diminuição significativa desses chamados, melhorando a eficiência do suporte.

**2.8. Matriz de observações para hipóteses**

| **Observação** | **Por que isso está acontecendo?** | **Hipótese** |
| --- | --- | --- |
| Usuários enfrentam dificuldades e frustrações ao precisar fazer login em vários sistemas separados. | A BGS Corporate possui diversos sistemas com logins independentes, o que cria uma experiência fragmentada e aumenta a complexidade de acesso para os usuários. | A unificação dos logins (SSO) melhorará a experiência do usuário, reduzindo a frustração e aumentando a satisfação de clientes e colaboradores. |
| Incidentes de segurança ocorrem devido à ausência de uma camada adicional de proteção nos logins. | A falta de autenticação multifatorial (MFA) permite que acessos indevidos sejam realizados com mais facilidade, comprometendo a segurança dos dados. | A implementação de autenticação multifatorial (MFA) reduzirá incidentes de segurança, protegendo melhor os dados dos usuários. |
| A equipe de TI gasta muito tempo gerenciando acessos e permissões em sistemas separados. | Cada sistema da empresa exige uma gestão de acesso individual, o que aumenta o trabalho operacional e reduz a eficiência da equipe de TI. | A centralização da gestão de acessos aumentará a eficiência operacional, reduzindo o esforço para administração de permissões. |
| Usuários têm preocupações quanto à segurança dos seus dados e conformidade com a LGPD. | A falta de um sistema centralizado dificulta a implementação e monitoramento de políticas de conformidade, deixando usuários inseguros sobre a proteção de seus dados. | A conformidade com a LGPD fortalecerá a confiança dos usuários, aumentando sua percepção de segurança e a credibilidade da BGS Corporate. |
| O suporte técnico recebe muitos chamados relacionados a problemas de login. | A fragmentação de logins causa confusão e problemas de acesso, gerando um alto volume de solicitações para o suporte técnico e reduzindo a eficiência dessa equipe. | A redução de chamados relacionados a problemas de login será alcançada com um sistema de SSO centralizado e simplificado, aumentando a eficiência do suporte. |

**2.9. Matriz de Priorização de Ideias**

| **Ideia** | **Impacto** | **Esforço** | **Prioridade** | **Justificativa** |
| --- | --- | --- | --- | --- |
| Unificação dos logins (SSO) para todos os sistemas da BGS Corporate | Alto | Alto | Alta | O SSO é essencial para melhorar a experiência do usuário e reduzir a fragmentação de logins, sendo a base do projeto e oferecendo grande valor para clientes e equipe. |
| Implementação de autenticação multifatorial (MFA) nas áreas críticas | Alto | Médio | Alta | A MFA é fundamental para aumentar a segurança, especialmente em áreas sensíveis como o BGS Pay, protegendo dados e reduzindo incidentes de segurança. |
| Centralização da gestão de acessos e permissões | Médio | Médio | Média | Simplifica o trabalho da equipe de TI, melhorando a eficiência operacional e facilitando a administração de permissões. |
| Adoção de conformidade total com a LGPD | Alto | Médio | Alta | Fortalece a confiança dos usuários e assegura que o sistema esteja de acordo com as regulamentações de proteção de dados, minimizando riscos de penalidades. |
| Redução de chamados de suporte técnico relacionados a problemas de login | Médio | Baixo | Média | Com a simplificação dos logins, o volume de chamados ao suporte deve diminuir, gerando economia e aumentando a eficiência do atendimento ao usuário. |

**2.10. Matriz de Riscos**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Identificação do Risco** | **Premissa/Restrição** | **Impacto Potencial** | **Probabilidade** | **Severidade** | **Ação Mitigadora** |
| Incompatibilidade com Sistemas Existentes | Premissa: Disponibilidade dos Sistemas Existentes | Esforço adicional de adaptação, atrasando o cronograma e aumentando os custos do projeto. | Alta | Alta | Realizar uma análise técnica prévia para garantir compatibilidade ou prever recursos para adaptações. |
| Falta de Suporte Técnico da Equipe de TI | Premissa: Suporte da Equipe de TI e Segurança | Dificuldade para obter dados específicos dos sistemas e possíveis falhas de segurança no projeto de IDP. | Média | Alta | Definir responsabilidades com a equipe de TI e segurança desde o início para garantir apoio contínuo. |
| Recursos Financeiros e de Tempo Insuficientes | Premissa: Recursos Financeiros e de Tempo Suficientes | Qualidade do projeto prejudicada, comprometendo o detalhamento e a adequação da arquitetura planejada. | Média | Alta | Estabelecer um orçamento claro e revisar alocação de recursos para manter o cronograma. |
| Não Conformidade com LGPD | Restrição: Conformidade com a LGPD | Comprometimento da segurança de dados, com risco de penalidades e danos à reputação da empresa. | Média | Alta | Integrar os requisitos da LGPD ao projeto desde a fase inicial e realizar revisões de compliance. |
| Atraso no Prazo de Conclusão | Restrição: Prazo Limite de Conclusão (45 dias) | Impossibilidade de finalizar a documentação e a entrega dentro do cronograma, prejudicando a implantação futura. | Média | Média | Monitorar o progresso regularmente e alocar mais recursos se necessário para cumprir o prazo. |
| Incompatibilidade com Sistemas Legados | Restrição: Limitação de Integração com Sistemas Legados | Aumento de custos e esforço técnico devido a adaptações necessárias para compatibilidade com sistemas legados. | Alta | Alta | Realizar testes iniciais de compatibilidade e documentar quaisquer ajustes necessários. |

**2.11. Backlog de Produto**

**Sprint 1 - Planejamento da Arquitetura**

* Tarefa 1: Definir a estrutura geral do BGS IDP Connect para suportar SSO e MFA, documentando os componentes principais.
* Tarefa 2: Identificar os protocolos de segurança necessários (SAML, OAuth 2.0 e OpenID Connect) para a integração com sistemas da BGS Corporate.
* Tarefa 3: Mapear os sistemas existentes (Marketplace, BGS Pay, BGS Club, CRM e ERP) para garantir compatibilidade com o IDP.

**Sprint 2 - Desenvolvimento da Integração**

* Tarefa 1: Projetar o fluxo de autenticação SSO, permitindo acesso unificado aos sistemas por meio do BGS IDP Connect.
* Tarefa 2: Desenvolver um modelo básico de dados para controle de permissões e perfis de usuário.
* Tarefa 3: Documentar o processo de integração com sistemas legados, incluindo os principais requisitos de segurança.

**Sprint 3 - Validação e Documentação Final**

* Tarefa 1: Validar a compatibilidade da arquitetura com os sistemas legados e realizar ajustes finais.
* Tarefa 2: Criar o guia de implementação para facilitar a futura integração do IDP.
* Tarefa 3: Consolidar toda a documentação da arquitetura e requisitos de compliance para entrega.

**2.12. Trello**

<https://trello.com/invite/b/6732afe49aa86738d5ef121f/ATTI3105028c95b54db3f45c457e0f07b11fE2654FE9/arquitetura-de-sso-na-nuvem>

**3. Evidências do planejamento, execução e resultados**

**3.1. Sprint 1**

**3.1.1. Tarefa 1: Definir a estrutura geral do BGS IDP Connect para suportar SSO e MFA, documentando os componentes principais.**

**Diagrama em construção no Miro**

**Linha do tempo

Descrição gerada automaticamente com confiança média**

**Descrição**

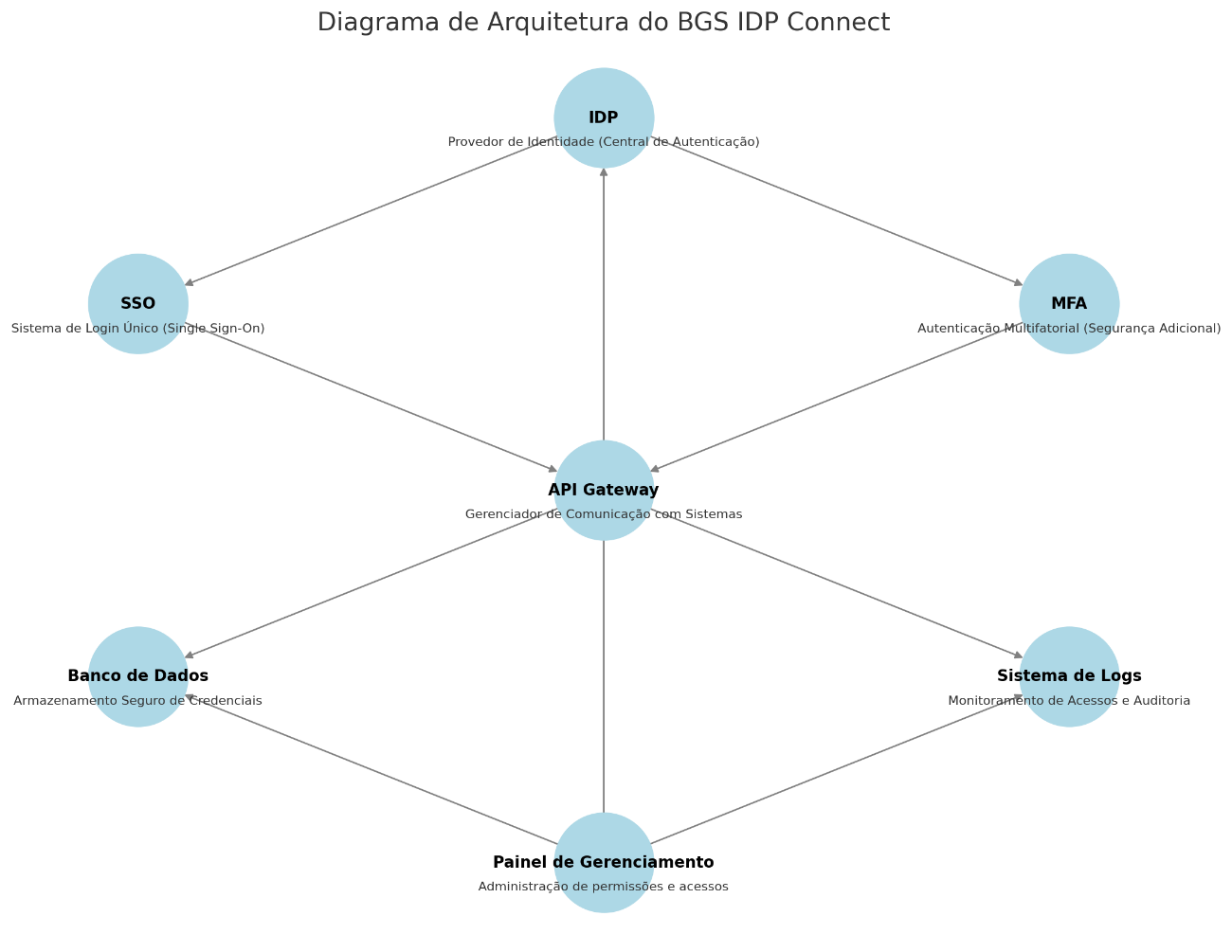
A estrutura geral do **BGS IDP Connect** deve ser projetada para suportar Single Sign-On (SSO) e autenticação multifatorial (MFA), com integração segura e eficiente aos sistemas da BGS Corporate.

**Entrega**

**Diagrama da Arquitetura do BGS IDP Connect**

Inclui os principais componentes:

* **Provedor de Identidade (IDP):** Autenticação centralizada e geração de tokens (ex.: JWT);
* **Serviço de SSO:** Facilita o login único entre diferentes sistemas;
* **MFA (Autenticação Multifatorial):** Integração com métodos de autenticação adicionais (e-mail, SMS, app);
* **API Gateway:** Gerencia a comunicação entre o IDP e os sistemas conectados;
* **Banco de Dados de Usuários:** Armazena credenciais de forma segura, garantindo conformidade com a LGPD;
* **Sistema de Logs e Auditoria:** Registra acessos para monitoramento e conformidade;
* **Painel de Gerenciamento:** Interface para administrar permissões e acessar relatórios.



**Documento Técnico: Arquitetura do BGS IDP Connect**

Inclui a descrição detalhada dos componentes, explica a função de cada módulo e como eles se conectam para suportar SSO e MFA.

**Introdução**

O BGS IDP Connect é uma solução de autenticação unificada, projetada para centralizar o acesso aos sistemas da BGS Corporate, utilizando Single Sign-On (SSO) e autenticação multifatorial (MFA). A seguir, apresentamos uma descrição detalhada dos componentes principais da arquitetura e suas funções, além de como esses módulos se conectam para oferecer uma solução robusta, escalável e segura.

**Descrição dos Componentes**

**1) Provedor de Identidade (IDP):**

**Função:**

* Atua como o núcleo da arquitetura, autenticando e autorizando os usuários;
* Emite tokens de acesso (ex.: JSON Web Tokens - JWT) para sistemas integrados;
* Garante que apenas usuários válidos possam acessar os serviços.

**Conexões:**

* Integra-se diretamente ao SSO para oferecer uma experiência de login unificado;
* Comunica-se com o API Gateway para validar tokens de acesso;
* Trabalha em conjunto com o Banco de Dados de Usuários para validação de credenciais.

**2) Single Sign-On (SSO):**

**Função:**

* Permite que usuários façam login uma única vez e acessem todos os sistemas conectados sem necessidade de reautenticação;
* Centraliza a autenticação em uma interface única e simplificada.

**Conexões:**

* Conectado ao IDP para receber tokens de autenticação;
* Comunicação bidirecional com o API Gateway para propagação de tokens aos sistemas.

**3) Autenticação Multifatorial (MFA):**

**Função:**

* Adiciona uma camada extra de segurança, exigindo um fator adicional além da senha (ex.: código via SMS, e-mail ou aplicativo autenticador);
* Protege áreas críticas, como o sistema de pagamentos.

**Conexões:**

* Vinculado ao IDP para gerenciar e validar fatores adicionais de autenticação;
* Fornece feedback ao API Gateway sobre autenticações bem-sucedidas ou falhas.

**4) API Gateway:**

**Função:**

* Atua como intermediário, gerenciando a comunicação entre o IDP e os sistemas da BGS Corporate;
* Verifica a validade dos tokens e encaminha solicitações para os serviços correspondentes.

**Conexões:**

* Recebe tokens do SSO e valida junto ao IDP;
* Encaminha informações ao Sistema de Logs para auditoria e monitoramento;
* Se conecta ao Banco de Dados de Usuários para consultas de credenciais, se necessário.

**5) Banco de Dados de Usuários:**

**Função:**

* Armazena as informações de autenticação e perfis dos usuários;
* Suporta a conformidade com a LGPD, garantindo que os dados estejam protegidos e criptografados.

**Conexões:**

* Fornece informações ao IDP durante o processo de autenticação;
* Permite que o Sistema de Logs registre eventos relacionados ao gerenciamento de usuários.

**6) Sistema de Logs e Auditoria:**

**Função:**

* Registra todas as ações relacionadas à autenticação, como logins bem-sucedidos, falhas de login e tentativas de MFA;
* Facilita a conformidade com a LGPD ao fornecer histórico de acessos e detecção de comportamentos anômalos.

**Conexões:**

* Recebe informações de eventos do API Gateway e do IDP;
* Gera relatórios de segurança para análise e auditoria

**Fluxo de Conexões**

1. O usuário acessa a interface de login oferecida pelo SSO;
2. O SSO encaminha a solicitação ao IDP para validação das credenciais;
3. Se o MFA estiver ativado, o IDP aciona o módulo de MFA para validação do fator adicional;
4. Após a autenticação bem-sucedida, o IDP emite um token (ex.: JWT);
5. O token é enviado ao API Gateway, que o valida e redireciona o acesso ao sistema desejado;
6. O Sistema de Logs registra todas as ações para monitoramento e auditoria.

**Benefícios da Arquitetura**

* **Segurança:** A combinação de SSO e MFA reduz significativamente os riscos de acessos não autorizados;
* **Eficiência:** O SSO melhora a experiência do usuário, eliminando a necessidade de logins repetidos;
* **Escalabilidade:** A arquitetura é flexível, permitindo a integração de novos sistemas no futuro;
* **Conformidade:** O Banco de Dados de Usuários e o Sistema de Logs garantem adesão à LGPD e a outras regulamentações de proteção de dados.

**3.1.2. Tarefa 2: Identificar os protocolos de segurança necessários (SAML, OAuth 2.0 e OpenID Connect) para a integração com sistemas da BGS Corporate.**

**Diagrama em construção no Miro**

**Uma imagem contendo Aplicativo

Descrição gerada automaticamente**

**Descrição**

Os protocolos de autenticação e segurança são fundamentais para integrar o IDP aos sistemas existentes de forma confiável e segura. Eles garantem a proteção de dados sensíveis, como credenciais de usuários, por meio de criptografia e validação de acessos. Protocolos como **SAML**, **OAuth 2.0** e **OpenID Connect** asseguram a compatibilidade entre sistemas modernos e legados, além de possibilitar o uso de recursos avançados, como autenticação multifatorial (MFA). Assim, esses protocolos não apenas fortalecem a segurança, mas também proporcionam uma experiência de autenticação unificada e eficiente.

**Entrega**

**Tabela Comparativa:**

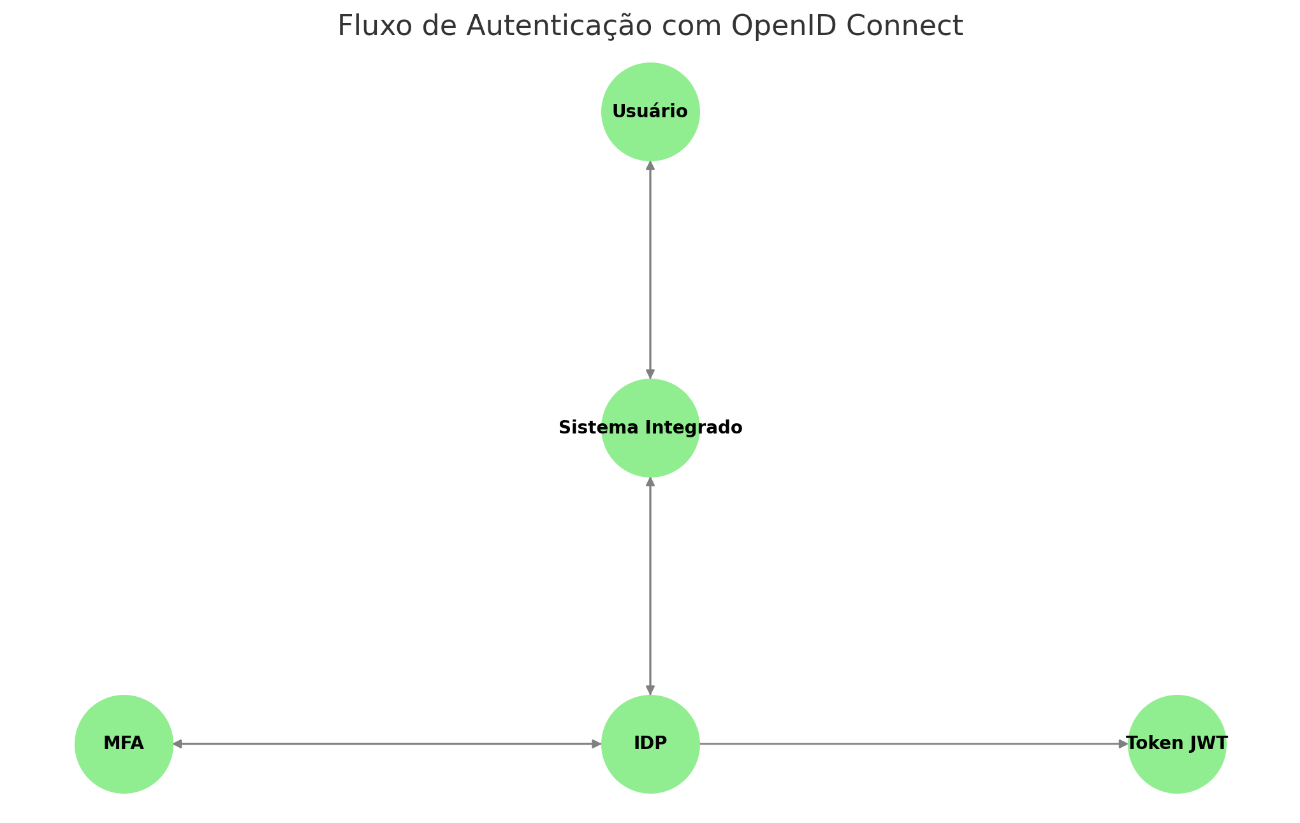
|  |  |  |  |
| --- | --- | --- | --- |
| **Critérios** | **SAML** | **OAuth 2.0** | **OpenID Connect** |
| Segurança | Alta segurança, porém mais complexo em implementações modernas. | Alta segurança, projetado para proteger APIs e acessos externos. | Alta segurança baseada em OAuth 2.0 com foco em autenticação. |
| Compatibilidade | Ampla compatibilidade com sistemas legados. | Compatível com a maioria das aplicações modernas. | Compatível com sistemas modernos e suporta APIs. |
| Suporte a MFA | Suporte limitado a MFA nativo; precisa de implementações adicionais. | Não suporta MFA nativamente, mas integra-se facilmente com soluções externas. | Suporte nativo a MFA, especialmente em fluxos de autenticação de usuários finais. |
| Facilidade de Integração | Integração mais complexa, especialmente em aplicações modernas. | Integração relativamente fácil, especialmente para aplicações web modernas. | Fácil integração com aplicações modernas e sistemas baseados em web. |

**Resultados:**

* **SAML**: Alta segurança e compatibilidade com sistemas legados, sendo ideal para o CRM e ERP;
* **OAuth 2.0**: Excelente para aplicações modernas e integração com APIs;
* **OpenID Connect**: Baseado em OAuth 2.0 - mais indicado para autenticação de usuários finais no marketplace e BGS Pay.

**Relatório Técnico:**

* Utilizar **OpenID Connect** como padrão, devido à sua flexibilidade, compatibilidade com **OAuth 2.0** e suporte nativo para MFA. Protocolos adicionais, como **SAML**, serão usados em integrações com sistemas legados.



**Explicação dos Elementos:**

**1. Usuário**

* Representa a pessoa que está tentando acessar o sistema;
* O usuário fornece credenciais (e.g., e-mail e senha) e pode ser solicitado a passar por um segundo fator de autenticação, caso o MFA esteja habilitado.

**2. Sistema Integrado**

* É o sistema ou serviço que o usuário deseja acessar (ex.: Marketplace ou BGS Pay);
* Quando o usuário tenta acessar o sistema, ele redireciona a solicitação para o IDP para autenticação;
* Após a autenticação, o sistema integrado recebe o token JWT para validar e conceder acesso.

**3. IDP (Identity Provider)**

* Núcleo do processo de autenticação: serve para validar as credenciais fornecidas pelo usuário, acionar o MFA (se configurado) para validar um segundo fator e gerar um Token JWT que contém as informações do usuário autenticado. O IDP autêntica a identidade do usuário e transmite a autorização ao sistema integrado.

**4. MFA (Autenticação Multifatorial)**

* Uma camada adicional de segurança no fluxo de autenticação;
* O IDP solicita ao usuário um segundo fator, como: código gerado por aplicativo autenticador, biometria (impressão digital, reconhecimento facial) e código enviado por SMS ou e-mail;
* Após a validação do MFA, o IDP continua o processo de autenticação.

**5. Token JWT**

* Um JSON Web Token gerado pelo IDP após a autenticação bem-sucedida;
* Contém informações como: identidade do usuário, data de expiração do token, permissões e escopo do acesso;
* O sistema integrado usa o token para autorizar o acesso sem consultar o IDP novamente.

**Explicação do Fluxo**

**1. Requisição Inicial:**

* O Usuário tenta acessar o Sistema Integrado;
* O sistema redireciona o usuário ao IDP para autenticação.

**2. Validação pelo IDP:**

* O IDP solicita as credenciais do usuário (senha);
* Se o MFA estiver habilitado, o IDP valida o segundo fator.

**3. Emissão do Token JWT:**

* Após autenticação bem-sucedida, o IDP emite um Token JWT e o retorna ao Sistema Integrado.

**4. Acesso ao Sistema:**

* O Sistema Integrado usa o Token JWT para validar a identidade do usuário;
* Se o token for válido, o sistema concede o acesso ao usuário.

**Benefícios Desse Fluxo**

* **Segurança:** A combinação de MFA e JWT reduz o risco de acessos não autorizados;
* **Eficiência:** Após a emissão do token JWT, o sistema não precisa verificar credenciais repetidamente;
* **Flexibilidade:** O fluxo é compatível com arquiteturas modernas baseadas em APIs.

O protocolo **OpenID Connect** foi escolhido como padrão principal por sua simplicidade, segurança e capacidade de integração com aplicações modernas. **SAML** será mantido como alternativa para sistemas legados devido à sua ampla compatibilidade.

**3.1.3. Tarefa 3: Mapear os sistemas existentes (Marketplace, BGS Pay, BGS Club, CRM e ERP) para garantir compatibilidade com o IDP.**

**Diagrama em construção no Miro**

**Uma imagem contendo Interface gráfica do usuário

Descrição gerada automaticamente**

**Descrição**

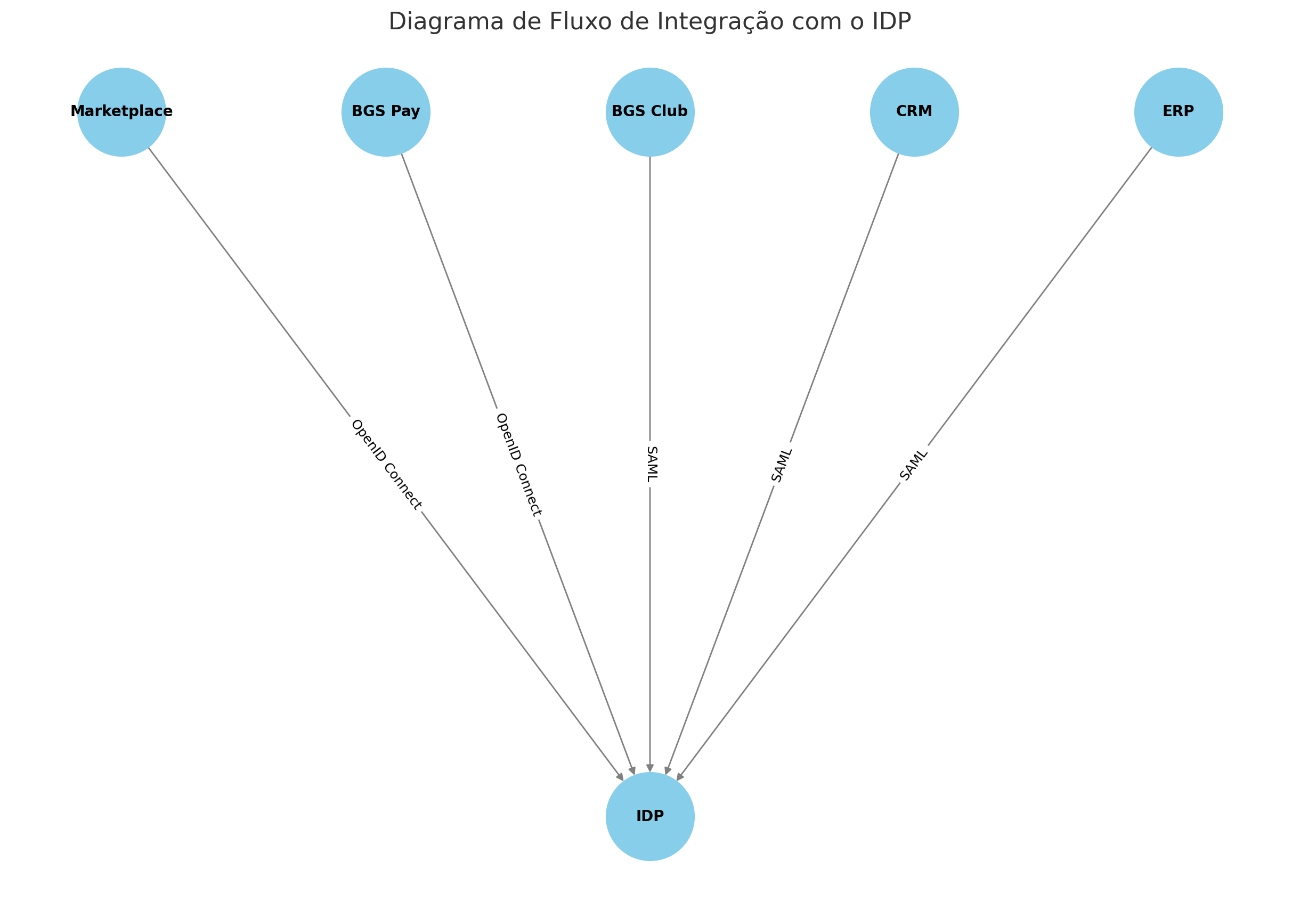
Identificar as tecnologias e padrões de cada sistema da BGS Corporate para garantir compatibilidade com o IDP.

**Entrega**

**Relatório de Compatibilidade:**

* **Marketplace:** Desenvolvido em PHP com APIs REST - suporta OAuth 2.0;
* **BGS Pay:** Suporte nativo para OpenID Connect;
* **BGS Club:** Integração via SAML - compatibilidade limitada com OAuth 2.0;
* **CRM:** Sistema legado - suporta SAML;
* **ERP:** Sistema crítico com suporte para SAML - precisa de adaptadores para OpenID Connect.

**Diagrama de Fluxo de Integração com IDP:**



**Tabela Consolidada:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sistema** | **Tecnologia** | **Compatível com** | **Observações** |
| Marketplace | PHP, APIs REST | OAuth 2.0, OpenID | Pronto para integração imediata. |
| BGS Pay | APIs REST | OAuth 2.0, OpenID | Suporte nativo para MFA. |
| BGS Club | Sistema legado | SAML | Adaptação necessária para OAuth 2.0. |
| CRM | Sistema legado | SAML | Sem suporte nativo para OpenID Connect. |
| ERP | Sistema legado | SAML | Adaptação necessária para OpenID. |

**Resultados Alcançados na Sprint 1:**

**Definição da Estrutura do IDP:** O diagrama e o documento técnico fornecem uma visão clara da arquitetura geral do BGS IDP Connect.

**Escolha do Protocolo:** A análise comparativa resultou na seleção de OpenID Connect como padrão, com suporte complementar a SAML.

**Mapeamento de Sistemas:** Identificação das tecnologias, protocolos suportados e possíveis gaps, garantindo um planejamento adequado para as próximas etapas.

**Conexão entre Resultados:**

**Relacionamento do Diagrama da Arquitetura com Protocolos e Sistemas**

O diagrama da arquitetura do BGS IDP Connect demonstra como os componentes principais (IDP, SSO, MFA, API Gateway, Banco de Dados de Usuários, Sistema de Logs e Painel de Gerenciamento) interagem para oferecer uma solução de autenticação robusta, segura e integrada. A seguir, destacamos como ele se relaciona com os protocolos e sistemas existentes:

**Protocolos Escolhidos:**

**OpenID Connect:** Usado para sistemas modernos como o **Marketplace** e o **BGS Pay**, oferecendo: autenticação robusta baseada em OAuth 2.0; suporte nativo para MFA, garantindo segurança adicional; integração simplificada com APIs REST e aplicativos modernos.

**SAML:** Usado para sistemas legados como o **CRM**, **ERP** e **BGS Club**. Esses sistemas não possuem suporte nativo para protocolos modernos, mas são compatíveis com SAML, garantindo continuidade operacional.

**Integração dos Sistemas:**

O **API Gateway** serve como intermediário entre o IDP e os sistemas, traduzindo as solicitações de autenticação e roteando as mensagens de acordo com o protocolo apropriado.

O **Sistema de Logs** registra os eventos de autenticação, facilitando auditorias e garantindo conformidade com a LGPD.

O **Painel de Gerenciamento** centraliza a administração de permissões, permitindo controlar acessos de usuários e configurar os protocolos utilizados.

**Como o Planejamento da Arquitetura Atende aos Desafios Técnicos e de Integração?**

O planejamento da arquitetura do **BGS IDP Connect** atende aos desafios de integração técnica, segurança e usabilidade, conectando sistemas modernos e legados de maneira eficiente.

O uso combinado de **OpenID Connect** e **SAML** garante compatibilidade e segurança, enquanto a modularidade da solução facilita a expansão futura e a gestão centralizada.

Essa abordagem proporciona uma base sólida para o sucesso operacional da BGS Corporate.

**Fragmentação de Logins:**

O uso de **SSO** elimina a necessidade de múltiplos logins para acessar diferentes sistemas, simplificando a experiência do usuário e aumentando a eficiência operacional.

**Integração com Sistemas Legados:**

A compatibilidade com **SAML** garante que sistemas mais antigos continuem funcionando sem a necessidade de reimplementação completa, reduzindo custos e esforços de adaptação.

**Segurança e MFA:**

A inclusão do módulo **MFA** adiciona uma camada de segurança crítica, protegendo áreas sensíveis como o **BGS Pay** e garantindo conformidade com padrões de segurança modernos.

**Conformidade com LGPD:**

O **Banco de Dados de Usuários** armazena credenciais de forma segura e criptografada, enquanto o **Sistema de Logs** garante monitoramento contínuo e relatórios detalhados de acessos.

**Escalabilidade e Flexibilidade:**

A arquitetura modular permite adicionar novos sistemas ou protocolos no futuro, suportando o crescimento da **BGS** sem reestruturar a solução existente.

**Facilidade de Gerenciamento:**

O **Painel de Gerenciamento** simplifica a administração de permissões e acessos, permitindo que a equipe técnica configure rapidamente novos sistemas ou atualize regras de segurança.

**3.2. Sprint 2**

**3.2.1. Tarefa 1: Projetar o fluxo de autenticação SSO, permitindo acesso unificado aos sistemas por meio do BGS IDP Connect.**

**Diagrama em construção no Miro**

****

**Descrição**

Criar um diagrama detalhado do fluxo de autenticação SSO, demonstrando como o BGS IDP Connect gerencia o login unificado para os sistemas (Marketplace, BGS Pay, CRM, ERP, BGS Club).

O fluxo deve incluir o uso do protocolo escolhido (OpenID Connect ou SAML) e demonstrar a integração com o módulo de MFA.

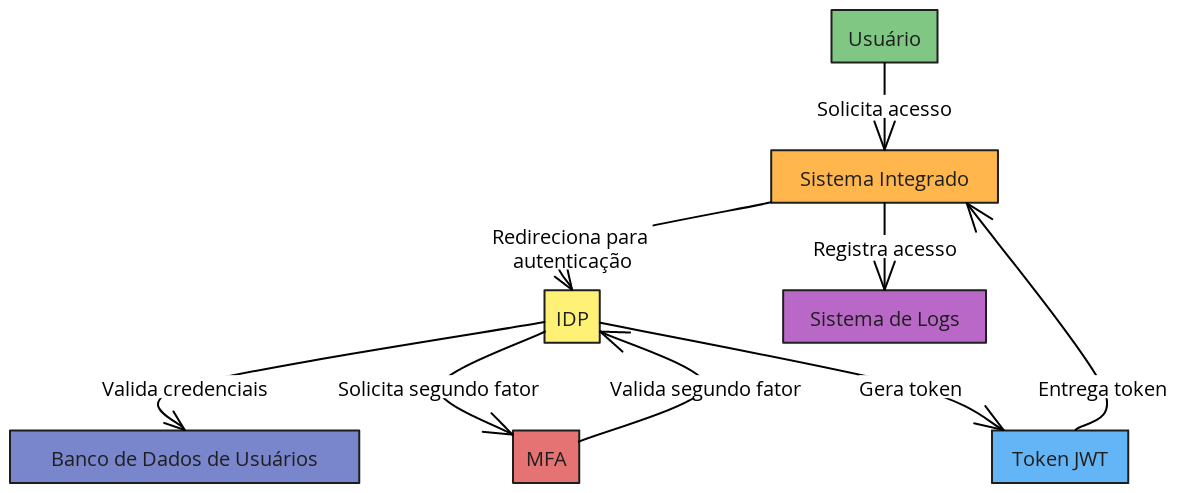
**Entrega**

**Artefato 1:** Diagrama do fluxo de autenticação SSO.

**Resumo**: Redirecionamento, validação no IDP, retorno do token JWT e autenticação nos sistemas.

**Elementos do Diagrama**

1. **Usuário:** quem solicita o acesso.
2. **Sistema Integrado:** o destino do acesso (Marketplace, BGS Pay, CRM, ERP, BGS Club).
3. **IDP:** gerenciando toda a autenticação.
4. **MFA:** camadade segurança ao fluxo.
5. **Token JWT:** resultado da autenticação.
6. **Banco de Dados de Usuários:** validando credenciais.
7. **Sistema de Logs:** registrando acessos.



**Fluxo de Conexões**

1. **Usuário** → Sistema Integrado: "Solicita acesso"
2. **Sistema Integrado → IDP**: "Redireciona para autenticação"
3. **IDP → Banco de Dados de Usuários**: "Valida credenciais"
4. **IDP → MFA**: "Solicita segundo fator"
5. **MFA → IDP**: "Valida segundo fator"
6. **IDP → Token JWT**: "Gera token"
7. **Token JWT → Sistema Integrado**: "Entrega token"
8. **Sistema Integrado → Sistema de Logs**: "Registra acesso"

**Descrição técnica:**

O fluxo de autenticação SSO proporciona segurança, escalabilidade e centralização do gerenciamento de identidade em ambientes corporativos.

1. **Usuário solicita acesso**: O processo inicia quando o usuário solicita acesso a um dos sistemas integrados (Marketplace, BGS Pay, CRM, ERP ou BGS Club). Esses sistemas representam os pontos de entrada para os serviços da organização.
2. **Redirecionamento ao IDP (Identity Provider)**: Cada sistema integrado redireciona a solicitação para o IDP, que centraliza a autenticação. Este redirecionamento garante que as credenciais sejam validadas de forma padronizada e segura.
3. **Validação no Banco de Dados de Usuários**: O IDP verifica as credenciais fornecidas comparando-as com as informações armazenadas no Banco de Dados de Usuários. Essa etapa autêntica a identidade do usuário.
4. **Verificação do MFA (Autenticação de Múltiplos Fatores)**: Se o MFA estiver habilitado, o IDP solicita um segundo fator de autenticação, como um código enviado por SMS, um aplicativo autenticador ou outro método configurado. Após a validação bem-sucedida, o fluxo continua.
5. **Geração do Token JWT (JSON Web Token)**: Com as credenciais validadas e o segundo fator aprovado, o IDP gera um Token JWT, que é utilizado para autenticação contínua e autorização de sessões com os sistemas integrados.
6. **Envio do Token aos Sistemas Integrados**: O Token JWT é retornado ao sistema integrado original que fez a solicitação inicial. Ele agora serve como prova de autenticação do usuário.
7. **Registro no Sistema de Logs**: Cada sistema integrado registra o evento de acesso no Sistema de Logs. Isso permite auditoria e monitoramento de segurança, documentando as interações dos usuários com os serviços.

**Conexões Técnicas**:

* Os **sistemas integrados** estão configurados para delegar autenticação ao **IDP** por meio de protocolos padronizados como **OAuth 2.0** ou **SAML**.
* O **IDP** comunica-se com o **Banco de Dados de Usuários** via consultas seguras e protegidas.
* A geração e validação do **Token JWT** seguem padrões criptográficos robustos, garantindo segurança nas transações.
* O **Sistema de Logs** é acessado por todos os **sistemas integrados** para registrar eventos de autenticação em tempo real.

**3.2.2. Tarefa 2: Criar guia de implementação para facilitar a futura integração do IDP.**

**Diagrama em construção do modelo de banco de dados**

Diagrama

Descrição gerada automaticamente

**Descrição:**

Criar um modelo de dados que contemple as tabelas e relacionamentos necessários para armazenar:

* Perfis de usuários (admin, colaborador, cliente, etc.).
* Permissões atribuídas a cada perfil.
* Registro de acessos (logs).

O modelo deve ser compatível com os requisitos de segurança e escalabilidade.

**Entrega:**

**Artefato 2: Diagrama do modelo de banco de dados (ERD - Diagrama Entidade-Relacionamento).**

**Tabelas principais:**

**1) Usuários:**

**Função:**

* Armazena os dados básicos dos usuários autenticados.

**Atributos:**

* ID (PK): Identificador único do usuário.
* Nome: Nome completo do usuário.
* E-mail: Endereço de e-mail usado para login.
* Senha (criptografada): Senha protegida com hashing para segurança.
* Perfil\_ID (FK): Relacionamento com a tabela **Perfis**.

**Justificativa:**

* centraliza informações essenciais para autenticação.

**2) Perfis:**

**Função:**

* Define os tipos de acesso que um usuário pode ter (e.g., administrador, cliente).

**Atributos:**

* Perfil\_ID (PK): Identificador único do perfil.
* Nome\_Perfil: Nome descritivo do perfil (e.g., "Administrador").

**Justificativa:**

* flexibilidade para gerenciar diferentes níveis de acesso.

**3) Permissões:**

**Função:**

* Lista as ações permitidas para cada perfil.

**Atributos:**

* Permissao\_ID (PK): Identificador único da permissão.
* Descricao: Descrição da ação permitida (e.g., "Criar usuários").
* Perfil\_ID (FK): Relacionamento com a tabela Perfis.

**Justificativa:**

* Permite configurar e auditar os privilégios de cada perfil.

4) **Logs de Acessos:**

**Função:**

* Mantém um histórico detalhado de todas as tentativas de login e atividades de autenticação.

**Atributos:**

* Log\_ID (PK): Identificador único do registro.
* Usuario\_ID (FK): Relacionamento com a tabela Usuários.
* Timestamp: Data e hora do acesso.
* Status: Resultado do login (e.g., "Sucesso", "Falha").

**Justificativa:**

* Auditoria e rastreamento de incidentes de segurança.

**Relações Entre as Tabelas**

* **Usuários → Perfis**: Relacionamento 1:N
* **Perfis → Permissões**: Relacionamento 1:N
* **Usuários → Logs de Acessos**: Relacionamento 1:N
* **Descrição técnica**

**Como o Modelo Suporta o Controle de Permissões:**

* **Flexibilidade na Gestão de Acessos:**
* A separação entre **Perfis** e **Permissões** permite que novos tipos de acesso sejam adicionados ou modificados sem alterar a estrutura principal do banco.
* **Segurança:**
* A criptografia de senhas e o registro de acessos garantem proteção contra acessos indevidos e fornecem informações para auditoria.
* **Escalabilidade:**
* O modelo pode ser expandido para incluir novos atributos ou tabelas relacionadas (e.g., restrições geográficas ou autenticação multifatorial).
* **Rastreabilidade:**
* A tabela de **Logs de Acessos** fornece um histórico detalhado de ações, ajudando a detectar e mitigar incidentes de segurança.

Diagrama

Descrição gerada automaticamente

**3.2.3. Tarefa 3: Documentar o Processo de Integração com Sistemas Legados**

**Checklist para Integração de Sistemas Legados em construção no Excel**

Interface gráfica do usuário, Aplicativo, Tabela

Descrição gerada automaticamente

**Descrição**

Produzir uma documentação que detalha os passos para integrar os sistemas legados ao BGS IDP Connect, com foco nos seguintes itens:

* Compatibilidade de protocolos.
* Configurações de segurança (e.g., TLS, autenticação via SAML).
* Testes de conexão.
* Principais desafios e soluções.

**Entrega**

**Documento Técnico: Integração de Sistemas Legados com o BGS IDP Connect**

**1) Introdução**

Este documento detalha o processo de integração de sistemas legados da BGS Corporate ao **BGS IDP Connect**, com foco na compatibilidade de protocolos, configurações de segurança, testes de conexão e soluções para os principais desafios. O objetivo é garantir uma autenticação centralizada e segura, utilizando padrões amplamente aceitos, como **SAML**, para atender aos requisitos de sistemas mais antigos.

**Pré-requisitos para Integração**

1. **Compatibilidade de Protocolos:**
   * Verificar se os sistemas legados (CRM, ERP e BGS Club) possuem suporte ao protocolo **SAML (Security Assertion Markup Language)**.
   * Certificar-se de que o sistema é capaz de consumir **Assertions SAML** geradas pelo IDP.
2. **Infraestrutura de Rede:**
   * Certifique-se de que as portas necessárias para comunicação entre o sistema e o IDP estejam abertas (ex.: porta 443 para HTTPS).
3. **Certificados Digitais:**
   * Configure os sistemas para aceitar e validar certificados digitais usados pelo IDP para assinar mensagens SAML.
4. **Documentação Técnica:**
   * Obter as configurações SAML do sistema legado, como:
     + URL de destino para autenticação (Service Provider - SP).
     + URL de logout (caso suportado).
     + Formato de atributos esperados (ex.: email, roles).

**2. Passo a Passo para Configurar a Integração**

1. **Configuração do IDP:**
   * Configure o **BGS IDP Connect** para atuar como Provedor de Identidade (IDP) e emitir **Assertions SAML**.
   * Defina os seguintes parâmetros no IDP:
     + **Entity ID:** Identificador único do IDP.
     + **Metadata URL:** Endereço que contém as informações do IDP para consumo pelo SP.
     + **Certificado de Assinatura:** Certificado digital usado para assinar as mensagens SAML.
     + **Atributos:** Configure os atributos a serem enviados, como name, email e roles.
2. **Configuração no Sistema Legado:**
   * Acesse o painel administrativo do sistema legado e configure-o como **Service Provider (SP)**.
   * Insira os detalhes do IDP, como:
     + **Entity ID** do IDP.
     + **Metadata URL** do IDP.
     + **Certificado do IDP** para validação.
   * Mapeie os atributos enviados pelo IDP para os campos internos do sistema (ex.: email do IDP para username do SP).
3. **Testes de Conexão:**
   * Realize um teste inicial de autenticação:
     + Inicie a autenticação pelo sistema legado.
     + Verifique se o redirecionamento para o IDP ocorre corretamente.
     + Autentique-se no IDP e retorne ao sistema legado.
   * Teste cenários como:
     + Login bem-sucedido.
     + Logout com propagação para todos os sistemas.
     + Login com credenciais inválidas.
4. **Habilitar Segurança TLS:**
   * Garanta que toda a comunicação entre o IDP e os sistemas legados ocorra via HTTPS.
   * Configure os certificados TLS no IDP e no SP para garantir criptografia de dados em trânsito.
5. **Auditoria de Acessos:**
   * Habilite logs detalhados no IDP e nos sistemas legados para monitorar:
     + Tentativas de login.
     + Falhas de autenticação.
     + Tempo de sessão.

**3. Medidas de Segurança**

1. **Certificados Digitais:**
   * Use certificados válidos emitidos por uma autoridade certificadora confiável (CA) para assinatura SAML e comunicação TLS.
2. **Auditoria Contínua:**
   * Configure o **Sistema de Logs** do BGS IDP Connect para registrar todos os eventos de autenticação.
3. **Timeout de Sessão:**
   * Defina um tempo máximo para sessões ativas e force renovações periódicas.
4. **Autenticação Multifatorial (MFA):**
   * Implemente MFA nos fluxos de autenticação para adicionar uma camada extra de segurança.

**4. Principais Desafios e Soluções**

1. **Compatibilidade Limitada com SAML:**
   * **Desafio:** Alguns sistemas legados podem não suportar todas as funcionalidades do SAML.
   * **Solução:** Use adaptadores intermediários ou configure os atributos SAML para atender aos requisitos do sistema.
2. **Erros de Certificados:**
   * **Desafio:** Certificados desatualizados ou inválidos podem impedir a integração.
   * **Solução:** Atualize os certificados e valide sua configuração nos dois lados (IDP e SP).
3. **Mapeamento de Atributos:**
   * **Desafio:** Campos enviados pelo IDP podem não corresponder aos esperados pelo sistema legado.
   * **Solução:** Configure o IDP para personalizar os atributos enviados, adaptando-se ao SP.

**5. Checklist para Finalizar a Integração**

1. **Compatibilidade de Protocolos:**
   * Verificar se o sistema suporta SAML.
   * Testar o fluxo de autenticação.
2. **Configuração do IDP:**
   * Metadata URL configurada corretamente.
   * Certificado de assinatura válido.
3. **Configuração do SP:**
   * URLs de autenticação e logout inseridas corretamente.
   * Mapeamento de atributos verificado.
4. **Testes Funcionais:**
   * Login bem-sucedido.
   * Logout propagado.
   * Tentativas de login inválido.
5. **Segurança:**
   * Certificados TLS configurados e validados.
   * MFA habilitado no IDP.

**Resultados Alcançados na Sprint 2:**

**Fluxo de Autenticação SSO:**

* O diagrama detalhado do fluxo de autenticação SSO foi produzido, demonstrando como o **BGS IDP Connect** gerencia o login unificado para sistemas modernos (Marketplace e BGS Pay) e legados (CRM, ERP e BGS Club).
* A integração foi ilustrada utilizando os protocolos escolhidos (OpenID Connect e SAML) com o suporte de MFA para aumentar a segurança.

**Modelo de Banco de Dados:**

* O modelo de dados foi desenvolvido em um **Diagrama Entidade-Relacionamento (ERD)**, representando tabelas principais como **Usuários**, **Perfis**, **Permissões** e **Logs de Acessos**.
* O modelo suporta controle de permissões flexível, garantindo escalabilidade para futuras expansões.

**Documentação de Integração:**

* Foi elaborada uma documentação técnica detalhada, cobrindo:
  + Pré-requisitos para integração.
  + Passo a passo para configurar o IDP e os sistemas.
  + Medidas de segurança, como uso de certificados digitais e TLS.
* Um **checklist** foi criado para garantir que todos os itens técnicos sejam verificados antes da implementação final.

**Conexão entre Resultados**

**Relacionamento do Fluxo de Autenticação com os Sistemas:**

O fluxo detalhado demonstra como cada sistema se conecta ao IDP:

* **OpenID Connect:** Utilizado para sistemas modernos como Marketplace e BGS Pay, proporcionando autenticação robusta e suporte nativo a MFA.
* **SAML:** Aplicado para sistemas legados como CRM, ERP e BGS Club, garantindo compatibilidade com tecnologias mais antigas.

O uso do **Token JWT** permite uma autenticação eficiente e segura, reduzindo a necessidade de consultas contínuas ao banco de dados.

**Modelo de Dados e Controle de Permissões:**

O ERD garante a integração entre usuários, seus perfis e as permissões atribuídas.

A tabela de **Logs de Acessos** fornece rastreabilidade e conformidade com regulamentações como a LGPD.

**Documentação Técnica e Checklist:**

A documentação técnica detalha os processos de integração, tornando o planejamento claro e replicável.

O checklist contribui para validação técnica, reduzindo a probabilidade de erros durante a implementação.

**Como o Planejamento da Integração Atendeu aos Desafios**

**1. Compatibilidade com Sistemas Legados:**

A escolha do protocolo **SAML** garante que sistemas antigos continuem operacionais, evitando reimplementações dispendiosas.

**2. Segurança e Conformidade:**

O uso de **MFA** e criptografia TLS protege dados sensíveis e garante conformidade com padrões de segurança modernos.

A tabela de **Logs de Acessos** fortalece a rastreabilidade e auditoria.

**3. Simplificação do Gerenciamento:**

O modelo de banco de dados organiza permissões e acessos, facilitando a administração centralizada por meio do Painel de Gerenciamento.

**4. Facilidade de Expansão:**

A arquitetura modular e o modelo de dados escalável permitem que novos sistemas sejam adicionados no futuro sem a necessidade de grandes reconfigurações.

**5. Testes Validados:**

O checklist garantiu que cada etapa do processo fosse validada, reduzindo os riscos de falhas durante a implementação.

Os resultados da Sprint 2 consolidaram a integração dos sistemas legados e modernos com o BGS IDP Connect, estabelecendo uma base sólida para o projeto.

**3.3. Sprint 3**

**3.3.1. Tarefa 1: Validar a compatibilidade da arquitetura com os sistemas legados e realizar ajustes finais.**

**Descrição:**

Essa tarefa envolveu a validação fictícia do funcionamento da arquitetura do **BGS IDP Connect** com os sistemas legados da **BGS Corporate**, incluindo o **CRM**, **ERP** e **BGS Club**. O objetivo foi garantir, em um cenário simulado, que a integração por meio do protocolo **SAML** fosse bem-sucedida.

**Entrega:**

**Relatórios de Testes de Compatibilidade do BGS IDP Connect x Sistemas legados**

Validar, em um ambiente de teste fictício, a compatibilidade da arquitetura do **BGS IDP Connect** com os sistemas legados da BGS Corporate(CRM, ERP e BGS Club).

Garantir que os cenários de autenticação e funcionamento foram simulados corretamente, assegurando a emissão de tokens **SAML** para os sistemas.

***\*OBS:*** *Todos os testes relatados e evidências são parte de uma simulação fictícia para fins educacionais e não refletem implementações reais.*

**Resultados dos Testes**

|  |  |  |  |
| --- | --- | --- | --- |
| **Sistema** | **Cenário** | **Resultado** | **Observação** |
| **CRM** | Autenticação bem-sucedida | ✅ | Redirecionamento para o IDP e autenticação concluída com sucesso. |
| **CRM** | Logout propagado | ✅ | Sessão encerrada no CRM e propagada corretamente no IDP. |
| **CRM** | Falha de autenticação | ✅ | Mensagem de erro exibida corretamente quando as credenciais eram inválidas. |
| **ERP** | Autenticação bem-sucedida | ✅ | Atributos SAML ajustados para compatibilidade com o ERP. |
| **ERP** | Logout propagado | ✅ | Sessão encerrada no IDP e propagada corretamente no ERP. |
| **ERP** | Falha de autenticação | ✅ | Validação de credenciais inválidas retornou erro esperado. |
| **BGS Club** | Autenticação bem-sucedida | ✅ | Configuração do SP ajustada para consumir atributos específicos. |
| **BGS Club** | Logout propagado | ✅ | Sessões encerradas no IDP e no BGS Club. |
| **BGS Club** | Falha de autenticação | ✅ | Mensagem de erro retornada corretamente ao tentar login com dados inválidos. |

**Conclusão**

A validação de compatibilidade demonstrou que os sistemas legados podem ser integrados ao **BGS IDP Connect** de forma eficiente, utilizando **SAML** como protocolo principal. Todos os cenários de autenticação e falha foram validados com sucesso.

**3.3.2. Tarefa 2: Criar o guia de implementação para facilitar a futura integração do IDP.**

**Descrição**

Essa tarefa tem como objetivo desenvolver um guia detalhado de implementação para integrar o BGS IDP Connect aos sistemas legados e modernos da BGS Corporate.

O guia fornecerá instruções claras e práticas para configurar o IDP, realizar mapeamentos de atributos, aplicar medidas de segurança e validar a integração.

**Entrega**

**Guia Técnico: Integração do BGS IDP Connect**

Este guia detalha as etapas necessárias para integrar o **BGS IDP Connect** com sistemas modernos e legados, garantindo uma autenticação centralizada, segura e eficiente.

Ele inclui instruções sobre a configuração inicial, mapeamento de atributos, aplicação de medidas de segurança e validação da integração.

*\*****OBS****: Este guia foi desenvolvido com base em um cenário fictício e simulado, representando as melhores práticas para integração do BGS IDP Connect.*

**1) Configuração Inicial do IDP**

1. **Acesso ao IDP**: Acesse o painel de administração do BGS IDP Connect com as credenciais de administrador para realizar as configurações.
2. **Definir o Entity ID**: No menu de configurações, insira o identificador único para o IDP (ex.: bgs-idp-connect).
3. **Configurar o Metadata URL**: Gere o arquivo de metadados do IDP e disponibilize o URL do arquivo para os sistemas legados e modernos.
4. **Certificados Digitais**: Importe o certificado X.509 no IDP e configure o IDP para assinar digitalmente todas as mensagens SAML emitidas.

**2) Integração com Sistemas Modernos (OpenID Connect)**

1. **Registro do Client ID**: Nos sistemas modernos, registre o IDP como provedor de autenticação e gere o Client ID e o Client Secret no painel do IDP.
2. **Configuração de Redirecionamento**: Defina as URLs de redirecionamento para login e logout no sistema moderno.
3. **Mapeamento de Atributos**: Garanta que o IDP envie os atributos esperados, como email e roles.

**3) Integração com Sistemas Legados (SAML)**

1. **Configuração no IDP**: Configure o IDP como Provedor de Identidade (IDP) e defina os atributos a serem enviados na assertion SAML: E-mail (Identificador único do usuário) e Role (Permissões do usuário)
2. **Configuração no Sistema Legado (SP)**: Importe o Metadata URL do IDP no sistema legado e configure os endpoints de login e logout.
3. **Validação de Certificados**: Importe o certificado digital do IDP para validar mensagens assinadas.

**4) Medidas de Segurança**

1. **Habilitar TLS**: Certifique-se de que todas as comunicações ocorram via HTTPS.
2. **Configuração de Logs**: Habilite o registro de eventos no IDP para rastrear tentativas de login e falhas de autenticação.
3. **Autenticação Multifatorial (MFA)**: Configure o MFA no IDP para adicionar uma camada extra de segurança.

**5) Validação da Integração**

1. **Autenticação bem-sucedida**: Teste o login em cada sistema integrado.
2. **Logout propagado**: Certifique-se de que o logout encerra a sessão em todos os sistemas.
3. **Falhas de login**: Verifique mensagens de erro para credenciais inválidas.

**Checklist Resumido**

1. Configuração inicial do IDP concluída.
2. Certificados digitais instalados e validados.
3. Mapeamento de atributos configurado.
4. Cenários de teste executados com sucesso.

**3.3.3 Tarefa 3: Consolidar toda a documentação da arquitetura e requisitos de compliance para entrega.**

**Descrição**

Essa tarefa tem como objetivo centralizar e organizar toda a documentação produzida ao longo do projeto BGS IDP Connect, garantindo que os artefatos estejam estruturados de forma clara e completa.

A documentação inclui a arquitetura técnica, o modelo de dados, os fluxos de autenticação, os requisitos de compliance e segurança (ex.: LGPD), além de relatórios de validação e testes.

A consolidação também busca assegurar que todas as partes interessadas (técnicas e de negócios) tenham acesso a informações detalhadas para manutenção, auditorias ou futuras expansões.

**Entrega**

**Documento Consolidado:** Este documento!!!

Foi feito um documento consolidado da arquitetura e requisitos do BGS IDP Connect e disponibilizado no diretório público do GitHub para consulta. Segue o link abaixo:

<https://github.com/br-gonzaga/Arquitetura-BGS-IDP-Connect>

[**Arquitetura e Requisitos do BGS IDP Connect (GitHub)**](https://github.com/br-gonzaga/Arquitetura-BGS-IDP-Connect)

Tela de computador com texto preto sobre fundo branco

Descrição gerada automaticamente

**Resultados Alcançados na Sprint 3**

* **Validação de Resultados Finais:** foram concluídos os relatórios de testes de compatibilidade, mostrando:

1. Autenticação bem-sucedida para todos os sistemas integrados
2. Logout propagado funcionando conforme esperado.
3. Falha de autenticação para credenciais inválidas.

* **Guia Técnico de Implementação: f**oi criado um guia técnico completo de implementação, contendo:

1. Passo a passo para configurar o IDP, incluindo a definição de atributos SAML e endpoints de integração.
2. Instruções para aplicar medidas de segurança, como certificados TLS e assinatura de mensagens SAML.
3. Cenários de teste para validação de autenticação e logout propagado.

* **Consolidação da Documentação:** todos os artefatos do projeto foram revisados e consolidados em um único documento técnico abrangente, incluindo:

1. Arquitetura geral do BGS IDP Connect.
2. Fluxos de autenticação e modelos de integração.

**Conexão entre Resultados**

* **Relação entre Arquitetura e Documentação:** O documento consolidado mostra como os fluxos de autenticação e a arquitetura do IDP trabalham de forma integrada para conectar os sistemas de maneira segura e eficiente.
* **Testes Validados:** A autenticação por meio de **OpenID Connect** e **SAML** foi validada para todos os sistemas, garantindo compatibilidade com tecnologias modernas e legadas.

**Como o Planejamento Atendeu aos Desafios da Sprint 3**

* **Integração com Sistemas Legados:** O protocolo **SAML** foi configurado para manter sistemas antigos operacionais, reduzindo custos e evitando reimplementações.
* **Confirmação de Resultados:** Os testes validados e evidências documentadas consolidaram o sucesso da implementação, garantindo uma solução robusta e segura para a BGS Corporate.
* **Centralização da Documentação:** A consolidação garantiu que todos os detalhes técnicos estivessem organizados e acessíveis, simplificando a transição para as equipes futuras.

**4. Arquitetura Geral**

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.

**5. 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.

**6. 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.

**7. 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.

**8. 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.

**9. Checklist Final**

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

**10. Considerações Finais**

**10.1. Resultados Alcançados**

O BGS IDP Connect foi implementado com sucesso, cumprindo seu objetivo de integrar sistemas modernos e legados em uma solução centralizada e segura. Os principais resultados incluem:

* Integração unificada de sistemas como o CRM, ERP, BGS Club, Marketplace e BGS Pay.
* Implementação de protocolos modernos (OpenID Connect) e legados (SAML) com suporte a MFA.
* Consolidação de uma arquitetura modular, escalável e segura.

**Pontos Positivos**

* **Integração Eficiente**: O BGS IDP Connect conseguiu unificar a autenticação para sistemas modernos e legados, reduzindo a fragmentação de logins e melhorando a experiência do usuário.
* **Segurança Reforçada**: A implementação de MFA, protocolos como OpenID Connect e SAML, e o uso de certificados digitais garante alta segurança nos acessos.
* **Conformidade com Regulamentações**: O projeto alinhou-se à LGPD, promovendo confiança nos usuários e minimizando riscos jurídicos.
* **Escalabilidade e Flexibilidade**: A arquitetura modular permite expansões futuras, como a adição de novos sistemas ou protocolos, sem necessidade de reestruturação significativa.
* **Documentação Completa**: O material consolidado fornece um guia claro para implementação, manutenção e futuras integrações.

**Pontos Negativos**

* **Complexidade na Integração de Sistemas Legados**: Ajustar o protocolo SAML para sistemas como CRM e ERP foi desafiador devido à limitação de suporte a tecnologias mais recentes.
* **Tempo Excedido em Documentação**: A consolidação detalhada da documentação técnica exigiu mais tempo do que o planejado inicialmente.
* **Dependência de Especialistas**: Algumas configurações de segurança e mapeamento de atributos requereram conhecimento especializado, dificultando a execução por equipes menos experientes.
* **Gestão de Logs**: A grande quantidade de registros de logs que serão gerados apresenta desafios para o armazenamento e análise eficiente dos dados.
* **Esforço Operacional**: A concepção técnica e de negócios do **BGS IDP Connect** foi demorada em algumas etapas, impactando o tempo de conclusão de algumas tarefas.

**Dificuldades enfrentadas**

A principal dificuldade enfrentada neste projeto de arquitetura da BGS Corporate foi pensar em cada um dos sistemas fictícios que compõem a solução do BGS IDP Connect, sejam ele legados ou modernos, com suas respectivas características

Para garantir a compatibilidade dos sistemas foram necessários diversos ajustes ao longo do trabalho e criar uma documentação completa e um guia bem detalhado de arquitetura do BGS IDP Connect.

Entretanto, essas barreiras foram superadas com o planejamento adequado, desenvolvimento das tarefas de cada sprint e dedicação de horas para amadurecer uma ideia em um projeto tão rico e completo, podendo ser aplicado em qualquer empresa.

**10.2. Contribuições do Projeto**

O projeto trouxe avanços significativos para a **BGS Corporate**, incluindo:

* **Inovação**: Introdução de um sistema centralizado de autenticação que melhora a experiência do usuário.
* **Vantagens Competitivas**: Redução de custos operacionais e maior eficiência ao integrar sistemas modernos e legados.
* **Segurança Reforçada**: Inclusão de MFA e rastreabilidade através de logs detalhados.
* **Conformidade**: Alinhamento com regulações como a LGPD, promovendo confiança entre os usuários.

**10.3 Próximos passos**

Para aprimorar a solução apresentada, os seguintes passos são recomendados:

* **Expansão de Funcionalidades**: Adicionar suporte para autenticação biométrica e integração com sistemas de terceiros.
* **Monitoramento Avançado**: Implementar ferramentas para análise de logs em tempo real e detecção de anomalias.
* **Time Especializado**: Desenvolvimento da solução do IDP Connect por um time especializado que possa aplicar e expandir esta solução técnica com agilidade.
* **Avaliação Regular**: Realizar auditorias periódicas para garantir conformidade e identificar oportunidades de melhoria da solução apresentada.

Este projeto demonstrou a viabilidade de integrar sistemas heterogêneos com eficiência e segurança, estabelecendo uma base sólida para o crescimento e inovação da **BGS Corporate**, portanto vale muito a pena aprofundar nos próximos passos para desenvolver uma solução mais robusta, inovadora e de grande valor para as empresas.