PROVA DE CONCEITO · MODERNIZAÇÃO DE SISTEMA LEGADO

SIPO
Sistema de Planejamento Orçamentário

Relatório executivo da migração do sistema para Java 21 e Jakarta EE 10, com paridade funcional verificada, lado a lado, entre o sistema migrado e uma cópia do legado construída a partir do código recebido.

DE

Java 7 · Java EE 6 · Seam 3 · JBoss AS 7.1
versões de 2010 a 2014

PARA

Java 21 · Jakarta EE 10
WildFly 39 · PostgreSQL 16

Destinatário: **Exército Brasileiro**
Sistema de origem: **DECEx · Assessoria de Tecnologia da Informação**
Data: **22 de setembro de 2026**
Versão: **1.6** · gerado da revisão **6dac5ae** do repositório

MigrAI

Execução e relatório
MigrAI

SUMÁRIO EXECUTIVO

O sistema foi migrado e está no ar, lado a lado com o original.

O SIPO saiu de uma pilha com versões de 2010 a 2014, cujo framework central não roda em nenhum servidor de aplicação ainda em suporte, para Java 21 e Jakarta EE 10. Os dois sistemas estão publicados lado a lado, sobre a mesma massa de dados, para conferência direta.

34
entidades de dados preservadas, de 34 existentes

1.767
testes de código, nenhum com falha

29
conferências de tela e de acesso entre os dois sistemas, todas iguais

728
pontos de função; 640 a 770 com a revisão independente

O que este documento sustenta

O que trava a pilha antiga é o framework. O Seam 3 exige uma versão de CDI (o mecanismo que liga os componentes de uma aplicação Java EE) que nenhum servidor em suporte oferece, e não tem versão compatível com a atual. Verificado executando o sistema. A seção 2 mostra a cadeia e o que não se sabe do ambiente do Exército.

A migração preservou o domínio inteiro. As 34 entidades de dados, as 46 telas e os 34 modelos de relatório foram transportados. As 34 alterações exigidas pela plataforma nova estão registradas uma a uma, com justificativa, e não contradizem as 29 conferências: elas estão no código, e as conferências olham o que o usuário vê.

A migração também corrigiu defeitos. Sete defeitos do código recebido foram corrigidos no caminho, entre eles uma tela que responde erro quando a tabela de pesquisa tem registros, e um valor de aprovação que dobrava em itens com dois grupos de despesa preenchidos.

Qualidade e segurança são medidas, não afirmadas. A mesma ferramenta apontou 522 itens no código recebido e nenhum aberto no migrado (seção 12), e o teste de segurança, pelas fases do NIST SP 800-115, teve os achados corrigidos e reconferidos (seção 13).

O que falta para produção está declarado. Não foi recebido banco de dados histórico, então nenhuma migração de dados reais é afirmada. A seção 9 detalha as quatro frentes que faltam e propõe os próximos passos, com responsável e prazo.

De onde para onde

CAMADA	CÓDIGO RECEBIDO	SISTEMA MIGRADO	SALTO
Linguagem	Java 7, de 2011	Java 21	14 versões
Plataforma	Java EE 6 com Seam 3	Jakarta EE 10	sucessora oficial
Servidor	JBoss AS 7.1, de 2012	WildFly 39	mesmo produto
Interface	PrimeFaces 5, de 2014	PrimeFaces 15	9 versões principais
Relatórios	JasperReports 3.7.2, de 2010	JasperReports 7.0	mesma ferramenta
Banco de dados	Esquema gerado pelo servidor	Migrações versionadas	controlado

A coluna do código recebido descreve o que o projeto declara: Java 7 no compilador, API Java EE 7 sobre framework e servidor que implementam Java EE 6, JBoss AS 7.1 nos testes. A configuração de produção do Exército não foi recebida, e não é afirmada aqui.

> **Para testar agora** (credenciais e roteiro na seção 10): poc-exercito.apps.migrai.com.br/sipo e poc-exercito-legado.apps.migrai.com.br/sipo

CONTEÚDO

O que está neste relatório

01	O sistema legado	Propósito, ciclo orçamentário e os módulos funcionais	04
02	Por que migrar	A cadeia de dependências, e o que não se sabe do ambiente atual	06
03	Para onde foi migrado	A pilha nova, componente a componente, e a razão de cada troca	07
04	O que foi migrado	Inventário comparado e as 34 diferenças registradas	08
05	Antes e depois	As mesmas telas nos dois sistemas, sobre os mesmos dados	09
06	Defeitos corrigidos	Sete falhas do código recebido, encontradas e resolvidas	11
07	Como foi validado	Testes, comparação automática e auditoria independente	12
08	Dimensionamento	Pontos de função, prazo, custo e a origem de cada premissa	16
09	O que falta para produção	Quatro frentes, e os próximos passos com responsável e prazo	19
10	Como testar	Endereços, credenciais e roteiro por perfil	22
11	Limites declarados	O que esta prova de conceito não demonstra, e os termos usados	23
12	Qualidade do código	Os dois códigos sob a mesma régua, indicador a indicador	24
13	Segurança	Teste de penetração, vulnerabilidades corrigidas e reteste	25

Como ler os números deste documento

O relatório separa deliberadamente duas naturezas de informação, e essa separação está marcada em cada seção.

NATUREZA	O QUE SIGNIFICA	ONDE APARECE
Fato verificado	Medido no código, no banco ou na execução, e reproduzível por quem tiver acesso ao repositório	Seções 1, 3, 4, 5, 6, 7 e itens 1 a 5 da seção 2. O ambiente de produção do Exército não foi verificado e está marcado como desconhecido
Contagem	Derivada de leitura do código por método declarado, auditável item a item	Seção 8, pontos de função
Premissa	Faixa de mercado adotada para converter contagem em prazo e custo. Substituível pelos históricos do cliente	Seção 8, prazo e custo
Estimativa preliminar	Prazos em dias úteis de roteiro e runbook, da mesma natureza das premissas	Seção 9

Os nomes usados neste relatório

NOME	O QUE DESIGNA
Código recebido	O código-fonte entregue pelo DECEx, sem configuração de produção, sem banco e sem histórico
Sistema legado	A cópia desse código que esta prova de conceito compilou, executou e publicou com dados sintéticos. É ela que aparece em todas as comparações e capturas
Sistema migrado	A versão nova, em Java 21 e Jakarta EE 10, publicada ao lado do legado sobre a mesma massa
SIPO em produção	A instalação em uso no Exército. Sua configuração, seu servidor e seus dados não foram recebidos, e nada neste relatório a descreve por observação direta

SEÇÃO 01

O que o SIPO faz

Pelo que o código recebido implementa, o SIPO é o sistema pelo qual o DECEx, suas Diretorias e os Estabelecimentos de Ensino constroem, priorizam, aprovam e acompanham o orçamento anual do ensino do Exército. A descrição foi levantada do código, das telas e dos dois guias de usuário que acompanham o material recebido, e cabe ao DECEx confirmá-la.

O ciclo que o sistema sustenta

01
Abertura e configuração do exercício

A administração abre o ano orçamentário e configura, por Organização Militar, quais ações e planos de detalhamento ficam disponíveis, com os tetos por grupo de despesa.

02
Pré-planejamento e planejamento

Cada Estabelecimento de Ensino levanta a demanda preliminar e depois registra o planejamento definitivo, ordenando prioridades e distribuindo valores por natureza de despesa.

03
Pré-aprovação e homologação

A Diretoria pré-aprova o que as escolas planejaram e o Departamento homologa em definitivo. Cada aprovação congela um valor e o vincula à escola, à ação e ao plano.

04
Execução e acompanhamento

O Departamento lança as notas de crédito que executam o planejamento aprovado e acompanha o saldo pelo monitoramento orçamentário.

Quem usa, e com que alcance

O sistema combina dois eixos de permissão, ambos definidos no código: o tipo da Organização Militar e o nível do usuário. É essa combinação que determina quais telas cada pessoa alcança e sobre quais dados.

TIPO DE ORGANIZAÇÃO	NÍVEL DO USUÁRIO	ALCANCE TÍPICO
Departamento (DECEx)	Administrador	Cadastros, configuração de exercício, execução orçamentária, monitoramento e todos os relatórios
Diretoria	Pré-aprovador	Pré-aprovação do planejamento das escolas subordinadas e relatórios consolidados
Departamento	Aprovador	Homologação definitiva do planejamento
Estabelecimento de Ensino	Planejador	Planejamento e pré-planejamento da própria escola, pesquisas e relatórios da própria organização

> O ciclo orçamentário tem um quinto eixo, paralelo ao financeiro: as **pesquisas de capacitação**. O Departamento libera um questionário por exercício, e cada escola declara capacitação de militares, capacitação de alunos do Colégio Militar e projetos de preservação do patrimônio histórico. É o insumo qualitativo do planejamento seguinte.

SEÇÃO 01 · CONTINUAÇÃO

Os módulos funcionais

Levantamento feito a partir das 46 telas e dos 34 controladores do sistema de origem. Todos os módulos abaixo foram transportados para o sistema novo.

MÓDULO	O QUE FAZ	NO MENU DO SISTEMA
Planejamento orçamentário	Núcleo do sistema. Registra itens de despesa do exercício, ordena por prioridade e distribui valores por natureza de despesa, com saldo calculado contra o teto configurado	Planejamento, com as abas Planejar, Detalhar, Prioridades e Pendências
Pré-planejamento	Rodada preliminar, com estrutura de dados própria e independente, para levantar a demanda antes da fase definitiva	Pré Planejamento, com as mesmas abas
Prioridades e aprovações	Fluxo de decisão em dois degraus: a Diretoria pré-aprova, o Departamento homologa. Cada aprovação congela valor, escola, ação e plano	Pré Planejamento (Aprovar) e Planejamento (Aprovar)
Notas de crédito	Registra a liberação efetiva do recurso contra um item aprovado, consumindo saldo e alimentando o acompanhamento	Execução
Monitoramento orçamentário	Visão instantânea do planejado e comprometido, por ação, plano, unidade gestora, prioridade e natureza de despesa	Monitoramento Orçamentário
Pesquisas e capacitação	Questionário por exercício sobre uso dos créditos, com três blocos declaratórios: capacitação de militares, de alunos e projetos de preservação	Pesquisa, Questionário, Liberar Pesquisa, Pesquisas Pendentes e Cadastro de Questões
Cadeia estratégica	Hierarquia de quatro níveis que liga orçamento ao Plano Estratégico do Exército: objetivo, estratégia, ação estratégica e iniciativa, com vigência por faixa de anos	Objetivo Estratégico, Estratégia, Ação Estratégica e Iniciativa Estratégica
Configuração de exercício	Define tetos orçamentários por organização, ação e plano de detalhamento. Permite clonar a configuração de um ano para o seguinte e encerrar o exercício	Exercícios Orçamentários e Tetos Orçamentários
Cadastros de apoio	Usuários, organizações militares, naturezas de despesa, planos de detalhamento, ações orçamentárias, processos e questões	Dados do Usuário, Organizações Militares, Natureza de Despesa, Planos de Detalhamento, Ação Orçamentária e Processos
Relatórios	Documentos de consolidação e prestação de contas, com filtros por exercício, organização superior, escola, ação e plano. Saída em PDF e planilha	Nove entradas do menu Relatórios, que acionam 22 modelos

Tamanho do sistema de origem

190
classes Java

34
entidades de dados

46
telas

34
modelos de relatório

Contagem gerada por ferramenta de inventário sobre o código recebido, reproduzível a qualquer momento, por nome distinto de arquivo. O código contém ainda 68 serviços de domínio e 77 arquivos de relatório compilados, que correspondem a 39 nomes distintos: o restante são cópias em dois diretórios.

SEÇÃO 02

O que prende a pilha é o framework

Este é o argumento técnico central do projeto, e não é de preferência: é de dependência. O framework não tem versão compatível com servidor em suporte.

A cadeia, elo a elo

#	CONSTATAÇÃO	COMO FOI VERIFICADO, E O QUE DECORRE
1	O framework da aplicação, Seam 3.1.0.Final, exige a versão 1.0 da especificação CDI	Servidores com CDI 1.1 ou superior recusam um evento que o Seam dispara ao iniciar. Verificado nesta prova de conceito: a aplicação não sobe
2	O componente que dispara esse evento não é opcional	Ele processa o arquivo que aponta qual é o autenticador da aplicação. Sem ele, o sistema não tem login. Desativar não é alternativa
3	Não há versão do Seam 3 compatível com CDI 1.1	O projeto foi encerrado em 2012 e sucedido pelo Apache DeltaSpike, que tem outra API. Não existe atualização de versão, só substituição
4	Logo, nenhum servidor em suporte hoje executa esta aplicação sem reescrita	Esta é a conclusão que não depende do ambiente: é propriedade da aplicação, não do servidor onde ela roda
5	O servidor que o projeto declara nos testes, JBoss AS 7.1 da comunidade, entra em laço infinito ao subir sob Java 8	Verificado com três versões diferentes da camada de módulos, o que isola a causa no servidor. Vale para a distribuição comunitária 7.1, que o projeto declara. A edição comercial correspondente, JBoss EAP 6 (da 6.3.3 em diante), é certificada para Java 8: se o Exército a usa, este item não se aplica, mas essa linha saiu de manutenção em 2019 e do suporte estendido em 2022, e os itens 1 a 4 continuam valendo

> **O QUE ESTE RELATÓRIO NÃO SABE SOBRE O AMBIENTE DO EXÉRCITO**
>
> O material recebido traz o código-fonte e a configuração de compilação, não a de produção: não há descritor de servidor nem documento de implantação. Qual servidor e qual JVM executam o SIPO hoje segue em aberto, e a resposta muda a urgência, não o caminho: num ambiente mais recente o sistema tem mais fôlego de suporte, mas o framework continua sem destino de atualização. Há inclusive um sinal contrário ao congelamento: o arquivo de integração contínua recebido compila com Java 17 e empacota em contêiner. Ele não foi tomado como prova do ambiente porque publica um artefato jar num projeto que gera war, o que indica um pipeline em construção. A pergunta está na seção 9.

O custo de permanecer

FRENTE	O QUE O CÓDIGO RECEBIDO IMPLICA, EM QUALQUER AMBIENTE
Segurança	Seam 3, PrimeFaces 5 e JasperReports 3.7 não recebem correção de vulnerabilidade. No código recebido, a senha é gravada como MD5 sem sal, algoritmo inadequado para esse uso há mais de uma década
Manutenção	A base de profissionais que domina Seam 3 diminui a cada ano. Com o servidor que o projeto declara, que exige Java 7, o legado só roda em processadores x64: não existe distribuição atual do Java 7 para ARM, cada vez mais comum em servidores e notebooks
Evolução	Bibliotecas atuais não são instaláveis na pilha antiga. Qualquer requisito novo que dependa de biblioteca moderna fica bloqueado
Operação	A geração automática de esquema está ativa no próprio empacotamento da aplicação. Se essa é a configuração de produção, o servidor pode alterar a estrutura do banco ao subir, sem controle de versão

SEÇÃO 03

A pilha nova, e a razão de cada troca

A escolha priorizou continuidade: mesma família tecnológica, para que o conhecimento da equipe permaneça válido, trocando só o que perdeu suporte.

Alternativas consideradas e descartadas: reescrever em outra plataforma (Spring Boot ou Quarkus, por exemplo) obrigaria a reconstruir telas e relatórios e descartaria o conhecimento em Java EE e PrimeFaces; permanecer no JBoss comercial (EAP) não resolve o Seam 3, que continua sem destino; trocar de banco não traz ganho, porque o PostgreSQL segue em suporte.

CAMADA	CÓDIGO RECEBIDO	SISTEMA MIGRADO	POR QUÊ
Linguagem	Java 7 (2011)	**Java 21**	Versão de suporte estendido corrente. O projeto declara Java 7, sem atualizações públicas desde 2015
Plataforma	Java EE 6	**Jakarta EE 10**	Sucessora oficial, renomeada ao passar da Oracle para a Eclipse Foundation. O projeto declara a API Java EE 7 no compilador, mas framework e servidor implementam Java EE 6
Framework	Seam 3.1	**CDI 4 nativo**	Seam foi descontinuado. As funções que ele cumpria existem na própria plataforma
Interface	PrimeFaces 5.0 (2014)	**PrimeFaces 15**	Mesma biblioteca de componentes, em versão atual e responsiva
Relatórios	JasperReports 3.7.2 (2010)	**JasperReports 7.0**	Mesma ferramenta, mesmos modelos de relatório, motor atualizado
Servidor	JBoss AS 7.1 (2012)	**WildFly 39**	Sucessor direto do mesmo produto, com suporte ativo
Banco	PostgreSQL	**PostgreSQL 16**	Mesmo banco. O modelo de dados foi preservado
Esquema	Geração automática ativa	**Migrações versionadas**	O servidor deixa de alterar a estrutura do banco; toda mudança é versionada e registrada

O que a migração acrescentou em segurança

FRENTE	NO CÓDIGO RECEBIDO	NO SISTEMA MIGRADO
Armazenamento de senha	MD5, sem sal	PBKDF2-HmacSHA256 com sal e 600.000 iterações. A senha antiga continua válida e é convertida no primeiro acesso
Autorização	Controle nas telas, sem garantia no servidor	Filtro que aplica a matriz de papéis no servidor para todas as rotas, com revalidação no banco a cada alteração
Cadastro público	Criava usuário já ativo	Cria usuário pendente, que nunca recebe perfil elevado
Sessão	Identificador sem rotação e cookie sem marcação de segurança	Identificador de sessão rotacionado após o login; cookie marcado como seguro, inacessível a script e restrito ao próprio site
Concorrência	Sem trava: a última gravação vencia em silêncio	Na aprovação, bloqueio no banco e conferência do estado visto na tela. No encadeamento financeiro, número de versão por registro: gravar ou excluir sobre tela desatualizada é recusado, com explicação (limites na seção 7)
Consulta de relatório	Código de ação concatenado no SQL	Parâmetro tratado pelo banco, o que impede injeção por esse caminho
Cabeçalhos de proteção	Ausentes	Toda resposta instrui o navegador a não adivinhar tipos de conteúdo, a não exibir o sistema dentro de outro site e a manter a conexão cifrada

SEÇÃO 04

Inventário comparado

Uma ferramenta de inventário compara os dois códigos classe a classe, tela a tela e campo a campo. O resultado é reproduzível.

ITEM	RECEBIDO	MIGRADO	LEITURA
Entidades de dados	34	34	Paridade integral. Nenhuma entidade perdida
Telas	46	48	Todas preservadas, mais painel e caixa de mensagens da demonstração
Classes Java	190	203	Todas preservadas, mais 13 classes de segurança e de fluxo. O sistema novo traz ainda 24 classes de teste, que o legado não tinha
Serviços de domínio	68	70	Todos preservados, mais dois novos
Modelos de relatório	34	39	Todos preservados, mais cinco recuperados que existiam só como binário
Arquivos descartados de propósito	2	0	Configuração do framework descontinuado (Seam e Drools), sem função na pilha nova

Contagens de 17 de setembro, por nome distinto de arquivo, sobre o código de produção dos dois lados. Os relatórios existem em cópias em mais de um diretório: 75 arquivos-fonte para 39 modelos no sistema novo, 77 binários para 39 nomes no código recebido.

As 34 alterações de código, uma a uma

São as diferenças que o comparador apontou entre os dois códigos em 17 de setembro. Cada uma foi revisada individualmente, com justificativa e identificação criptográfica dos arquivos de origem e destino. **Nenhuma foi suprimida do resultado do comparador**, o que impede que uma omissão nova passe despercebida: desde então ele aponta mais diferenças, em grande parte mudanças intencionais nos modelos de relatório.

QTD	CATEGORIA	NATUREZA DA DIFERENÇA
11	Tela de login e cabeçalho	Nove rótulos que eram chaves de tradução passaram a português explícito, mais dois atributos de comportamento: a condição de exibição do formulário de login e a ação de saída. Campos, obrigatoriedade, conversor de CPF e ação de login preservados
8	Consultas de pré-planejamento	Separadas das consultas definitivas, porque as duas famílias de tabela compartilham nome de coluna mas apontam para tabelas diferentes
3	Precisão monetária em relatório	Tetos migrados de ponto flutuante para decimal exato
2	Configuração do framework removido	Arquivos do Seam e do Drools, sem função na pilha nova
2	Mapeamento de dados	Nomes de coluna alinhados ao que o banco realmente gera, e uma relação ajustada para que uma configuração de pesquisa atenda mais de uma escola
2	Formatação monetária do monitoramento	Concatenação de texto substituída por conversor de moeda. Valores gravados, ações e regras não mudaram
2	Correção de defeito em tela de pesquisa	Detalhada na seção 6
4	Contrato de método, espaço de nomes e total de relatório	Um método de sessão que não podia ser mantido em componente sem estado; a assinatura do gerador de relatório; o mesmo método no espaço de pacotes novo; e a consulta ajustada para totalizar cada valor uma única vez

Os cinco relatórios recuperados existiam apenas como arquivo compilado, sem fonte editável; foram reconvertidos, com registro criptográfico de cada um, e voltaram a ser passíveis de manutenção.

SEÇÃO 05

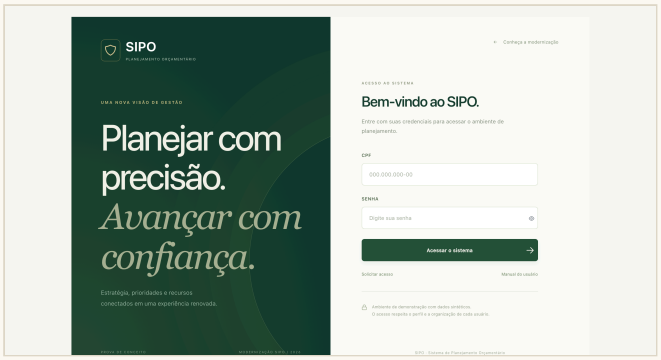
As mesmas telas, os mesmos dados

As capturas abaixo saíram das duas aplicações publicadas por esta prova de conceito, a cópia do legado e o sistema migrado, na mesma rota, com a mesma conta e sobre a mesma massa sintética. Nada foi montado para a apresentação.

SISTEMA LEGADO

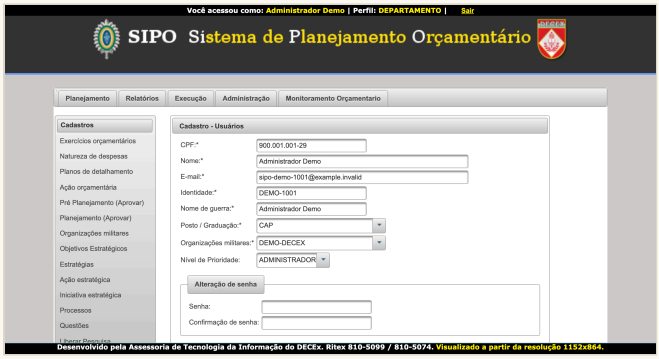


SISTEMA MIGRADO

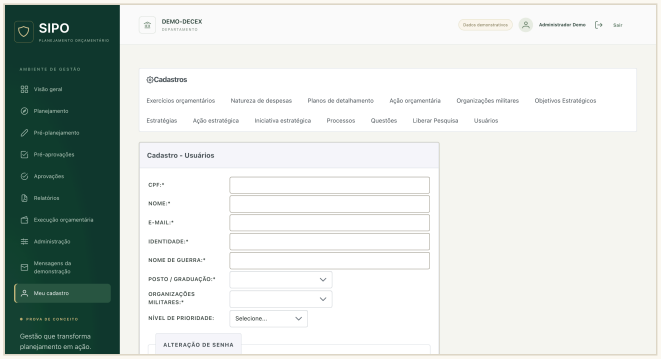


Acesso ao sistema. O campo de CPF, a máscara, a obrigatoriedade e a ação de autenticação são os mesmos. O que mudou é a apresentação e o fato de a tela nova funcionar em qualquer largura de tela.

SISTEMA LEGADO



SISTEMA MIGRADO

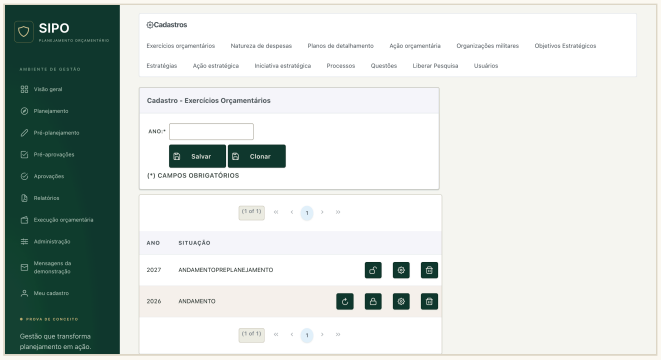


Cadastro de usuários. Os mesmos campos e a mesma lista de organizações militares, com os mesmos registros, porque os dois sistemas leem a mesma massa de dados sintética.

SISTEMA LEGADO



SISTEMA MIGRADO



Exercícios orçamentários. Os dois exercícios da massa aparecem nos dois sistemas, com a mesma situação. O sistema migrado acrescenta as ações de alterar situação e encerrar exercício na própria listagem.

SEÇÃO 05 · CONTINUAÇÃO

O mesmo dado, duas leituras

O recorte abaixo é do mesmo registro, aberto nos dois sistemas: ação 20XE, plano DEMO-ENS, unidade DEMO-EE1, prioridade 1, natureza 339030.

SISTEMA LEGADO



SISTEMA MIGRADO



O valor. O sistema legado exibe R$ 320000.00, sem separador de milhar e com ponto decimal. O migrado exibe R$ 320.000,00. A diferença tem causa técnica: o código recebido pedia a moeda ao sistema operacional sem informar o país, e o resultado dependia da configuração do servidor. Em ambiente com idioma diferente, o mesmo código chega a imprimir o símbolo de dólar. A migração fixou o formato brasileiro em oito pontos do sistema, com teste que roda propositalmente sob configuração estrangeira.

E o rodapé da tela antiga declara: "Visualizado a partir da resolução 1152x864". O código recebido foi desenhado para monitor de mesa em resolução fixa. O migrado responde a qualquer largura, inclusive telefone.

SEÇÃO 06

Sete defeitos do código recebido, encontrados e corrigidos

Transportar um sistema exige lê-lo inteiro. Nessa leitura apareceram falhas no código recebido, confirmadas em execução sobre dados sintéticos, que a modernização corrigiu no caminho. Se esse código é o que está em produção, os efeitos descritos abaixo ocorrem lá.

#	DEFEITO NO CÓDIGO RECEBIDO	EFEITO E CORREÇÃO
1	Tela de configuração de pesquisa aponta para propriedades que não existem no modelo de dados	**A tela responde erro quando a tabela tem registros.** Não aparece em banco vazio, apenas quando a tabela de configuração de pesquisa tem registros, como na massa sintética e como se espera de um banco em uso. Corrigido para as propriedades existentes. Verificável nos dois endereços publicados
2	Valor de aprovação calculado como a soma dos grupos 3 e 4	**Item com os dois grupos preenchidos tinha o valor dobrado no registro de aprovação.** Corrigido para usar o valor correspondente à natureza de despesa do item
3	Monitoramento escolhia o primeiro grupo com valor acima de zero	**Item de grupo 4 era registrado como grupo 3** quando ambos estavam preenchidos, e diárias eram ignoradas nesse caso. Corrigido para seguir a natureza de despesa
4	Falha ao atualizar o monitoramento era silenciosamente ignorada	**O planejamento era gravado deixando o monitoramento desatualizado, sem aviso a ninguém.** Agora a falha desfaz a gravação e é informada
5	Moeda formatada sem informar o país	O símbolo e o formato dependiam da configuração do servidor. Corrigido para o formato brasileiro em oito pontos do sistema, com teste que roda propositalmente sob configuração estrangeira
6	Cadastro público criava usuário já ativo	**Quem alcança a página de cadastro obtém uma conta já ativa**, embora o guia do usuário que acompanha o material diga que o acesso depende de aprovação do DECEx. Agora a conta nasce pendente e depende de liberação
7	Senhas guardadas em MD5	Algoritmo inadequado para senha há mais de uma década. Substituído por PBKDF2 com sal e 600.000 iterações, preservando o acesso de quem tem senha antiga

Defeitos adicionais encontrados nos relatórios

O preenchimento dos relatórios com dados revelou falhas que só aparecem em execução: colunas de alunos do ensino médio invertidas, custo unitário que perdia centavos e podia dividir por zero, filtro textual onde o motor exige valor lógico, e um relatório com ano fixo no código em vez do exercício selecionado pelo usuário. Todos corrigidos.

> ACHADO DE SEGURANÇA NO MATERIAL RECEBIDO
>
> O código-fonte entregue contém **uma credencial de servidor de e-mail escrita diretamente no código**, em GeradorEmail.java. Ação recomendada, com urgência: revogar essa credencial no servidor de e-mail (responsável: DECEx/ATI) e confirmar à MigrAI, porque ela está exposta em qualquer cópia do código-fonte que exista. A ação abre a tabela de próximos passos da seção 9. No material preparado para esta prova de conceito a credencial foi substituída por leitura de variável de ambiente, e o valor original nunca entrou em registro de versão deste trabalho.

> ALCANCE DESTA VERIFICAÇÃO
>
> Estes defeitos foram identificados por leitura do código e confirmados em execução sobre dados sintéticos. Não foi possível medir com que frequência eles afetam a operação real, porque não houve acesso ao banco de produção. A recomendação é que a equipe do DECEx verifique, nos registros atuais, se há valores de aprovação dobrados em itens com dois grupos preenchidos.

SEÇÃO 07

Como se sabe que funciona

A validação responde a uma pergunta específica: o sistema novo faz o que o antigo fazia? Cinco camadas, contadas separadamente, respondem a uma parte cada, de 1.767 testes de código a 29 conferências entre os dois sistemas.

1.767
testes de código, de 155 classes

95,7%
das linhas cobertas, ante 14,4%

185
verificações em 35 telas

0
falhas em qualquer camada

CAMADA	O QUE VERIFICA
Testes de unidade 1.680 casos, de 145 classes	Regras de valor por grupo de despesa, senha, autorização por perfil, fluxo de aprovação, proteção de pesquisa finalizada, cálculo de saldo e teto, conversores e validadores, e a compilação dos 75 arquivos de modelo de relatório
Testes contra PostgreSQL 87 casos	Persistência real, escopo entre escolas, edição e aprovação concorrentes, gravação concorrente do mesmo lançamento, exclusão sobre tela vencida, alimentação do monitoramento, gravação de tetos e exclusão de nota de crédito; a conferência de que o modelo de dados abre sobre a estrutura versionada; e 39 conferências automáticas, uma por modelo de relatório, de que a consulta de cada um funciona sobre a estrutura que a publicação cria
Navegação automatizada 185 verificações	35 telas em computador e telefone, incluindo login, saída, restrição a visitante e o cadastro público, com busca ativa por sinais de erro de servidor
Fluxos de gravação 8 roteiros, 4 antes	Cadastro e ativação de usuário; planejamento com pré-aprovação e homologação; pesquisa; execução orçamentária com notas de crédito; configuração de exercício e tetos; cadeia estratégica; escopo de relatórios; edição simultânea do mesmo lançamento, com duas sessões reais. Cada gravação é conferida no banco e os registros criados são removidos ao final
Links e menus 32 links, 19 cliques	Todo link desenhado em 24 telas é seguido com a sessão, e cada item dos menus de Cadastros e Relatórios é clicado, reprovando destino fora da aplicação, erro ou volta ao login
Acabamento das telas 33 telas, cinco perfis	Título de aba repetido, chave de tradução crua, texto em inglês, identificador repetido no HTML, campo sem rótulo, rolagem horizontal em 390, 768 e 1280 px, erro de JavaScript, resposta 4xx ou 5xx e diálogo que não fecha com a tecla Esc
Comparação com o sistema legado 29 conferências	Os dois sistemas sobem lado a lado, sobre a mesma massa, e o conteúdo de 20 telas de negócio é comparado

A comparação entre os dois sistemas

É a evidência mais direta deste relatório, e o critério dela merece explicação. A comparação é de **dados, não de aparência**: a interface foi redesenhada por requisito, então exigir telas idênticas reprovaria a modernização justamente por ter feito o que se pediu.

O critério é assimétrico de propósito: **o sistema novo pode acrescentar, não pode perder**. Dado que o legado mostra e o novo não mostra reprova a comparação. Conteúdo que só o novo apresenta é registrado como recurso adicional.

O QUE É COMPARADO	RESULTADO	OBSERVAÇÃO
Acesso dos cinco perfis	5 de 5	As mesmas credenciais funcionam nos dois sistemas
Recusa de senha incorreta	aprovado	Os dois recusam
Conteúdo de telas de negócio	20 de 20	Nenhum dado presente no legado está ausente no novo
Sanidade do próprio comparador	3 de 3	Modelo de página descontado das telas, cobertura mínima de telas com conteúdo próprio, ausência de erros de script
Total de conferências	**29**	**Nenhuma divergência**

A comparação da página anterior tem uma exceção declarada, com o motivo registrado: a tela de configuração de pesquisa, em que o legado responde erro (defeito 1 da seção 6). Nesse caso a verificação exige apenas que o sistema novo responda, porque um defeito conhecido do sistema antigo não pode reprovar a migração que o corrigiu.

SEÇÃO 07 · CONTINUAÇÃO

A suíte de testes foi refeita

A primeira medição de cobertura mostrou que os 238 testes originais cobriam **14,4% das linhas**, e que os controladores de tela, o maior pacote do sistema, estavam em 0,4%: a maior parte dos casos vinha da compilação dos modelos de relatório, um caso por arquivo. A suíte foi reescrita em oito frentes paralelas, com uma regra: um teste só conta quando afirma um resultado observável. Percorrer getter e setter não conta.

MEDIDA	ANTES	DEPOIS
Casos de teste	238	1.767
Classes de teste	20	155
Cobertura de linhas	14,4%	95,7%
Cobertura de ramos	14,8%	88,9%
Roteiros de gravação	4	8

Cobertura mede o que foi executado, não o que foi verificado. Para provar que os testes sabem falhar, cada frente introduziu **41 mutações** de comportamento no código de produção e confirmou que pelo menos um teste falhava em cada uma. As 41 foram pegas. Na rodada da auditoria independente vieram mais seis, cada uma retirando uma correção nova, e todas foram acusadas. Uma amostra das 41:

ONDE	MUTAÇÃO INTRODUZIDA	TESTE QUE ACUSOU
Tela de planejamento	trava de prioridade já aprovada invertida	gravação de prioridade aprovada (14 casos)
Tela de pré-detalhe	grupo 3 somado ao saldo em vez de subtraído	cálculo de planejado e saldo contra o teto
Serviço de planejamento	recusa de natureza de despesa repetida removida	lançamento por demanda com natureza já usada
Serviço de usuários	situação inicial do usuário trocada	cadastro de usuário por administrador
Exercício orçamentário	ordenação invertida	ordenação pela sigla da organização superior
Tela de cadastro	limpeza do formulário removida do botão Novo	o formulário continua ligado ao registro da linha clicada (13 casos)

SEIS DEFEITOS QUE A LEITURA DE TELA NÃO PEGAVA, E UMA RODADA COMO USUÁRIO

Os três roteiros novos exercitam telas que a comparação com o legado não alcançava, porque gravam dados em vez de apenas lê-los. Apareceram cinco defeitos funcionais, todos corrigidos e cobertos por teste: a tela de execução não listava as naturezas de despesa da prioridade escolhida; uma configuração de exercício nova era recusada como já existente; a atualização de tetos falhava na gravação; onze campos de cinco telas rejeitavam dígitos por incompatibilidade de máscara entre PrimeFaces 5 e 15; e **a exclusão de nota de crédito dizia ter excluído sem apagar a linha**, porque a cascata da coleção do lançamento refazia a gravação em silêncio. O sexto foi encontrado pelo próprio cliente no primeiro acesso: **os menus de Cadastros e de Relatórios levavam para fora da aplicação**, porque o PrimeFaces 15 deixou de prefixar o contexto nos links absolutos que o 5 prefixava, e nenhum roteiro clicava no menu. Foi corrigido no mesmo dia, e a camada de links e menus acima existe por causa dele. Em seguida, um agente de teste percorreu o sistema publicado como usuário, por cliques, nos cinco perfis e também a 390 px de largura: **37 achados, 31 corrigidos no mesmo dia** (valor e data em formato americano, exclusão de organização que não excluía, menus, rótulos técnicos, componentes em inglês, confirmações ausentes), 2 não reproduzidos e 3 comportamentos do código recebido, mantidos e documentados.

SEÇÃO 07 · CONTINUAÇÃO

A segunda rodada, em ambiente descartável

A primeira rodada de teste como usuário custou caro em um ponto: o testador rodou sobre a mesma base que o cliente usava e estragou registros, que precisaram ser reparados um a um. Na segunda rodada ele recebeu uma cópia descartável do ambiente, com banco e instância próprios, e o alvo passou a ser o acabamento das telas.

Apareceram **vinte e quatro defeitos que todos os outros gates deixavam passar**. Dois eram de perda de dado, e são os que mais importam.

O QUE ACONTECIA	POR QUÊ, E O QUE MUDOU
Gravar depois de clicar numa linha sobrescrevia aquele registro nas 13 telas de cadastro	Clicar numa linha liga o formulário ao registro, e não havia como desligá-lo: quem digitava dados novos e salvava apagava o registro selecionado. Cada tela ganhou um botão que devolve o formulário ao estado de cadastro novo
Excluir prioridade ora não apagava nada, ora apagava a prioridade errada em seis serviços	Sempre com mensagem de sucesso. A coleção do pai tem cascata total: se o registro ainda estiver nela quando o contexto é descarregado, a gravação é refeita sem erro visível. É o mesmo arranjo que já fizera a exclusão de nota de crédito mentir, e que agora foi fechado em todos os pontos onde existia, com teste contra o banco real e conferência pela interface
Um erro de validação travava o próprio cadastro em 14 controladores	O tratamento de falha zerava o identificador do registro em edição, então a gravação seguinte virava inclusão. No cadastro do próprio usuário isso mostrava o nome de uma classe Java na tela
Número de processo ilegível	A máscara de níveis era aplicada a qualquer código: "DEMO-01" aparecia como "DE.MO.-0.1", e o usuário não achava o próprio registro na lista
Todas as telas com o mesmo título de aba	Quem trabalha com várias abas abertas não distinguia uma da outra. Agora são 33 títulos, um por tela
Rolagem horizontal em 28 telas no tablet	Larguras fixas em pixels, herdadas do código recebido. O conteúdo passa a caber, e o que não cabe rola dentro da área de trabalho
Pré-aprovar prioridade sem natureza de despesa derrubava a tela	A regra recusa corretamente, mas a exceção subia até o servidor e o usuário caía na página de erro. Agora a recusa vira mensagem na própria tela, com o motivo escrito para quem lê
Foco do teclado invisível	Itens de menu, abas e campos de seleção não davam sinal ao receber o foco: quem navega por tabulação perdia a posição
Clonar exercício com um ano novo devolvia erro 500	A consulta pelo ano lançava exceção quando o ano não existia, e o usuário caía numa página de erro com link para o login. A clonagem também anunciava sucesso sem copiar nada: agora devolve quantas configurações copiou e a tela diz o que aconteceu
Código repetido aceito em objetivos e estratégias	Dois cadastros bloqueiam duplicidade por restrição no banco e dois não tinham restrição nenhuma. A regra passou a valer no servidor, junto com a recusa de vigência terminando antes de começar

Os demais eram de acabamento: diálogo que não fechava com a tecla Esc, coluna cortada na listagem, campo sem rótulo, acento faltando em texto fixo e em e-mail, ano de exercício sem faixa de validação, botão que não respondia sem dizer por quê.

> **SUSPEITA NÃO É DEFEITO**
>
> Três achados foram descartados na conferência, e o critério vale registro: só entra na lista o que se reproduz. Dois vinham da forma como o roteiro de teste preenchia os campos, e não do sistema; o terceiro era efeito de um defeito já identificado, não uma regra de perfil. Nenhum virou correção.

SEÇÃO 07 · CONTINUAÇÃO

O que a auditoria independente achou

Em 22 de setembro de 2026 um auditor externo testou 19 alegações deste relatório nos dois sistemas no ar, sem acesso ao código.

Sete foram confirmadas, entre elas a paridade de dado, o bloqueio por URL e os defeitos 1, 2 e 3 da seção 6. **Nove viraram achado**, um deles sem veredito, e três ficaram fora de alcance por dependerem do código. Seis achados são só do código recebido. Três confirmam o que este relatório já descrevia: cabeçalhos e cookie de sessão sem proteção, rota protegida que sem sessão não leva ao login, moeda fora do padrão. Três são acréscimos do auditor: a biblioteca jQuery 1.11.0, de 2014; o identificador de sessão na URL; e, o mais grave, um cadastro público que cria, sem autenticação, conta de administrador já ativa.

ACHADO NO SISTEMA MIGRADO	O QUE ERA, E O QUE MUDOU
A segunda gravação do mesmo lançamento apagava a primeira crítico; igual no legado	Dez entidades do encadeamento financeiro ganharam número de versão, conferido pelas três telas financeiras antes de gravar: gravação sobre tela vencida é recusada, com explicação. A seção 3 dizia que isso já valia; valia só na aprovação, e a frase foi corrigida
Nota de crédito não podia ser lançada pela interface	A seleção existia, mas só aceita natureza de despesa encerrada, que é a regra, e nada na tela dizia isso. A linha da grade passou a ser selecionável, e a mensagem explica a regra
Valor lançado não aparecia no monitoramento (sem veredito)	Regra herdada: só entra no monitoramento o item de planejamento encerrado, e no ambiente do auditor nenhum estava. Provada contra PostgreSQL nos dois caminhos e escrita na tela

Antes de responder, uma validação independente

Um time de sete agentes verificadores e um crítico de completude testou cada item nos dois sistemas e achou falhas na nossa primeira correção e defeitos antigos do código recebido, todos corrigidos:

ONDE	O QUE ACONTECIA, E O QUE MUDOU
Na nossa primeira correção só no migrado	Reordenar prioridade quebrava até com um só usuário, e a segunda edição da mesma prioridade ou nota de crédito dava erro ou falso aviso de concorrência, porque a tela não recebia a versão nova. A grade selecionável deixava abrir nota para natureza não encerrada, agora recusada em três camadas
No código recebido também no legado	Gravar prioridade na aba Planejar regravava valores antigos e apagava os incluídos depois; o segundo aprovador desfazia a aprovação do primeiro e recebia sucesso; tela aberta antes do encerramento reabria o item; excluir lançamento ou nota de crédito sobre tela vencida apagava o que outro usuário gravara; o monitoramento duplicava linhas; trocar a natureza de lançamento gravado derrubava a tela

Provas: 1.767 testes sem falha, entre eles 27 de concorrência nas telas e serviços e 14 contra PostgreSQL nas suítes novas; 11 roteiros de navegador aprovados em modo estrito; dois aprovadores e duas sessões reais conferidos pela interface. Nas demais telas, gravação barrada pela versão leva a uma página que diz que nada foi gravado e o que fazer.

Na varredura passiva do auditor, 80 alertas no migrado e 163 no legado. Os dois alertas de risco médio no migrado têm resposta: a falta de token anti-CSRF (36) é coberta pelo estado de visão do Faces, guardado no servidor, e pelo cookie restrito ao próprio site; o estilo embutido na política de conteúdo (14) fica, pelos 492 atributos de estilo das telas herdadas, e a execução de script segue fechada. Tela autenticada deixou de ir para o cache do navegador, e o cookie de infraestrutura que gerava os três alertas de cookie foi eliminado.

Os resíduos do auditor nos dois bancos, como 31 prioridades que inflavam o planejado da escola DEMO-EE1 e, no legado, a conta de administrador criada sem autenticação, foram removidos com autorização, uma transação por banco. A nota de crédito de referência, de R$ 125.000,00, que sumira sem rastro, foi reposta.

> **O QUE FICA PARA A PRÓXIMA ETAPA**
>
> Tetos, situação do exercício, cadastros de apoio e usuários seguem o código recebido: a última gravação vence. Excluir prioridade em tela vencida pode apagar valor de outro usuário, e dois lançamentos simultâneos podem somar acima do teto. O gateway compartilhado, fora deste repositório, não redireciona HTTP para HTTPS.

SEÇÃO 08

Quanto vale este sistema, em pontos de função

A medição usa a técnica de Análise de Pontos de Função, que dimensiona o sistema pelo que ele entrega ao usuário, independentemente da tecnologia. É a métrica adotada nas contratações federais de software, a exemplo do Roteiro de Métricas de Software do SISP.

A contagem

TIPO DE FUNÇÃO	QUANTIDADE	PONTOS	O QUE REPRESENTA
Arquivos lógicos internos	16	136	Grupos de dados que o sistema mantém, como planejamento, pesquisa e configuração de exercício
Arquivos de interface externa	0	0	O sistema não lê dados de outro sistema. Verificado por busca dirigida no código
Entradas externas	84	317	Operações que alteram dados: incluir, alterar, excluir, aprovar, homologar, clonar exercício
Saídas externas	18	116	Relatórios e consultas com cálculo ou totalização
Consultas externas	37	159	Listagens e relatórios que apenas recuperam e formatam
Total	**155**	**728**	**Pontos de função não ajustados**

Contagem feita sobre o sistema migrado, que entrega o mesmo escopo do legado, a partir de 159 artefatos medidos elemento a elemento: 37 arquivos de modelo de dados (34 entidades e 3 classes auxiliares), 36 controladores, 47 arquivos de tela (sem o modelo de layout, que o inventário da seção 4 inclui) e 39 modelos de relatório. A planilha com as 155 funções, seu tipo e sua complexidade está no repositório, em docs/pontos-de-funcao.md. Não foi aplicado fator de ajuste, seguindo a norma ISO/IEC 20926, que o retirou da contagem funcional.

> MARGEM DESTA CONTAGEM
>
> Uma segunda contagem, feita por método automatizado independente sobre o mesmo código (outro modelo de linguagem, sem acesso à primeira), chegou a **640 pontos, com margem de 40**, contra os 728 desta. As divergências estão em classificações de relatório entre saída e consulta, e em quanto os ciclos preliminar e definitivo devem ser contados separadamente. **Trate o tamanho como 640 a 770 pontos**: o piso é a segunda contagem sem a margem, e o teto é esta contagem mais a margem. Para fim contratual, recomenda-se contagem IFPUG formal, com homologação dos processos elementares junto ao gestor do negócio, o que não foi feito.

Distribuição

COMPONENTE	PONTOS	PARTICIPAÇÃO	LEITURA
Dados	136	18,7%	O peso em transações e relatórios, acima de 80%, confirma o que se vê no uso: o SIPO é um sistema de processo e de prestação de contas, não um sistema de cadastro
Entradas	317	43,5%	
Saídas	116	15,9%	
Consultas	159	21,8%	

SEÇÃO 08 · CONTINUAÇÃO

Prazo e custo das alternativas

MUDANÇA DE NATUREZA DA INFORMAÇÃO

Tudo até aqui é contagem, auditável no código. **Desta página em diante são premissas comerciais.** Produtividade por ponto de função não é grandeza normativa: não existe número oficial. As faixas abaixo são de mercado e podem ser substituídas pelos históricos do Exército sem invalidar a contagem.

PREMISSA	VALOR ADOTADO	BASE
Tamanho funcional	728 pontos	Contagem da página anterior. A faixa de 640 a 770 é aplicada na página seguinte
Horas produtivas por pessoa ao mês	140 h	De 168 nominais, descontando feriados, férias e reuniões
Capacidade da equipe	840 h por mês na construção; 700 h na migração	7 pessoas com 6,0 em dedicação integral na construção; 5 pessoas com 5,0 na migração. Composição na planilha de contagem. Prazo = esforço dividido pela capacidade mensal
Valor-hora	R$ 150 a R$ 250	Faixa praticada em contratos de fábrica de software no setor público brasileiro, com encargos e impostos. Premissa comercial, não cotação: equivale a R$ 1.800 a R$ 4.000 por ponto de função na construção do zero, a confrontar com os contratos vigentes do órgão
Produtividade, construção do zero	12 a 16 h por ponto	Faixa de mercado de 8 a 20 h. A posição mediana superior se justifica pelos 22 modelos de relatório acionáveis, a maioria com totalização, pelas regras de saldo contra teto e pelo duplo ciclo de planejamento. Numa contratação prevalecem os índices do Roteiro de Métricas do SISP
Fator de redução na migração	0,32 a 0,42	Derivado atividade a atividade, na página seguinte: o domínio, as regras e as telas já existem e servem de especificação

Os dois caminhos

DIMENSÃO	CONSTRUIR DO ZERO	MIGRAÇÃO ASSISTIDA	DIFERENÇA
Escopo entregue	728 pontos	728 pontos	igual
Esforço	8.740 a 11.650 h	2.800 a 4.890 h	58% a 68% menor
Prazo	10 a 14 meses	4 a 7 meses	50% a 60% menor
Equipe	7 pessoas, 6,0 em dedicação integral	5 pessoas, 5,0 em dedicação integral	2 a menos
Custo	**R$ 1,31 mi a R$ 2,91 mi**	**R$ 419 mil a R$ 1,22 mi**	**58% a 68% menor**

O que estes prazos são, e o que não são. Eles respondem a uma pergunta de comparação: quanto custaria entregar este mesmo escopo técnico pelo caminho convencional. **Não são o cronograma desta prova de conceito:** o repositório registra 43 commits de uma única pessoa entre a noite de 16 e a madrugada de 18 de setembro de 2026, com as ferramentas de migração assistida por inteligência artificial da MigrAI e revisão humana de cada alteração registrada. Esse tempo não é comparável às faixas acima porque exclui a migração de dados reais e a homologação institucional, tratadas na seção seguinte. Percentuais da coluna Diferença calculados sobre os extremos correspondentes de cada faixa.

SEÇÃO 08 · CONTINUAÇÃO

De onde vem o fator de redução

O fator de 0,32 a 0,42 pesa mais da metade do resultado, então é mostrado atividade a atividade: peso na construção do zero e quanto sobra na migração.

ATIVIDADE	PESO DO ZERO	REAPROVEITADO	SOBRA	POR QUÊ
Levantamento e análise de requisitos	15%	90%	1,5%	As regras estão codificadas em 36 controladores e 68 serviços. Não há oficina de requisitos
Modelagem de dados	8%	95%	0,4%	34 entidades e o esquema físico preservados. Trabalho limitado à troca de espaço de pacotes
Desenho de telas	10%	70%	3,0%	46 telas preservadas em estrutura e campos. Há retrabalho real de componentes e identidade visual
Implementação das regras	30%	55%	13,5%	Maior bloco residual: Seam 3 para CDI, injeção e escopos reescritos, persistência gerida pelo contêiner, Java 7 para Java 21
Implementação da interface	12%	60%	4,8%	JSF 2 para Jakarta Faces 4, espaços de nomes, conversores e componentes PrimeFaces atuais
Relatórios	10%	90%	1,0%	39 modelos preservados; o JasperReports roda nas duas pilhas. Trabalho restrito ao carregamento e aos sub-relatórios
Testes e homologação	12%	10%	10,8%	Segundo maior bloco: o legado não tinha testes, e toda a paridade precisa ser provada
Gestão, arquitetura e implantação	3%	20%	2,4%	Nova arquitetura de contêiner e pipeline de publicação
Fator resultante	**100%**		**37,4%**	**Faixa adotada de 0,32 a 0,42, com 0,37 ao centro: redução de 58% a 68%**

O custo sobre a faixa de 640 a 770 pontos

Com as mesmas premissas, o custo fica entre **R$ 1,15 mi e R$ 3,08 mi** para construir do zero e entre **R$ 369 mil e R$ 1,29 mi** na migração assistida. A faixa é larga por construção e estreita assim que o Exército substitui as premissas pelos seus índices contratados.

O que o número não captura

A métrica dimensiona escopo entregue. Três ganhos ficam fora dela: **o risco de perda de regra**, porque na reconstrução cada regra precisa ser redescoberta e as não documentadas são a principal fonte de defeito; **a continuidade do modelo de dados**, que viabiliza a virada com o histórico intacto, sem projeto separado de conversão; e **a cobertura de testes criada**, 1.767 casos onde antes não havia nenhum, ativo permanente que reduz o custo de manutenção.

> SOBRE COMPARAÇÕES DE DESEMPENHO
>
> Este relatório não publica percentual de ganho de produtividade da prova de conceito: um número desses só teria valor com medição controlada das duas abordagens sobre o mesmo escopo, o que não foi feito. As comparações desta seção derivam de premissas declaradas, não de medição.

Pesos por atividade: distribuição usual de esforço por fase em projetos de sistemas de informação. A planilha completa, com as 155 funções e a derivação de cada cenário, está em docs/pontos-de-funcao.md no repositório.

SEÇÃO 09

O que separa esta prova de conceito da operação

A prova de conceito provou o que se propôs: o sistema migrado funciona e preserva o comportamento do original. Quatro frentes separam isso de um sistema em produção. Duas são dimensionáveis hoje. Duas dependem de informação que só o Exército possui.

Frente 1 · Migração de dados reais

Não foi recebido banco de dados do sistema em operação, então esta frente **não recebe estimativa**. O esforço de uma migração de dados é função de volume, quantidade de defeitos de qualidade e quantidade de decisões de negócio sobre registros ambíguos. Nenhuma das três é conhecida hoje.

O que já existe e será reaproveitado: a estrutura inicial do banco em script versionado; um comparador de bancos que confere colunas, restrições, contagens, valores linha a linha e sequências; e o teste que valida o modelo de dados e a consulta de cada relatório contra a estrutura que a publicação realmente cria.

As dez perguntas que o DECEx precisa responder para esta frente ser dimensionável

#	PERGUNTA	POR QUE DETERMINA O TAMANHO
1	Volume por tabela	Define tempo de extração, carga e reconciliação, e se a janela de corte cabe
2	Quantos exercícios de histórico migrar	Migrar todo o histórico e migrar os três últimos são projetos de portes diferentes. É a variável de maior impacto no prazo
3	Qualidade dos dados	Cada classe de defeito vira uma regra de transformação e uma decisão de negócio
4	Existem registros órfãos	O esquema alvo aplica 54 chaves estrangeiras. Órfãos fazem a carga falhar e exigem decisão caso a caso
5	O banco real tem objetos fora dos mapeamentos	O código recebido gera o esquema automaticamente, modo que acumula objetos e nunca os remove. Só uma cópia do banco real responde
6	Retenção e dados pessoais	O sistema guarda CPF, posto, nome e organização de cada usuário
7	Migrar senhas ou forçar redefinição	As duas opções funcionam, com consequências operacionais diferentes
8	Janela de indisponibilidade aceitável	O ciclo é sazonal. O corte não pode cair no pico do planejamento
9	Haverá ambiente de ensaio	Sem ensaio, o primeiro teste real da carga é o próprio corte
10	Critério de aceite da reconciliação	Diferença zero, ou diferenças nomeadas e aprovadas. Precisa ser acordado antes

As perguntas 1, 3, 4 e 5 são respondidas por uma cópia do banco; as perguntas 2 e 6 a 10 são decisões do DECEx, que cabem num ofício ou numa reunião de trabalho de duas horas.

> **Duas diferenças de esquema já estão mapeadas**, porque o sistema legado foi efetivamente executado nesta prova de conceito: os nomes das colunas de junção da configuração de plano, e a restrição que limitava uma configuração de pesquisa a uma única escola. Ambas são tratáveis na carga, e a técnica usada aqui, descobrir o esquema por introspecção em vez de assumi-lo, é diretamente reaproveitável.

SEÇÃO 09 · CONTINUAÇÃO

As outras três frentes

Frente 2 · Homologação institucional

A validação feita foi técnica: prova que o sistema novo faz o que o antigo fazia sobre a mesma massa. Só o usuário do DECEx pode confirmar aderência às regras reais, aos casos de borda do ciclo orçamentário e à conferência dos relatórios contra documentos oficiais conhecidos.

> UM PONTO DE MÉTODO QUE MUDA O RESULTADO
>
> O critério de aceite da homologação deve ser **"o sistema faz o que a norma manda"**, não "o sistema faz o que o legado fazia". São coisas diferentes. A paridade com o legado já está verificada e é um gate de engenharia. Quando as duas divergirem, ou seja, quando o legado fizer algo que a norma não prevê, a divergência é decisão do Exército e deve ser registrada como tal, não resolvida em silêncio pela equipe técnica.

Frente 3 · Requisitos não funcionais

A publicação atual usa uma instância única, adequada à demonstração. Antes de escalar é preciso decidir o tratamento do estado de sessão, que hoje é mantido no servidor: manter cada usuário preso a uma instância, replicar a sessão entre instâncias, ou guardá-la fora do servidor de aplicação, cada saída com custo e efeito diferentes. Faltam ainda teste de carga com volume real, cópia de segurança com recuperação ensaiada, monitoração com alarme e destinatário definidos, e a decisão de onde o sistema roda em produção. Do lado da segurança, a seção 13 mostra o que já foi testado e corrigido; o que falta é o teste de intrusão manual por especialista e a revisão de perfis de acesso com o DECEx. Entram também nesta frente os limites de concorrência e de publicação registrados ao fim da seção 7.

Uma pergunta antecede essas: qual servidor de aplicação e qual JVM executam o SIPO hoje. A resposta não muda o caminho técnico, porque o impedimento está no framework, mas define por quanto tempo o ambiente atual ainda tem suporte e se a convivência dos dois sistemas durante o corte cabe na infraestrutura existente. Ela é o item 2 dos próximos passos.

Frente 4 · Operação e transferência

O repositório já traz doze documentos técnicos além do README, e as rotinas automatizadas executam o que a documentação afirma, o que reduz o risco de documentação que envelhece sem ninguém perceber. Faltam o manual de operação (runbook), material de treinamento por perfil, plano de suporte e transferência de conhecimento.

Quadro consolidado

FRENTE	DIMENSIONÁVEL HOJE	O QUE IMPEDE A ESTIMATIVA
Dados reais	Não	Nenhum banco foi recebido. Faltam as respostas das dez perguntas da página anterior
Homologação	Parcialmente. Roteiro e estrutura de evidência: 5 a 8 dias úteis de um analista	A condução depende da disponibilidade dos homologadores e do número de achados, desconhecido antes de começar
Não funcionais	Parcialmente. A configuração técnica é estimável item a item	Faltam decisões do Exército: onde hospedar, qual disponibilidade exigir, quais tempos de recuperação, quem recebe alarme
Operação	Parcialmente. Manual de operação: 4 a 6 dias úteis	Número de turmas de treinamento e nível de serviço de suporte dependem de definição institucional

SEÇÃO 09 · CONTINUAÇÃO

O que se pede do Exército, e o que a MigrAI faz em seguida

Três informações destravam o dimensionamento da implantação: uma cópia do banco de produção, o ambiente que executa o SIPO hoje e os homologadores por perfil. Os passos abaixo estão em ordem de dependência.

Próximos passos propostos

#	AÇÃO	RESPONSÁVEL	PRAZO SUGERIDO
1	Revogar a credencial de e-mail exposta no código recebido e confirmar à MigrAI	DECEx/ATI	Imediato
2	Informar servidor de aplicação, JVM e sistema operacional da produção	DECEx/ATI	5 dias úteis
3	Disponibilizar cópia do banco de produção, anonimizada ou em ambiente isolado, e responder às dez perguntas da frente 1	DECEx/ATI	15 dias úteis
4	Indicar homologadores por perfil: administrador, aprovador, pré-aprovador e planejador	DECEx	10 dias úteis
5	Dimensionar as frentes 1, 3 e 4 com as respostas acima e apresentar o plano de implantação	MigrAI	10 dias úteis após os itens 2 e 3
6	Conduzir a homologação assistida sobre a massa real, registrando cada divergência como decisão	DECEx e MigrAI	A combinar no plano

O caminho mais curto para destravar. Uma cópia do banco de produção em ambiente isolado, mais as decisões de hospedagem e de disponibilidade, tornam três das quatro frentes estimáveis com a mesma disciplina de evidência aplicada ao resto deste relatório. O item 1 não depende de nada: a credencial exposta no código recebido deve ser revogada antes de qualquer outra providência.

O que a MigrAI entrega em cada resposta

QUANDO O EXÉRCITO RESPONDE	A MIGRAI DEVOLVE
O ambiente de produção (item 2)	A leitura definitiva da seção 2 para esse ambiente, com o prazo de suporte restante e o plano de convivência dos dois sistemas durante o corte
A cópia do banco (item 3)	O relatório de qualidade dos dados, as respostas mensuráveis às dez perguntas da frente 1 e a estimativa da migração de dados
Os homologadores (item 4)	O roteiro de homologação por perfil, com critério de aceite "o sistema faz o que a norma manda" e registro de cada divergência como decisão

SEÇÃO 10

Como conferir você mesmo

Os dois sistemas estão publicados. Abra-os em janelas lado a lado: eles leem a mesma massa de dados, então a comparação é direta.

Endereços

Publicados em nuvem pública (Google Cloud, região us-central1, Estados Unidos), com dados exclusivamente sintéticos: nenhum dado do Exército foi enviado para fora do país.

O QUÊ	ENDEREÇO
Apresentação da migração	poc-exercito.apps.migrai.com.br
Sistema migrado	poc-exercito.apps.migrai.com.br/sipo
Sistema legado	poc-exercito-legado.apps.migrai.com.br/sipo

Perfis de acesso

As mesmas credenciais valem nos dois sistemas. A senha, comum aos cinco perfis, é **cfwEQa4YNRYMhE-ltMHnFR1cBkpbYCka**, e vale só nesta demonstração, sobre dados sintéticos.

PERFIL	CPF DE ACESSO	O QUE ESSE PERFIL ALCANÇA
Administrador	900.001.001-29	Todos os cadastros, configuração de exercício, execução e relatórios
Aprovador	900.001.002-00	Homologação definitiva do planejamento
Pré-aprovador	900.001.005-52	Pré-aprovação do planejamento das escolas
Planejador, escola 1	900.001.003-90	Planejamento da própria escola
Planejador, escola 2	900.001.004-71	Planejamento de outra escola, útil para conferir o isolamento entre organizações

CPFs fictícios, gerados para a demonstração.

Roteiro sugerido

#	O QUE FAZER	O QUE OBSERVAR
1	Entrar como administrador nos dois sistemas	As mesmas credenciais funcionam em ambos
2	Aba Planejamento; depois aba Monitoramento Orçamentário, que abre a janela Monitorar Orçamento	Na ação 20XE, prioridade 1: migrado R$ 320.000,00; legado R$ 320000.00
3	Digitar no endereço a tela usuario/configurapesquisa.xhtml	O legado responde erro. O migrado apresenta a listagem. É o defeito 1 da seção 6
4	Reduzir a janela do navegador, ou abrir pelo telefone	O legado não acompanha. O migrado reorganiza o conteúdo
5	Entrar como planejador da escola 1 e abrir, pelo endereço, administracao/aprovarPlanejamento.xhtml	O servidor devolve ao painel: recusa no servidor, não só na tela
6	Entrar como planejador da escola 2	Só aparecem os dados da própria escola
7	Menu Relatórios, por exemplo Planejamento Geral	O documento sai com os dados da organização selecionada e sem dados de outras

Ao testar o legado: a primeira abertura pode levar alguns minutos, porque o JBoss AS 7.1 percorre a aplicação inteira ao subir; diante de página em branco, aguarde um minuto e recarregue.

SEÇÃO 11

O que esta prova de conceito não demonstra

Um relatório técnico precisa dizer também o que não demonstrou. Os itens abaixo estão registrados no próprio repositório do projeto.

LIMITE	SITUAÇÃO
Nenhum dado real foi migrado	Não foi recebido banco de dados nem cópia de segurança do sistema em operação. O material entregue continha apenas código-fonte. Toda a demonstração usa massa sintética, e nenhuma importação ou reconciliação de registros reais é afirmada
Não houve homologação pelo usuário	A validação foi técnica: prova que o sistema novo faz o que o antigo fazia sobre a mesma massa. Só o usuário do DECEx pode confirmar aderência às regras reais de negócio e aos casos de borda do ciclo orçamentário
Não é comprovação de disponibilidade nem de carga	A publicação usa uma instância única, adequada à demonstração. Não foram executados teste de carga com volume real nem verificação de alta disponibilidade
Não há vínculo institucional	Esta prova de conceito não declara parceria, aprovação ou uso operacional pelo Exército Brasileiro. É um exercício técnico sobre código recebido
Envio de e-mail não integra a demonstração	As mensagens do sistema são gravadas em caixa interna, visível à administração, sem envio externo
Um defeito do material recebido foi preservado	Um modelo de relatório (preplanejamentoadministrador), presente em duas cópias, chegou com marcadores de conflito de versionamento não resolvidos. A definição válida foi recuperada do arquivo compilado, e o defeito original permanece registrado em vez de ser apagado

Termos usados neste relatório

TERMO	SIGNIFICADO AQUI
CDI	Mecanismo padrão do Java EE que liga os componentes de uma aplicação. O Seam 3 depende da primeira versão dele
Framework	Conjunto de bibliotecas sobre o qual a aplicação é escrita. No código recebido, o Seam 3
PBKDF2 e MD5	Formas de guardar senha. O MD5 é rápido demais para isso, o que facilita a quebra; o PBKDF2 torna lenta cada tentativa
Estrutura de banco versionada	A forma das tabelas registrada em scripts numerados, aplicados na ordem e nunca editados depois
Conferência (paridade)	Comparação automática entre os dois sistemas publicados, tela a tela, sobre a mesma massa de dados
Massa sintética	Dados fictícios, gerados para a demonstração, sem correspondência com registros reais
Ponto de função	Unidade de tamanho de software pelo que ele entrega ao usuário, independente da tecnologia
FTE	Pessoa em dedicação integral. Duas pessoas a meio período contam como 1,0
Publicação (deploy)	Colocar uma versão do sistema no ar. Aqui, toda publicação sai de uma imagem imutável identificada
Manual de operação (runbook)	Procedimentos para operar o sistema no dia a dia: subir, parar, recuperar, monitorar

SEÇÃO 12

A mesma régua nos dois códigos

Os dois códigos foram analisados pelo mesmo SonarQube, com o mesmo perfil de regras, na mesma máquina, com as mesmas exclusões. A pergunta é direta: a modernização melhorou a qualidade do código, e em quanto?

522
apontamentos no código recebido

0
apontamentos abertos no migrado

50 h
de dívida técnica eliminada

D → A
nota de confiabilidade e de segurança

INDICADOR	RECEBIDO	MIGRADO	LEITURA
Linhas de código	20.051	22.255	o migrado é 11,0% maior: ganhou tratamento de erro, validações e proteções
Apontamentos abertos	**522**	**0**	**dezessete corrigidos no código, dez aceitos com justificativa registrada**
Bugs	26	0	comparação de objetos com `==`, contrato de ordenação violado, valor nulo desreferenciado
Vulnerabilidades	1	0	credencial de e-mail escrita no código (seção 6)
Hotspots a revisar	22	0	os 3 do migrado foram revisados e justificados
Code smells	495	0	texto repetido, código comentado, comparação com `true`
Dívida técnica	50 h	0	estimativa da própria ferramenta para sanar o que apontou
Linhas duplicadas	16,3%	11,9%	queda de 27% em proporção
Complexidade cognitiva	1.714	1.913	11,6% acima do original: as regras de negócio foram preservadas, e o acréscimo vem das validações e travas novas
Cobertura de testes	0%	95,7%	o código recebido não trazia suíte de testes

O que estava errado, em padrões repetidos

Os 522 apontamentos do código recebido não são 522 problemas diferentes. Concentram-se em poucos hábitos repetidos ao longo de dez anos: **108** criações de coleção sem o operador diamante, **90** textos literais repetidos em vez de constante, **51** blocos de código comentado deixados no arquivo, **27** usos de `tamanho igual a zero` em vez de `está vazio`, **14** escritas diretas no console em vez de registro em log. São sinais de código que envelheceu sem manutenção de forma, não de um sistema mal concebido.

> **COMO LER ESTA COMPARAÇÃO COM HONESTIDADE**
>
> Três ressalvas. Primeira: o sistema migrado é **maior**, e mais código com menos apontamentos é o resultado que interessa. Segunda: **zero aberto não é zero levantado**. Ao longo do projeto o Sonar apontou 27 itens no migrado; dezessete foram corrigidos e dez aceitos, cada um com justificativa escrita na própria ferramenta, auditável. Os cinco mais recentes, achados em código novo pelas duas medições de 22 de setembro, estão entre os corrigidos. Terceira: a nota do Sonar mede **forma**, não aderência às regras do ciclo orçamentário. Essa parte é o que a seção 7 valida, e o que só a homologação do DECEx confirma.

SEÇÃO 13

Teste de penetração, com correção e reteste

O sistema migrado foi submetido a um teste de segurança estruturado pelas fases do NIST SP 800-115, com os achados classificados pelo OWASP Top 10 (2021) e os testes dinâmicos orientados pelo OWASP Web Security Testing Guide. Cada achado foi classificado, corrigido e reconferido com a mesma varredura.

0
alertas de risco alto ou médio não justificado

0
vulnerabilidades conhecidas no pacote da aplicação

0
hotspots de segurança a revisar

21
telas sem violação de política de conteúdo

CAMADA	FERRAMENTA	O QUE COBRE
Estática (SAST)	Semgrep (regras OWASP Top 10, auditoria de segurança) e SonarQube	injeção, criptografia fraca, desserialização, configuração insegura, segredo no código
Composição (SCA)	Trivy, sobre o pacote da aplicação e as duas imagens publicadas	vulnerabilidades conhecidas nas dependências e no sistema operacional
Dinâmica (DAST)	OWASP ZAP 2.16, autenticado como administrador	cabeçalhos, sessão, CSRF, XSS, injeção, exposição de erro
Política de conteúdo	rotina própria de verificação	ausência de violação de Content Security Policy nas 21 telas de negócio

As varreduras ativas rodaram contra uma instância isolada, com cópia da massa de demonstração, nunca contra o ambiente publicado: uma varredura ativa grava dados e derruba sessões.

Correções que ficaram no sistema

Cabeçalhos e sessão. Toda resposta passou a trazer as proteções de navegador contra interpretação indevida de conteúdo, enquadramento em outro site e vazamento de endereço. O cookie de sessão ganhou a restrição que impede envio em requisição vinda de outro site.

Política de conteúdo. As telas passaram a declarar a origem permitida de cada tipo de recurso, com identificador aleatório por requisição para os scripts. O único script embutido no modelo de página virou arquivo próprio.

Erro não conta mais a vida do servidor. Falha, sessão expirada, página inexistente e acesso negado respondem com páginas próprias, sem pilha de execução nem versão de componente, inclusive em requisições parciais de tela.

Dependências e imagem. As bibliotecas da aplicação com vulnerabilidade conhecida foram atualizadas, e a imagem passou a ser montada com um servidor enxuto, só com as partes que a aplicação usa. O pacote da aplicação ficou sem nenhuma vulnerabilidade conhecida, e a imagem inteira caiu de 165 para 75.

SEÇÃO 13 · CONTINUAÇÃO

Antes e depois, na mesma varredura

A varredura que encontrou cada achado foi repetida depois da correção, com o mesmo plano e o mesmo perfil de acesso. A coluna Depois é o resultado da segunda passagem, sobre o mesmo pacote que está publicado.

ACHADO	ANTES	DEPOIS	CLASSIFICAÇÃO E CORREÇÃO
Risco alto (dinâmico)	1	0	falso positivo: os números apontados como dado pessoal são identificadores do estado de visão do Faces. O critério de aceite só tolera esse alerta quando toda evidência tem esse formato
Risco médio (dinâmico)	2	1	ausência de Content Security Policy, corrigida com política por requisição; o alerta restante (style embutido, exigido pelos componentes de tela) é aceito com justificativa, e a execução de script continua restrita
Risco baixo (dinâmico)	1	0	página de erro do servidor expunha pilha de execução e versões; substituída por páginas próprias, e requisição forjada passou a responder 403
Vulnerabilidades no pacote da aplicação	10	0	bibliotecas de leitura de dados, de registro em log e de relatórios atualizadas para versões corrigidas
Vulnerabilidades na imagem publicada	165	75	servidor provisionado só com as camadas usadas e correções do sistema operacional aplicadas na construção; as 75 restantes estão em bibliotecas do próprio servidor e em pacotes sem correção publicada, e viram item de manutenção
Hotspots do Sonar	18	0	gerador pseudoaleatório trocado por gerador criptográfico; rastros de erro impressos no console viraram registro em log sem dado pessoal
Achados do Semgrep	8	0	nenhum verdadeiro positivo; classificados um a um, com a justificativa registrada

O critério que impede a regressão

O teste não é um exercício de uma vez só. As três camadas rodam automaticamente a cada publicação, sobre a mesma imagem que vai ao ar, e o resultado é comparado com um critério de aceite escrito no repositório: a publicação é reprovada diante de **qualquer alerta de risco alto** ou de **qualquer alerta médio que não esteja na lista de aceitos com justificativa**. Aceitar um achado exige registrar por escrito o motivo, e a lista é revista a cada mudança. Sem isso, o número de hoje não diz nada sobre o sistema de amanhã.

Desde 20 de setembro o CI do GitHub está bloqueado por cobrança da conta. Nesse intervalo os mesmos gates rodam localmente e contra o endereço público, e a varredura ativa mais recente é de 18 de setembro, contra instância local isolada.

> O QUE ESTE TESTE NÃO COBRE
>
> Não houve teste de carga nem de negação de serviço, nem engenharia social. A varredura ativa cobriu as 88 páginas distintas alcançadas com perfil de administrador. **Um teste de intrusão manual por especialista continua recomendado antes da entrada em produção**, e um sistema em operação real exige ainda revisão de perfis de acesso com o DECEx. O detalhamento completo, achado a achado, está no repositório, em docs/seguranca.md.

ENCERRAMENTO

O sistema está no ar. A conferência é sua.

Este relatório foi escrito para ser verificado, não para ser acreditado. Cada afirmação tem origem apontada, e os dois sistemas estão publicados para que a comparação seja feita diretamente, sem intermediário.

SISTEMA MIGRADO	poc-exercito.apps.migrai.com.br/sipo
SISTEMA LEGADO	poc-exercito-legado.apps.migrai.com.br/sipo
APRESENTAÇÃO	poc-exercito.apps.migrai.com.br
EXECUÇÃO	MigrAI
CONTATO	contato@migrai.com.br · migrai.com.br
REPOSITÓRIO	github.com/brunohelius/poc-exercito, revisão 6dac5ae; acesso concedido a pedido ao contato acima
EVIDÊNCIAS	Pasta docs/evidence do repositório, mais os recibos das rotinas de validação e de paridade
VERSÃO	1.6, de 22 de setembro de 2026. A 1.1 reescreveu a seção 2; a 1.2 separou o código recebido do ambiente de produção; a 1.3 acrescenta as seções 12 e 13 e atualiza a seção 7 com a suíte de testes refeita; a 1.4 registra a rodada de teste como usuário e as correções que ela gerou; a 1.5 acrescenta a segunda rodada, feita em ambiente descartável e voltada ao acabamento das telas; a 1.6 registra a auditoria independente e a validação feita antes de responder a ela, descreve as correções que as duas geraram e os limites que ficam para a próxima etapa, e corrige a frase da seção 3 sobre concorrência

MigrAI