

PROJETO ACADÊMICO

Diagnóstico e Redesenho do Serviço de Concessão de Acesso Lógico a Sistemas

Autores:

- Mauricio da Silva Marinho
- Breno Zanferdini Preischartt

Disciplina: Transformação Digital no Governo

Curso: Mestrado em Administração Pública – Ênfase em Ciência de Dados e IA

Instituição: IDP Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa

Ano: 2026

RESUMO EXECUTIVO

Este trabalho apresenta o diagnóstico e o redesenho do serviço de concessão de acesso lógico a sistemas negociais em um órgão público. A partir de evidências do processo atual — incluindo análise de solicitações por e-mail, interação com gestores e observação do fluxo operacional — foram identificadas fricções relevantes, alta incidência de retrabalho (failure demand) e violações do princípio once-only.

O estudo mapeia a jornada “as-is”, evidenciando dependência de processos manuais, ausência de padronização e riscos operacionais, como a existência de acessos indevidos.

Como resposta, propõe-se um redesenho “to-be” na forma de um MVP testável, baseado em um portal integrado à base de RH e ao Active Directory, com automação de validações, aprovações simplificadas e revogação automática.

O trabalho também define métricas de sucesso, hipóteses de melhoria e um experimento piloto para validação da solução, alinhando-se às diretrizes de transformação digital no governo e ao foco centrado no usuário.

1. INTRODUÇÃO

A transformação digital no setor público exige o redesenho de serviços a partir da perspectiva do usuário, com foco na redução de fricções, eliminação de redundâncias e aumento da eficiência.

O presente trabalho analisa o processo de concessão de acesso lógico a sistemas negociais, com o objetivo de compreender o fluxo atual (as-is), identificar problemas estruturais e propor um redesenho testável (to-be) centrado no usuário.

2. CONTEXTO DO SERVIÇO

2.1 Descrição do serviço

O serviço analisado consiste na concessão de acesso lógico a sistemas negociais internos, permitindo que servidores desempenhem suas atividades com segurança e conformidade.

2.2 Público-alvo

- Empregados públicos
- Terceirizados autorizados
- Estagiários (quando aplicável)
- Gestores técnicos e negociais

2.3 Canais atuais

- E-mail institucional
- Documentos em PDF
- Assinaturas manuais ou digitais

2.4 Volume e características operacionais

Aproximadamente 3,6 mil requisições por ano sobre acesso lógico a recursos informáticos, ou 50 requisições diárias em média (dias úteis).

2.5 Restrições legais e operacionais

Foram considerados normativos e portarias pertinentes ao tema e restringindo o compartilhamento de dados. Dados que identificam áreas, pessoas e processos reais foram suprimidos ou substituídos para evitar qualquer inconformidade legal ou administrativa.

- Normas de segurança da informação (Política de Segurança da Informação, Manual de Segurança da Informação e Comunicações e LGPD).
- Segregação de funções.
- Auditorias internas e externas.
- Dependência da base de RH.

3. STAKEHOLDERS E ATORES

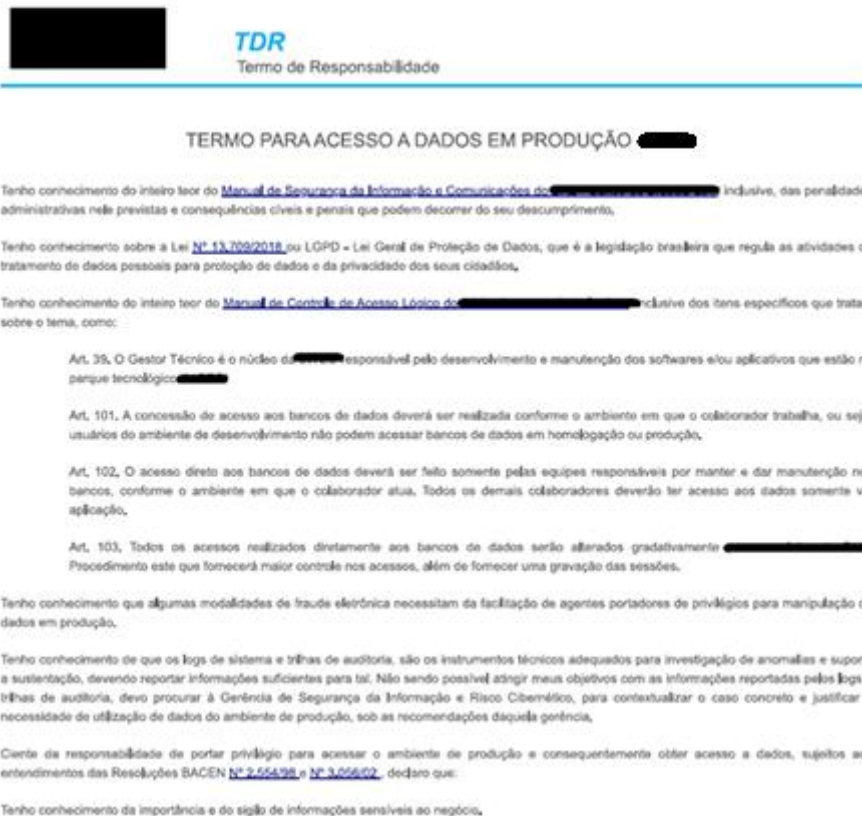
Ator	Papel
Servidor requisitante	Solicita acesso
Gestor técnico (TI)	Avalia e executa
Gestor negocial	Autoriza acesso
RH	Fonte de vínculo
Active Directory	Gestão de identidade
Auditoria	Controle e conformidade

4. EVIDÊNCIAS PRIMÁRIAS

O diagnóstico foi baseado em evidências primárias coletadas diretamente no contexto do serviço, incluindo:

- Análise de solicitações reais por e-mail, antes de melhorias no processo.
- Observação do fluxo operacional da área de TI para os casos de concessão de acesso a dados e privilégios a sistemas negociais.
- Interação com gestor técnico responsável (mensagens trocadas entre o primeiro nível e o gestor).
- Análise de documentos e comunicações utilizadas.

Exemplo dos termos de ciência e responsabilidade para concessão de acesso a banco de dados:



Trecho do Termo de Responsabilidade a ser assinado pelo requisitante

TERMO PARA ACESSO A DADOS EM PRODUÇÃO

Tenho conhecimento do inteiro teor do [Manual de Segurança da Informação e Comunicações](#), inclusive, das penalidades administrativas nele previstas e consequências cíveis e penais que podem decorrer do seu descumprimento.

Tenho conhecimento sobre a Lei [Nº 13.709/2018](#) ou LGPD – Lei Geral de Proteção de Dados, que é a legislação brasileira que regula as atividades de tratamento de dados pessoais para proteção de dados e da privacidade dos seus cidadãos.

Tenho conhecimento do inteiro teor do [Manual de Controle de Acesso Lógico](#), inclusive dos itens específicos que tratam sobre o tema, como:

Art. 39. O Gestor Técnico é o núcleo da responsável pelo desenvolvimento e manutenção dos softwares e/ou aplicativos que estão no parque tecnológico.

Art. 101. A concessão de acesso aos bancos de dados deverá ser realizada conforme o ambiente em que o colaborador trabalha, ou seja, usuários do ambiente de desenvolvimento não podem acessar bancos de dados em homologação ou produção.

Art. 102. O acesso direto aos bancos de dados deverá ser feito somente pelas equipes responsáveis por manter e dar manutenção nos bancos, conforme o ambiente em que o colaborador atua. Todos os demais colaboradores deverão ter acesso aos dados somente via aplicação.

Art. 103. Todos os acessos realizados diretamente aos bancos de dados serão alterados gradativamente. Procedimento este que fornecerá maior controle nos acessos, além de fornecer uma gravação das sessões.

Tenho conhecimento que algumas modalidades de fraude eletrônica necessitam da facilitação de agentes portadores de privilégios para manipulação de dados em produção.

Tenho ciência que consultas malformadas ou abusivas executadas contra bancos de dados de produção podem degradar a performance dos sistemas dependentes podendo leva-los a indisponibilidade.

Tenho ciência que sou responsável pela revisão dos acessos periódicos dos usuários sob minha responsabilidade, conforme preconizado no Manual de Controle de Acesso Lógico, a saber:

"...§ 2º. A revisão de acessos tem por objetivo evitar acessos indevidos e deverá refletir os direitos de acesso dos usuários, bloqueando qualquer acesso que não seja estritamente necessário ao desempenho de suas funções."

Diante do exposto, necessitamos que ratifique a necessidade do acesso ao ambiente de produção para a execução das atividades desempenhadas pelo(a) solicitante. manifeste ciência, das implicações e penalidades estabelecidas ao usuário pelo uso inadequado do recurso a ele(a) disponibilizado.

Os casos omissos ou não previstos neste Termo de Responsabilidade serão tratados pela Área de Segurança da Informação e Risco Cibernético.

Declaro que estou ciente das determinações acima,

Ciente

Termo de Responsabilidade onde o gestor do dado deve registrar ciência.

Neste caso o usuário solicita via e-mail ao primeiro nível, que encaminha à área técnica responsável pela administração de banco de dados, que submete o pedido à área responsável pela administração de dados que envolve a área de segurança da informação, que envia um termo de ciência ao gestor negocial (responsável pelos dados) e outro termo de responsabilidade ao usuário solicitante.

Constatadas as assinaturas, as respostas voltam o mesmo fluxo, até que a área responsável pela administração de banco de dados implemente a concessão de acesso.

5. JORNADA ATUAL (AS-IS)

A jornada atual do usuário evidencia um processo fragmentado, com múltiplos pontos de contato e baixa previsibilidade.

Etapas principais:

1. Solicitação por e-mail.
O usuário solicita via e-mail à área técnica.
2. Envio de termos.
Após percorridos os trâmites administrativos, os termos são encaminhados ao dono do recurso tecnológico objeto da requisição e ao requisitante.
3. Assinaturas.
Assinados os termos, são devolvidos à área técnica.
4. Conferência manual.
Validadas as assinaturas e que se trata de um requisitante ativo no RH, o fluxo segue para a concessão do acesso.
5. Criação de acesso.
A área técnica concede o acesso ao recurso solicitado.
6. Revogação manual.
O requisitante uma vez desligado da empresa ou remanejado para outro setor deve perder o acesso mediante solicitação de revogação de acesso que parte do gestor negocial.

6. FRICÇÕES IDENTIFICADAS

1. Solicitação sem padrão (fricção de design).
Os e-mails seguem sem muita formalidade.
2. Uso de PDFs e assinaturas (fricção estrutural).
Algumas áreas tem dificuldades com assinatura digital e, no início do processo, alguns termos eram impressos e assinados manualmente, digitalizados e devolvidos.
3. Validação manual de vínculo (failure demand).
A verificação da legitimidade da requisição parte de uma consulta ao RH sobre a sua situação funcional.
4. Falta de integração com sistemas.
5. Revogação manual.

7. DEMANDA DE FALHA (FAILURE DEMAND)

Observou-se incidência significativa de retrabalho no processo.

Principais causas:

- Solicitações incompletas.
E-mails de solicitação eram retornados requerendo justificativas e contextualização, algumas vezes dados pessoais para prosseguimento do fluxo e análise da pertinência e legitimidade da requisição.
- Erros em documentos.
Alguns e-mails e formulários seguiam com dados errados (matrícula, nome do perfil desejado...)
- Falta de padronização. Os dados chegavam de várias maneiras, as vezes no corpo do e-mail, as vezes anexados ao e-mail.
- Validações manuais.
As consultas ao RH eram manuais, sem integração de sistemas.

Avaliando uma janela de um ano de requisições no início do processo dos termos (PDF) e considerando e-mails retornados para solicitação de dados adicionais para viabilizar a análise, foi possível identificar 41% de retrabalho.

8. VIOLAÇÕES DO PRINCÍPIO ONCE-ONLY

- Repetição de dados já existentes no RH.
Em muitos e-mails trocados foi identificada a solicitação de dados que já poderiam ser validados em bases do RH.
- Repetição de autorizações.
O gestor negocial, por vezes, registrava o 'de acordo' mais de uma vez, por e-mail e na assinatura do seu termo.
- Validação manual de vínculo.
- Revogação não automatizada.

9. MÉTRICAS DEFINIDAS

Dimensão	Indicador	
Tempo	Lead time	5,8 dias
VOLume	Interações por solicitação	2,7 e-mails (média)
Qualidade	Taxa de retrabalho	41%

10. PROPOSTA TO-BE (MVP)

Visão geral

Implementação de portal de gestão de acessos integrado a:

- Base de RH
- Active Directory

- Perfis padronizados

Fluxo simplificado

1. Usuário acessa portal
2. Dados são pré-preenchidos
3. Solicitação estruturada
4. Aprovação simplificada
5. Provisionamento automático
6. Revogação automática

Porta de requisição (evidência)

The screenshot displays the 'Gerenciamento Integrado de Serviços de TI' (Integrated IT Service Management) portal. The main interface is titled 'GERIT - Acompanhamento de Incidentes Críticos' and 'Criar Nova Interação'. The form is divided into several sections:

- Interação:** ID da Interação (IT02614474), ID do GTA (1), Tempo de Tratamento (00:00:04).
- Informações do contato:** Matricula, Nome Completo, Cargo, Lotação, Telefone, Email.
- Informações do destinatário do serviço:** Matricula, Nome Completo, Cargo, Lotação, Telefone, Email, Matrônisio (with a filter note: 'Utilize * para filtrar a lista (ex: *28785 para trazer todos que terminam com 28785)'), Notificar por.
- Metadados:** Fase, Status, Status de Aprovação, Categoria, Subcategoria, Área, Grupo Designado, Serviço Metadado, IC Alterado, Impacto, Urgência, Origem, Fonte de Conhecimento, Ambiente, Localização.

o portal de requisição de serviços já encontra-se integrado ao AD e à base do RH, sendo a solução mais interessante para automação do novo fluxo de solicitação e concessão de acesso.

11. DESENHO DO MVP E EXPERIMENTO

Hipóteses

- Redução do tempo de atendimento.
No início do projeto, esperava-se reduzir o lead time para 1 dia.
- Redução de retrabalho.
O retrabalho, as idas e vindas de e-mails solicitando dados complementares, deveria cessar, reduzindo em pelo menos, 50% o retrabalho (os 41% de requisições retornadas deveriam ficar em 20,5%).
- Melhoria da experiência do usuário.
A experiência do usuário não era mensurada antes do portal, mas havia muitas reclamações informais de serviço. O novo portal possui pesquisa de satisfação, a meta era 4 de 5.

Piloto

- Alvo: O início do projeto contemplou apenas áreas técnicas.
- Duração: 30 dias

Métricas

- Lead time
- Retrabalho
- Satisfação do usuário

Critérios de decisão

- Continuar
- Ajustar
- Interromper

12. RISCOS E MITIGAÇÕES

- Integração com sistemas.
A integração com o RH poderia ser um problema, uma vez que seria necessário interagir com APIs proprietárias da solução de RH.
- Resistência à mudança.
A solução do RH estava em fase de transição, gerando certa resistência dos gestores pelo possível impacto no atraso de cronogramas.
- Dados inconsistentes.
Não havia garantias de dados atualizados caso não fosse possível integrar com o RH em tempo de projeto.

13. DECISÕES E TRADE-OFFS

Para viabilizar a implementação do MVP dentro de um escopo controlado e testável, foram adotadas decisões conscientes de redução de complexidade, com impactos positivos e limitações associadas.

• Escopo reduzido para piloto

O redesenho não contempla todos os sistemas e unidades organizacionais do órgão, sendo inicialmente aplicado a um subconjunto representativo.

Trade-off: essa decisão reduz o risco operacional e permite aprendizado rápido, mas limita a generalização imediata dos resultados. A expansão dependerá da validação do piloto.

• Perfis padronizados

Foram adotados perfis de acesso padronizados por sistema, substituindo concessões individualizadas.

Trade-off: há perda de granularidade e flexibilidade em casos específicos, porém ganha-se em escalabilidade, redução de erros e maior clareza para gestores na tomada de decisão.

- **Integração simplificada**

As integrações com a base de RH e o Active Directory foram concebidas de forma simplificada no MVP, priorizando validações essenciais.

Trade-off: reduz o esforço inicial de implementação e acelera o piloto, mas pode exigir evolução futura para lidar com cenários mais complexos (exceções, inconsistências e regras avançadas).

- **Exclusão de funcionalidades avançadas**

Funcionalidades como dashboards analíticos, auditoria avançada e automações adicionais foram deliberadamente excluídas do MVP.

Trade-off: essa decisão permite foco na validação do fluxo principal e entrega rápida de valor, mas adia ganhos adicionais de governança e inteligência operacional para fases posteriores.

14. ONE-PAGER EXECUTIVO

Problema: processo manual e ineficiente

Causa: falta de integração e padronização

Solução: portal integrado com automação

Impacto esperado:

- Redução de tempo
- Redução de retrabalho
- Melhoria da satisfação do usuário

Próximo passo: execução de piloto

15. CONCLUSÃO

O diagnóstico evidenciou um processo ineficiente, com alto retrabalho e riscos operacionais.

O redesenho proposto, baseado em um MVP testável, permite validar melhorias de forma incremental, reduzindo riscos e aumentando a eficiência do serviço.

O trabalho demonstra a importância do foco no usuário e da utilização de abordagens experimentais na transformação digital do setor público.

REFERÊNCIAS

- Lei nº 14.129/2021
- Material da disciplina