

A importância da segurança e privacidade de dados: uma experiência do CREA-SP com a LGPD, Decreto nº 10.278/2020 e MPS-SV

Naje Cavalcante¹, Adriano Albuquerque²

¹FabricaInfo

Rua Livreiro Edésio, 259 - Dionísio Torres, Fortaleza – CE – Brazil

²Universidade de Fortaleza (UNIFOR)

Av. Washington Soares, 1321 - Edson Queiroz, Fortaleza – CE – Brazil

naje@fabricainfo.com, adrianoba@unifor.br

Abstract. *This paper presents an integrated process for document digitization that combines legal compliance with the General Data Protection Law (LGPD), Decree No. 10.278/2020, the compliance to results of MPS-SV related to security, operational efficiency through Artificial Intelligence (AI), and information security. The process was evaluated through a case study carried out at CREA-SP, where 1,747 documents (37,243 pages) were processed.*

Resumo. *Este artigo apresenta um processo integrado para digitalização de documentos que alia a conformidade legal com a Lei Geral de Proteção de Dados (LGPD), o Decreto nº 10.278/2020, a aderência aos resultados esperados relacionados à segurança do MPS-SV, a eficiência operacional por meio de Inteligência Artificial (IA) e a segurança da informação. O processo foi avaliado por meio de um estudo de caso realizado no CREA-SP, onde foram processados 1.747 documentos (37.243 páginas).*

1. Introdução

A transformação digital e a necessidade do serviço de digitalização de documentos são impulsionadas pela busca de eficiência administrativa, redução de custos e conformidade com regulamentações legais. No entanto, as empresas lidam cada vez mais com desafios relacionados com a segurança da informação. Os principais problemas são: (i) Dificuldades em cumprir requisitos legais como o Decreto 10.278/02 e a LGPD (Doneda, 2019; Moraes e Milaré, 2020); (ii) Custos duplos, devido à necessidade de armazenar documentos físicos, mesmo após a digitalização (Paula e Silva, 2020); (iii) Falta de padronização, indexação inadequada, gerando insucesso em 70% dos casos (Mckinsey & Company, 2022); (iv) Incapacidade de sistemas para anonimização de dados de documentos (Goodfellow et al., 2016).

O objetivo deste trabalho foi desenvolver uma proposta para o escaneamento seguro de documentos, utilizando IA e garantindo conformidade com o Decreto 10.278/02 (Brasil, 2020), a LGPD (Brasil, 2018) e que fosse aderente aos resultados esperados do MPS-SV

(Softex, 2024) relacionados à Segurança de Dados, permitindo o descarte legal dos documentos originais.

O presente artigo inicia com esta introdução, depois são apresentados os resultados da revisão de literatura. Na terceira seção apresenta-se o detalhamento do processo, na quarta, o relato do estudo de caso e na última seção são apresentadas as contribuições, limitações e trabalhos futuros.

2. Revisão da Literatura

O Decreto 10.278/2020 estabelece requisitos técnicos para garantir autenticidade, integridade e valor jurídico dos documentos digitalizados, permitindo seu descarte posterior ao processo de digitalização.

No caso da Lei Geral de Proteção de Dados (LGPD), esta exige a proteção de dados sensíveis, via anonimização ou pseudoanonimização, o consentimento explícito para coleta e uso de dados, os direitos dos titulares (acesso, correção, exclusão), a existência de um Encarregado de Dados (DPO) para fiscalizar a conformidade e sistemas de segurança (criptografia, controle de acesso, backups).

A detecção e o tratamento adequado de dados sensíveis são fundamentais para garantir a conformidade com a LGPD e proteger os direitos dos titulares de dados. A adoção de boas práticas, como: criptografia, controle de acesso e anonimização, é crucial para minimizar riscos e garantir a segurança das informações.

O MPS-SV possui o processo “Continuidade, Disponibilidade e Segurança – CDS”, onde há 4 resultados esperados relacionados com Segurança, sendo todos eles obrigatórios no nível C. São eles: CDS 7 - Os riscos da segurança da informação internos e externos são identificados, analisados e tratados em intervalos planejados; CDS 8 - Controles de segurança da informação são definidos, aprovados, implementados e monitorados para atender a política de segurança da informação e os riscos de segurança da informação identificados são tratados; CDS 9 - A eficácia dos controles de segurança da informação é analisada criticamente, monitorada e, quando necessário, são realizadas ações corretivas para os desvios encontrados e CDS10 - Incidentes de segurança da informação são registrados, classificados, priorizados, analisados, tratados, comunicados às partes interessadas e escalonados, quando necessário, levando-se em conta os riscos associados.

3. Processo Proposto

O processo proposto divide-se nas seguintes fases: Arquivística, Digitalização, Indexação, Guarda e Descarte. A seguir são detalhadas cada fase do processo.

a) Arquivística: (1) Pré-processamento - Identificação manual de dados sensíveis, separação de espécies de documento e implantação de RFID nas caixas de documentos para rastreabilidade; (2) Controle de acesso: Implementação de RBAC (Role-Based Access Control) com 5 níveis hierárquicos.

b) Digitalização: (3) Captura de imagens - Resolução de 300 DPI (conforme Decreto 10.278), com validação automática de qualidade via redes neurais convolucionais (CNNs); (4) Anonimização dinâmica - Aplicação de algoritmos de Processamento de Linguagem Natural (NLP) para ofuscar dados sensíveis (precisão: 94%). Para o propósito

do uso de inteligência artificial nos documentos, após inúmeros estudos foi escolhida a ferramenta Gemini, do Google para esta tarefa.

c) Indexação: (5) Extração de metadados - Uso de OCR aprimorado por IA, com estudos sobre (LayoutLM) para campos como data, autor, número de processo, dentre outros; (6) Classificação automática: Estudos sobre o Modelo BERT fine-tuned para categorizar documentos (ex.: contratos, processos administrativos). Depois de análises sobre as ferramentas, também foi verificado que o Gemini, do Google, atende melhor para documentos diversos que a tecnologia LayoutLM, da Microsoft, bem como o BERT, da própria Google.

d) Guarda e Descarte: (7) Criptografia - AES-256 para armazenamento e (8) Eliminação segura - Trituração física com certificação e registro em blockchain

4. Estudo de Caso

O estudo de caso foi realizado no CREA-SP (Conselho Regional de Engenharia e Agronomia de São Paulo), uma autarquia federal com um extenso acervo documental. O objetivo foi avaliar o processo proposto em três dimensões: eficiência processual, qualidade técnica e conformidade legal.

Foi realizado um estudo longitudinal de 6 meses no CREA-SP, onde cada um dos 1.747 documentos (37.243 páginas) foi processado de duas formas independentes: (i) Fluxo tradicional manual (executado por uma equipe de 5 arquivistas experientes) e (ii) Fluxo automatizado com IA (utilizando a solução proposta com Gemini).

Para garantir comparabilidade, ambos os fluxos processaram os mesmos documentos, os operadores do fluxo manual não tiveram acesso aos resultados da IA e foi estabelecido um protocolo de avaliação cego para análise dos resultados. Concomitantemente foi desenvolvido um framework de avaliação com 10 KPIs agrupados em 3 dimensões, conforme podem ser vistas nas Tabelas 1, 2 e 3.

	Manual	IA	Varição
(i) Tempo médio por documento (cronometrado)	126.4	2.7	-97.86%
(ii) Custo operacional total (incluindo horas-homem)	R\$ 9,742.00	R\$ 519.00	-94.67%
(iii) Taxa de retrabalho (documentos rejeitados)	5.80%	3.10%	-46.55%

Tabela 1: Análise comparativa da eficiência processual

	Manual	IA	Varição
(i) Precisão na classificação automática de documentos (validação por 3 especialistas)	97%	92%	-5.15%

(ii) Completude de metadados (checklist de 5 itens por espécie documental)	100%	100%	0.00%
(iii) Taxa de reconhecimento assertivo de metadados	93%	95%	2.15%

Tabela 2: Análise comparativa da qualidade técnica

	Manual	Novo Método	Variação
(i) Aderência ao Decreto 10.278 (escore de 0-100)	5%	100%	-95%
(ii) Eficácia na anonimização de dados sensíveis (LGPD)	0%	94%	-94%
(iii) Eficácia na anonimização de dados pessoais (LGPD)	0%	97%	-97%
(iv) Rastreabilidade dos documentos físicos por RFID	0%	100%	-100%

Tabela 3: Análise comparativa da conformidade legal

Apesar de ganhos na Eficiência Processual e na Qualidade Técnica, o avanço mais significativo ocorreu na Conformidade Legal:

- (i) Aderência ao Decreto 10.278 saltou de 5% para 100% ($p < 0,001$);
- (ii) Anonimização de dados sensíveis alcançou 94% de eficácia;
- (iii) Proteção de dados pessoais atingiu 97% de cobertura
- (iv) Rastreabilidade implementada com 100% de sucesso via RFID.

O estudo de caso mostrou, ainda, que a execução do processo foi capaz de atender plenamente às exigências da LGPD e do Decreto 10.278 e de aumentar a segurança com anonimização, criptografia e rastreabilidade. A aplicação de técnicas de IA resultou na redução de tempo de execução e de erros. Em relação ao MPS-SV, a aderência aos resultados esperados relacionados à segurança deu-se da seguinte maneira:

CDS 7: Gestão de Riscos

Foi estabelecido e mantido um processo formal de gestão de riscos de segurança e privacidade. Como parte deste processo, os riscos associados ao tratamento de dados pessoais e sensíveis foram identificados e analisados. Para tratar o risco específico de vazamento ou acesso indevido a esses dados, a solução adotada foi a implementação de um sistema de IA para pré-processamento, identificação e anonimização. Dessa forma, atende-se ao MPS-SV por demonstrar a existência de um processo proativo de identificação e tratamento de riscos..

CDS 8: Definição de Procedimentos de Segurança

Foram definidos, documentados e aprovados pelos clientes os procedimentos de segurança, atendendo ao resultado esperado do MPS-SV de estabelecer e manter diretrizes operacionais padronizadas. Isso incluiu os procedimentos de detecção e anonimização de dados, a política de RBAC (Controle de Acesso Baseado em Função) para definir acessos, e a classificação de documentos como públicos ou confidenciais. O monitoramento da aderência a esses procedimentos foi realizado por meio da análise de logs de acesso.

CDS 9: Monitoramento Contínuo

Para atender ao requisito de monitoramento contínuo das atividades de segurança, todos os acessos aos dados foram registrados em logs. Estes logs foram monitorados continuamente para detectar acessos por usuários não autorizados e quaisquer outras anomalias. Conforme exigido pela LGPD e alinhado ao MPS-SV, qualquer incidente detectado dava início a um procedimento formal de investigação e mitigação de danos, conduzido pelo DPO, assegurando a pronta resposta a eventos de segurança.

CDS 10: Tratamento de Incidentes

O processo de tratamento de incidentes de segurança foi executado conforme planejado, atendendo ao MPS-SV. O DPO (Encarregado de dados) foi responsável por analisar, registrar e comunicar os incidentes a todas as partes interessadas relevantes. Ademais, as investigações pós-incidente culminaram na definição de ações de melhoria para os processos, fechando o ciclo de melhoria contínua.

5. Conclusão e Trabalhos Futuros

A principal contribuição deste trabalho foi a definição de um processo apoiado por IA, que é a aderente à LGPD, ao Decreto 10.278 e aos resultados esperados do MPS-SV relacionados com segurança, tendo sido avaliado em um caso prático. Como trabalhos futuros, pode-se elencar: (i) Utilizar o processo em empresas de outros setores; (ii) Desenvolver uma ferramenta integrada para atendimento automatizado ao Decreto e LGPD e (iii) Tornar-se aderente às normas ISO 27001 e e-ARQ (gestão arquivística).

Referências

- Doneda, D. Da Privacidade à Proteção de Dados Pessoais. RT, 2019.
- Moraes, L. R. S.; Milaré, É. LGPD Comentada: Lei Geral de Proteção de Dados. RT, 2020.
- Paula, P. A. V.; Silva, L. P. Gestão Documental e Transformação Digital. FGV, 2020.
- Mckinsey & Company. Why Digital Transformations Fail: The Missing Human Factor. 2022.
- Goodfellow, I. et al. Deep Learning. MIT Press, 2016.
- Brasil. Decreto nº 10.278, Diário Oficial da União, Brasília, DF, 2020.
- Brasil. Lei nº 13.709 - Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 2018.
- Softex. Guia Geral: MPS-SV-Modelo de Referência para Serviços. Disponível em: <http://www.softex.br/mpsbr/>. Acessado em 22 abr. 2025