SEGURANÇA DE DADOS E GOVERNANÇA DA INFORMAÇÃO NA ERA DIGITAL: UMA ANÁLISE À LUZ DA LGPD, DOS CIS CONTROLS E DO PPSI

Francisco Carlos de Sousa
Instituto Federal Catarinense – Campus São Bento do Sul
Estudante de ADS – Estácio
E-mail: francisco.sousa@ifc.edu.br, *São Bento do Sul, brasil*

Resumo: A segurança da informação tornou-se um desafio central diante do aumento do uso de tecnologias digitais e do tratamento massivo de dados pessoais. Este trabalho analisa a proteção de dados à luz da LGPD, dos CIS Controls v8 e do Programa de Privacidade e Segurança da Informação (PPSI). A pesquisa evidencia que a adoção integrada de políticas de gestão de ativos, controle de acessos e governança da informação é essencial para mitigar riscos e prevenir incidentes de segurança.

Palavras-chave: Segurança da Informação; Proteção de Dados; LGPD; Governança da Informação; CIS Controls.

INTRODUÇÃO

A transformação digital tem promovido profundas mudanças na forma como organizações públicas e privadas operam, impulsionando a automação de processos, a digitalização de serviços e o uso intensivo de dados. Nesse cenário, os dados pessoais passaram a ser considerados ativos estratégicos, fundamentais para a tomada de decisão, a inovação e a prestação de serviços à sociedade. Entretanto, o aumento do volume de dados tratados também ampliou a superfície de ataque das organizações. Relatórios recentes apontam que uma parcela significativa das violações de segurança ocorre por meio do uso indevido ou roubo de credenciais, evidenciando fragilidades na gestão de contas, ativos e acessos. Diante desse contexto, a segurança da informação deixou de ser apenas uma questão técnica, passando a envolver aspectos legais, organizacionais e estratégicos. No Brasil, a

promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD) representou um marco regulatório ao estabelecer princípios, direitos e deveres relacionados ao tratamento de dados pessoais. Contudo, a efetividade da lei depende da adoção de medidas técnicas e administrativas adequadas, alinhadas a boas práticas e frameworks reconhecidos. Assim, este artigo analisa a segurança de dados na era digital, articulando a LGPD com frameworks internacionais e políticas institucionais brasileiras.

2 Segurança da Informação e Proteção de Dados A segurança da informação pode ser compreendida como o conjunto de práticas, processos e controles destinados a proteger informações contra acessos não autorizados, alterações indevidas, perda ou indisponibilidade. Tradicionalmente, esse conceito está fundamentado nos princípios da confidencialidade, integridade e disponibilidade, frequentemente ampliados para incluir autenticidade e rastreabilidade. No contexto da proteção de dados pessoais, a segurança da informação assume papel central, uma vez que falhas nos controles podem resultar em vazamentos e uso indevido de informações sensíveis. A proteção de dados, portanto, não se limita à adoção de ferramentas tecnológicas, mas envolve políticas organizacionais, definição clara de responsabilidades e conscientização dos usuários.

3 A Lei Geral de Proteção de Dados Pessoais (LGPD) A Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados Pessoais, estabelece diretrizes para o tratamento de dados pessoais no Brasil, aplicáveis tanto ao setor público quanto ao privado. A LGPD tem como objetivo proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade do titular dos dados. Entre seus principais dispositivos, destaca-se o art. 46, que determina que os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas. Dessa forma, a LGPD exige uma postura ativa das organizações em relação à gestão de riscos e à implementação de controles de segurança.

4 Frameworks de Segurança da Informação

4.1 CIS Controls v8 O CIS Controls v8, desenvolvido pelo Center for Internet Security, é um conjunto de controles priorizados que orientam a implementação de medidas práticas de segurança cibernética. Dentre esses controles, destacam-se: Controle 5 – Gestão de Contas: trata da visibilidade, inventário, revisão e proteção de contas de usuários e de serviço; Controle 6 – Gestão do Controle de Acesso: aborda a concessão de acessos baseada em privilégios mínimos e necessidade de uso; Controles 1 e 2: relacionados ao inventário de ativos institucionais e de software. Esses controles reconhecem que credenciais representam o principal vetor de ataque e que sua má gestão compromete a segurança dos sistemas e dos dados.

4.2 Programa de Privacidade e Segurança da Informação (PPSI) No âmbito da Administração Pública Federal, o Programa de Privacidade e Segurança da Informação (PPSI), coordenado pela Secretaria de Governo Digital, estabelece diretrizes e modelos para a implementação da segurança da informação alinhada à LGPD. O Modelo de Política de Gestão de Ativos, em sua versão 2.3, orienta os órgãos públicos quanto à identificação, inventário, classificação, proteção e descarte de ativos de informação. O modelo operacionaliza controles do Guia do Framework de Privacidade e Segurança da Informação, especialmente os Controles 1, 2 e 12, promovendo uma abordagem sistemática de governança da informação e gestão de riscos.

5 Gestão de Ativos, Contas e Controle de Acesso A gestão de ativos de informação é um dos pilares da segurança de dados, uma vez que dados pessoais estão sempre associados a ativos como sistemas, bancos de dados, dispositivos e identidades digitais. Sem um inventário atualizado e uma classificação adequada dos ativos, torna-se inviável aplicar controles de segurança proporcionais ao risco. No que se refere à gestão de contas, práticas como a desativação de contas inativas, a restrição de privilégios administrativos e o uso de autenticação multifator (MFA) são fundamentais para reduzir a superfície de ataque. Contas administrativas, em especial, são alvos prioritários de agentes maliciosos, pois permitem amplo controle sobre sistemas e

dados. A centralização da gestão de identidades e acessos por meio de soluções de Identity and Access Management (IAM) contribui para a padronização de políticas, auditoria de acessos e resposta rápida a incidentes.

6 Modelos Atuais e Boas Práticas em Segurança de Dados Além dos frameworks já citados, outros modelos reforçam as boas práticas em segurança da informação: ISO/IEC 27001: norma internacional que estabelece requisitos para um Sistema de Gestão de Segurança da Informação; NIST Cybersecurity Framework: estrutura baseada em identificar, proteger, detectar, responder e recuperar; Arquitetura Zero Trust: modelo que parte do princípio de que nenhum usuário ou dispositivo deve ser automaticamente confiável. A integração desses modelos permite a adoção de uma abordagem de defesa em profundidade (defense in depth), combinando múltiplas camadas de proteção para reduzir a probabilidade e o impacto de incidentes de segurança.

7 Discussão A análise dos modelos e normativos apresentados evidencia que a proteção efetiva de dados pessoais exige mais do que conformidade legal. É necessário transformar requisitos normativos em práticas operacionais, incorporando a segurança da informação à cultura organizacional. Frameworks como o CIS Controls e políticas institucionais como o PPSI oferecem caminhos práticos para essa transformação, ao detalhar medidas concretas e responsabilidades claras. No entanto, a efetividade dessas iniciativas depende do comprometimento da alta administração e da capacitação contínua dos usuários.

8 Considerações Finais Este artigo demonstrou que a segurança de dados na era digital é um desafio multifacetado, que envolve aspectos técnicos, legais e organizacionais. A LGPD estabelece o marco regulatório, enquanto frameworks internacionais e políticas nacionais fornecem os meios para sua implementação prática. Conclui-se que a adoção integrada de políticas de gestão de ativos, gestão de contas, controle de acesso e governança da informação é essencial para a mitigação de riscos e a proteção dos dados pessoais. Organizações que investem em

segurança de forma estratégica tornam-se mais resilientes, confiáveis e alinhadas às exigências legais e sociais contemporâneas.

MATERIAL E MÉTODOS

A pesquisa caracteriza-se como **qualitativa, exploratória e bibliográfica**, fundamentada na análise de legislações, normas técnicas, frameworks de segurança da informação e documentos institucionais. Foram analisados a Lei Geral de Proteção de Dados Pessoais, os CIS Controls v8 e o Modelo de Política de Gestão de Ativos do Programa de Privacidade e Segurança da Informação (PPSI), além de relatórios técnicos de segurança.

RESULTADOS E DISCUSSÃO

A análise evidenciou que a maioria dos incidentes de segurança está relacionada à má gestão de credenciais e ativos de informação. Os CIS Controls destacam a importância do inventário de ativos, da gestão de contas e do controle de acessos como medidas prioritárias para reduzir a superfície de ataque.

O PPSI, por sua vez, fornece diretrizes práticas para a implementação da segurança da informação no setor público, alinhando-se às exigências da LGPD. A integração entre esses modelos fortalece a governança da informação e contribui para a prevenção de vazamentos de dados e acessos não autorizados.

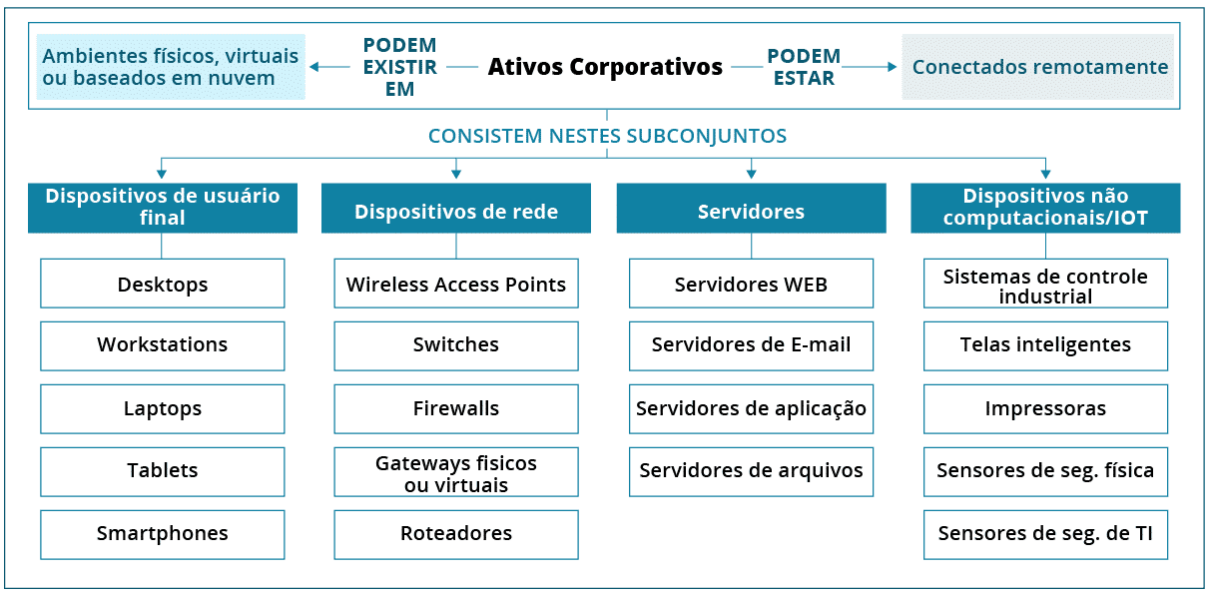


Figura 1. Ativos corporativos. Fonte: Adaptado de CIS (2022).

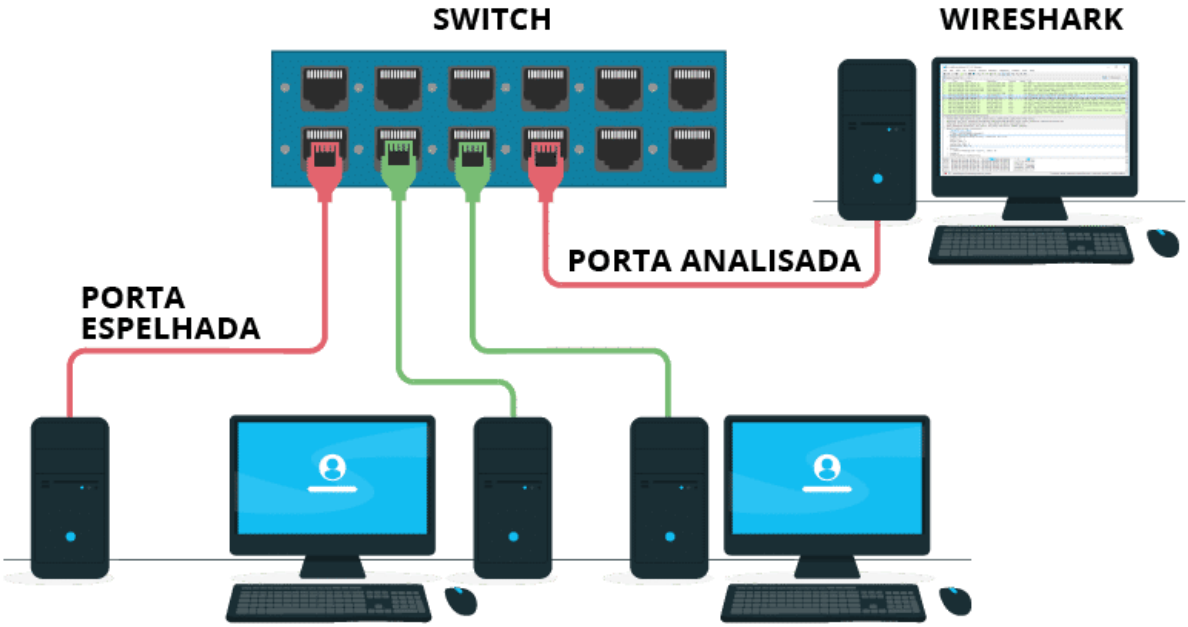
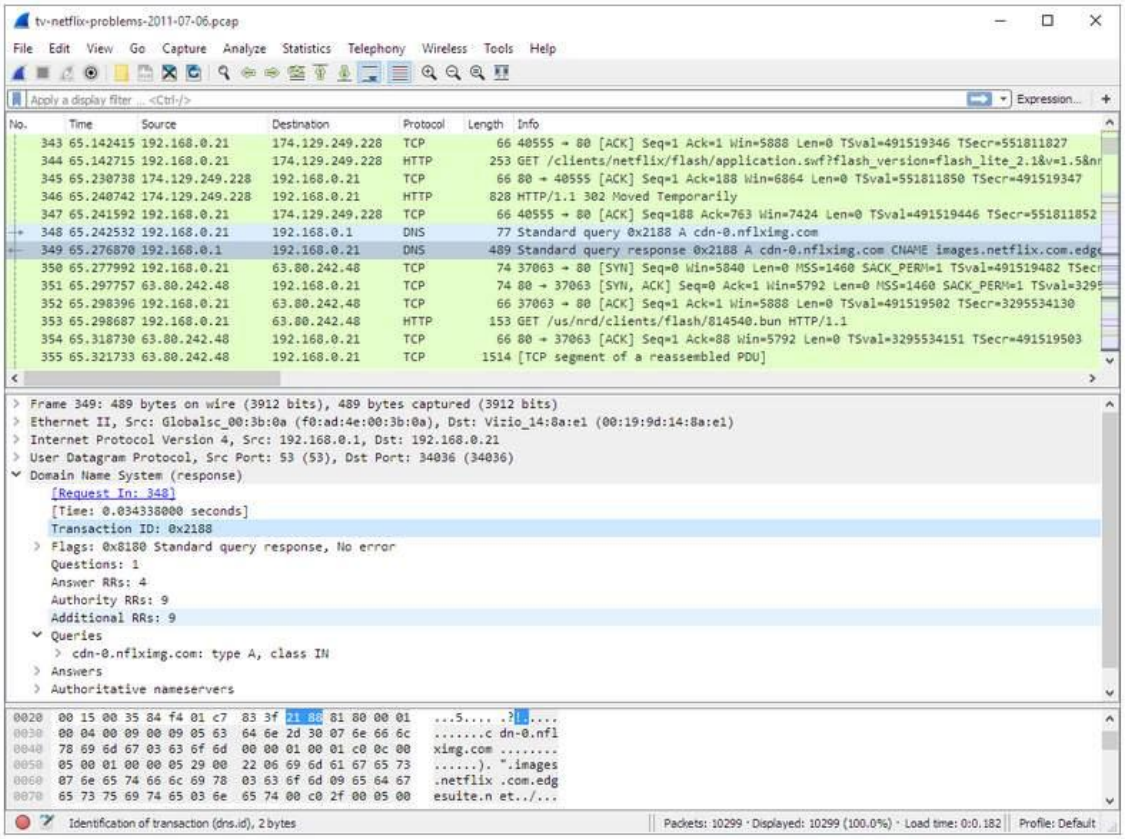
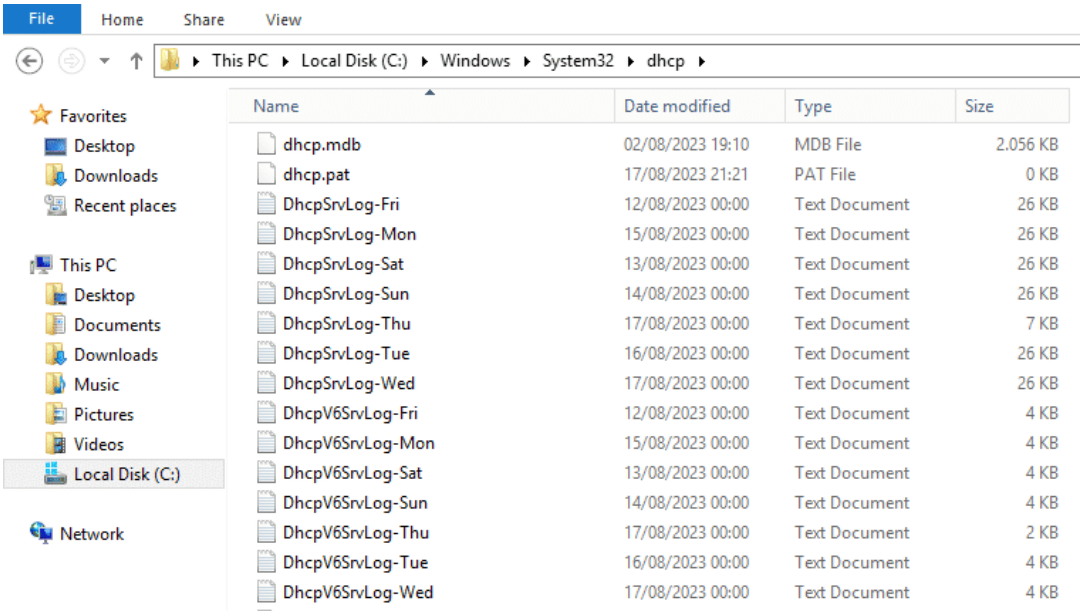


Diagrama básico de um espelhamento de porta. Fonte: Autoria própria.



Tela básica do Wireshark com a coleta dos dados. Fonte: Wireshark ([s. n.]).



Exemplo dos logs DHCP do IPV4 no Windows. Fonte: Autoria própria.

CONCLUSÃO

Conclui-se que a segurança de dados na era digital exige uma abordagem integrada, que combine requisitos legais, frameworks técnicos e políticas institucionais. A adoção de práticas como gestão de ativos, controle de acessos, autenticação multifator e governança da informação é fundamental para a mitigação de riscos e a proteção dos dados pessoais.

AGRADECIMENTOS

Escreva os agradecimentos aqui.

REFERÊNCIAS

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. **Modelo de Política de Gestão de Ativos**. Programa de Privacidade e Segurança da Informação (PPSI), versão 2.3, 2024.

CENTER FOR INTERNET SECURITY. **CIS Controls v8**. 2021.

CHENG, L.; LIU, F.; YAO, D. Enterprise data breach: causes, challenges, prevention, and future directions. *Wires Data Mining and Knowledge Discovery*, v. 7, n. 5, 2017.

IBM. *Cost of a Data Breach Report 2023*. 2023.

THALES. *Data Threat Report – Global Edition*. 2023.