SEGURANÇA DA INFORMAÇÃO E A IMPORTANCIA DA (LGPD)

Letícia Padovan Veloso

Faculdade de Tecnologia de Assis
Leticia.padovan@fatec.sp.gov.br

Prof. Dra. Fernanda Reis da Siva

Faculdade de Tecnologia de Assis
Fernanda.silva193@fatec.sp.gov.br

RESUMO

A segurança da informação, fundamentada na Lei Geral de Proteção de Dados Pessoais (LGPD), destaca-se pela sua importância crucial. Realça-se, assim, a necessidade imperativa de proteger dados digitais contra ameaças cibernéticas e de cumprir rigorosamente as regulamentações legais. Este estudo explora conceitos fundamentais, tais como confidencialidade, integridade e disponibilidade, além de sublinhar a LGPD através de métodos de segurança da informação que são aplicados nos ambientes digitais. Um exemplo notável de método de proteção é o pentest, que enfatiza a necessidade de abordagens proativas para salvaguardar dados num ambiente digital em constante transformação. As considerações finais sublinham a contínua relevância da segurança da informação e a imperiosa necessidade de se cumprir a LGPD na prática, a fim de mitigar os riscos cibernéticos e prevenir vazamentos de dados.

Palavras-chave: Ameaças cibernéticas. Proteção. Acessos não autorizados. Segurança. Confidencialidade. LGPD.

ABSTRACT

Information security, based on the General Data Protection Law (LGPD), stands out for its crucial importance. This highlights the imperative need to protect digital data against cyber threats and to strictly comply with legal regulations. This study explores fundamental concepts, such as confidentiality, integrity and availability, in addition to underlining the LGPD through information security methods that are applied in digital environments. A notable example of a protection method is pretesting, wich emphasizes the need for proactive approaches to safeguarding data in an ever-changing digital environment. The final considerations underline the continued

Keywords: Cyber threats. Protection. Unauthorized access. Security. Confidentiality.

1 INTRODUÇÃO

Todo mundo está envolvido com a Segurança da Informação, muitas vezes por meio de contramedidas de segurança. Essas contramedidas são, por vezes, impostas por normas regulatórias, e às vezes implementadas por meio de normas internas. Considere, por exemplo, o uso de senha em um computador. Nós normalmente vemos tais medidas como um incômodo, uma vez que elas tomam o nosso tempo e nem sempre compreendemos do que elas nos protegem conforme dito por Hintzberen, 2015.

A proteção das informações é fundamental para garantir a segurança dos dados digitais, construir a credibilidade dos clientes e atender às normas legais. Com o progresso tecnológico e a crescente quantidade de informações compartilhadas *online*, a segurança dos dados se torna cada vez mais prioritária (IBM, 2023).

A Segurança da Informação abrange uma ampla gama de medidas e práticas projetadas para guardar Informações confidenciais, desde dados pessoais até segredos comerciais e governamentais. Nesta introdução, serão explorados os princípios fundamentais da proteção, sua importância crescente e as ameaças que a rodeiam, além de destacar a necessidade de implementar estratégias para proteger os seus dados digitais**.** Num mundo digital onde as ameaças cibernéticas são uma preocupação constante, proteger-se de acessos não autorizados é essencial para o sucesso e a sustentabilidade do seu negócio (IBM, 2023).

A segurança da informação é um campo multidisciplinar que engloba tecnologia, políticas, práticas e conscientização para proteger informações vitais contra ameaças internas e externas. Esta área ganhou destaque com a iniciação da era digital, onde dados são os recursos mais valiosos para usuários, empresas e governos. Aqui estão alguns pontos importantes e a serem considerados: Confidencialidade, Integridade e Disponibilidade, Ameaças, Políticas e Procedimentos, Tecnologia de Segurança (Hintzberen, 2015).

Se está vivendo um mundo de constante e acelerada circulação de informações e dados. Diante de intensas rotinas e com o mundo digital ganhando espaço em nossos ambientes, acabamos nos adaptando às novas realidades

sem dimensionar muitos dos impactos que cercam a virtualização ou digitalização de processos conforme Hoepers (2020).

> A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n° 13.709/2018, foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade, e a livre formação da personalidade de cada indivíduo. A Lei fala sobre o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado, englobando um amplo conjunto de operações que podem ocorrer em meios manuais ou digitais (Gov.br, 2018).

No âmbito da LGPD, o tratamento dos dados pessoais pode ser realizado por dois agentes de tratamento – o Controlador e o Operador. Além deles, há a figura do Encarregado, que é a pessoa indicada pelo Controlador para atuar como canal de comunicação entre o Controlador, o Operador, os(as) titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

2 CONCEITOS UTILIZADOS EM SEGURANÇA DA INFORMAÇÃO

É necessário ter um sistema documentado onde os ativos e processos de Segurança da Informação, identificados e descritos. Todo e qualquer ativo ou processo de segurança da informação deve ser atribuído a pessoas. Essas pessoas devem ser competentes para as atribuições dadas. Além disso, a coordenação e a supervisão dos aspectos de Segurança da Informação referentes ao relacionamento com os fornecedores devem ser identificadas e documentadas por Hintzberen (2015).

O Encarregado da Segurança da Informação (*Information Security officer - iso*) desenvolve a política de segurança da informação de uma unidade de negócio com base na política da empresa e assegura que ela seja seguida. Gerente de Segurança da Informação (*Information Security Manager – ISM*) desenvolve a política de segurança da informação dentro da organização de TI e assegura que ela seja seguida.

Além dessas funções, que são especificamente voltadas para a Segurança da Informação, uma organização pode ter um Encarregado da Política de Segurança da Informação (*Information Security Policy Officer*) ou um Encarregado da Proteção de Dados (*Data Protection Officer*) Hintzberen, 2015.

O conceito de privacidade de dados e sua relevância são temas com grande importância. a privacidade de dados representa um dos fundamentos da segurança da informação, concentrando-se na preservação da confidencialidade das informações pertencentes a uma empresa e seus clientes. Isso é alcançado por meio de um tratamento apropriado que habilita a empresa a cumprir com as regulamentações em vigor de acordo com TOTVS (2021).

O *pentest* também conhecido como "teste de invasão". É uma prática de segurança cibernética na qual os especialistas em segurança simulam ataques cibernéticos contra sistemas de computadores, redes ou aplicativos para identificar e explorar vulnerabilidades de segurança que possam ser exploradas por invasores reais (Almeida Jr., 2021).

2.1 SEGURANÇA DA INFORMAÇÃO E SUA CAPACIDADE ESTRATÉGICA DE PROTEÇÃO

Para reduzir as chances de exploração do sistema, o teste de penetração pode ser empregado para avaliar a capacidade de proteção do sistema e sua infraestrutura. Uma validação de segurança ofensiva pode descobrir, antes de um atacante, uma vulnerabilidade que acarretaria grandes prejuízos para a instituição. Além disso, o teste de invasão pode ajudar a proteger os controles de segurança (Almeida Jr., 2021).

> Pode parecer que não, mas o teste de invasão é uma atividade de defesa, pois ele geralmente é feito em ambiente controlado e ultimamente tem se mostrado essencial por diversos motivo. Esses métodos são para tentar impedir os crimes virtuais que são resultado desde processo evolutivo e despreparado da internet, pois, à medida que avançavam os métodos de propagação e transferência de dados pela rede, muitos usuários acabam se esquecendo de atribuir um método de proteção voltado à segurança dos usuários (Almeida Jr., 2021).

> O comado banner grabbing3, ou, em português, captura de banners, é uma técnica usada para recolher informações sobre um sistema de computador em uma rede e os serviços em execução em suas portas abertas (Fraga, 2018). Os administradores podem usar isso para fazer um inventário dos sistemas e serviços em sua rede. No entanto, um intruso pode usar o Banner Grabbing a fim de encontrar host de rede que estão executando versões de aplicativos e sistema

> operacionais com explorações conhecida alguns exemplos de portas de serviço usadas para captura de banner são aquelas usadas pelo HTTP (Protocolo de Transferência de Texto), o FTP (Protocolo de Transferência de Arquivos) e o SMTP (Protocolo de Transferência de Correio Simples) – portas 80, 21 e 25, respectivamente. Ferramentas comumente usadas para realizar a captura de banners são telnet que está incluída na maioria dos sistemas operacionais, e o netcat. (Fraga, 2018).

a aplicação de testes de invasão e técnicas como o banner grabbing são cruciais para a manutenção da segurança cibernética. Através dessas práticas, é possível identificar e mitigar vulnerabilidades antes que possam ser exploradas por atacantes mal-intencionados, garantindo assim a integridade e a proteção dos sistemas e dados das organizações. A constante evolução das ameaças digitais exige um esforço contínuo e proativo por parte dos administradores de sistemas para que estejam sempre um passo à frente dos possíveis invasores. Portanto, a implementação de tais medidas não apenas fortalece a segurança, mas também assegura a confiança e a continuidade das operações em um ambiente digital cada vez mais complexo e desafiador.

2.2 CONCEITOS DE SEGURANÇA

Para entender como a segurança pode ser gerenciada, diversos conceitos importantes devem ser explicados primeiro. “Vulnerabilidade”, “ameaça”, “risco” e “exposição” são termos frequentemente usados para representar a mesma coisa, mesmo que tenham diferentes significados e relações entre si; é importante entender a definição de cada palavra, mas mais importante ainda é entender as suas relações com outros conceitos. Antes de começarmos a definir uma estratégia de segurança, precisamos saber o que estamos protegendo e do que estamos protegendo. A metodologia que se empregou para ajudar a obter algum conhecimento sobre isso é chamada de análise do risco. Existem várias formas de realizar uma análise do risco (Hintzberen, 2015).

A segurança da informação é alcançada pelo meio da implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Esses controles precisam ser estabelecidos, implementados, monitorados,

revisados e melhorados, onde necessário, para assegurar que os objetivos específicos de segurança e do negócio da organização sejam atendidos. Isso deve ser feito em conjunto com outros processos de gerenciamento de negócio para definir, alcançar, manter e melhorar a segurança da informação pode ser essencial para manter a vantagem competitiva, o fluxo de caixa, a rentabilidade, a observância da lei e a imagem comercial (Hintzberen, 2015).

2.3 Á SEGURANÇA DA INFORMAÇÃO E A LEI GERAL DE PROTEÇÃO DE DADOS

Com a aplicação apenas a polícia federal contra o tratamento ilegal de dados pessoais realizados por qualquer pessoa, seja natural ou jurídica de direito público ou privado. Abrangência total. Havendo seu descumprimento, sempre incidirá a LGPD, exceto o artigo 4º (não incidência). Objetivo = proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. A Lei se propõe em dar um equilíbrio a relação jurídica existente entre as partes a fim de sejam observados pelos responsáveis pelo tratamento. (Hoepers, 2020)

Em que pese a LGPD ter por expresso em seu fundamento o direito à privacidade, é perceptível que a proteção de dados pessoais ultrapassa esse âmbito (pessoal), compreendendo questões coletivas, ao passo que determinados danos causados pelo tratamento indevido de dados, em razão de sua própria natureza, porquanto difusos, exigem uma tutela jurídica coletiva pormenorizada e específica. (Hoepers, 2020)

A disciplina da proteção de dados pessoais tem como fundamentos:

I - O respeito à privacidade;

II - A autodeterminação informativa;

III - A liberdade de expressão, de informação, de comunicação e de opinião;

IV - A inviolabilidade da intimidade, da honra e da imagem;

V - O desenvolvimento econômico e tecnológico e a inovação;

VI - A livre iniciativa, a livre concorrência e a defesa do consumidor; e
VII Os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (Gov.br, 2018)

> Este artigo prevê de forma taxativa as hipóteses de transferência internacional dos dados de titulares, e algumas delas são interessantes abordar. O primeiro inciso tem como finalidade garantir a proteção de dados, inclusive, fora do país, uma vez que tais dados sairão de uma base nacional. Assim, a transferência internacional dos dados apenas será permitida e estará em regularidade com a lei se for para países que tiverem uma lei de proteção de dados parecida com a nossa, no sentido de proteção e segurança. Logo, se os dados forem transmitidos para um país europeu que aplica a GDPR, esta transação está em conformidade com a regra, porém se a transferência dos dados para um estado dos Estados Unidos que possui uma lei de proteção de dados mais branda, tal transferência está irregular, por exemplo. Ademais, o artigo, no segundo inciso, traz uma alternativa para a transferência de dados internacionais quando o país onde passarão esses dados não tiver uma lei rigorosa e bem estruturada que garanta adequada proteção. (Hoepers, 2020)

a Lei Geral de Proteção de Dados (LGPD) desempenha um papel fundamental na proteção dos direitos de privacidade e liberdade dos indivíduos, ao mesmo tempo em que promove um equilíbrio nas relações jurídicas envolvendo o tratamento de dados pessoais. A abrangência da LGPD vai além da esfera individual, englobando também aspectos coletivos que demandam uma proteção jurídica detalhada e específica. A disciplina da proteção de dados pessoais é sustentada por princípios como o respeito à privacidade, a autodeterminação informativa e a inviolabilidade da intimidade, além de promover o desenvolvimento econômico e tecnológico. A transferência internacional de dados é cuidadosamente regulada para assegurar que os dados dos titulares estejam protegidos de acordo com padrões equivalentes de segurança, garantindo assim a conformidade e a proteção global.

3 METODOLOGIA

A metodologia adota uma abordagem qualiquantitativa, combinando elementos de pesquisa qualitativa e quantitativa para oferecer uma análise abrangente. A revisão bibliográfica permitiu identificar as principais práticas e tendências na área de segurança da informação, além de destacar a importância da conformidade com a LGPD para mitigar riscos cibernéticos.

3.1 FONTE DE PESQUISA

Para garantir uma ampla compreensão do tema, foram selecionadas diversas fontes de informação, incluindo:

Livros: As obras de referência que abordam conceitos fundamentais e avançados sobre segurança da informação e legislação relacionada à proteção de dados que foram *Pentest* em aplicações wev: Avalie a segurança contra ataques, Tecnologias e Educação: Representações sociais na sociedade da informação, Fundamentos de Segurança da Informação, LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: Estudo direcionado e comentado da Lei Geral de Proteção de Dados, Técnicas de Invasão.

3.2 PROCEDIMENTOS DE COLETA DE DADOS

A coleta de dados seguiu um roteiro estruturado, dividido em várias etapas:

Levantamento Inicial: Identificação de palavras-chave relevantes, como "segurança da informação", "LGPD", "proteção de dados", "cibe segurança", entre outras. A busca foi realizada em bases de dados acadêmicas e bibliotecas digitais. Seleção de Fontes: Avaliação da relevância e qualidade das fontes encontradas. Revisão Crítica: Leitura e análise crítica dos textos selecionados, destacando os principais pontos, debates e conclusões apresentados pelos autores.

Os resultados da coleta de dados revelaram várias tendências e insights importantes:

- Importância da Conformidade com a LGPD: A maioria dos estudos ressaltou a necessidade crucial de conformidade com a LGPD para garantir a proteção dos dados pessoais e evitar penalidades legais.
- Práticas de Segurança da Informação: Foram identificadas várias práticas recomendadas para a proteção de dados, incluindo o uso de firewalls, criptografia e testes de penetração (pentest).
- Desafios em Ambientes Digitais: Os autores destacaram os desafios contínuos enfrentados pelas organizações na proteção de dados em um ambiente digital em constante evolução, incluindo a adaptação a novas ameaças cibernéticas e a implementação de medidas proativas de segurança.
- Abordagens Proativas: A necessidade de abordagens proativas foi enfatizada, com várias fontes recomendando a implementação de políticas de segurança contínuas e treinamentos regulares para funcionários.

3.3 PROCEDIMENTOS DE ANÁLISE DE DADOS

Análise de Conteúdo: Os textos foram examinados para extrair categorias temáticas relevantes, como as ameaças à segurança da informação, as medidas de proteção recomendadas e os impactos legais da LGPD.

Comparação e Integração de Dados: As informações coletadas de diferentes fontes foram comparadas e integradas para construir uma visão coesa e abrangente do tema.

4 CONSIDERAÇÕES FINAIS

Neste trabalho, examinamos a importância da segurança da informação com base na LGPD em um cenário digital cada vez mais complexo e interconectado. Destacamos a necessidade crucial de proteger os dados digitais contra ameaças cibernéticas, garantir a confidencialidade, integridade e disponibilidade das informações, além de cumprir as regulamentações legais e normativas que a lei Geral de Proteção de Dados (LGPD).

Baseamos nossas analises em diversas fontes acadêmicas e essas referências forneceram insights valiosos sobre os princípios e práticas fundamentais de segurança da informação, bem como as diretrizes e padrões reconhecidos internacionalmente para o gerenciamento eficaz da segurança da informação.

Reconhecemos que a segurança da informação é um desafio em constante evolução, com novas ameaças surgindo e regularmente e exigindo respostas adaptativas e proativas. Portanto, é essencial que as organizações adotem uma abordagem abrangente e multifacetada para a segurança da informação, e usando a LGPD para orientar, integrando tecnologias de segurança robustas, políticas e procedimentos claros, além de promover uma cultura organizacional de conscientização e responsabilidade em relação à segurança da informação.

À medida que avançamos em um ambiente digital cada vez mais dinâmico e interconectado, a segurança da informação tem que se orientar nos direitos para não errar conforme a LGPD, continuará sendo uma prioridade crítica para organizações de todos os setores. Ao adotar uma abordagem proativa e baseada em melhores práticas para a segurança da informação, as organizações podem mitigar efetivamente os riscos cibernéticos e proteger os ativos mais valiosos: seus dados.

5 REFERÊNCIAS

ALMEIDA JR., José Augusto. **Pentest em aplicações wev**: Avalie a segurança contra ataques. Rua Vergueiro, 3185 - 8º andar 04101-300 – Vila Mariana – São Paulo – SP – Brasil: Casa do Código, 2021.

BERNARDINO, Fernada Amaral. **Tecnologias e Educação**: R**epresentações sociais na sociedade da informação**. Editora e Livraria Appris Ltda. Rua José Tomasi, 924 - Santa Felicidade Curitiba/PR - CEP: 82015-630 Tel: (41) 3156-4731 | (41) 3030-4570: Annris, 2013.

BM, Ibm. **Soluções de segurança: proteção de dados. Proteja dados críticos,** 2023. Disponível em: https://www.ibm.com/br-pt/data-security?utm_content=SRCWW&p1=Search&p4=43700078893192521&p5=p&gad_source=1&gclid=Cj0KCQjwwYSwBhDcARIsAOyL0fi5xfnCWRIv9Tiyl1H4ms56F8EeadSF60T3ZTByaDediJEHLxWvoZ0aApwrEALw_wcB&gclsrc=aw.ds. Acesso em: 20 mar. 2024.

FRAGA, Bruno. **Técnicas de Invasão**. São Paulo: Labrador., 2018. 387 p.

GOV.BR, Gov. **Lei Geral de Proteção de Dados Pessoais (LGPD**). A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n° 13.709/2018,, 2018. Disponível em: https://www.gov.br/esporte/pt-br/acesso-a-informacao/lgpd. Acesso em: 20 mar. 2024.

HINTZBEREN, Jule; HINTZBEREN, Kees ; SMULDERS, Andre ; BAARS, Hasns. **Fundamentos de Segurança da Informação: com base na iso 27001**. 3. ed. Rua Teodoro da Silva, 536 A – Vila Isabel 20560-001 Rio de Janeiro-RJ: BRASport, 2015.

HOEPERS, Fabricio; ROTH, Gabriela; ROCHA, Gustavo; HAAG, Luciana Dornelles; CAVALCANTI, Ricardo De Lima; PAIVA, Sabrina Martins; AYRES, Samantha Sobrosa; REVERBEL, Valentine; BERNARDI, Vitória**. LEI GERAL DE PROTEÇÃO DE DADOS ESSOAIS: Estudo direcionado e comentado da Lei Geral de Proteção de Dados**. PORTO ALEGRE: COMISSÃO DE DIREITO DA TECNOLOGIA E INOVAÇÃO DA OAB/RS, 2020. 61 p.