SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE: CONSCIENTIZAÇÃO E CAPACITAÇÃO DO FATOR HUMANO COMO ESTRATÉGIA DE MITIGAÇÃO DE RISCOS EM UMA INSTITUIÇÃO FEDERAL DE ENSINO SUPERIOR (IFES)

INFORMATION SECURITY AND PRIVACY: AWARENESS AND TRAINING OF THE HUMAN FACTOR AS A RISK MITIGATION STRATEGY IN A FEDERAL INSTITUTION OF HIGHER EDUCATION (IFES)

ÁREA TEMÁTICA: SEGURANÇA DA INFORMAÇÃO

Amarildo Maia Rolim, Universidade de Brasília, Brasil, amarildo.rolim@sti.ufc.br

Virgínia de Melo Dantas Trinks, Universidade de Brasília, Brasil, vividantasnatal@gmail.com

…

RESUMO

O objetivo deste trabalho é apresentar uma contextualização baseada em pesquisas bibliográficas, artigos e normativos do Governo Federal, demonstrar a importância da mitigação dos riscos em Segurança da Informação e Privacidade através da capacitação e conscientização do fator humano em uma Instituição Federal de Ensino Superior. Considerando que há recomendações e orientações do Governo Federal para que os servidores estejam capacitados para lidar com a privacidade e segurança da informação, essa pesquisa buscou ainda, identificar dentro deste cenário, as ações do Governo Federal que reforcem a importância de se trabalhar os riscos que envolvem o fator humano e de estar em conformidade com essas recomendações. A capacitação dos responsáveis pelo tratamento de dados é tão importante quanto a implementação de políticas e recursos tecnológicos de segurança. Por isso, a conscientização e o treinamento dos operadores de dados e porque não dizer de toda comunidade Universitária são fundamentais. O atual cenário mostrado nesse estudo comprova que o ser humano pode ser visto como a maior barreira ou a maior fragilidade da Instituição. Ou seja, mesmo com grande investimento em tecnologias, os seres humanos ainda podem causar fragilidades nos sistemas de informação. Isso ocorre pela própria natureza humana que é propensa a erros, como clicar em links maliciosos, digitar senhas inseguras e fornecer informações pessoais a terceiros não autorizados. Assim, os resultados deste estudo evidenciam que o Governo Federal deve se adaptar às melhores práticas de Segurança da Informação e Privacidade, ficando clara a importância da mitigação dos riscos envolvidos no que diz respeito ao fator humano através de estratégias de capacitação e conscientização.

Palavras-chave: Privacidade. Conformidade. Capacitação.

ABSTRACT

This work aims to present a contextualization based on bibliographic research, articles, and Federal Government regulations, demonstrating the importance of mitigating Information Security and Privacy risks through training and awareness of the human factor in a Federal Higher Education Institution. Considering that the Federal Government has recommendations and guidelines for staff to be trained to deal with privacy and information security, this research also sought to identify, within this scenario, Federal Government actions that reinforce the importance of addressing risks involving the human factor and complying with these recommendations. Training those responsible for data processing is as important as implementing security policies and technological resources. Therefore, data operators' awareness and training and the entire university community are essential. The current scenario presented in this study proves that human beings can be seen as the institution's most significant barrier or greatest weakness. In other words, even with significant investment in technology, humans can still cause weaknesses in information systems. This is due to human nature, which is prone to errors such as clicking on malicious links, entering insecure passwords, and providing personal information to unauthorized third parties. Therefore, the results of this study highlight that the Federal Government must adapt to best practices in Information Security and Privacy, highlighting the importance of mitigating the risks involved concerning the human factor through training and awareness strategies.

1 INTRODUÇÃO

Com a evolução das tecnologias digitais, habilidades, conhecimentos e competências são características imprescindíveis para a realização das atividades diárias sem colocar em risco a segurança das informações das organizações. Segundo Fontes (2017), a informação seja qual for sua forma, representa um recurso valioso para a empresa. Em contrapartida, a cultura de valorização das informações não acompanha o mesmo ritmo, especialmente em empresas de pequeno e médio porte, ao contrário, caminha a passos lentos.

Para Eleuterio (2015), o uso das tecnologias da informação (TI) tem sido reconhecido como uma importante ferramenta para as organizações nos níveis estratégicos. Castilho (2018) contribui ao afirmar que as TIC são populares, estão em todos os lugares, estão em casa, nos escritórios, nas escolas, em todas as organizações. Portanto, uma Instituição Federal de Ensino Superior utiliza-se dessas tecnologias em seus processos internos, tornando-os mais eficientes, possibilitando um aumento da qualidade dos serviços oferecidos à sociedade.

Considerando esse novo cenário de transformação digital, que para a IBM (2024), é uma iniciativa estratégica que visa integrar tecnologia em todas as áreas de uma empresa, buscando avaliar e modernizar os processos, os produtos, as operações e o stack de tecnologia de uma organização para viabilizar uma inovação contínua, rápida e voltada para o cliente. Assim, as instituições de ensino superior passam por uma grande transformação impulsionada pela revolução tecnológica que vem transformando a educação nas últimas décadas. Essa transformação digital traz grandes desafios, pois redefine a forma como os estudantes aprendem, os professores ensinam e as instituições trabalham.

É nesse novo cenário que surge a preocupação com a garantia da proteção dessas informações. O grande desafio, portanto, é manter em segurança a informação, por todo o seu ciclo de vida e em conformidade com as Leis e Normativos.

Com a promulgação da Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n° 13.709/2018, esse desafio aumenta, pois, incluem a necessidade de adequação tecnológica e de processos, a falta de recursos para implementação e treinamento, a complexidade da legislação e a necessidade de manter a conformidade de forma contínua. Ademais, a exigência de conformidade com regulamentações legais demanda a adoção de padrões rigorosos de proteção de dados, sem comprometer a eficiência operacional, o que se tem mostrado uma tarefa desafiadora (Fayayola; Olorunfemi; Shoetan, 2024).

A necessidade de proteção das informações surge portanto com o grande fluxo de informações tratadas em um ambiente de uma IFES acrescida da utilização de novas tecnologias. Esse aumento no fluxo de dados impõe desafios significativos a empresas privadas e públicas, que precisam adotar medidas robustas para gerenciar e proteger essas informações de maneira eficaz (Saraswat; Meel,2022).

Embora as ameaças externas estejam presentes e sejam, muitas vezes, ponto principal de discussão, as ameaças internas também representam um risco significativo às Instituições e podem assumir várias formas, incluindo pessoas internas que involuntariamente ou inadvertidamente, comprometem a segurança através da negligência no momento da realização do tratamento das informações. Portanto, estratégias para mitigação dos riscos devem ser elaboradas trabalhando não somente fatores técnicos, mas fatores humanos com a sensibilização e capacitação de todos. Complementa Moraes (2019), esses riscos exigem atitudes conscientes e proativas por parte dos gestores, no que se refere à segurança das informações corporativas, de seus clientes, colaboradores e fornecedores.

Um novo estudo divulgado pela Mimecast (2025) revelou um dado alarmante sobre segurança da informação: 95% das falhas de segurança registadas em 2024 foram causadas por erro humano. Realizado entre 1.100 profissionais da área de Tecnologia da Informação e Segurança da Informação, revela que mesmo com investimento de bilhões em novas tecnologias, os incidentes com dados continuam acontecendo, em especial decorrentes de falhas dos próprios funcionários. Portanto os riscos envolvendo tecnologia foram superados pelo risco humano. Este cenário torna-se então desafiador quando os ataques estão cada dia mais sofisticados. Por outro lado, o estudo demonstra que os líderes de segurança desenvolveram sua estratégia no ano passado para lidar melhor com o risco humano.

Outra contribuição de Mimecast (2025), é a comprovação de que o treinamento e conscientização sobre segurança ajudou os funcionários a identificar ataques cibernéticos na maioria das organizações (87%), mas 66% ainda estão preocupados que a perda de dados de pessoas internas aumentará em 2025, e 33% ainda temem erros humanos no tratamento de ameaças por e-mail. Ao passo que apenas 8% dos funcionários são responsáveis por 80% dos incidentes. Assim, as soluções de Gestão de Riscos Humanos visam equilibrar inovação e produtividade com melhores estratégias de prevenção, em vez de depender apenas da remediação pós-incidente. Essa mudança reconhece que a conscientização sobre segurança por si só não é suficiente e que as organizações precisam de uma plataforma de Gestão de Riscos Humanos para lidar com o problema.

Um estudo da Verizon em 2021, “Data Breach Investigations Report” (DBIR) mostra que a maioria das violações de dados, como “ransomware” e “phishing”, envolve um fator humano, e ainda, das violações de dados contabilizadas no ano de 2020, 85% envolveram algum tipo de interação humana.

Diante do exposto, as pessoas envolvidas no tratamento de dados e informações nas organizações não acompanham a evolução das novas tecnologias e desconhecem normas e procedimentos a serem seguidos, assim, fica evidente que esse desconhecimento muitas vezes é ocasionado pela falta de divulgação das normas e a oferta de capacitação, que, em muitos casos torna-se uma porta de entrada para possíveis ataques. A vulnerabilidade do indivíduo no ciberespaço e a proteção da informação pessoal nas relações comerciais passaram a ficar em evidência (Siqueira, Contin, Barufi & Lehfeld, 2021).

A falta de conhecimento das pessoas sobre as Leis e Normativos deixa o ambiente institucional propício a ataques que irão utilizar a vulnerabilidade humana. Para Fonseca (2009), é necessário orientar os colaboradores a cumprir essas regras, garantindo que todos entendam o motivo de cada normativa e se sintam comprometidos com a segurança da informação. Complementa Dantas (2011), a fuga das informações e a sua exposição involuntária ocorrem em momentos simples do dia a dia da empresa, o que torna os recursos humanos uma das maiores preocupações para a implementação de políticas e treinamentos voltados para a proteção das informações.

Para Dourado Alves (2016) as ações devem fazer com que as pessoas compreendam e respeitem as políticas e princípios de segurança da informação, sejam conscientizadas da sua responsabilidade pela proteção das informações e encorajadas a praticar a segurança em suas operações diárias.

Portanto, esse novo momento vem corroborar com a necessidade de um programa permanente de conscientização e capacitação dos colaboradores envolvidos no tratamento de dados pessoais nas IFES. Uma vez que há este risco, a preocupação de como as informações são manipuladas entre os usuários em uma rede,torna necessário tomada de medidas que visam a segurança da informação (COELHO; RASMA; MORALES, 2013).

Diante do exposto, é objetivo deste estudo demonstrar a importância de um Programa de Capacitação e Conscientização como estratégia para mitigação dos riscos que envolvem o fator humano em uma Instituição Federal de Ensino Superior.

Adicionalmente, como objetivos específicos, busca-se:

1. Destacar a relevância das ações de capacitação e conscientização, garantindo que todos os usuários sejam devidamente treinados e compreendam suas responsabilidades no que se refere à segurança da informação;
2. Mostrar o alinhamento das ações de capacitação e conscientização com os normativos do Governo Federal e o Programa de Privacidade e Segurança da Informação (PPSI).

Para Moreira, Santana e Miranda (2014) os estudos sobre a tecnologia da informação têm despertado a atenção de pesquisadores, por sua ampla disseminação nos diversos ambientes organizacionais, com ampla abrangência, explorando diversos aspectos relativos aos seus impactos, que podem ser percebidos nas organizações a partir da introdução da tecnologia de informação. Consequentemente, as instituições de ensino superior enfrentam o desafio de estarem preparadas para enfrentar os desafios relativos à segurança da informação e privacidade das informações que estão sob sua custódia. Ao final deste estudo, espera-se contribuições que sirvam de subsídio para o fortalecimento das ações de capacitação e conscientização em segurança da informação e privacidade, consolidando uma cultura institucional orientada pela proteção de dados e resiliência operacional. Não menos importante, contribuir mostrando ainda a necessidade da conformidade, seja em leis, normas ou padrões, pois a conformidade também auxilia e muitas vezes guia a gestão de riscos.

O presente trabalho segue a estrutura básica de um artigo, estando dividido em XX seções onde inicialmente o tema e a contextualização do estudo é apresentado na introdução. A seção-2 traz o referencial teórico, que visa nortear um alinhamento conceitual acerca da Segurança da Informação e o Fator Humano. Na seção-3 a metodologia empregada para se atingir o objetivo do estudo e na seção-4 os resultados obtidos com as discussões, e por fim, as conclusões na seção-5.

2 REFERENCIAL TEÓRICO

No cenário descrito onde o mundo encontra-se conectado e as informações são compartilhadas em tempo real, considerando ainda a conformidade com os normativos do Governo Federal, a Segurança da Informação (SI) torna-se um tema crucial para as Instituições. O aumento da conectividade demanda cuidados frente às ameaças às quais se expõem os sistemas de informação e comunicação, especialmente quando conectados à rede mundial de computadores (UNIVERSIDADE DE BRASÍLIA, 2010, p. 27).

Para IBM (2024), a Segurança da informação (InfoSec) é a proteção de informações importantes contra acesso não autorizado, divulgação, uso, alteração ou interrupção. Ajuda a garantir que os dados organizacionais confidenciais estejam disponíveis para usuários autorizados, permaneçam confidenciais e mantenham sua integridade.

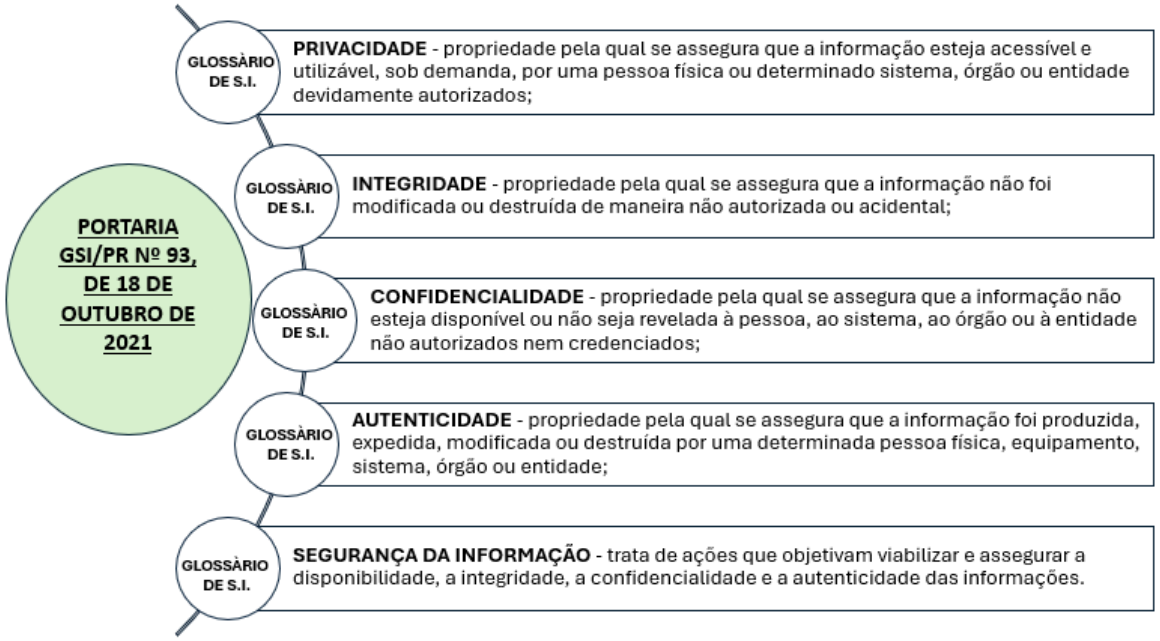
O que se percebe, portanto, é que a informação possui um grande valor para as organizações públicas e privadas, por este motivo, é de suma importância sua proteção contra ameaças. Nesse sentido, para as organizações, a informação se tornou um bem de valor inestimável, e a implementação de sistemas que abordam as vulnerabilidades emergentes é crucial para o seu bom funcionamento (Coutinho *et al*., 2017).

Em Brasil (2018), a Política Nacional de Segurança da Informação (PNSI) define em seu escopo os pilares da Segurança da Informação como: disponibilidade, integridade,

confidencialidade e a autenticidade da informação a nível nacional. É importante destacar que as melhores práticas em Segurança da Informação devem começar com a própria gestão da Instituição. Como ponto de partida é crucial para todo o processo que seja elaborada e aprovada pela gestão superior uma Política de Segurança da Informação contendo todas as diretrizes a serem seguidas pela totalidade de profissionais envolvidos com as atividades do órgão, sejam funcionários efetivos, terceirizados e fornecedores.

Os conceitos básicos de Segurança da Informação podem ser encontrados no Glossário de Segurança da Informação do Governo Federal (Brasil, 2021), como mostra a Figura 1:

Figura 1 - Conceitos básicos de Segurança da Informação



Fonte: Adaptação Brasil (2021)

Em Brasil (2022), a Cartilha de Gestão em Segurança da Informação do Gabinete de Segurança Institucional afirma que a segurança da informação deve ser uma prioridade nos órgãos da Administração Pública Federal. Assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade dos seus ativos de informação, em particular aqueles que, na atual conjuntura dos serviços digitais, são suscetíveis a incidentes cibernéticos.

A segurança da informação é uma responsabilidade compartilhada. Ao entendermos e gerenciarmos os riscos de forma proativa, podemos proteger melhor nossos ativos digitais e garantir a continuidade dos negócios. Contamos com a colaboração de todos para manter nossa organização segura. Neste estudo, o fator humano foi abordado do ponto de vista das vulnerabilidades que, conforme Sêmola (2014), podem ser divididas em físicas, naturais, *hardware*, *software*, mídia, comunicação e humanas. O autor ainda afirma que as vulnerabilidades são falhas que, por si sós, não provocam incidentes, por serem elementos passivos que dependem de um agente que as explore, tornando-as ameaças para a segurança.

Dessa forma, mitigar os riscos é o objetivo da Segurança da Informação, diminuindo assim a probabilidade de ocorrência de um incidente de segurança e como consequência ocasionar impacto negativo sobre a continuidade do negócio.

Quando tratamos do comportamento humano em Segurança da Informação, estamos considerando um potencial para ataques que resultem em incidentes. A dificuldade é

exatamente a mudança de comportamentos em virtude de situações a que são submetidos. Essa situação ocorre muitas vezes por não saber como proceder em algumas situações, essa incapacidade então é explorada pelas ameaças de SI. A maioria dos problemas em TI e sistemas de informação origina-se de ações humanas, tornando os humanos fatores críticos que afetam a eficácia da segurança da informação (Safianu; Twum; B., 2016).

De acordo com a Kaspersky (2024), os riscos por estar online estão se tornando altamente severos para as empresas. Nos últimos dois anos, 77% das empresas sofreram pelo menos um incidente cibernético. Por isso, é compreensível que as organizações queiram implementar medidas para mitigar esses riscos. Idem, o uso inapropriado de recursos de TI e a violações de segurança de TI cometidas por funcionários foram duas das maiores ameaças experimentadas pelas empresas, com um custo médio por incidente de USD 337.561,00.

O relatório *The Global Risks Report* (World Economic Forum (WEF), 2022), publicado pelo Fórum Econômico Mundial, destaca a prevalência de problemas de cibersegurança relacionados a erros humanos, onde aproximadamente 95% dos problemas nesse domínio são atribuídos a falhas humanas, enquanto ameaças internas a empresas, sejam intencionais ou acidentais, contribuem para 43% de todas as violações.

Lyra (2015, p. 47) reforça a importância desse fator, indicando que

> "A cooperação dos usuários é essencial para a eficácia da segurança. Eles exercem um forte impacto sobre a confidencialidade, a integridade e a disponibilidade da informação, pois, por exemplo, o usuário que não mantiver a confidencialidade da senha, não evitar o registro dela em papéis que não estão guardados em locais seguros, não utilizar senhas de qualidade ou ainda que compartilhe senhas individuais, compromete a segurança da informação."

Esses riscos podem ser minimizados através da criação de políticas, normas e procedimentos. Destaca-se, porém, que, sua efetividade é condicionada a divulgação e a compreensão podendo ser resolvido com treinamentos e conscientização constantes.

Importante destacar que a Constituição Federal Brasileira estabelece em seu art. 37 que,

> "a administração pública, em todas as suas esferas, direta e indireta, de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios, obedecerá aos princípios da legalidade, impessoalidade, moralidade, publicidade e eficiência. O princípio da legalidade, neste contexto, significa que a administração pública só pode atuar quando houver previsão legal para tanto, ou seja, ela está vinculada à lei e só pode fazer o que a lei permite ou determina".

Em um estudo realizado com dados da plataforma *Egress Prevent* (EGRESS, 2021) aponta que o erro humano é o gatilho mais comum para seus prompts de prevenção de perda de dados em tempo real. Sendo o fator humano a causa mais comum citada, portanto, essa situação demonstra preocupação para a segurança da informação, estando diretamente ligado à falta de conhecimento sobre boas práticas de segurança.

De acordo com Camillo & Hess (2020), à medida que o cenário de ameaças cibernéticas cresce e evolui, as organizações resilientes serão aquelas que enfrentarem as ameaças contemplando nível tecnológico sem deixar de lado o comportamento humano, fazer com que as pessoas trabalhem de forma colaborativa e que tenha a participação de todos.Como visto, além de uma boa infraestrutura de proteção de dados, outra vertente que requer atenção redobrada é o fator humano, em nossa era digital a informação tem um valor altíssimo, mas paralelo a essa situação encontramos os riscos de vazamento que aumentam em

escala exponencial. O tratamento deste risco pode ser iniciado com uma cultura sedimentada de valorização das informações.

Para a IBM (2024), no sentido mais simples, uma ameaça à cibersegurança, ou ameaça cibernética, é uma indicação de que um hacker ou agente mal-intencionado está tentando obter acesso não autorizado a uma rede para lançar um ataque cibernético.

Como exemplos comuns de ameaças, encontramos o ataque de engenharia social, que manipula psicologicamente a pessoa, explorando fraquezas humanas para obter informações confidenciais, acesso não autorizado a sistemas e redes corporativas (Salahdine; Kaabouch (2019). Outra ameaça, é a técnica de phishing, predominante nos ataques de engenharia social, tem por objetivo a descoberta de informações pessoais, financeiras ou credenciais de login, muitas vezes por meio de mensagens eletrônicas fraudulentas (Jain; Gupta, 2022). Essas mensagens frequentemente se passam por comunicações legítimas de instituições confiáveis, como bancos, lojas online, serviços de e-mail e redes sociais.

No entendimento da IBM (2024), frequentemente chamada de "hacking humano", a engenharia social manipula os alvos para que tomem ações que exponham informações confidenciais, ameacem o bem-estar financeiro próprio ou de sua organização ou comprometam a segurança pessoal ou organizacional. O phishing é a forma mais conhecida e difundida de engenharia social. O phishing usa e-mails, anexos de e-mails, mensagens de texto ou chamadas telefônicas fraudulentas para induzir pessoas a compartilhar dados pessoais ou credenciais de login, fazer download de malware, enviar dinheiro para cibercriminosos ou realizar outras ações que as deixem expostas a crimes cibernéticos.

Dentro desse cenário, a prevenção contra ataques de engenharia social se torna um componente crítico da estratégia e segurança de dados nas IFES. Ou seja, é fundamental a prevenção de ataques de engenharia social através da adoção de medidas eficazes de prevenção como a capacitação e conscientização.

Para Gabbay (2003) há dois tipos de classificação para ameaças:

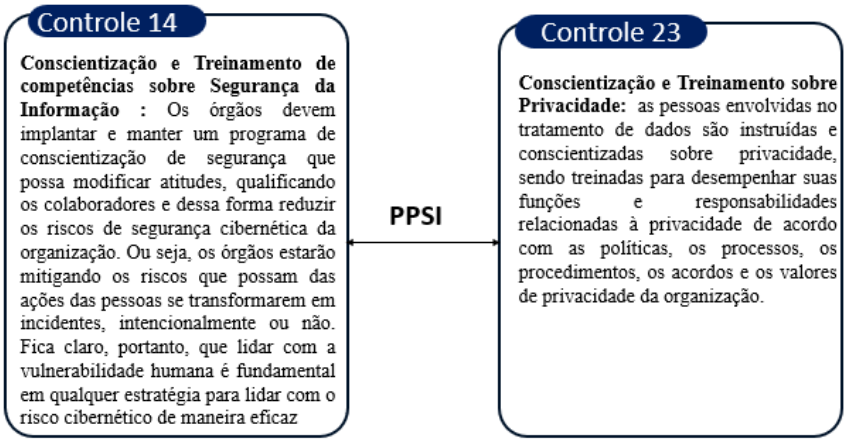
1) Internas - geralmente os responsáveis por danos causados internamente são funcionários insatisfeitos, que querem prejudicar o desenvolvimento do trabalho ou tirar vantagens financeiras. Outros responsáveis são prestadores de serviços e funcionários terceirizados. Como exemplo de ameaças internas destacam-se o roubo de informações, a alteração ou destruição de informações, os danos físicos a hardware e alteração de configurações e danos lógicos à rede;
2) Externas - são aquelas causadas por indivíduos que não pertencem a organização e/ou que estão efetuando ataques remotamente. Seus objetivos variam desde indisponibilizar serviços ou máquinas até roubar informações sigilosas.

O Governo Federal demonstra preocupação com os riscos causados pelo comportamento humano quando lança em 2021 o Programa de Privacidade e Segurança da Informação (PPSI), com objetivo de melhorar a maturidade e a resiliência dos órgãos e entidades do SISP, dentro da temática segurança da informação e privacidade. Em seu conteúdo, encontramos dentre os denominados eixos de atuação do PPSI, o eixo Pessoas, responsável por fomentar ações que visam promover a mudança cultural em todos os níveis da estrutura organizacional dos órgãos e entidades, por meio de sensibilização, conscientização e capacitação visando o adequado uso dos recursos de tecnologia da informação e na execução dos processos de trabalho referente à temática (Brasil, 2021). Esse eixo então reforça ainda mais a necessidade de um programa de capacitação e conscientização

sobre o tema, além de mostrar a necessidade da conformidade com as ações do Governo Federal.

De fato, ao analisar os controles ou medidas que devem ser implementadas para proteção dos dados e informações, abrangendo temáticas como segurança cibernética, proteção de dados e privacidade, encontramos dois controles específicos para o eixo pessoas, como mostra a figura 2:

Figura 02 - PPSI - Controles para o eixo pessoas



Fonte: Adaptação Brasil 2021

Por sua vez, a Conscientização e Treinamento sobre Privacidade (Controle 23) segue o que determina o art. 50 da LGPD, os controladores e operadores, no âmbito de suas competências, devem aplicar medidas educativas periódicas apropriadas para as pessoas que têm acesso aos dados pessoais (Brasil, 2018). Complementa, o programa de treinamento em privacidade deve:

a) Implementar e manter uma estratégia abrangente de treinamento e conscientização destinada a garantir que o pessoal entenda suas responsabilidades e procedimentos de proteção de dados pessoais;
b) Criar mecanismos para manter o pessoal com responsabilidades de proteção de dados pessoais atualizado sobre os desenvolvimentos no ambiente regulatório, contratual e tecnológico que possam afetar a conformidade de privacidade pela organização;
c) Administrar treinamento básico e direcionado de proteção dados pessoais com base em funções, regularmente (por exemplo, anual) ou conforme necessário (por exemplo, após um incidente);
d) Garantir que o pessoal certifique (manualmente ou eletronicamente) a aceitação das responsabilidades pelos requisitos de proteção de dados pessoais periodicamente;
e) Incluir a conscientização sobre notificação de incidentes para assegurar que membros relevantes estejam cientes das possíveis consequências para a organização (por exemplo, consequências legais, perda de negócios e dano à imagem).

Outra ação do Governo Federal que vem contribuir com a importância da temática estudada foi a criação do Centro de Excelência em Privacidade e Segurança da Informação do Governo Digital, que tem como missão promover a cultura de privacidade e segurança da informação nos órgãos e entidades da administração pública federal direta, autárquica e fundacional, melhorando assim as habilidades dos servidores públicos federais.

Não menos importante, o Governo Federal ainda reafirma a preocupação com o fator humano, quando publica a Política Nacional de Segurança da Informação (PNSI) (Brasil, 2018) e traz em seu arcabouço:

a) Art. 3º, são princípios da PNSI - a educação como alicerce fundamental para o fomento da cultura em segurança da informação;
b) Art. 4º São objetivos da PNSI - fomentar a formação e a qualificação dos recursos humanos necessários à área de segurança da informação. Ou seja, define como necessidade a existência de controles para proteção da informação e que esses controles sejam efetivados e revisados, considerando o valor da informação para a organização, assegurando dessa forma os pilares listados acima.

Por fim, a conformidade com o PPSI é então crucial para a garantia da segurança e da privacidade durante as atividades relacionadas ao tratamento de dados de forma legal. Portanto, estar em conformidade com o PPSI significa a valorização e execução de um programa que vise a mudança de atitude das pessoas através da capacitação e conscientização.

2.1 Lei Geral de Proteção de Dados

Destaca-se ainda que no Brasil, a Lei Geral de Proteção de Dados (LGPD) entrou em vigor em 2018, inspirada no conjunto de leis e regulamentos sobre a proteção de dados da União Europeia. (Assis e Mendes, 2019). O que existe e persiste até os dias atuais é a preocupação no mundo inteiro de como dados pessoais são coletados e utilizados sem regulamentação alguma (DIVINO, 2019). Para evitar sanções regulatórias e impulsionar o crescimento do cliente, as empresas que gerem dados devem adotar as melhores práticas para desenvolver e manter um programa eficaz de proteção de dados (PIURCOSKY et at., 2019).

A LGPD traz claramente quais são os fundamentos relacionados à proteção de dados pessoais, que devem servir para nortear toda e qualquer ação que envolva seu tratamento, como mostra a figura 3. São eles:

Figura-3 Fundamentos da LGPD

Fonte: Cartilha Lei Geral de Proteção de Dados Pessoais – DNIT (2021)

Elaborada com dez capítulos que totalizam 65 artigos, a LGPD, esclarece os principais conceitos envolvidos durante todo o processo de coleta, tratamento e armazenamento de dados pessoais:

a) Finalidade: a realização do tratamento deve ocorrer para propósitos legítimos, específicos, explícitos e informados ao(à) titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
b) Adequação: a compatibilidade do tratamento deve ocorrer conforme as finalidades informadas ao(à) titular, de acordo com o contexto do tratamento;
c) Necessidade: o tratamento deve se limitar à realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
d) Livre acesso: é a garantia dada aos(às) titulares de consulta livre, de forma facilitada e gratuita, à forma e à duração do tratamento, bem como à integralidade de seus dados pessoais;
e) Qualidade dos dados: é a garantia dada aos(às) titulares de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
f) Transparência: é a garantia dada aos(às) titulares de que terão informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
g) Segurança: trata-se da utilização de medidas técnicas e administrativas qualificadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
h) Prevenção: compreende a adoção de medidas para prevenir a ocorrência de danos por causa do tratamento de dados pessoais;
i) Não discriminação: sustenta que o tratamento dos dados não pode ser realizado para fins discriminatórios, ilícitos ou abusivos;
j) Responsabilização e prestação de contas: demonstração, pelo Controlador ou pelo Operador, de todas as medidas eficazes e capazes de comprovar o cumprimento da lei e a eficácia das medidas aplicadas.

Um ponto importante da LGPD e que começa a quebrar paradigmas na coleta de dados é explicitado por Oliveira et al. (2019), apenas os dados que servem a um propósito deliberadamente iniciado e garantem controle e transparência nas atividades de processamento entre controladores e processadores de dados devem ser coletados. Necessário ainda o entendimento de todos os que são responsáveis pelo tratamento de dados pessoas dos conceitos definidos pela LGPD, esses conceitos devem ser trabalhados nos treinamentos pois estão diretamente ligados aos níveis de cuidado que os operadores de dados devem ter e que muitas vezes não possuem nenhum entendimento e nem conhecem as consequências de um vazamento.

Um conceito em especial merece atenção no âmbito da LGPD, o consentimento, definido como um acordo explícito, inequívoco e concedido livremente por um titular de dados para permitir o processamento de seus dados pessoais. Para Leme e Blank (2020) é fundamental o consentimento qualificado do titular dos dados sensíveis para o seu tratamento, e também a utilização de sistemas digitais seguros como meios de proteger os direitos fundamentais da pessoa. A LGPD estabelece, de maneira clara, o que são dados pessoais, priorizando a finalidade e necessidade da sua utilização, quesitos de tratamento que devem ser previamente informados ao cidadão. Outro entendimento importante é que os titulares de dados têm direito a: aprovação de que seja realizado tratamento dos dados e que sejam anonimizados, acesso e retificação, bloqueio e descarte, anulação do consentimento, portabilidade, informação sobre os dados distribuídos, entendimento sobre a destinação, de

não consentimento e ter ciência sobre o que pode acontecer, além da reavaliação de decisões automatizadas (DIVINO, 2019).

A LGPD tem sua aplicação unificada para empresas de qualquer porte, portanto, torna-se necessário o ímpeto em aplicar segurança tecnológica para evitar violações às disposições legais. [Hussain et al. 2020]. Porém, torna-se crucial para a conformidade da Lei, entender seus impactos práticos nas atividades de tratamento de dados. Então, para entender esses impactos é necessário conhecer o que é importante e necessário para realização das atividades diárias dos operadores de dados.

Segundo Paulo (2021), alcançar a conformidade com a LGPD implica em promover a transparência, um princípio fundamental que é respaldado pela Constituição brasileira, que já estipulava o direito das pessoas de terem acesso às suas próprias informações de forma detalhada e em linguagem clara. Então, a LGPD reforça esse direito, determinando que quem realiza o tratamento de dados pessoais deve deixar claro suas finalidades de tratamento. A lei caracteriza como primordial uma boa comunicação e disponibilização de informações aos titulares de dados (proprietários dos dados pessoais) sobre a coleta, utilização e tempo de retenção dos dados pessoais processados (ROCHA et al. 2019).

Como órgão fiscalizador a Autoridade Nacional de Proteção de Dados (ANPD) é responsável por fiscalizar o cumprimento da LGPD, além da fiscalização, a ANPD ainda é responsável pela aplicação de multas e sanções para as organizações que cometem infrações. Podendo ser uma simples advertência ou multa com limite de R$50 milhões (Lopes & Amaral 2022).

De acordo com a Vert (2019), a LGPD requer que as organizações adotem uma cultura que valorize as informações. Além de soluções tecnológicas, é necessário estabelecer uma estrutura de governança de dados que envolva toda a empresa. Percebe-se, portanto, que é fundamental que os funcionários compreendam a importância dos dados e assumam a responsabilidade pelo seu tratamento. Ou seja, é necessário o envolvimento dos funcionários na adoção dessas mudanças, visto que, a conformidade com a referida lei não deve ser vista apenas como uma obrigação regulatória, mas sim uma questão estratégica. Um dos principais desafios para as instituições é a promoção de uma mudança cultural interna em relação ao tratamento de dados pessoais, o que demanda tempo e investimentos financeiros, alcançar a conformidade com a LGPD implica em transformações que não são simples, nem céleres (Crespo, 2021).

A LGPD em seu art. 50° estabelece regras e boas práticas de governança sobre segurança de proteção de dados:

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais (BRASIL, 2018).

Em Brasil (2023), a Autoridade Nacional de Proteção de Dados (ANPD) entende que o tratamento de dados pessoais pelo Poder Público possui muitas peculiaridades, que decorrem, em geral, da necessidade de compatibilização entre o exercício de prerrogativas estatais típicas e os princípios, regras e direitos estabelecidos na Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018 – lgpd).

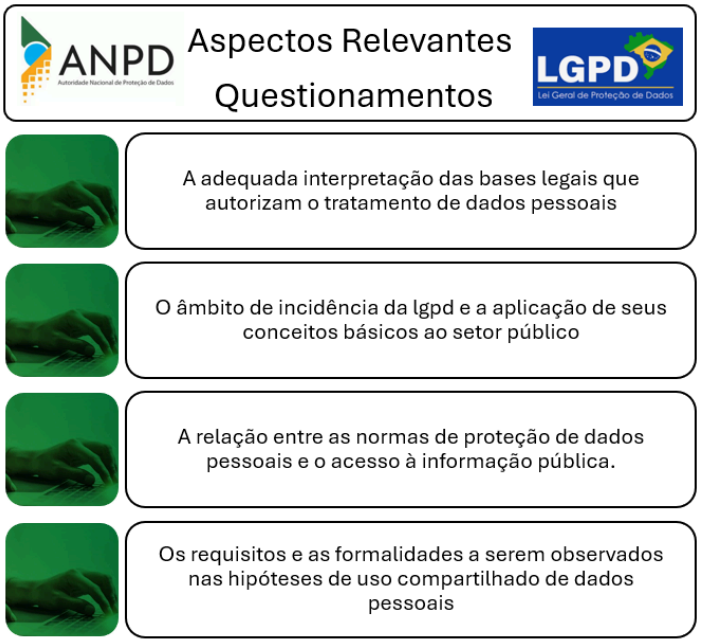
Portanto, a capacitação dos operadores de dados de uma IFES em relação à LGPD (Lei Geral de Proteção de Dados) é crucial para garantir a conformidade com a lei e a segurança dos dados pessoais. A capacitação deve abranger conceitos da LGPD, direitos dos titulares, medidas de segurança, procedimentos em casos de incidentes e responsabilidades dos operadores. A LGPD exige que os operadores sigam práticas de transparência e responsabilidade, garantindo a proteção dos dados pessoais e construindo confiança com os titulares.

2.2 Lgpd na Administração Pública Federal (APF)

Não diferente das outras organizações, a Administração Pública Federal (APF) e nesse contexto são inseridas as Instituições Federais de Ensino Superior (IFES) enfrentam as mesmas questões relativas à grande difusão no uso da internet, principalmente com a oferta de serviços digitais, com um grande fluxo de informações compartilhadas da própria APF e dados pessoais que são de titulares que se utilizam dos serviços oferecidos. É inegável a transformação que a internet trouxe, diminuindo distâncias, rápida difusão de informação dentre outras vantagens, o que a torna imprescindível nas relações humanas, sendo, portanto, essencial que a APF siga o caminho da inovação, conectada e participando dessa onda de transformação mundial.

De acordo com Brasil (2023), entre outros aspectos relevantes, muitos órgãos e entidades públicas têm questionado a Autoridade Nacional de Proteção de Dados (ANPD) sobre alguns aspectos relevantes como mostra a figura 4:

Figura 4 - Aspectos Relevantes Questionados a ANPD



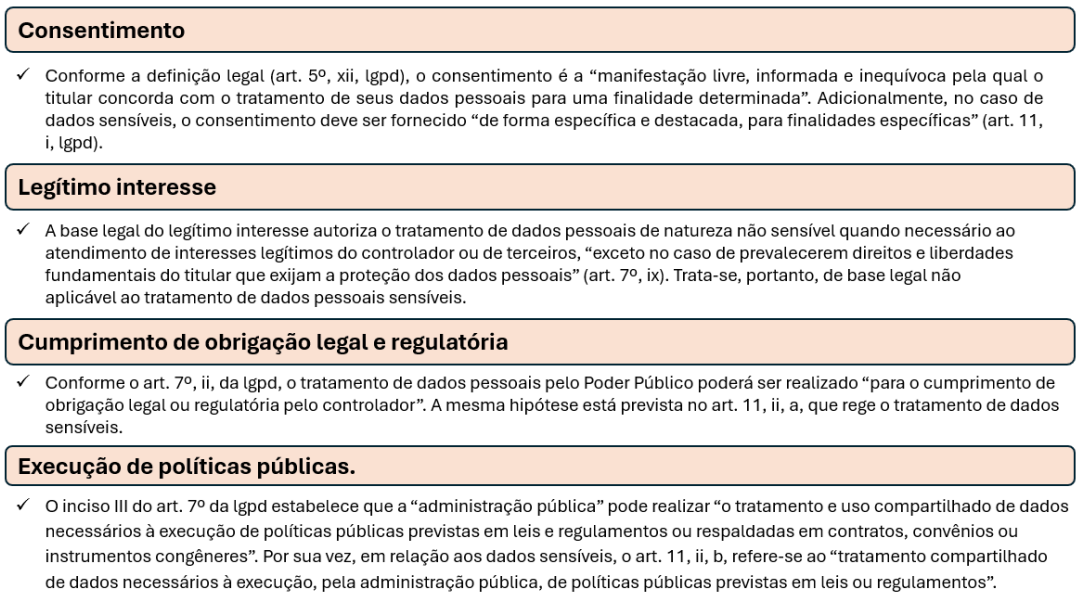
Fonte: Adaptação de Brasil (2023)

Especificamente em relação ao Poder Público, a lgpd (art. 55–J, xi e xvi) prevê que a ANPD pode solicitar informe específico sobre o âmbito, a natureza dos dados e demais detalhes envolvidos na operação, bem como realizar auditorias sobre o tratamento de dados pessoais. O art. 52, § 3°, estabelece que as sanções podem ser aplicadas às entidades e aos órgãos públicos, com expressa exclusão das penalidades de multa simples ou diária. (BRASIL, 2023).

Ponto de partida para o tratamento de dados pelo setor público é a identificação da base legal aplicável. Ou seja, o tratamento de dados pessoais pelo Poder Público deve se amparar em uma das hipóteses previstas no art. 7º ou, no caso de dados sensíveis, no art. 11 da LGPD. Esses dispositivos devem ser interpretados em conjunto e de forma sistemática com os critérios adicionais previstos no art. 23, que complementam e auxiliam a interpretação e a aplicação prática das bases legais no âmbito do Poder Público.

Brasil (2023) explica que considerando os questionamentos encaminhados à ANPD e as peculiaridades do tratamento de dados pessoais pelo Poder Público, bem como o previsto na Agenda Regulatória do biênio 2021–2022[6], a análise pode ser limitada às seguintes bases legais como mostra a figura 5:

Figura 5 - Tratamento de Dados Pessoais Pelo Poder Público - Bases Legais



Fonte: Adaptação de Brasil (2023)

Para a Autoridade Nacional de Proteção de Dados, o conceito de políticas públicas não é definido na LGPD, não tendo sido editada regulamentação sobre o tema até o presente momento. Em Brasil (2023) encontramos que a recomendação é que sejam consideradas as definições usuais do termo, conforme a praxe administrativa considerando ao menos, dois aspectos, a existência de ato formal que institui a política pública, o que pode ocorrer mediante ato normativo (lei ou regulamento) ou por ajustes contratuais (contratos, convênios e instrumentos congêneres).

Como descrito pela ANPD, a LGPD não fez referência às políticas públicas instituídas em ajustes contratuais, art. 11, I, b. Por isso, no caso de tratamento de dados sensíveis pelo Poder Público, a base legal é mais restrita, uma vez limitada a políticas públicas previstas em "leis e regulamentos".

A ANPD ainda caracteriza no aspecto material, uma política pública como um programa ou ação governamental específica, a ser executada por uma entidade ou por um órgão público. Maria Paula Dallari Bucci contribui com o tema ao destacar que, "como tipo ideal, a política pública deve visar a realização de objetivos definidos, expressando a seleção de prioridades, a reserva de meios necessários à sua consecução e o intervalo de tempo em que se espera o atingimento dos resultados.

Portanto, para a ANPD o conceito de política pública deve ser interpretado de forma ampla, de modo a abranger qualquer programa ou ação governamental, definido em instrumento formal, isto é, lei, regulamento ou ajuste contratual, conforme o caso, cujo conteúdo inclui, em regra, objetivos, metas, prazos e meios de execução.

Por fim, também na hipótese de execução de política pública deve ser observado o disposto no art. 23 da LGPD, em especial a exigência de que o tratamento seja realizado para o atendimento da finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público.

Apesar de publicada em 2018, a LGPD no Brasil, somente entrou em vigor em sua quase totalidade em agosto de 2020 e em agosto de 2021 os arts. 52, 53 e 54 entraram em vigor, protegendo as pessoas da comercialização e utilização indevida de dados pessoais. Assim, em agosto de 2018, foi promulgada a Lei nº 13.709, Lei Geral de Proteção de Dados ("LGPD") com a finalidade de unificar as disposições relativas ao assunto, criar conceitos importantes, hipóteses de tratamento de dados, penalidades para o caso de descumprimento, criar a autoridade de fiscalização, entre outros (BRASIL, 2018). Desta feita, encontra-se definido em seu conteúdo conceitos importantes como mostra a figura 6:

Figura 6 - Conceitos importantes da LGPD

DADO PESSOAL	DADO PESSOAL SENSIVEL	TITULAR DOS DADOS	TRATAMENTO
• (art. 5º, I), Dado Pessoal - informação relativa a uma pessoa física identificada ou identificável, ainda que incidentalmente revelada. É considerada identificável uma pessoa física que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador (considerado "informação confidencial"), como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica, hábitos de consumo ou a um ou mais elementos específicos da identidade física, econômica, cultural ou social dessa pessoa física (BRASIL, 2018).	• (art. 5º, II), Dado pessoal sensível - é uma categoria especial de dado sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. Ou seja, dados pessoais da esfera íntima do titular de dado, que possam gerar preconceitos ou discriminação, se revelados (BRASIL, 2018).	• (art. 5º, V), Titular dos dados pessoais - será toda pessoa física identificada ou identificável, a quem se referem os dados pessoais que são objeto de tratamento, como por exemplo os empregados de uma empresa, seus clientes pessoa física, fornecedores etc. (BRASIL, 2018).	• (art. 5º, X) Tratamento - diz respeito a qualquer operação ou um conjunto de operações efetuadas com dados pessoais ou com conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a coleta, o registro, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou sua destruição, por exemplo (BRASIL, 2018).

Fonte: Adaptação de Brasil (2018)

A LGPD trata especificamente no Capítulo IV do Tratamento de Dados Pessoais pelo Poder Público. Este capítulo, que abrange os artigos 23 a 32, define como a administração pública deve lidar com dados pessoais, estabelecendo regras e princípios para garantir a proteção desses dados.

Dentro do Capítulo IV, destacam-se os seguintes pontos importantes:

a) Artigo 23 - Define quais pessoas jurídicas de direito público interno se submetem à LGPD quando realizam tratamento de dados pessoais, enfatizando a necessidade de finalidade, objetivos e um vetor axiológico claros;

b) Artigo 25 - Trata da interoperabilidade e estruturação dos dados pessoais para uso compartilhado, visando a execução de políticas públicas, prestação de serviços públicos e disseminação de informações;
c) Artigo 28 - Estabelece que o tratamento de dados pessoais pelo Poder Público deve seguir os princípios e diretrizes da LGPD, com foco na finalidade, adequação, necessidade e segurança;
d) Artigo 32 - Menciona a possibilidade da Autoridade Nacional de Proteção de Dados (ANPD) solicitar a publicação de relatórios de impacto à proteção de dados pessoais e sugerir padrões e boas práticas.

A Lei ainda impõe ao Poder Público a obrigação de fornecer informações claras e atualizadas sobre a base legal e a necessidade do tratamento dos dados coletados. Além disso, exige a designação de um encarregado pelo tratamento de dados pessoais, conforme previsto no artigo 39 da LGPD. Importante frisar que, quando atuam na implementação de políticas públicas, empresas públicas e sociedades de economia mista estão sujeitas às mesmas regras aplicáveis aos órgãos públicos.

Um dos principais desafios enfrentados pela Administração Pública será garantir que o compartilhamento de dados pessoais ocorra sem comprometer a segurança e a proteção dessas informações em todas as etapas — da coleta à eliminação. Isso se torna ainda mais complexo diante da possibilidade de interoperabilidade entre órgãos, que só pode ocorrer quando estiver alinhada com finalidades legítimas, como a execução de políticas públicas ou a oferta de serviços públicos.

A transparência e o direito de acesso garantem ao titular a oportunidade de acompanhar o uso de seus dados pessoais, verificando se estão corretos, atualizados e compatíveis com a finalidade que motivou sua coleta, utilização ou compartilhamento — especialmente no caso do Poder Público, limitado à implementação de políticas públicas ou à oferta de serviços à população.

Diante do que estabelece a legislação, passou a ser imprescindível implementar medidas técnicas e administrativas capazes de resguardar os dados pessoais contra incidentes acidentais ou atos ilícitos de destruição, perda, modificação, divulgação ou acesso indevido, sob risco de sanções civis ou administrativas.

É de conhecimento geral que os sistemas de tecnologia da informação estão sujeitos a invasões por agentes mal-intencionados, o que os torna expostos a eventuais manipulações indevidas. Diante disso, e considerando a constante evolução tecnológica, é responsabilidade do Poder Público direcionar investimentos à melhoria contínua dos sistemas de inteligência e tecnologia, com o objetivo de assegurar a proteção e a integridade dos dados pessoais dos titulares, em especial daqueles classificados como sensíveis.

Assim, é destacada a necessidade de adoção de medidas preventivas destinadas a evitar danos decorrentes do tratamento de dados pessoais. Essa necessidade reforça a importância da implementação de boas práticas de segurança, com o propósito de consolidar uma cultura de proteção de dados. A LGPD, nesse contexto, busca promover a maturidade dos mecanismos de governança e gestão de dados, prevenindo riscos desde as etapas iniciais do tratamento.

No que diz respeito à responsabilização e prestação de contas, a lei é clara ao exigir que o controlador comprove a adoção de medidas eficazes capazes de garantir o cumprimento

das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas. Este talvez seja o cerne da questão no âmbito público, tendo em vista a complexidade e enorme responsabilidade no tocante ao tratamento de dados de grande parte da população brasileira.

Portanto, é certo que a administração pública necessitará investir significativamente em três pilares:

a) Tecnologia, instituindo uma política robusta de segurança em TI, evitando possíveis adulterações, vazamentos, compartilhamento ou uso ilícito ou indevido;
b) Processos, mapeando-os para entender todo o fluxo do tratamento de dados, desde a sua coleta até a destruição, além de identificar os riscos inerentes ao tratamento;
c) Pessoas, capacitando-as e conscientizando-as, promovendo a cultura da integridade, ressaltando a importância em estar e permanecer em conformidade com a lei.

Portanto, no atendimento aos princípios da segurança e prevenção, a Administração Pública Federal, que é responsável pelo tratamento de dados pessoais, deve investir em soluções de segurança da informação, empregando medidas técnicas e administrativas para a garantia dos conceitos e direitos trazidos pela LGPD. Para Siqueira (2019), dentro destas medidas preventivas incluem-se a restrição de acesso a dados, mecanismos de defesa em caso de incidentes, instituição de boas práticas e de governança, utilização de softwares atualizados e seguros, bem como todas as medidas razoáveis e alcançáveis para que os dados não se tornem alvo de vazamentos.

Tratando-se das situações de interesse da Administração Pública, portanto, deve restar claro que os dados são necessários ao exercício da autoridade pública e, como exemplo disso, é possível citar o tratamento de dados pessoais para a execução de políticas públicas como as relacionadas à implementação de saneamentos básicos, pagamentos de auxílio, cadastramento de empresas para o recebimento de incentivos fiscais etc. (COTS; OLIVEIRA, 2019).

Em relação ao tratamento de dados para fins de pesquisa, questão que ganha relevo, por exemplo, quando se trata de universidades federais, sempre que possível, a lei impõe a necessidade de realizar a anonimização dos dados. Sendo assim, se o estudo não depende da identificação do titular para se realizar ou se os dados coletados e tratados são excessivos, o tratamento deve ser considerado ilegal (CARNEIRO; SILVA; TABACH, 2019).

A legislação também permite o tratamento de dados pessoais para o exercício regular de direitos em processo judicial, administrativo ou arbitral. O legislador, neste caso, deixa claro que a proteção de dados pessoais não deve comprometer o direito o qual as partes têm de produzir provas umas contra as outras, ainda que estas envolvam dados pessoais da parte contrária (FRAZÃO, 2018).

Em relação ao tratamento de dados para a proteção da vida ou tutela à saúde (incisos VII e VIII), trata-se de hipóteses específicas que vão além da proteção à privacidade em prol do interesse coletivo. São situações de interesse público, e visto a relevância do bem jurídico aqui protegido (a vida), o tratamento destes dados pessoais poderá ser realizado ainda que seja para a proteção da vida de um terceiro, e não somente do titular dos dados pessoais (COTS; OLIVEIRA, 2019).

Deste modo, fica demonstrado o impacto gerado pela LGPD na Administração Pública Federal, principalmente pelos princípios da prevenção e segurança. Estando, portanto, a APF incumbida de se preparar para se adequar, efetivamente, às disposições da LGPD,

principalmente por meio da formação de pessoal, sob pena de incorrer nas sanções legais. A preocupação do fator humano é reforçada por Araujo & Callado (2022), ao afirmarem que a capacitação do capital humano, incluindo gestores e servidores, é fundamental para o sucesso da implementação da gestão de riscos capaz de identificar vulnerabilidades em uma organização.

O que se espera, portanto, é que as organizações passem a ter um olhar diferente sobre o tema fator humano na segurança cibernética, e que busquem assegurar que as pessoas estejam envolvidas no tratamento das informações estejam suficientemente sensibilizados e com conhecimento necessário, como consequência estarão mitigando riscos e aumentando a resiliência através da construção de uma cultura de cibersegurança sólida, onde se reconhece a importância da informação e as preocupações com a cibersegurança passam a fazer parte do dia a dia de todos.

2.3 Fator humano e as ameaças cibernéticas

O que encontramos hoje nesse cenário de evolução tecnológica é que as pessoas não estão preparadas para todo esse progresso devido à falta de conhecimentos necessários para o enfrentamento dessa nova realidade, associada ao crescente número de ciberataques e da sua sofisticação. Para Moreira et al. (2021), a tecnologia, embora ofereça inúmeras vantagens, também traz desafios, riscos e ameaças, introduzindo complexidades adicionais e potenciais vulnerabilidades que exigem uma gestão cuidadosa.

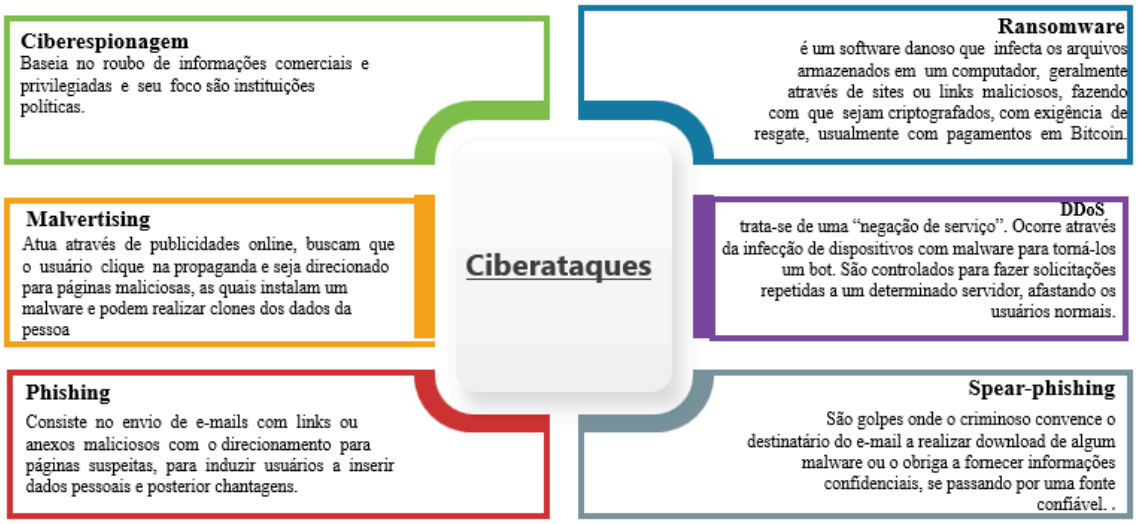
Para Parsons et al. (2017), as pessoas são o elo mais fraco na proteção do sistema de segurança da informação de uma organização. Não restam dúvidas que, as pessoas representam ainda o elo mais fraco na segurança da informação e representam uma das maiores vulnerabilidades da cibersegurança, e desta forma tornam-se o principal alvo dos ciberataques. No dizer de Bermejo et al. (2018), no âmbito organizacional, as incertezas ocorrem a todo momento. Uma incerteza se refere a situações em que não há informações suficientes para entendimento do cenário ou conhecimento quanto às consequências de determinado evento. O Programa de Privacidade e Segurança da Informação (PPSI), instituído pela Portaria SGD/MGI nº 852, de 28 de março de 2023, orienta os órgãos e entidades do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) na implementação de práticas robustas de privacidade e segurança da informação. O programa tem como objetivo elevar a resiliência e a maturidade institucional, garantindo maior proteção aos dados e sistemas da administração pública. Para o PPSI, as ações das pessoas podem causar incidentes, intencionalmente ou não. É mais fácil para um atacante induzir um usuário a clicar em um link ou abrir um anexo de e-mail para instalar malware e entrar na rede de uma organização, do que fazer um exploit de rede diretamente. Nenhum programa de segurança pode lidar com o risco cibernético de maneira eficaz sem um meio de lidar com essa vulnerabilidade humana fundamental. Cada usuário do órgão em qualquer nível tem riscos diferentes.

Segundo a empresa de antivírus Kaspersky (2022), cibersegurança é o ato de proteger os ativos da empresa, ou seja, servidores, sistemas eletrônicos, redes, e dados contra possíveis ataques maliciosos. Assim, ao fazer a capacitação, as Instituições Federais de

Ensino Superior (IFES) estariam se adequando não somente ao PPSI e à LGPD como também às melhores práticas de SI da atualidade.

De acordo com a pesquisa da Fortinet, em 2022 ocorreram 103 bilhões de tentativas de ataques cibernéticos no Brasil. Em maio de 2021 seis instituições sofreram ciberataque, entre elas, a Universidade Federal do Rio de Janeiro (UFRJ), a Universidade Federal de Alagoas (UFAL), Universidade Federal do Tocantins (UFT), Universidade Federal de Minas Gerais (UFMG), Universidade Federal da Grande Dourados (UFGD) e a Universidade Federal da Bahia (UFBA). É importante destacar que, quando consideramos o cenário de uma Instituição Federal de Ensino Superior, os riscos envolvidos não se limitam à proteção de dados, mas também resguarda o conhecimento produzido, incluindo segredos industriais e propriedade intelectual (Junior et al. 2014). As universidades precisam garantir que os dados estejam sempre protegidos contra corrupção, destruição ou roubo em potencial (Ismail et al., 2022). Estas instituições gerenciam, segundo Bittencourt et al. (2024), grandes quantidades de pesquisas valiosas e dados sensíveis, o que as torna alvos atrativos para criminosos cibernéticos, espionagem e hackers em geral. Na figura 7 são apresentadas algumas das principais ameaças em cibersegurança com base no documento de Boas Práticas de Cibersegurança em Teletrabalho, elaborado pelo CNCS (ANDRADE, et al., 2020) (TERESO et al., 2021):

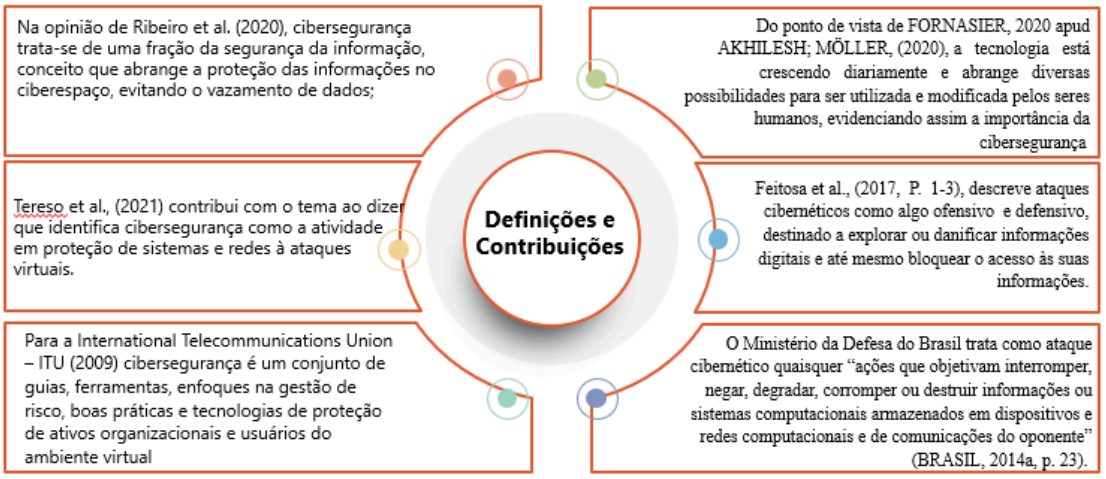
Figura 7 - Ameaças em Cibersegurança



Fonte: o Autor

A seguir, na figura 8 apresentamos uma lista com definições e contribuições sobre cibersegurança, com o objetivo de promover uma melhor compreensão do tema:

Figura 8 - Definições e contribuições



Fonte: o Autor

A crescente sofisticação dos ciberataques torna indispensável o conhecimento dos principais conceitos da área. Entender o vocabulário da cibersegurança é o primeiro passo para adotar boas práticas, prevenir riscos e fortalecer a resiliência digital. A tecnologia, embora ofereça inúmeras vantagens, também traz desafios, riscos e ameaças, introduzindo complexidades adicionais e potenciais vulnerabilidades que exigem uma gestão cuidadosa (Moreira et al., 2021).

3. METODOLOGIA

Este estudo fez uso do método de pesquisas bibliográficas de caráter exploratório descritivo em normativos do Governo Federal, artigos científicos, livros, dissertações e publicações. De acordo com Eco (2010), com a pesquisa bibliográfica é possível o levantamento e a organização de informações imprescindíveis, a partir de materiais já publicados, para fundamentar teoricamente o estudo. Ou seja, a pesquisa bibliográfica vai permitir a revisão de obras publicadas sobre a teoria que irá direcionar este trabalho científico.

No decorrer deste estudo, abordou-se inicialmente a segurança da informação, mostrando sua importância na proteção das informações contra acessos não autorizados, perdas, alterações não autorizadas e interrupções, garantindo a confidencialidade, integridade e disponibilidade dos dados, além de contextualizar a importância das informações para os órgãos e a necessidade da compreensão dessa importância por parte do quadro de funcionários dos órgãos do SISP.

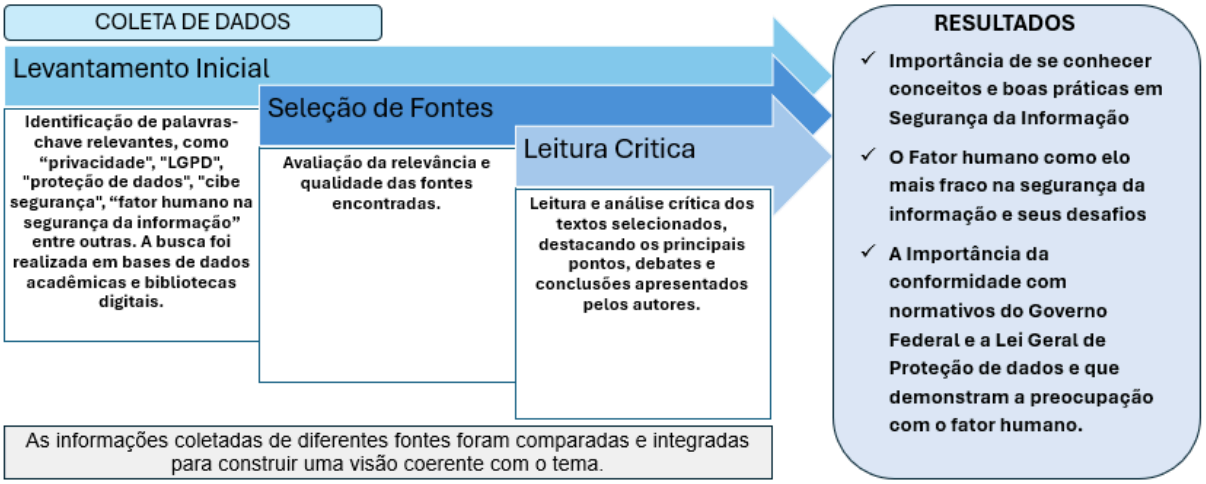
Em seguida foi realizada uma análise do comportamento humano inserido no contexto da segurança da informação e que para muitos autores é considerado o "elo mais fraco", sendo necessário um tratamento diferenciado pelo enorme desafio que o fator humano representa quando buscamos uma mudança de comportamento e de atitudes, dessa forma, será possível comprovar a importância da capacitação e conscientização para que as pessoas envolvidas no tratamento das informações reconheçam os riscos e adotem uma postura defensiva através das melhores práticas de segurança. Em outras palavras, a capacitação e conscientização como estratégia para mitigação dos riscos gerados por esses comportamentos inseguros.

Finalmente, abordou-se a questão da conformidade com normativos e Leis a exemplo da Lei Geral de Proteção de Dados e o Programa de Privacidade e Segurança da Informação,

sendo possível identificar a importância das ações voltadas aos riscos que envolvem o fator humano.

Para identificar e compreender a importância da mitigação dos riscos humanos na Segurança da Informação e Privacidade, a pesquisa seguiu um processo estruturado em 4 etapas interligadas como mostra a figura 9, garantindo uma análise abrangente e contextualizada. Essas etapas incluíram a definição do escopo da pesquisa, a coleta e análise de dados através do levantamento inicial, a seleção de fontes, a realização de uma leitura crítica e a validação dos resultados.

Figura-9 Etapas da Pesquisa



Fonte: Autor

4 RESULTADOS E DISCUSSÕES

De fato, um bom programa de conscientização de segurança da informação e privacidade, tem como objetivo fornecer conhecimentos para todos os funcionários de uma empresa sobre segurança da informação (AFINAL, 2019).

Para Carvalho & Coleto (2024) capacitar e conscientizar não é somente medida de proteção, é uma exigência legal para estar em conformidade com a Lei Geral de Proteção de Dados (LGPD). Dessa forma, é necessário a efetivação de uma estratégia proativa, com foco na prevenção e conscientização contra ameaças, assegurar a privacidade e integridade dos dados seguindo diretrizes estabelecidas para tratamento de dados pessoais. Na verdade, o que se busca é a transformação desses comportamentos inseguros, uma mudança de atitude ou porque não dizer uma mudança de cultura nas Instituições, é dar um tratamento diferenciado no momento que esses comportamentos são identificados. É investir em conhecimento com a implementação de programas de conscientização e treinamentos continuados, não esquecendo que a compreensão necessária para efetivação dessas mudanças passa pelo uso de uma linguagem acessível e que represente os normativos da instituição, leis e normativos federais, pois somente assim vai propiciar uma nova cultura de segurança e privacidade.

As situações rotineiras, por falta de conhecimento sobre como agir, ou mesmo as de risco, pelo grau de responsabilidade, tornam o fator humano e suas ações uma vulnerabilidade bastante explorada pelas ameaças de SI (CARNEIRO et al., 2013).

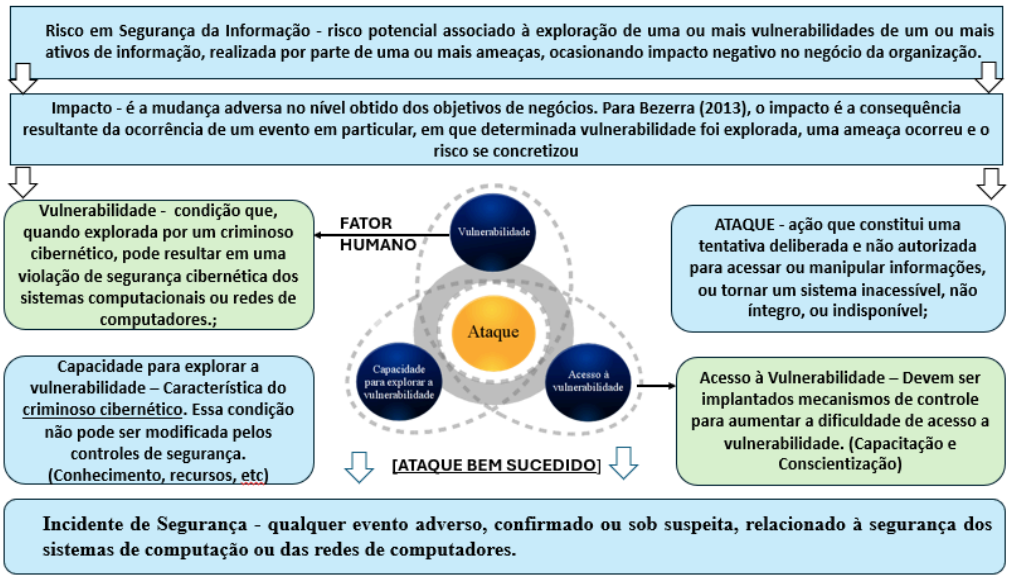
Não compreender os normativos, que muitas vezes é ocasionado pela falta de clareza dos documentos, o baixo conhecimento para que seja possível uma mudança de atitude para a preservação da Segurança da Informação deve ser entendida e trabalhada em seus conteúdos

ao oferecer a capacitação sobre o tema e palestras de conscientização. Assim, será possível mitigar riscos, melhorando a segurança das informações e o próprio desempenho na realização das atividades diárias. Para o Centro de Estudos, Respostas a Incidentes (CERT), estratégias voltadas a mitigar riscos baseadas em treinamento e conscientização se traduzem brevemente como: o aumento da conscientização sobre ameaças internas e ameaças externas não intencionais e a motivação para ter cuidado com elas.

A mitigação desses riscos ocorre, portanto, através de um programa de conscientização e treinamento que venha a fortalecer as atividades humanas, se tornando desse modo a barreira tão desejada contra ameaças cibernéticas. Essa barreira somente é construída quando as pessoas estão bem informadas, fazendo com que entendam os riscos e passem a adotar comportamentos seguros ao reconhecer sinais de possíveis riscos e que possam adotar melhores práticas de segurança.

Entender a importância da segurança da informação em uma IFES, considerando o fator humano como objeto do estudo, se faz necessário o entendimento de conceitos básicos de SI que estão intimamente alinhados com o tema estudado. Afinal, se existe a vulnerabilidade, fator humano, que pode ser explorada através das ameaças existentes, deixando sujeito os dados da Instituição as ameaças existentes, gerando um risco para a Instituição, esses riscos devem ser trabalhados com a finalidade de diminuir a probabilidade de se efetivarem. Portanto, torna-se necessário o entendimento de técnicas e métodos usados por indivíduos ou grupos mal-intencionados para comprometer a segurança de sistemas, esse entendimento passa pela compreensão de conceitos básicos como riscos, vulnerabilidades e ameaças, como mostra a figura 10:

10 - O fator Humano x Ataque em segurança da informação



Fonte: O Autor

Como boa prática, a criação de uma cultura de segurança e privacidade que contemple desde o alto escalão até o nível operacional se torna muito mais efetiva. Entender que privacidade e segurança da informação é responsabilidade de todos diminui bastante os riscos envolvidos. Muito importante a participação da Administração Superior das IFES nesse processo, a mudança para ser efetiva deve começar pelos gestores.

A ISO/IEC 27001 (2022) destaca a conscientização, afirmando que todas as pessoas que desempenham funções em uma organização devem estar cientes da política de segurança da informação, qual a sua contribuição para a eficácia do Sistema de Gestão da Segurança da

Informação (SGSI), os benefícios que o melhor desempenho da segurança da informação pode trazer, bem como as implicações que não conformidades são capazes de acarretar.

Dentro desse processo de mudanças de cultura organizacional a comunicação é uma ferramenta essencial na geração de resultados positivos. Deve haver um canal de comunicação para que as pessoas, os envolvidos no tratamento de dados pessoais, relatem incidentes de segurança. Neste momento deve haver a compreensão por parte de todos que a represália não existe.

De acordo com Neiva Santos de Oliveira (2018), é importante ficar atento a valores como compromisso, empatia, transparência, profissionalismo e sentido crítico pois temos que considerar que as organizações lidam diariamente, com diferentes pessoas. Ou seja, tentar satisfazer a todos com dignidade, valorizando sempre a sua contribuição e nunca esquecendo que o fazem pelo sucesso da empresa e deles e das suas famílias. Portanto, a instituição deve propiciar um ambiente seguro não só tecnologicamente, mas também funcionalmente. O objetivo então é fazer com que cada indivíduo envolvido no tratamento de dados e informações tenha conhecimento suficiente sobre Segurança da Informação e Privacidade para poder usar durante o desenvolvimento de suas atividades diárias.

Segundo Fonseca (2009), a informação encontra-se exposta a diversos tipos de ataques, seja através de meios lógicos, físicos ou humanos. As organizações realizam grandes investimentos em tecnologias que manipulam as informações contra acessos não-autorizados, porém é deixado de lado o fator humano que têm impacto alto como exposto. O que pode permitir que a vulnerabilidade do fator humano permaneça ou porque não dizer só aumente.

O fator humano representa então, um enorme desafio na segurança da informação. Assim sendo, não mitigar os riscos inerentes a esses comportamentos pode levar a consequências negativas de alto impacto, pois há medidas eficientes que podem ser adotadas para reduzir as vulnerabilidades resultantes de comportamentos inseguros.

O que se deseja é transformar pessoas em barreira defensiva, reconhecendo sua importância no contexto da Segurança da Informação agregado a um tratamento específico para que seja efetivo. O que pode ser atingido a partir de investimento em conhecimento e mudança cultural, o uso de linguagem simples e clareza nos normativos.

Portanto, considera-se que o desenvolvimento de uma cultura de reconhecimento do valor das informações, através da conscientização sobre a relevância dos dados, sobre as responsabilidades de todos no processo de tratamento dos dados e sobre as implicações que um vazamento de dados é necessário para adequação a atualidade e a regulamentos como a Lei Geral de Proteção de Dados.

Esse processo de conscientização e capacitação necessita, portanto, ser conduzido de forma contínua, estar em constante atualização, envolver treinamentos, palestras, informativos, estabelecer códigos de conduta, bem como implementação de ferramentas de proteção e controle de acesso aos dados.

Assim, resta evidente a importância da mitigação de riscos em segurança da informação e privacidade através de uma estratégia de conscientização e capacitação. Outra compreensão trazida por esse estudo é a necessidade de quebra de paradigma onde é necessário que se entenda que não existem somente vulnerabilidades técnicas nesse cenário, os fatores humanos estão envolvidos e são considerados riscos à Segurança da Informação. Pois, são esses mesmos fatores humanos que podem ser explorados se transformando em um incidente de segurança.

Combater ameaças cibernéticas de maneira eficiente vai além do uso de tecnologias sofisticadas, exige, acima de tudo, o engajamento consciente e a capacitação constante das pessoas. Grande parte dos ataques bem-sucedidos explora vulnerabilidades humanas, como o uso de senhas fracas, o acesso a links maliciosos ou o compartilhamento indevido de dados. Por isso, é fundamental que iniciativas futuras priorizem programas educativos contínuos, personalizados de acordo com os diferentes perfis e níveis de conhecimento dos usuários.

Um aspecto relevante a ser destacado é a incorporação da alfabetização básica e ampla em segurança da informação como componente fundamental na formação de profissionais. Diante da intensificação do uso da tecnologia e do aumento constante de incidentes cibernéticos, essa capacitação torna-se indispensável para todos, independentemente do setor em que atuem. A sensibilização quanto à segurança da informação contribui para a proteção de dados sensíveis, prevenção de fraudes, continuidade dos processos organizacionais e mitigação de riscos legais e financeiros. Dentro desta estratégia podemos destacar temas como:

a) Proteção de Dados - Profissionais com conhecimentos em segurança da informação possuem maior habilidade para reconhecer e se defender de ameaças como phishing, malware e ataques de engenharia social, contribuindo diretamente para a proteção de dados sensíveis da organização e de seus clientes;
b) Prevenção de Perdas - A sensibilização para a segurança da informação contribui significativamente para minimizar prejuízos financeiros e impactos operacionais causados por incidentes cibernéticos, como exposições indevidas de dados, paralisações de sistemas e sanções decorrentes do descumprimento de normas regulatórias;
c) Conformidade Regulatória - Diversos setores estão sujeitos a leis e normas que determinam a adoção de práticas de segurança da informação. Nesse contexto, a alfabetização em segurança capacita os colaboradores a compreenderem essas exigências legais e a atuarem em conformidade com elas;
d) Cultura de Segurança - Ao investir na alfabetização em segurança, desenvolve-se uma cultura organizacional em que cada colaborador assume um papel ativo na proteção das informações, contribuindo para o fortalecimento da postura de segurança da empresa;
e) Autonomia e Consciência - A alfabetização digital em segurança da informação não apenas ensina como proteger dados, mas também capacita os indivíduos a tomarem decisões mais seguras e conscientes no ambiente online.

Em síntese, incorporar a alfabetização em segurança da informação à formação dos colaboradores deixou de ser opcional e passou a representar uma estratégia essencial, capaz de gerar vantagens significativas tanto para os profissionais quanto para as instituições.

5. CONCLUSÃO

Embora o fator humano possa representar uma vulnerabilidade na segurança da informação, quando bem instruído, capacitado e engajado, transforma-se em um importante aliado na proteção das informações institucionais. Nesse contexto, a LGPD estabelece um novo paradigma: as organizações devem repensar a forma como tratam os dados pessoais, promovendo uma cultura voltada à proteção dos direitos fundamentais, como a liberdade e a privacidade, em todas as interações que envolvam esses dados.

Ao passo que, a adequação a LGPD é complexa devido exatamente a necessidade de mudanças de comportamento em relação às boas práticas no tratamento dos dados. A LGPD pode ser aproveitada como um guia, pois apresenta como principal objetivo mitigar riscos à proteção da privacidade dos indivíduos.

No que se refere ao objetivo específico de destacar a relevância das ações de capacitação e conscientização, garantindo que todos os usuários sejam devidamente treinados e compreendam suas responsabilidades no que se refere à segurança da informação, fica claro que uma cultura organizacional que valoriza a segurança da informação pode incentivar os funcionários a adotarem comportamentos seguros e agirem como defensores da segurança. Cada vez que a segurança da informação é uma prioridade em todos os níveis da organização, os funcionários se sentem responsáveis por proteger os dados e os recursos da IFES, tornando-se uma efetiva barreira contra ameaças internas e externas. Quando as pessoas estão engajadas e têm voz ativa na implementação e revisão das medidas de segurança, conseguem colaborar com suas concepções e conhecimentos para fortalecer a segurança da informação.

No que se refere ao objetivo específico de demonstrar o alinhamento das ações de capacitação e conscientização com os normativos do Governo Federal e com o Programa de Privacidade e Segurança da Informação (PPSI), evidencia-se a preocupação do Governo em assegurar a conformidade com todas as leis, regulamentos e diretrizes aplicáveis. Tal postura reforça a importância do fator humano na proteção da informação e da privacidade.

Essa preocupação ficou evidenciada pela referência ao Controle 23 do PPSI, que trata da Conscientização e Treinamento sobre Privacidade, e ao Controle 14, referente à Conscientização e Treinamento de Competências em Segurança da Informação. Além disso, reforça-se o alinhamento com o artigo 50 da LGPD, que estabelece a adoção de medidas educativas, como a implementação de uma estratégia abrangente de capacitação e conscientização, voltada a assegurar que os colaboradores compreendam suas responsabilidades e os procedimentos relativos à proteção de dados pessoais.

Outro ponto de alinhamento relevante diz respeito aos propósitos do Centro de Excelência em Privacidade e Segurança da Informação do Governo Digital, cuja missão é incentivar a consolidação de uma cultura voltada à privacidade e à segurança da informação nos órgãos e entidades da administração pública federal direta, autárquica e fundacional. Ademais, evidencia-se a aderência à Política Nacional de Segurança da Informação (PNSI), especialmente ao disposto no Art. 4º, que reconhece como essencial o incentivo à formação e capacitação de recursos humanos na área de segurança da informação.

Por fim, atingidos todos os objetivos específicos, o objetivo geral de Demonstrar a importância de um Programa de Capacitação e Conscientização como estratégia para mitigação dos riscos que envolvem o fator humano em uma Instituição Federal de Ensino Superior, também foi atingido, uma vez que foi percebido que o papel dos envolvidos no tratamento de dados é fundamental para o sucesso no desafio da adequação de uma IFES a LGPD e a manutenção da Segurança da Informação. A mudança de comportamento desenvolvida durante um programa de capacitação e conscientização tem potencial para mudar o atual cenário. Com adoção de estratégias centradas em pessoas vai ser possível mudar consideravelmente o comportamento humano o que poderá reduzir os riscos relacionados à segurança da informação.

5.1 Trabalhos Futuros

Esse estudo não encerra essa discussão, pelo contrário, demonstra a necessidade de sua ampliação. Serão necessários outros estudos que abordem a segurança da informação e a

privacidade em uma IFES, para compreensão de aspectos específicos das necessidades de treinamento para se obter a eficácia no processo de mitigação dos riscos que envolvem pessoas.

Nesse contexto, destaca-se a importância de desenvolver estratégias voltadas à conscientização e capacitação dos servidores que atuam no tratamento de dados nas instituições. A implementação dessas ações contribui para a mitigação dos riscos associados, reduzindo não apenas prejuízos financeiros, mas também danos à reputação e à imagem de uma IFES.

Diante do constante avanço tecnológico e da crescente complexidade das ameaças digitais, torna-se essencial planejar e implementar ações futuras voltadas à capacitação e conscientização em segurança da informação. Essas ações devem ser contínuas, atualizadas e alinhadas às melhores práticas nacionais e internacionais, bem como aos normativos de proteção de dados e segurança institucional.

Por fim, destaca-se a importância da criação de um método sistemático de monitoramento e avaliação contínua, por meio do estabelecimento de mecanismos que permitam medir a efetividade das ações executadas. Para isso, é essencial definir indicadores que possibilitem ajustes constantes e aprimoramentos nos programas de capacitação e conscientização. Um exemplo prático seria a adoção de trilhas de aprendizagem personalizadas conforme o perfil dos usuários, incluindo cursos regulares sobre boas práticas em segurança da informação, legislação vigente — como a LGPD — e procedimentos de resposta a incidentes cibernéticos.

Referências

AFINAL, o que é plano de conscientização em segurança da informação? 2019.
Disponível em: https://www.alertasecurity.com.br/afinal-o-que-e-plano-de-conscientizacaoem-seguranca-da-informacao/. Acesso em: 04 mar. 2025.

AKAYAMA KANAGUSKU, A. R., & GASETA, E. (2023). FATOR HUMANO NA SEGURANÇA DA INFORMAÇÃO: DESMISTIFICANDO O ELO MAIS FRACO. *FatecSeg - Congresso De Segurança Da Informação*.
Disponível em: https://www.fatecourinhos.edu.br/fatecseg/index.php/fatecseg/article/view/114

ANDRADE FILHO, J. P. de; MOTTA, G. H. M. B. Modelo de maturidade de processos para avaliação da conformidade com a LGPD: um estudo de caso em uma instituição educacional no Brasil. Revista Principia, *[S. l.]*, v. 62, 2024. DOI: 10.18265/2447-9187a2025id8652.
Disponível em: https://periodicos.ifpb.edu.br/index.php/principia/article/view/8652. Acesso em: 24 abr. 2025.

ASSIS E MENDES. Direito digital, empresarial e Proteção de dados. Histórico das leis de proteção de dados e da privacidade na internet, 2019.
Disponível em: https://assisemendes.com.br/historico-protecao-de-dados. Acesso em 24 set. 2022.

BEZERRA, Edson Kowask. Gestão de Riscos de TI: NBR 27005. Rio de Janeiro: Escola Superior de Redes, RNP, 2013.

BITTENCOURT, O. T., Carvalho, R. L. de, Barbosa, G. V. and Santos, G. F. do (2024) "Segurança cibernética nas universidades: uma revisão sistemática da literatura sobre a gestão de segurança da informação no ensino superior", InterSciencePlace, vol. 19.

BRASIL. Lei 13.709 de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da República Federativa do Brasil, 15 agosto de 2018.
Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 31 fev. 2025.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil. Brasília, DF: Presidente da República,. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 30 jul. 2025.

BRASIL, Ministério da Gestão e Inovação em Serviços Públicos. Modelo de Política de Segurança da Informação, agosto de 2024. Brasília, 2024. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-eguranca/ppsi/modelo_politica_seguranca_informacao.pdf. Acesso em: 10 mar 2025.

BRASIL, Autoridade Nacional de Proteção de Dados (ANPD). Tratamento de Dados Pessoais Pelo Setor Público, junho de 2023. Brasília, 2023. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia-poder-publico-anpd - Acesso em: 02 Jul 2025.

BRASIL, Ministério da Gestão e Inovação em Serviços Públicos. Framework de Privacidade e Segurança da Informação, junho de 2021. Brasília, 2021. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/framework. Acesso em: 10 mar 2025.

BRASIL, Laboratório Nacional de Computação Científica. Os quatro pilares da segurança da informação – Confidencialidade, Disponibilidade, Integridade e Autenticidade. Agosto de 2024, Brasília, 2024. Disponível em: https://www.gov.br/lncc/pt-br/centrais-de-conteudo/campanhas-de-conscientizacao/gestao-de-seguranca-da-infor

macao/os-quatro-pilares-da-seguranca-da-informacao-2013-confidencialidade-disponibilidade-integridade-e-autenticidade. Acesso em: 10 mar 2025.

BRASIL, Ministério da Gestão e Inovação em Serviços Públicos. Programa de Privacidade e Segurança da Informação (PPSI), agosto de 2021. Brasília, 2021. Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca. Acesso em: 10 mar 2025.

BRASIL, Gabinete de Segurança Institucional da Presidência da República. Glossário de Segurança da Informação. Outubro de 2021. Brasília, 2021. Disponível em: https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/glossario-de-seguranca-da-informacao-1. Acesso em: 10 mar 2025.

BRASIL, Gabinete de Segurança Institucional da Presidência da República. Política Nacional de Segurança da Informação (PNSI). Dezembro de 2028. Brasília, 2018. Disponível em: https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/politicas-nacionais/politica-nacional-de-seguranca-da-informacao-pnsi. Acesso em: 10 mar 2025.

BRASIL, Gabinete de Segurança Institucional da Presidência da República. IN 01, Estrutura de Gestão da Segurança da Informação. Maio de 2020. Brasília, 2020. Disponível em: https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/legislacao/copy_of_IN01_consolidada.pdf. Acesso em: 10 mar 2025.

BRASIL, Gabinete de Segurança Institucional da Presidência da República. Cartilha de Gestão de Segurança da Informação. Dezembro de 2022. Brasília, 2022. Disponível em: https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/cartilha-de-gestao-de-seguranca-da-informacao/CartilhadeSegurancaInformao.pdf. Acesso em: 02 mai 2025.

BUCCI, M. P. O conceito de política pública em direito. In: BUCCI, M. P. Políticas públicas: reflexões sobre o conceito jurídico. São Paulo: Saraiva, 2006, p. 39.

CAMILLO, MARK; HESS, SEBASTIAN. American International Group. AIG. Human Cyber Risk – The first line of defence. Disponível em: https://www.aig.co.uk/content/dam/aig/emea/united-kingdom/documents/Insights/cyber-human-factor.pdf. Acesso em 02 mar. 2025. Citado na página 3.

CARNEIRO, L. E. S.; ALMEIDA, M. B.. Gestão da Informação e do Conhecimento no âmbito das práticas de Segurança da Informação: O fator humano nas organizações. Bibli: Revista Eletrônica de Biblioteconomia e Ciência da Informação,v.18, n.37, p.175-202, 2013.

CARNEIRO, Isabelle da Nóbrega Rito; SILVA, Luiza Caldeira Leite; TABACH, Danielle. Tratamento de dados pessoais. In: FEIGELSON, Bruno; SIQUEIRA, Henrique Albani (Coord.). Comentários à Lei Geral de Proteção de Dados: Lei 13.709/2018. São Paulo: Revista dos Tribunais, 2019.

CARVALHO, B., & COLETO, B. (2024). A relevância da prevenção contra ataques de engenharia social no âmbito empresarial por uma perspectiva da LGPD. *Revista Terra & Cultura: Cadernos De Ensino E Pesquisa, 40*(especial), 170-186.
Disponível em: http://periodicos.unifil.br/index.php/Revistateste/article/view/3160/2911
COLWILL, C.
Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S1363412710000051?via%

COTS, Márcio; OLIVEIRA, Ricardo. Lei geral de proteção de dados pessoais comentada. São Paulo: Revista dos Tribunais, 2018.

COUTINHO, M. M., SANTOS, R. N. DOS, CUSTODIO, V. H. DA S., AMARAL, E. C., SABINO, E., & ABE, N. (2017). Estudo de caso: Principais pilares da segurança da informação nas organizações. *Revista Gestão em Foco*, v. 9, p. 489–500. Disponível em: https://portal.unisepe.com.br/unifia/wp-content/uploads/sites/10001/2018/06/052_estudo5.pdf

CRESPO, M. Proteção de dados pessoais e o poder público: noções essenciais. *In*: CRAVO, D. C.; CUNDA, D. Z. G.; RAMOS, R. (org.). Lei Geral de Proteção de Dados e o Poder Público. Porto

Alegre: Escola Superior de Gestão e Controle Francisco Juruena; Centro de Estudos de Direito Municipal, 2021. p. 16-28. Disponível em: https://lproweb.procempa.com.br/pmpa/prefpoa/pgm/usu_doc/ebook_lgpd_e_poder_publico_23052021.pdf. Acesso em: 15 fev. 2025.

Dantas, Marcus Leal. Segurança Da Informação: Uma Abordagem Focada Em Gestão De Riscos. Olinda: Livro Rápido, 2011. 150 P. Isbn 978-85-406-0047-8.

DA SILVA BELARMINO, G., MATOS BEZERRA MOTTA, G., FONSÊCA PINHEIRO DE LIMA, LF, & ROUSY DIAS RICARTE, D. (2024). Recomendações para Conformidade com a LGPD a partir de uma Revisão Sistemática da Literatura. Revista Eletrônica Argentina-brasil De Tecnologias Da Informação E Da Comunicação. 1(18).

DIVINO, S. B. S. Reflexões céticas, principiológicas e econômicas sobre o consentimento necessário à coleta e tratamento de dados. Derecho PUCP, N° 83, 2019.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: elementos da formação da Lei geral de proteção de dados. 2. ed. São Paulo: Revista dos Tribunais, 2019.

DOURADO, Luzia Moreira de Abreu; ALVES, André Luiz. Um estudo sobre os habilitadores do COBIT® 5 sob a perspectiva da segurança da informação. 2016. [18] f. Artigo (Grau em Curso) – Pontifícia Universidade Católica de Goiás, Goiânia, 2016.

DROESCHER, F. D.; SILVA, E. L. Pesquisador e a produção científica. Perspectivas em Ciência da Informação, v. 19, n. 1, p. 170-189, 2014. Disponível em: </https://www.scielo.br/j/pci/a/ww5zR3KhYCk65bPkWJyTQtf/?lang=pt>. Acesso em: 30 mai 2025.

ECO, U. Como se faz uma tese. São Paulo: Editora Perspectiva, 2010.

EGRESS SOFTWARE TECHNOLOGIES. Insider Data Breach Survey Report, 2021. Disponível em: https://www.egress.com/blog/what-is-human-layer-security/2021-insider-breach-survey . Acesso em 26 abr, 2025. Citado na página 6.

ELEUTERIO, M. A. M. Sistema de Informações Gerenciais Na Atualidade. 1ª Edição. Curitiba: Intersaberes, 2015.

EMILIO Gonçalves, Ígor Ramos Bezerra da Silva, Carlos Eduardo Miranda Zottmann, João Souza Neto, Rafael Rabelo. Universidades sob ataque hacker: riscos de negócio para segurança cibernética em universidades brasileiras. 2025. Programa de Pós Graduação Profissional em Engenharia Elétrica (PPEE). Universidade de Brasília, Brasília, 2025.

FAYAYOLA, O. A.; OLORUNFEMI, O. L.; SHOETAN, P. O. Data privacy and security in it: a review of techniques and challenges. Computer Science & IT Research Journal, v. 5, n. 3, p. 606-615, 2024. DOI: https://doi.org/10.51594/csitrj.v5i3.909.

FERNANDES, J.; ALMEIDA, F. Implementação do Framework de Segurança em Instituições Públicas. Journal of Cybersecurity Management, v. 6, n. 2, p. 102-119, 2021.

Fonseca, Paula Fernanda. Gestão De Segurança Da Informação: O Fator Humano. 2009. [16] F. Artigo (Especialização Em Redes E Segurança De Computadores) – Pontifícia Universidade Católica Do Paraná, Curitiba, 2009.

FONTES, EDISON LUIZ GONÇALVES. Segurança da informação. Saraiva Educação SA, 2017.

FRAZÃO, Ana. Nova LGPD: as demais hipóteses de tratamento de dados pessoais. Jota, 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-as-demais-hipoteses-de-tratamento-de-dados-pessoais-19092018>. Acesso em: 24 Jun. 2025.

GARRATECH. A importância do fator humano na segurança da informação, 2025. Disponível em: A importância do fator humano na segurança da informação (garratech.com.br). Acesso em: 20 mar. 2025. Citado na página 5.

GIL, A. C. Como elaborar projetos de pesquisa. São Paulo, SP: Atlas, 2002.

GOOGLE ACADÊMICO. Sobre o google acadêmico. [2011]. Disponível em: <http://scholar.google.com.br/intl/pt-BR/scholar/about.html>. Acesso em: 30 mai 2025.

GUALBERTO, É. S.. Proposição de uma Ontologia de Apoio à Gestão de Riscos de Segurança da Informação. iSys – Revista de Sistemas da Informação. Rio de Janeiro, v.6, n.1, p.30-43, 2013.

CANALTECH. Erro humano causa 95% das falhas de segurança, revela estudo. Março de 2025. Disponivel em: https://canaltech.com.br/seguranca/erro-humano-causa-95-das-falhas-de-seguranca-revela-estudo/. Acesso em: 23 abr 2025.

IBM. O que é segurança da Informação. Julho de 2024. Disponível em: https://www.ibm.com/br-pt/topics/information-security. Acesso em: 10 mar 2025.

IBM. O que é a Transformação Digital ?. Maio de 2024. Disponível em: https://www.ibm.com/br-pt/topics/digital-transformation. Acesso em: 23 mai 2025.

ISMAIL, W. B. W. et al. (2022) “An information security policy development process in higher education institution: a case study approach”, Proceedings of the 2022 9th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), IEEE, pp. 147–152.

HUSSAIN, F., HUSSAIN, R., NOYE, B., AND SHARIEH, S. (2020). Enterprise api security and gdpr compliance: Design and implementation perspective. IT Professional, 22(5):81–89.

JAIN, A. K.; GUPTA, B. A survey of phishing attack techniques, defence mechanisms and open research challenges. Enterprise Information Systems , Taylor & Francis,v. 16, n. 4, p. 527–565, 2022

JUNIOR, A. E. de A., Santos, E. M. dos and Albuquerque, E. S. de (2014) “Segurança da Informação em um Instituto de Pesquisa: uma análise utilizando a norma ISO/IEC 27002:2005”, Revista Formadores, vol. 7, no. 2, p. 71.

LEME, R. S.; BLANK, M. JURISPRUDÊNCIA E LEGISLAÇÃO SANITÁRIA COMENTADAS LEI GERAL DE PROTEÇÃO DE DADOS E SEGURANÇA DA INFORMAÇÃO NA ÁREA DA SAÚDE. CADERNOS IBERO-AMERICANOS DE DIREITO SANITÁRIO, BRASÍLIA, 9(3), 2020.

LOPES, F. AND AMARAL, M. A. A. (2022). Implementação da lei geral de proteção de dados pessoais (LGPD) em uma instituição, sem fins lucrativos, atuante na área da educação básica. PROJETOS E RELATO´RIOS DE ESTA´GIOS, 4(1):21–21.

LYRA, MAURÍCIO R. Governança da Segurança da Informação. 1. ed. Brasília, 2015

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito. São Paulo: Saraiva, 2014.

MIMECAST. O Estado do Risco Humano 2025. Março de 2025. Disponivel em: https://www.mimecast.com/resources/ebooks/state-of-human-risk-2025/. Acesso em: 23 mai 2025.

MOREIRA, L. B.; SANTANA, A. P; MIRANDA, A. R. A. Os Impactos da Implementação do SAP R/3 em uma Empresa do Setor de Laticínios. Revista Ciências Administrativas , v.18, n. 1, 2014. Disponível em: http: // periodicos.unifor.br/rca/article/view/ 3328. DOI: http: // dx.doi.org/ 10.5020/ 2318-0722.18.1.%25p

MORESI, E. A. D. Delineando o valor do sistema de informação de uma organização. Ciência da Informação on Line, Brasília, v.29, n.1, p.14-24, 2000.

NEIVA SANTOS DE OLIVEIRA, F. (2018). Comunicação das Organizações: Um olhar sobre a importância da Comunicação Interna. *Media & Jornalismo*, *18*(33), 61-74. https://doi.org/10.14195/2183-5462_33_4. Acesso em 17 de Maio de 2025. Citado na página 7.

O. N. SIQUEIRA, A. C. CONTIN, R. B. BARUFI, L. S. A (hiper)vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD. . Lehfeld Revista Eletrônica Pesquiseduca: 2021.

PAULO, ANA CAROLINA RIBEIRO DE MORAES. LGPD: por mais ações orientadas à transparência. Análise Editorial, 2021. Disponível em: https://analise.com/opiniao/lgpd-por-mais-acoes-orientadas-a-transparencia. Acesso em: 23 mar. 2025.

PIURCOSKY, F. P.; COSTA, M. A.; FROGERI, R. F.; CALEGARIO, L. L. A lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos. SUMA DE NEGOCIOS, 10(23), 89-99, 2019.

ROCHA, C. P. D., CARNEIRO, A. V. S., MEDEIROS, M. V. B., and Melo, A. (2019). Segurança da informação: A iso 27001 como ferramenta de controle para lgpd. Revista de Tecnologia da Informação e Comunicação, Faculdade Estácio do Pará, 2(3):78–97.

RIBEIRO, Ramiro et al. Cibersegurança e Segurança da Informação Contábil: Uma Análise da Percepção do Profissional Contábil.Ragc, Monte Carmelo, v. 8, n. 32, p. 71-85, 20 abr. 2020.

SEVERINO, A. J. Metodologia do Trabalho Científico. São Paulo, SP: Cortez, 2007.

SAFIANU, OMAR; TWUM, FRIMPONG; B., J. Information System Security Threats and Vulnerabilities: Evaluating the Human Factor in Data Protection. International Journal of Computer Applications, v. 143, n. 5, p. 8–14, jun. 2016. ISSN 09758887. DOI: 10.5120/ijca2016910160. Disponível em: http://www.ijcaonline.org/archives/volume143/number5/safianu-2016-ijca-910160.pdf. Acesso em: 30 abr. 2025.

SALAHDINE, F.; KAABOUCH, N. Social engineering attacks: A survey. Future internet, MDPI , v. 11, n. 4, p. 89, 2019.

SANTOS, R. G. T. A Lei Geral de Proteção de Dados Brasileira: uma política pública regulatória. 2020. Monografia (Especialização) – Instituto Serzedello Corrêa Brasília, 2020. Disponível em: https://portal.tcu.gov.br/biblioteca-digital/a-lei-geral-de-protecao-de-dados-brasileira-uma-politicapublica-regulatoria.htm. Acesso em: 14 fev. 2025.

SARASWAT, A. K.; MEEL, V. Protecting data in the 21st century: challenges, strategies and future prospects. Information Technology in Industry, v. 10, n. 2, p. 26-35, 2022. Disponível em: http://www.it-in-industry.org/index.php/itii/article/view/854. Acesso em: 14 fev. 2025

STEVES, MICHELLE; GREENE, KRISTEN; THEOFANOS, Mary. National Institute of Standards and Technology. NIST. A Phish Scale: Rating Human Phishing Message Detection Difficulty, 2019. Disponível em: https://csrc.nist.gov/publications/detail/conference-paper/2019/02/24/rating-human-phishing-message-detection-difficulty. Acesso em: 23 abr 2025. Citado na página 3.

TEFFÉ, C. S.; VIOLA, M. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. Revista Eletrônica do Direito Civil. a. 9, n. 1, 2020.

UNIVERSIDADE DE BRASÍLIA. Faculdade de Ciência da Informação (Ed.). Gestão da segurança da informação e comunicações. Brasília, DF: Faculdade de Ciência da Informação, 2010. 121 p. (Série segurança da informação, v. 1).

VERIZON. Data Breach Investigations Report (DBIR), 2021. Disponível em: https://www.verizon.com/business/resources/reports/dbir/. Acesso em 02 fev. 2025. Citado na página 4.
Vert. LGPD: o desafio de implementar uma cultura digital, 2019.Disponível em: https://vert.com.br/2019/05/29/cultura-digital/. Acesso em: 03 fev. 2025.

WORLD ECONOMIC FORUM (WEF). The Global Risks Report 2022. 17th Edition. Geneva: Wef, 2022. Disponível em: https://www.weforum.org/publications/global-risks-report-2022/ . Acesso em: 29 abr. 2025. https://www.weforum.org/publications/global-risks-report-2022/