INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA BAHIA
***CAMPUS* VALENÇA**
CURSO DE TECNOLOGIA EM ANÁLISE E DESENVOLVIMENTO DE SISTEMAS

KLEBER JÚNIO DOS SANTOS COSTA

A Segurança de Dados nas Empresas do Centro Comercial de Valença: Uma Análise das Práticas e Desafios

Valença

2023

KLEBER JÚNIO DOS SANTOS COSTA

A Segurança de Dados nas Empresas do Centro Comercial de Valença: Uma Análise das Práticas e Desafios

Trabalho de Conclusão de Curso de graduação em Tecnologia em Análise e Desenvolvimento de Sistemas do Instituto Federal de Educação, Ciência e Tecnologia da Bahia (IFBA), *campus* Valença, como requisito para obtenção do grau de Tecnólogo em Análise e Desenvolvimento de Sistemas.

Orientador(a): BRUNO DE JESUS SANTOS

Valença

2023

FICHA CATALOGRÁFICA ELABORADA PELO SISTEMA DE BIBLIOTECAS DO IFBA, COM OS DADOS FORNECIDOS PELO(A) AUTOR(A)

C837s Costa, Kleber Júnio dos Santos

A segurança de dados nas empresas do centro comercial de Valença: uma análise das práticas e desafios / Kleber Júnio dos Santos Costa; orientador Bruno de Jesus Santos -- Valença : IFBA, 2023.

43f.

Trabalho de Conclusão de Curso (Tecnologia Análise e Desenvolvimento de Sistemas) -- Instituto Federal da Bahia, 2023.

1. Segurança da informação. 2. Cibersegurança. 3. Empresas. 4. segurança digita. I. Santos, Bruno de Jesus, orient. II. TÍTULO.

CDD:005.8

FOLHA DE APROVAÇÃO

KLEBER JÚNIO DOS SANTOS COSTA

A SEGURANÇA DE DADOS NAS EMPRESAS DO CENTRO COMERCIAL DE VALENÇA: UMA ANÁLISE DAS PRÁTICAS E DESAFIOS

Trabalho de Conclusão de Curso de graduação apresentado como requisito parcial para obtenção do título de Bacharel em Tecnologia em Análise e Desenvolvimento de Sistemas, do Instituto Federal de Educação, Ciência e Tecnologia da Bahia (IFBA), *campus* Valença.

Aprovado em

Valença, 04 de dezembro de 2023

Banca examinadora

Prof. Esp. Bruno de Jesus Santos – Orientador

Instituto Federal de Educação, Ciência e Tecnologia – *Campus* Valença

Prof. Me. Ernando Passos Batista Junior

Instituto Federal de Educação, Ciência e Tecnologia – *Campus* Valença

Prof. Dr. Francesco Bonelli

Instituto Federal de Educação, Ciência e Tecnologia – *Campus* Valença

DEDICATÓRIA

Dedico este trabalho a todos que estiveram ao meu lado durante esta jornada acadêmica, pois cada conquista é fruto de um esforço conjunto. Aos amigos do PRD, verdadeiros companheiros de todas as horas, pela paciência, incentivo e risadas que tornaram os desafios mais leves. Aos meus pais e minha amada esposa por serem a luz que iluminou os dias mais difíceis. A presença de vocês tornou cada passo dessa jornada mais significativo.

AGRADECIMENTOS

Aos estimados professores da faculdade, que compartilharam seu conhecimento, desafiaram meu pensamento e incentivaram meu crescimento intelectual, expresso minha gratidão. Suas orientações foram a bússola que guiou este trabalho, transformando cada desafio em uma oportunidade de aprendizado. Aos respeitáveis professores do ensino médio, cuja dedicação e paixão pelo ensino foram sementes plantadas em minha trajetória, agradeço por terem sido inspirações e pilares fundamentais no meu desenvolvimento acadêmico.

Aos amigos fora da faculdade, que estiveram presentes com apoio moral e incentivo, minha sincera gratidão. Suas palavras de estímulo foram combustíveis que impulsionaram este percurso.

Este trabalho é fruto da contribuição de cada um de vocês, professores e amigos, que, de formas diversas, moldaram minha jornada acadêmica. Que este texto expresse a profundidade da minha gratidão por suas influências positivas em meu percurso educacional.

"Tente uma, duas, três vezes e, se possível, tente a quarta, a quinta e quantas vezes for necessário. Só não desista nas primeiras tentativas, a persistência é amiga da conquista. Se você quer chegar aonde a maioria não chega, faça o que a maioria não faz." - Bill Gates

RESUMO

Num contexto empresarial cada vez mais permeado pela digitalização, a cibersegurança emerge como um elemento crítico para a integridade e proteção dos dados. Esta pesquisa, focada nas empresas do centro comercial de Valença, buscou identificar os desafios enfrentados por essas organizações no universo da segurança digital. A abordagem compreendeu desde a análise do conhecimento e conformidade com a Lei Geral de Proteção de Dados (LGPD) até a avaliação de métodos avançados de armazenamento seguro e eficácia de programas de treinamento em cibersegurança.

A pesquisa revela lacunas na aplicação da cibersegurança por parte das empresas locais, apontando para um cenário de vulnerabilidade que transcende o aspecto legal. Ao explorar métodos de armazenamento, identificou-se uma resistência persistente à transição para práticas mais seguras, como evidenciado pela prevalência de arquivos e pastas físicas. A análise detalhada não apenas destaca as deficiências existentes, mas sugere um caminho claro para fortalecer a cibersegurança nas empresas de Valença. Este trabalho contribui para a compreensão dos desafios específicos enfrentados pelas empresas locais, fornecendo não apenas uma análise crítica, mas também recomendações práticas para elevar o nível de segurança digital.

Palavras-chave: Segurança da informação. Cibersegurança. Empresas. LGPD.

ABSTRACT

In the ever-evolving landscape of contemporary business, cybersecurity stands as a critical cornerstone for the integrity and protection of sensitive data. This research delves into the intricate practices and challenges faced by businesses in the commercial center of Valença, aiming to unveil the nuances of their cybersecurity endeavors. The investigation encompasses an analysis of the comprehension and compliance with the General Data Protection Law (LGPD) and extends to the evaluation of advanced methods for secure data storage and the effectiveness of cybersecurity training programs.

Revealing significant gaps in the understanding and practical application of cybersecurity concepts among local businesses, this study transcends the legal aspect, painting a picture of vulnerability. The exploration of data storage methods identifies a persistent resistance to transition to more secure practices, exemplified by the prevalence of physical files and folders. This detailed analysis not only highlights existing deficiencies but also suggests a clear path to fortify cybersecurity in Valença's businesses. The study contributes to an understanding of the specific challenges faced by local enterprises, providing not only a critical analysis but also practical recommendations to elevate the standard of digital security.

Key words: Information security. Cybersecurity. Companies. LGPD (Brazilian General Data Protection Law).

SUMÁRIO

1 INTRODUÇÃO

Na era digital, onde dados se tornaram ativos estratégicos, a cibersegurança emerge como uma necessidade para as organizações que almejam prosperar no cenário comercial contemporâneo. Este estudo concentra sua atenção nas empresas do centro comercial de Valença, buscando não apenas entender, mas também analisar a fundo as práticas, desafios e oportunidades que permeiam a segurança digital nesse contexto. A interconexão global e a crescente dependência de ambientes digitais expõem essas empresas a ameaças cibernéticas, desde violações de dados até comprometimentos de privacidade. Nesse contexto, a compreensão e conformidade com regulamentações como a Lei Geral de Proteção de Dados (LGPD) tornam-se cruciais, não apenas como uma exigência legal, mas como um pilar fundamental na construção de uma base sólida para práticas de cibersegurança robustas.

A complexidade do ambiente cibernético, aliada às particularidades das empresas locais, delineia um panorama desafiador. Desde o conhecimento sobre as obrigações legais até a implementação de medidas efetivas, cada aspecto demanda atenção. Além disso, a transição para métodos seguros de armazenamento de dados e a conscientização dos colaboradores tornam-se elos essenciais nessa cadeia de segurança digital. Essa pesquisa teve como objetivo geral investigar a segurança de dados nas empresas localizadas no centro comercial de Valença. Buscando compreender quais as práticas atualmente em vigor e identificar potenciais áreas de aprimoramento relacionadas à cibersegurança e à proteção de dados.

Para isso será necessária uma coleta de dados para esta pesquisa que abordou parâmetros cruciais sobre segurança nas empresas do centro comercial de Valença, assim entender como ocorre a proteção dos dados e entender as necessidades na segurança. Portanto teve como objetivos específicos mapear as práticas de proteção de dados adotadas pelas empresas do centro comercial de Valença, avaliar a percepção da empresa sobre os riscos associados à falta de adequação à LGPD, tais como sanções e danos à reputação, compreender como as empresas, estão traçando estratégias para garantir a proteção de dados e identificar qual política de segurança de dados

2 FUNDAMENTAÇÃO TEÓRICA

A adequação das empresas à cibersegurança tornou-se algo imprescindível no atual contexto digital, onde tudo se movimenta ao redor da tecnologia. É muito fácil encontrar pessoas com algum dispositivo eletrônico, realizando tarefas do dia a dia, comprando, acessando notícias e comunicando-se, nesse cenário, dados privados estão circulando pela rede acontecendo em segundo plano.

O laboratório de inteligência e ameaças, FortiGuard Labs Brasil registrou no primeiro semestre de 2022, 31,5 bilhões de tentativas de ataques cibernéticos a empresas. Segundo Alexandre Bonatti, diretor da Fortinet, uma das justificativas para que haja tantos ataques no país é o baixo investimento em cibersegurança no Brasil. Hackers com más intenções estão procurando uma brecha para acessar dados privados ou de empresas.

2.1 REDES DE COMPUTADORES

Nessa era de digital onde as empresas têm seus dados circulando por um conjunto de sistemas computacionais interligados que permitem a troca de informações e dados, chamada de rede de computadores, existem diferentes tipos de redes, cada uma com suas características e finalidades específicas. É de grande importância ter isso fixado, para proteger seus dados e de seus clientes, temos redes locais (LAN), são redes privadas localizadas em uma área geográfica pequena, como um escritório ou prédio, redes metropolitanas (MAN), estas redes cobrem uma área geográfica maior do que as LANs, geralmente abrangendo uma cidade inteira, redes de longa distância (WAN), estas redes cobrem grandes áreas geográficas, como países ou continentes. A internet é um exemplo de uma WAN.

As redes estão interligadas através da internet, que por sua vez também tem sua divisão, internet: é uma rede global de computadores que utiliza o protocolo TCP/IP para conectar dispositivos em todo o mundo. Ela permite a comunicação e a troca de informações entre usuários, independentemente de sua localização geográfica. Ethernet: é uma tecnologia de rede local (LAN) que permite a comunicação entre dispositivos conectados à mesma rede. Ela usa um sistema de cabos para transmitir dados entre os dispositivos na rede. Cada um

desses conceitos desempenha um papel crucial na forma como as informações são compartilhadas e gerenciadas no mundo digital atual.

2.2 AMEAÇAS À SEGURANÇA DA INFORMAÇÃO

A obtenção de uma vantagem competitiva sólida exige que as empresas não apenas adotem, mas também abracem a tecnologia de forma estratégica. Como Neves, Pavani, Sales e Lopes (2021) destacam, dominar o mercado atual implica em obter informações detalhadas e relevantes sobre os clientes. Esses insights não são mais um luxo, mas uma necessidade de entender as demandas em constante mudança e as expectativas dos clientes.

Nesse contexto, as empresas estão recorrendo a ferramentas avançadas, como análise de dados, inteligência artificial e aprendizado de máquina, para extrair informações valiosas dos enormes volumes de dados gerados diariamente. Essas tecnologias capacitam as empresas a compreender melhor o comportamento do cliente, antecipar tendências e personalizar experiências, assim manipulando os usuários trazendo a eles a pena o que a empresa quer.

No entanto, é importante notar que o mero investimento em tecnologia não é suficiente. As empresas também devem estar dispostas a adaptar suas estratégias e processos para a segurança da informação. Se não investir na cibersegurança todo o trabalho será perdido.

Dados, Informação e Segurança são conceitos fundamentais no mundo da tecnologia da informação. Os dados são fatos brutos que não foram processados e analisados, podendo vir em várias formas, como números, palavras, imagens, sons e muito mais. Por si só, os dados podem não ter significado ou contexto. A informação, por outro lado, é o resultado do processamento, manipulação e organização dos dados de tal forma que eles têm um valor adicional além do valor do dado em si. A informação é o que dá aos dados um contexto e um propósito. A segurança é uma preocupação primordial para empresas e indivíduos, pois uma violação de segurança pode resultar em perda de confidencialidade, integridade e disponibilidade de dados e informações. Portanto, é importante entender a diferença entre dados e informações e a importância da segurança na proteção desses ativos valiosos.

De acordo com Takeuchi (2023, p. 8) “O sucesso (ou falha) de qualquer ataque cibernético depende de fatores técnicos, principalmente, mas também de fatores humanos.” É de grande importância para a segurança das empresas, ter um ótimo software de antivírus, manter todo sistema atualizado pois um dos principais meios de acesso dos hackers aos sistemas é por meio de falhas encontradas em softwares, sistemas operacionais e drivers desatualizados. Utilizar um sistema de criptografia de dados é uma ótima forma técnica para dificultar, que sofra ataques cibernéticos. O backup é uma opção, fornecendo uma recuperação eficiente de dados por meio de um servidor externo, um HD externo ou na nuvem. É essencial não abrir mão dessa ferramenta.

Segundo Freitas (2018, p.1) “A engenharia social utiliza técnicas para explorar a vulnerabilidade ocasionada pelo fator humano no intuito de driblar as barreiras de segurança tecnológicas”. Esta abordagem se baseia na manipulação psicológica de indivíduos para que eles divulguem informações confidenciais ou realizem ações que possam comprometer a segurança de um sistema. A engenharia social é eficaz porque, muitas vezes, é mais fácil explorar a propensão natural do ser humano à confiança do que tentar encontrar maneiras de hackear o software. Isso destaca a importância da conscientização e educação em segurança cibernética como uma linha de defesa. A conscientização e a educação em segurança cibernética são linhas de defesa essenciais contra essas ameaças.

O vazamento de dados por fatores humanos é algo muito importante para considerar, pois as brechas de segurança em empresas podem ocorrer devido a erros humanos. Além disso, ações intencionais também podem ser uma fonte de vazamento de informações. É importante que as empresas invistam em treinamentos para conscientizar seus funcionários sobre as melhores práticas de segurança cibernética e ferramentas de segurança para proteger seus sistemas contra ameaças externas. Como os usuários no dia a dia acreditam que está tudo bem ao usar seus dispositivos eles subestimam os riscos cibernéticos, mostrando não possuir uma consciência sobre a importância da segurança da informação, assim ficam expostos. Podendo fazer com que os usuários evitem medidas de segurança, como senhas complexas, em favor de conveniência, os erros e enganos humanos são uma fonte significativa de vulnerabilidades de segurança.

A busca por informações fornecidas sobre os clientes e a adoção de tecnologias avançadas são elementos interligados que capacitam as empresas a competir e prosperar em um ambiente de negócios em constante transformação. A capacidade de inovação e adaptação tecnológica tornou-se um diferencial competitivo vital em uma era pós-pandemia, pois é preciso ter responsabilidade pois algumas empresas abraçam essa mudança e estão procurando não importa como dominar o mercado, como os dados são informações valiosas e assim tentar manipular as necessidades dos clientes.

Para enfrentar esse desafio, é imperativo que as empresas implementem métodos claros e abrangentes para aumentar a conscientização em segurança da informação e treinem os funcionários sobre a importância crítica da proteção de dados e sistemas de organização.

A conscientização em segurança da informação desempenha um papel fundamental na mitigação de riscos cibernéticos. É um investimento importante para garantir que todos os indivíduos estejam cientes dos riscos existentes, compreendam as boas práticas de segurança e sejam capazes de tomar medidas como permissão para proteger os dados e sistemas de organização. É uma necessidade urgente em um mundo cada vez mais digital, onde a segurança da informação é uma preocupação constante.

De acordo com Silveira, Avelino e Souza (2016, p. 4), as corporações podem analisar os dados recebidos dos seus consumidores e organizar estratégias personalizadas para seus produtos e serviços. No entanto, é fundamental destacar que essa análise de dados deve ser realizada com extrema atenção à segurança da informação.

A coleta, armazenamento e análise de dados de clientes envolvem informações sensíveis que precisam ser protegidas contra ameaças cibernéticas. É preciso investir significativamente em medidas de segurança cibernética robustas.

A negligência na segurança de dados pode resultar em violações de privacidade e danos à reputação da empresa, é imperativo que implementem

políticas e tecnologias de segurança de informações sólidas para garantir a integridade e a confidencialidade dos dados do cliente.

A análise de dados para estratégias personalizadas é uma ferramenta poderosa para as empresas, mas essa análise deve ser acompanhada de um compromisso igualmente forte com a segurança da informação. O equilíbrio entre a personalização eficaz e a proteção dos dados do cliente é essencial para o sucesso a longo prazo das corporações na era digital, para isso a cibersegurança toma medidas e delimita regras para que os dados sejam trabalhados de forma segura.

2.3 CIBERSEGURANÇA

A Cibersegurança, um campo de importância crucial no mundo digital atual, é fundamentada através da CID - Confidencialidade, Integridade e Disponibilidade. A Confidencialidade assegura que as informações sejam acessíveis apenas por indivíduos autorizados, empregando mecanismos de segurança como autenticação de usuários, senhas, listas de controle de acesso e criptografia. A Integridade diz respeito à precisão e consistência dos dados, garantindo que as informações permaneçam inalteradas durante o armazenamento e a transferência, a menos que sejam modificadas por uma ação autorizada. A Disponibilidade assegura que os dados estejam sempre acessíveis para os usuários autorizados quando necessário, o que envolve a manutenção dos sistemas operacionais, a realização regular de backups e a existência de planos de recuperação de desastres. Esses três pilares são vitais para o estabelecimento da cultura de proteção de dados e são desenvolvidos simultaneamente para garantir a segurança da informação nas organizações.

De acordo com Caldas e Freire (2013, p. 6) “A reflexão torna-se muito pertinente se colocada em termos de qual a extensão do impacto que os ciberataques têm na segurança nacional.” Um ataque cibernético é uma ação realizada por criminosos virtuais com o objetivo de desabilitar sistemas de computador, extrair informações ou utilizar um sistema comprometido para realizar ataques subsequentes. Os ciberataques representam uma ameaça significativa à segurança governamental. Eles têm o potencial de comprometer a confidencialidade, integridade e disponibilidade de dados e sistemas públicos.

Isso pode afetar várias áreas críticas, incluindo saúde, eleições, defesa e infraestrutura.

Além disso, os ciberataques podem causar danos econômicos, operacionais e reputacionais aos órgãos públicos e aos cidadãos afetados. Isso pode levar a perdas financeiras substanciais e a uma diminuição da confiança do público nas instituições governamentais. Os cibercriminosos exploram vulnerabilidades e fragilidades na legislação, na regulação e na fiscalização do ciberespaço. Isso pode permitir que eles realizem atividades ilícitas com impunidade.

Por fim, os ciberataques podem ser usados para influenciar ou desestabilizar o cenário político, social e democrático do país. Isso pode ser feito através de campanhas de desinformação, espionagem ou sabotagem. Essas atividades podem ter um impacto profundo na estabilidade e segurança de uma nação. O uso da internet, embora traga inúmeros benefícios, também apresenta uma série de ameaças. Isso inclui uma variedade de atividades maliciosas, como roubo de identidade, fraude financeira, espionagem cibernética e ciberataques a infraestruturas críticas.

Além disso, a internet pode ser usada para disseminar desinformação e propaganda, o que pode ter sérias consequências sociais e políticas. A desinformação pode influenciar as opiniões públicas, incitar o ódio e a violência, e até mesmo influenciar os resultados das eleições. A privacidade online é outra grande preocupação. A coleta e o uso indevido de dados pessoais por empresas e governos podem levar a violações de privacidade. Além disso, a vigilância online pode resultar em censura e repressão, a dependência excessiva da internet pode levar a problemas de saúde mental, como ansiedade e depressão. Também pode contribuir para o isolamento social e a diminuição das habilidades sociais. Portanto, é crucial estar ciente dessas ameaças ao usar a internet e tomar medidas adequadas para se proteger.

Os malwares, ou softwares maliciosos, são programas desenvolvidos com a intenção de causar danos a sistemas de computadores ou para roubar

informações sensíveis. Existem vários tipos de malwares, cada um com suas próprias características e métodos de operação. Os vírus, por exemplo, são softwares que se replicam e infectam arquivos e programas em um computador. Quando esses arquivos infectados são executados, o vírus é ativado e pode se espalhar, causando danos significativos ao sistema. Os Cavalos de Tróia, por outro lado, são malwares que se disfarçam de software legítimo. Eles enganam o usuário para que instale o software, que então libera o malware em seu sistema. Isso pode resultar em roubo de dados ou controle remoto do sistema pelo cibercriminoso.

Os Worms são outro tipo de malware que se auto replica em sistemas informatizados sem a necessidade de utilizar um programa hospedeiro. Eles podem se espalhar rapidamente e causar danos generalizados. O Adware é um tipo de malware que exibe publicidade indesejada e às vezes maliciosa na tela do usuário. Embora possa parecer inofensivo, o adware pode ser usado para rastrear a atividade online do usuário e coletar informações pessoais. O Spyware é um tipo de malware que se esconde no dispositivo do usuário, monitora suas atividades e rouba informações sensíveis. Isso pode incluir dados financeiros, informações de conta e logins. Cada tipo de malware apresenta uma ameaça única e requer uma abordagem diferente para prevenção e remoção. Portanto, é crucial estar ciente dessas ameaças ao usar a internet e tomar medidas adequadas para se proteger.

A cibersegurança é de suma importância na proteção contra ciberataques. Ela serve como a primeira linha de defesa contra criminosos cibernéticos, protegendo dados e sistemas públicos de serem comprometidos. Através da implementação de medidas de segurança robustas, como firewalls, software antivírus e práticas de segurança de dados, a cibersegurança pode prevenir a maioria dos ciberataques. Além disso, a cibersegurança também desempenha um papel crucial na minimização dos danos causados por um ciberataque. Isso é feito através da detecção rápida de atividades suspeitas, permitindo uma resposta imediata para conter o ataque e limitar seu impacto. A cibersegurança também é essencial para manter a confiança do público nas instituições governamentais. Ao demonstrar que o governo leva a sério a proteção dos dados do público, a confiança na capacidade do governo de proteger seus cidadãos é reforçada.

A cibersegurança ajuda a proteger o país contra tentativas de desestabilização política e social. Ao proteger as infraestruturas críticas contra ciberataques, ela ajuda a garantir a estabilidade e segurança da nação. Assim como no setor governamental, a cibersegurança é de vital importância para as empresas, as empresas modernas dependem fortemente de sistemas digitais para suas operações diárias, tornando-as alvos atraentes para cibercriminosos. A cibersegurança protege esses sistemas e os dados confidenciais que eles contêm contra ciberataques.

A implementação de medidas de segurança robustas pode prevenir a maioria dos ciberataques, protegendo a empresa contra interrupções operacionais e perdas financeiras. Além disso, uma resposta rápida a um ciberataque pode limitar seu impacto e minimizar os danos. A confiança dos clientes e parceiros comerciais em uma empresa pode ser seriamente prejudicada se seus dados forem comprometidos. Portanto, a cibersegurança também é crucial para manter a reputação da empresa e a confiança do cliente.

Por último, mas não menos importante, as empresas desempenham um papel crucial na economia de um país. Ao proteger as empresas contra ciberataques, a cibersegurança contribui para a estabilidade econômica do país como um todo. Portanto, investir em cibersegurança não é apenas uma decisão empresarial sensata, mas também uma contribuição importante para a segurança nacional.

2.4 LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados (Lei nº 13..709/18 – LGPD), na legislação a norma ISO 27000 que estabelece diretrizes para a gestão da segurança da informação, proporcionando um ambiente seguro para o armazenamento e processamento de dados. Vigilante na preservação dos dados pessoais, com procedimentos necessários na era digital, onde os dados pessoais são considerados uma mercadoria valiosa, segundo Almeida e Soares (2022, p. 36) “LGPD em toda a sua extensão, prevê obrigações para que as empresas e as instituições possam manter o registro e tratamento dos dados visando em ações futuras.” Portanto, a aplicação da LGPD nas empresas não só garante a

conformidade legal, mas também promove a confiança dos clientes ao demonstrar o compromisso da empresa com a proteção de seus dados.

A cibersegurança foi desenvolvida em 1987, e mesmo assim ainda os dados pessoais continuam sendo vazados, falta da aplicação facilitando a distribuição desses dados. A legislação precisou atualizar para aplicação da LGPD, podendo ser aplicada a qualquer operação de tratamento realizada por pessoa natural ou jurídica, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados.

A LGPD busca garantir que os métodos indicados pela Cibersegurança, em conformidade com a Tríade CID, sejam respeitados e atendidos. Isso implica que as práticas de proteção de dados devem garantir a confidencialidade, integridade e disponibilidade das informações, conforme os princípios da cibersegurança, para estar em conformidade com a LGPD.

De acordo com Silveira, Avelino e Souza (2016, p. 219) “O mercado de dados pessoais se baseia nas necessidades de informação das empresas, instituições públicas e usuários finais.” Com isso, as empresas devem garantir que o consentimento para o tratamento de dados foi obtido de acordo com a LGPD e manter registro das operações de tratamento de dados pessoais que realizam. A LGPD impõe uma série de obrigações às empresas para garantir a proteção adequada dos dados pessoais, para garantir que as empresas venham realmente aplicar as normas, a lei prever multas severas.

2.5 CUMPRIMENTO DAS OBRIGAÇÕES DA LGPD PELAS EMPRESAS

A Lei Geral de Proteção de Dados (LGPD), em vigor no Brasil, impõe uma série de obrigações às empresas a fim de garantir que o tratamento de dados pessoais seja realizado de maneira responsável e segura. Este trabalho tem como objetivo analisar as principais obrigações impostas pela LGPD às empresas e destacar a importância de seu cumprimento para proteger os dados pessoais e garantir a conformidade com a legislação.

Uma das obrigações fundamentais sob a LGPD é a obtenção de consentimento adequado para o tratamento de dados pessoais. As empresas devem assegurar que os titulares dos dados tenham pleno conhecimento e

escolha sobre como suas informações serão utilizadas. Seguindo todo Artigo 7º da LGPD detalha as condições para o tratamento de dados pessoais, no inciso I deixa bem claro que o tratamento de dados pessoais só poderá ocorrer com a obtenção de consentimento.

O artigo 37, é estipulado que as empresas são obrigadas a manter registros detalhados das operações de tratamento de dados pessoais que realizam. Esses registros são essenciais para demonstrar conformidade com a LGPD e permitir rastreabilidade das ações realizadas. A elaboração de um relatório de impacto à proteção de dados pessoais é uma obrigação relevante para avaliar e mitigar riscos relacionados ao tratamento de informações sensíveis, esse dever da empresa está regido no artigo 38 da LGPD.

Sobre os responsáveis pelos dados, no caso o titular, a lei também deixa claro no artigo 9º, inciso V da lei que as empresas devem comunicar aos titulares dos dados qualquer alteração na finalidade para a qual os dados foram coletados. Isso garante que os titulares tenham controle sobre suas informações, assim tendo mais confiabilidade na segurança dessa empresa.

A Responsabilidade Solidária é um princípio importante na LGPD, estabelecido no Artigo 42 da lei. De acordo com esse princípio, tanto o controlador de dados quanto o operador de dados (processador) podem ser considerados igualmente responsáveis por eventuais violações da legislação de proteção de dados. Isso significa que se um terceiro (um operador, por exemplo) que está envolvido no tratamento de dados pessoais causar uma violação, o controlador (a entidade que detém e define a finalidade do tratamento) também pode ser responsabilizado. A Responsabilidade Solidária destina-se a garantir que todas as partes envolvidas no tratamento de dados pessoais estejam cientes de suas obrigações e atuem em conformidade com a LGPD.

Os princípios da transparência e controle são destacados nos incisos I e II do Artigo 6º, a transparência é crucial. As empresas devem fornecer informações claras aos titulares sobre como seus dados são tratados, é de suma importância que os titulares possam excluir e editar seus dados não adianta querer fazer o cadastro de novos clientes, para ter um banco de dados bem elaborado a vezes,

e depois privar os titulares não permitindo que exerçam controle sobre essas informações.

O Artigo 39 aborda a necessidade de treinamento de funcionários no contexto da proteção de dados pessoais. O treinamento de funcionários é um elemento crítico para garantir que todos os membros da equipe estejam cientes das responsabilidades e boas práticas relacionadas à proteção de dados pessoais. A LGPD exige que as empresas estabeleçam programas de treinamento destinados a educar seus funcionários sobre as disposições da lei, bem como sobre as políticas internas da empresa relacionadas à proteção de dados, com esse treinamento aos funcionários além de garantir a conformidade com a LGPD, ele ajuda a reduzir o risco de violações de dados e a fortalecer a proteção de informações pessoais.

O Artigo 41 menciona a necessidade de as empresas estabelecerem políticas internas para garantir a conformidade com a LGPD, essas políticas internas são essenciais para orientar os funcionários e todos os envolvidos no tratamento de dados pessoais sobre as práticas e procedimentos necessários para proteger esses dados e garantir a conformidade com a lei. Incluindo a designação de um Encarregado de Proteção de Dados (DPO) para supervisionar as atividades, promovendo boas práticas de segurança e proteção de dados pessoais.

A Responsabilização por Infrações, como definida no Artigo 52, é uma medida importante para garantir que as empresas levem a sério a proteção de dados pessoais. Ela incentiva a conformidade com a legislação, promovendo boas práticas de proteção de dados e reforçando a responsabilidade das empresas em relação à privacidade e à segurança das informações pessoais de seus clientes, funcionários e parceiros. Portanto, as empresas devem estar preparadas para adotar medidas corretivas e punitivas quando necessário, de acordo com a LGPD, a fim de proteger os direitos dos titulares dos dados e manter a confiança do público.

O cumprimento das obrigações da LGPD pelas empresas é essencial para garantir a proteção dos dados pessoais e a conformidade com a legislação. A LGPD busca equilibrar os interesses comerciais com a privacidade dos indivíduos,

e as empresas desempenham um papel crucial nesse processo. A implementação adequada dessas obrigações não apenas reduz os riscos legais e financeiros, mas também reforça a confiança dos clientes e parceiros. Portanto, é fundamental que as empresas adotem medidas proativas para garantir a conformidade com a LGPD e, ao fazer isso, contribuam para um ambiente digital mais seguro e respeitoso com a privacidade.

3 PROCEDIMENTOS METODOLÓGICOS

Esta pesquisa tem como objetivo principal investigar a segurança de dados nas empresas localizadas no centro comercial de Valença. Buscando compreender essa questão crítica, foi elaborada uma abordagem qualitativa, pois permite aprofundar na compreensão das práticas de cibersegurança. Ela não apenas busca respostas "sim" ou "não", mas explora as nuances e as razões por trás das decisões e ações das empresas em relação à segurança de dados.

Bem, essa pesquisa busca minuciosamente avaliar a competência dos profissionais que desempenham um papel crucial nesse processo de controladores de dados pessoais. O objetivo subjacente é compreender as práticas atualmente em vigor e identificar potenciais áreas de aprimoramento relacionadas à cibersegurança e à proteção de dados.

A seleção das empresas do centro comercial de Valença como o público-alvo desta pesquisa é respaldada por sua posição estratégica e vital na região, bem como pela relevância crítica da cibersegurança no cenário empresarial contemporâneo. Essas organizações, ao operar em setores diversos como sapataria, venda de roupas, óticas, clínicas odontológicas, supermercados, casa de embalagem, farmácias, loja para material de construção, lojas de eletrodomésticos, desempenha um papel central na economia local, detêm dados pessoais de clientes, funcionários e parceiros de negócios. A crescente interconectividade e a digitalização dos processos comerciais tornaram essas empresas suscetíveis a uma ampla gama de ameaças cibernéticas, incluindo ataques de ransomware, vazamento de dados e instruções maliciosas.

Portanto, investigar a postura de cibersegurança dessas empresas não apenas é de importância estratégica para a proteção dos interesses das partes

interessadas, mas também contribui significativamente para a compreensão de como a implementação da LGPD pode ser um recurso valioso na mitigação dessas ameaças. A pesquisa almeja identificar lacunas e áreas de melhoria nas práticas de cibersegurança dessas empresas, com o objetivo exploratório para identificar a proteção dos dados, consolidando, assim, a confiabilidade e a integridade das informações.

Para garantir uma análise abrangente e representativa das práticas de cibersegurança nas empresas do centro comercial de Valença, uma amostra de 40 empresas de onde se encontram aproximadamente 80 empresas, a amostra selecionada de forma aleatória, tendo 20 empresas do ramo de roupa e sapataria, 3 supermercados, 2 óticas, 5 clínicas odontológicas, 2 lojas de eletrodomésticos, 3 empresas de multimídia e variedades, 2 lojas de material de construção e 3 farmácias. Essa abordagem visa capturar uma gama mais ampla de perspectivas e práticas em relação à proteção de dados e cibersegurança. A escolha de empresas de diversos setores, tamanhos e estruturas organizacionais oferece uma visão mais holística das complexidades envolvidas na gestão de informações sensíveis em um ambiente comercial diversificado.

A amostra aleatória contribui para minimizar o viés de seleção, permitindo que empresas de diferentes perfis e contextos sejam incluídas na pesquisa. Isso é fundamental para garantir que a pesquisa reflita de maneira precisa as variações nas práticas de cibersegurança e nas políticas de proteção de dados nas empresas do centro comercial de Valença. A diversidade da amostra também é fundamental para avaliar os impactos e desafios da LGPD em um espectro mais amplo de negócios locais, fornecendo uma base sólida para recomendações futuras na área de cibersegurança e privacidade de dados.

A pesquisa foi projetada seguindo uma sequência lógica de etapas para garantir sua eficácia e relevância. Inicialmente, a pesquisa foi precedida por uma revisão da literatura para compreender as melhores práticas em cibersegurança e a relação da LGPD com a proteção de dados em contextos empresariais. Isso serviu como base teórica sólida para a pesquisa. Onde foi encontrado todo objetivo da pesquisa, os desafios propostos para trabalhar com o público alvo, para entender qual seria a melhor forma de encontrar respostas.

Depois da escolha do público alvo, a etapa subsequente envolveu o desenvolvimento de um questionário estruturado, que foi projetado para coletar dados relevantes sobre as práticas de cibersegurança e a conformidade com a LGPD nas empresas do centro comercial de Valença. Com os tópicos-chave identificados, o próximo passo foi formular perguntas relevantes para cada tópico. As perguntas foram projetadas de forma a serem claras, concisas e não tendenciosas, evitando induzir respostas específicas. Além disso, as perguntas foram elaboradas de maneira a abranger diferentes aspectos de cada tópico. O questionário incluiu perguntas sobre políticas de segurança de dados, treinamento de funcionários, incidentes de segurança e outras áreas relacionadas à cibersegurança. Após a formulação inicial das perguntas, o questionário passou por um processo de revisão por especialistas, incluindo profissionais de cibersegurança, especialistas em LGPD e pesquisadores qualificados. Essa revisão ajudou a aprimorar a clareza das perguntas e garantir sua relevância.

Antes da aplicação completa, o questionário passou por um teste piloto com um grupo seleto de empresas locais, onde basicamente foi perguntado sobre como estavam se adequando com a LGPD, não incluídas na amostra final. Isso permitiu identificar problemas potenciais, como perguntas mal interpretadas ou dificuldades de resposta. Com base no feedback do teste piloto, o questionário foi refinado. O questionário foi organizado de forma lógica, com uma sequência que facilitasse a compreensão por parte dos respondentes.

As perguntas foram agrupadas por tópico e apresentadas em uma ordem que fluísse naturalmente, garantindo que as informações obtidas fossem relevantes para os objetivos da pesquisa. Esse questionário serviu como uma ferramenta valiosa para a coleta de informações das empresas do centro comercial de Valença, fornecendo dados essenciais para a análise das práticas de cibersegurança e conformidade com a LGPD.

De acordo com Selltiz (1965, p. 172), formulário "é o nome geral usado para designar uma coleção de questões que são perguntadas e anotadas por um entrevistador numa situação face a face com outra pessoa". A aplicação do questionário nas empresas do centro comercial de Valença foi realizada de maneira pessoal, diretamente com o responsável de cada empresa. Essa

abordagem direta de coleta de dados, oferece várias vantagens e contribui para a qualidade e confiabilidade dos resultados da pesquisa. Pois como vamos estar falando diretamente com o representante, assim conseguimos ter uma pesquisa mais qualificada.

Antes da aplicação do questionário, foi estabelecido um contato direto com os responsáveis de cada empresa. Esse contato inicial tinha como objetivo apresentar a pesquisa, explicar seu propósito e solicitar a participação voluntária no estudo. Esse processo de comunicação permitiu estabelecer um relacionamento de confiança com os respondentes, tornando-os mais receptivos à pesquisa. Durante a aplicação do questionário, foi observado que muitos dos entrevistados nas empresas do centro comercial de Valença tinham um conhecimento limitado ou, em alguns casos, nulo, sobre a LGPD (Lei Geral de Proteção de Dados). Essa falta de familiaridade com a legislação representou uma dificuldade inicial na coleta de dados, uma vez que a LGPD desempenha um papel central na pesquisa em questão.

Durante essas entrevistas, foi esclarecida qualquer dúvida que os respondentes pudessem ter e orientações sobre o questionário, os entrevistados receberam informações sobre os direitos dos titulares de dados, as responsabilidades das empresas, e as penalidades associadas ao não cumprimento da legislação. Além disso, a pesquisa destacou os benefícios da conformidade com a cibersegurança e LGPD, incluindo o fortalecimento da confiança dos clientes e parceiros comerciais, a proteção da reputação da empresa e a redução de riscos relacionados à segurança de dados. Esse envolvimento direto permitiu uma compreensão mais profunda das respostas e uma interpretação adequada das informações fornecidas.

Essa abordagem educativa não apenas permitiu uma compreensão mais profunda por parte dos entrevistados, mas também promoveu a conscientização sobre a importância da proteção de dados em um ambiente de negócios cada vez mais digital. Isso, por sua vez, contribuiu para a coleta de dados mais informados e revelou a necessidade de educação contínua sobre cibersegurança e privacidade de dados nas empresas locais. Portanto, a dificuldade inicial em relação ao conhecimento limitado sobre a LGPD foi abordada de maneira eficaz

por meio de explicações detalhadas e acessíveis, enriquecendo a qualidade dos dados coletados e destacando a necessidade de conscientização contínua sobre o tema. Como o questionário foi aplicado pessoalmente, essa abordagem pessoal permitiu estabelecer conexões locais, demonstrando interesse e respeito pelas empresas do centro comercial de Valença, o que pode ser valioso tanto para pesquisas futuras quanto para a formulação de recomendações práticas em cibersegurança e conformidade com a LGPD. Visando assim fortalecer esses laços e ter um resultado positivo no centro comercial de Valença, pois como houve uma explicação antes da aplicação, os responsáveis pela empresa já têm no mínimo um conhecimento prévio sobre as práticas em cibersegurança e como baseado na legislação regida pela LGPD podem se adequar da melhor forma.

4 ANÁLISE DA PESQUISA

O capítulo em questão representa a essência desta pesquisa, onde os insights cruciais obtidos por meio das entrevistas e da aplicação do questionário sobre cibersegurança e adequação à LGPD nas empresas do centro comercial de Valença serão minuciosamente examinados. Este estágio crítico da pesquisa oferece a oportunidade de mergulhar profundamente nas respostas obtidas, identificar padrões, correlações e lacunas nas práticas de cibersegurança, bem como avaliar o nível de aderência das empresas à Lei Geral de Proteção de Dados Pessoais.

A riqueza de informações coletadas, junto com a diversidade das empresas participantes, promete revelar um panorama abrangente do estado atual da cibersegurança nesse cenário local específico. A análise aprofundada dos dados permitirá a formulação de conclusões robustas, possibilitando, assim, contribuições significativas para o entendimento das dinâmicas de segurança de dados.

A coleta de dados ocorreu por meio de entrevistas presenciais com os responsáveis de empresas selecionadas aleatoriamente, esta abordagem visou abranger uma ampla diversidade de perspectivas, permitindo uma análise abrangente das práticas de cibersegurança e adequação à LGPD no contexto empresarial local. Este estudo foca no setor comercial, buscando contribuir para

o entendimento e aprimoramento das práticas de segurança de dados nas empresas de Valença.

Inicialmente, a chegada nas empresas foi primordial para pesquisa, pois foi necessário explicar de forma clara, mostrando o propósito e relevância para o contexto empresarial. A reação dos entrevistados foi geralmente receptiva, destacando uma conscientização crescente sobre a importância da cibersegurança. Muitos expressaram interesse em contribuir para o estudo, reconhecendo a relevância de suas práticas de dados para a segurança e confiabilidade dos negócios.

A estratégia de interação pessoal revelou-se crucial na dinâmica das entrevistas, proporcionando um ambiente aberto e colaborativo. Essa abordagem permitiu não apenas a coleta eficiente de respostas, mas também a oportunidade imediata de esclarecer quaisquer dúvidas que os entrevistados pudessem ter em relação à pesquisa.

O questionário elaborado para as entrevistas foi desenhado para abranger uma gama abrangente de aspectos relacionados à cibersegurança nas empresas do centro comercial de Valença. Cada pergunta foi formulada com o propósito específico de obter insights detalhados e construir uma compreensão abrangente do panorama de proteção de dados nesse contexto empresarial.

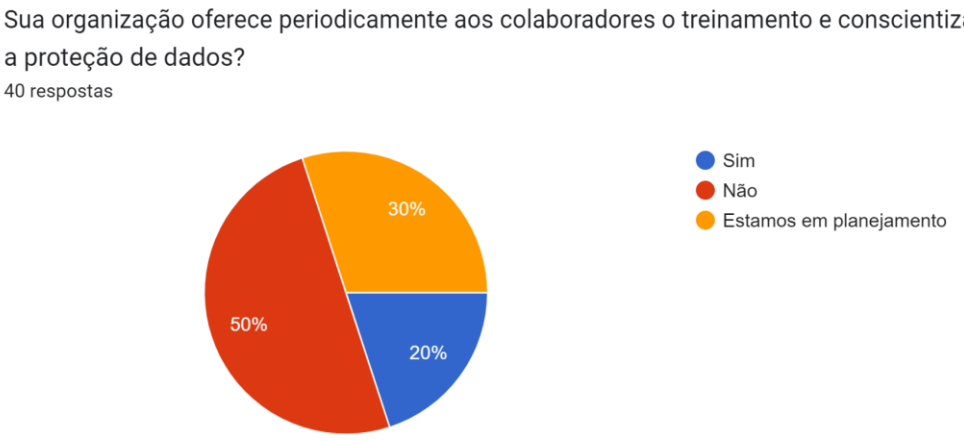


Gráfico 1: Práticas de Treinamento e Conscientização sobre Proteção de Dados nas Organizações de Valença

A análise da seção dedicada ao treinamento e conscientização revela uma variedade de abordagens de políticas pelas empresas do centro comercial de Valença em relação à educação de seus colaboradores sobre cibersegurança. Notavelmente, 20% das empresas afirmam ter implementado programas de treinamento de forma eficaz, diminuindo o comprometimento atual. Em contrapartida, 50% declaram não possuir iniciativas de treinamento, sinalizando uma possível lacuna na conscientização e preparação para as práticas de cibersegurança e LGPD. Além disso, 30% estão em fase de planejamento, evidenciando uma intenção futura de implementação de programas educativos. Essa distribuição heterogênea destaca a diversidade de posturas entre as empresas, sinalizando a necessidade de estratégias diferenciadas para fortalecer a conscientização e a educação em cibersegurança, alinhadas com as demandas da LGPD. A compreensão dessas será crucial para desenvolver recomendações específicas e resultados adaptados às necessidades individuais das empresas, aprimorando suas práticas de treinamento e, por conseguinte, fortalecer a cultura de segurança de dados e conformidade com a legislação vigente.

Indagando sobre como as empresas armazenam dados e controlam o acesso, a pesquisa direcionou o foco para a infraestrutura tecnológica e as medidas de segurança inovadoras. Essa área de questionamento permitiu avaliar a robustez dos sistemas de armazenamento e controle de dados.

Gráfico 2: Práticas de armazenamento empregadas pelas empresas do centro comercial de Valença.

Com as respostas coletadas foi possível ter uma visão penetrante sobre as práticas de armazenamento empregadas pelas empresas do centro comercial de Valença. Os resultados revelam uma distribuição distribuída: 22,5% utilizam drives na rede, 12,5% optam por memória externa, 22,5% escolhem a memória local do computador, enquanto importantes ainda 42,5% recorrem a arquivos e pastas físicas. A opção majoritária por arquivos e pastas físicas, embora tradicionais, expõe as empresas a riscos substanciais, especialmente no contexto de cibersegurança. Essa abordagem antiquada pode resultar em vulnerabilidades graves, como acesso não autorizado, perda de dados financeiros devido a eventos adversos como incêndios ou inundações, e dificuldades inerentes na implementação de medidas eficazes de controle de acesso.

Diante das respostas que os arquivos são armazenados em pastas e arquivos físicos, foi orientado sobre os riscos e a promoção de práticas de armazenamento digital seguro tornam-se imperativas para melhorar a resiliência das empresas diante de ameaças cibernéticas. A análise dos métodos de armazenamento não apenas delineia o panorama atual, mas também aponta para áreas críticas que requerem atenção imediata na busca por uma estratégia de cibersegurança mais robusta e homologada com as demandas da era digital.

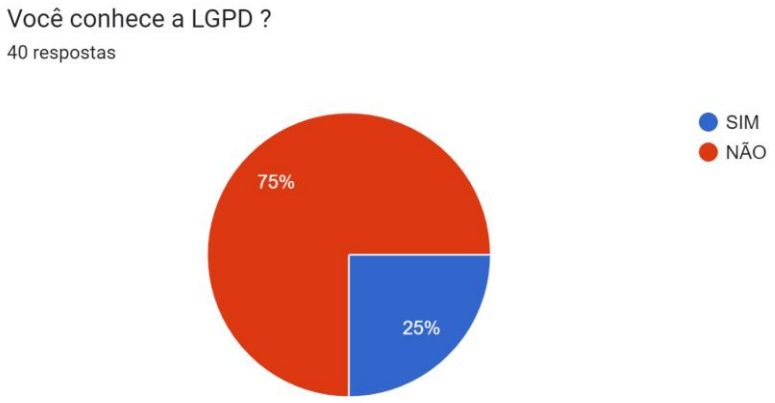


Gráfico 3: Conhecimento da LGPD das empresas.

Sobre o conhecimento da LGPD o questionário apresentou uma realidade preocupante: 75% das empresas do centro comercial de Valença indicam não ter conhecimento sobre a Lei Geral de Proteção de Dados. Esta lacuna no

entendimento da legislação, que visa salvaguardar a privacidade e a segurança das informações pessoais, não representa apenas um desafio de conformidade legal, mas também amplia os riscos substanciais relacionados à cibersegurança.

A LGPD, ao estabelecer diretrizes rigorosas para a coleta, armazenamento e processamento de dados pessoais, não apenas resguarda a privacidade dos indivíduos, mas também exige que as empresas implementem medidas sólidas de segurança de dados. O desconhecimento generalizado sobre essa legislação significa que a maioria das empresas pode estar inadvertidamente negligenciando práticas essenciais de proteção de dados, o que, por sua vez, cria uma vulnerabilidade específica a ameaças cibernéticas.

De acordo com Martins (2022 p. 111) “com o aumento dos ciberataques, a proteção dos dados pessoais está, mais do que nunca, dependente da cibersegurança”. A relação entre a LGPD e a cibersegurança é essencial para compreender a amplitude das consequências. A legislação não apenas estabelece disposições para o tratamento responsável dos dados, mas também pressupõe a implementação de medidas robustas de segurança da informação. A falta de conhecimento sobre essas diretrizes pode resultar em práticas restritas de coleta, armazenamento e processamento de dados, aumentando exponencialmente a probabilidade de transparência de segurança.

Portanto, a conscientização sobre a LGPD não é meramente uma formalidade legal, mas um aviso crucial para a cibersegurança. A falta de compreensão cria uma vulnerabilidade que pode ser explorada por fatores maliciosos. Nesse contexto, é imperativo que as empresas não apenas busquem conformidade com a legislação, mas também incorporem a LGPD como um elemento central em suas estratégias de segurança de dados, fortalecendo, assim, sua resiliência contra ameaças cibernéticas. A compreensão completa da legislação e sua relação direta com a cibersegurança são essenciais para garantir a proteção integral dos dados e a sustentabilidade das operações empresariais em um cenário digital em constante evolução.

Aprofundar-se nas respostas fornecidas pelos participantes revelou um panorama complexo e multifacetado das práticas de cibersegurança e adequação à Lei Geral de Proteção de Dados (LGPD) nas empresas do centro comercial de Valença. Os cruzamentos de dados destacaram desafios importantes e áreas de oportunidade que desempenham um papel crucial na construção de uma estrutura robusta para a segurança da informação.

A análise desses dados não apenas evidencia as lacunas existentes, mas aponta caminhos claros para fortalecer a postura de cibersegurança e conformidade com a LGPD. Ações imediatas na educação sobre a legislação, modernização dos métodos de armazenamento e implementação de programas de treinamento abrangentes são essenciais para construir uma base sólida de segurança da informação.

De acordo com Garcia e Masseno (2022, p. 260) "... conseguir alcançar um nível de maturidade quanto à sensibilização e conscientização". Nesse contexto, as recomendações futuras se concentram na promoção da conscientização sobre a LGPD, na migração para métodos de armazenamento mais seguros e na expansão dos programas de treinamento. A construção de parcerias estratégicas, seja com consultoria especializada ou organizações similares que já trilharam esse caminho com sucesso, pode servir como um estudo específico nessa jornada para uma cibersegurança robusta, consciente e em total conformidade com as diretrizes legais vigentes.

Em suma, esta análise é uma bússola para o futuro da segurança digital e da conformidade legal. As recomendações derivadas desses resultados não são meramente sugestões, mas diretrizes cruciais para fortalecer as bases da cibersegurança com compromisso contínuo com a evolução das práticas empresariais.

5 CONSIDERAÇÕES FINAIS

Neste capítulo serão apresentadas as conclusões e as recomendações para a continuidade de futuras pesquisas nesta área de estudo.

Diante da análise sobre as práticas de cibersegurança nas empresas do centro comercial de Valença, emerge um panorama complexo e repleto de lacunas, como a falta de conhecimento sobre a LGPD, falta de treinamento dos profissionais sobre cibersegurança e a despadronização do armazenamento de dados. Este estudo, feito de forma exploratória, foi fundamentado em metodologias sobre cibersegurança e LGPD nas empresas, entrevistas detalhadas e análises dos dados coletados, buscou transcender as camadas mais profundas das práticas empresariais.

Durante a condução das entrevistas, um aspecto notável foi a receptividade dos entrevistados, mesmo diante de um tema tão técnico como a cibersegurança. A interação pessoal permitiu esclarecer dúvidas imediatamente, criando um ambiente propício para compartilhar insights valiosos sobre as práticas de cibersegurança e conformidade com a LGPD nas empresas de Valença. Esse aspecto contribuiu significativamente para a qualidade e profundidade das respostas obtidas, tornando o processo de coleta de dados uma experiência fluida e produtiva.

As recomendações decorrentes dessa análise não são meras sugestões, mas diretrizes essenciais para a construção de uma base sólida de segurança cibernética e conformidade com a LGPD. A promoção de conscientização sobre a legislação, a modernização dos métodos de armazenamento e a expansão dos programas educativos emergem como imperativos para fortalecer as defesas digitais e garantir uma postura empresarial alinhada com as demandas da era digital.

Nesse contexto, o desdobramento futuro deste estudo deve envolver a implementação prática dessas recomendações, por meio de parcerias estratégicas, investimentos em tecnologias seguras e a contínua capacitação dos colaboradores. A cibersegurança não é uma meta estática, mas uma jornada contínua que exige adaptação constante às ameaças emergentes e a evolução das práticas globais. Através de programas de capacitação adaptados, consultoria especializada, eventos educativos, um centro de recursos dedicado e parcerias estratégicas.

REFERÊNCIAS

ALMEIDA, Siderly do Carmo Dahle de; SOARES, Tania Aparecida. Os impactos da Lei Geral de Proteção de Dados-LGPD no cenário digital. **Perspectivas em Ciência da Informação**, v. 27, p. 26-45, 2022.

BARZOTTO, Luciane Cardoso; COSTA, Ricardo Hofmeister de Almeida Martins. **Estudos sobre LGPD–Lei Geral de Proteção de Dados–lei nº 13.709/2018**: doutrina e aplicabilidade no âmbito laboral. 2022.

CALDAS, Alexandre; FREIRE, Vicente. **Cibersegurança**: das preocupações à ação. Instituto da Defesa Nacional, 2013.

COTINO, Lorenzo. Cibersegurança. 2021.

DE OLIVEIRA FORNASIER, Mateus; SPINATO, Tiago Protti; RIBEIRO, Fernanda Lencina. Ransomware e cibersegurança: a informação ameaçada por ataques a dados. **Revista Thesis Juris**, v. 9, n. 1, p. 208-236, 2020.

FORNASIER, Mateus de Oliveira; KNEBEL, Norberto Milton Paiva. O titular de dados como sujeito de direito no capitalismo de vigilância e mercantilização dos dados na Lei Geral de Proteção de Dados. **Revista Direito e Práxis**, v. 12, p. 1002-1033, 2021.

MAHLE, Ana Cristina Oliveira. **A autodeterminação informativa como fundamento da Lei Geral de Proteção de Dados Brasileira:** uma análise a partir da LGPD. 2021.

NEVES, Denise Lemes Fernandes et al. A segurança da informação de encontro às conformidades da LGPD. **Revista Processando o Saber**, v. 13, p. 186-198, 2021.

OLIVEIRA, José Clovis Pereira de et al. **O questionário, o formulário e a entrevista como instrumentos de coleta de dados: vantagens e desvantagens do seu uso na pesquisa de campo em ciências humanas.** In: III Congresso Nacional de Educação. 2016. p. 1-13.

SILVEIRA, Jonas Rafael; LUNARDI, Guilherme Lerch; CERQUEIRA, Lucas Santos. RELAÇÃO ENTRE CULTURA E SEGURANÇA DA INFORMAÇÃO: COMO EVITAR FALHAS DECORRENTES DO “JEITINHO BRASILEIRO”?. **REAd. Revista Eletrônica de Administração (Porto Alegre)**, v. 29, p. 143-170, 2023.

SILVEIRA, Sergio Amadeu; AVELINO, Rodolfo; SOUZA, Joyce. A privacidade e o mercado de dados pessoais. **Liinc em revista,** v. 12, n. 2, 2016.

TAKEUCHI, Eduardo Costa. **Fatores humanos em cibersegurança: uma revisão sistemática da literatura.** 2023.

ANEXO

Anexo I - QUESTIONÁRIO PILOTO

1) Cargo na empresa ?

2) Sua empresa é:

A) Organização pública

B) Organização privada

C) MEI

3) Você conhece a LGPD ?

A) SIM

B) NÃO

4) Sua organização nomeou o encarregado de proteção de dados(DPO) ?

A) SIM

B) NÃO

5) Sua organização possui um canal (telefone, email e site) para comunicação com o encarregado de proteção de dados (DPO) ?

A) SIM

B) NÃO

6) Sua organização oferece periodicamente aos colaboradores o treinamento e conscientização sobre a proteção de dados?

A) SIM

B) NÃO

7) Sua organização contratou ou pretende contratar uma consultoria para contribuir com a adequação à LGPD ?

A) Pretende contratar

B) Não será contratada consultoria

C) Contratou e os trabalhos já iniciaram

D) Processo de contratação em andamento

E) Não sei informar

8) Sua organização realizou alguma análise de planejamentos dos projetos futuros ?

A) SIM

B) NÃO

9) A empresa em qual frequência realiza o mapeamento de dados:

A) em andamento
B) concluído
C) não foi iniciado
D) desconheço o assunto

10) Em qual fase está a revisão dos contratos de prestadores de serviços (terceirizados) e colaboradores:

A) em andamento
B) concluído
C) não se aplica
D) não foi iniciado
E) desconheço o assunto

11) Sua organização tem comitê multidisciplinar de proteção de dados pessoais ?

A) Não
B) Sim

12) Sua organização trata/manipula dados pessoais sensíveis ?

A) SIM
B) NÃO

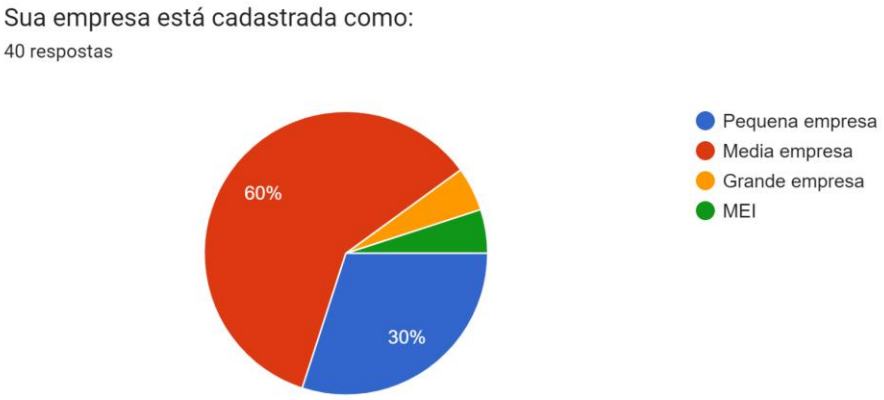
13) Sua organização trata/manipula dados de criança e/ou adolescentes ?

A) SIM
B) NÃO

Anexo II - QUESTIONÁRIO FINAL

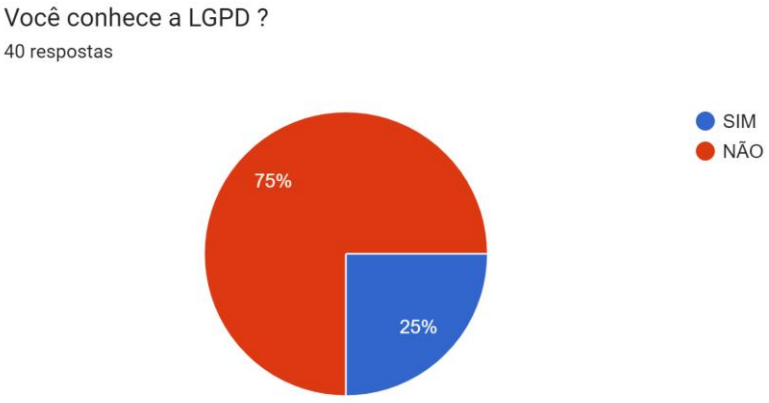
Sua empresa está cadastrada como:

A) Organização pública
B) Organização privada
C) MEI



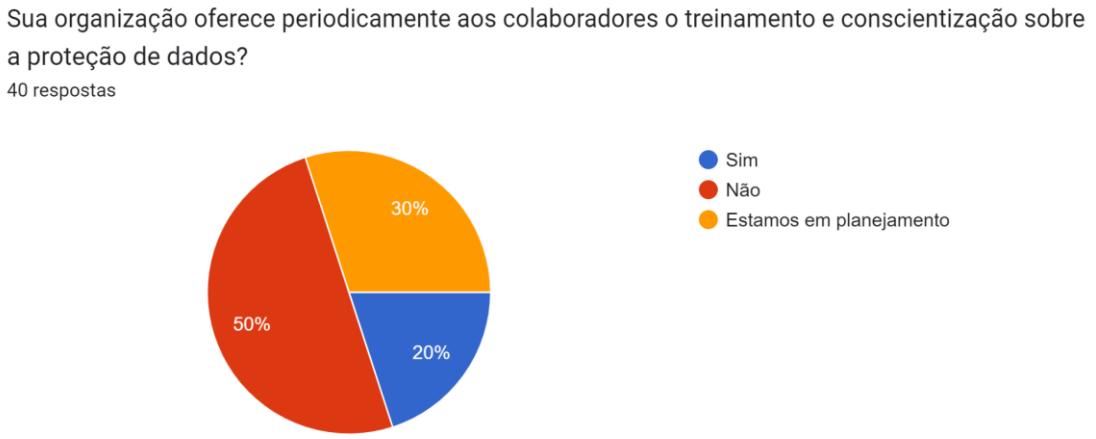
Você conhece a LGPD ?

A) SIM
B) NÃO



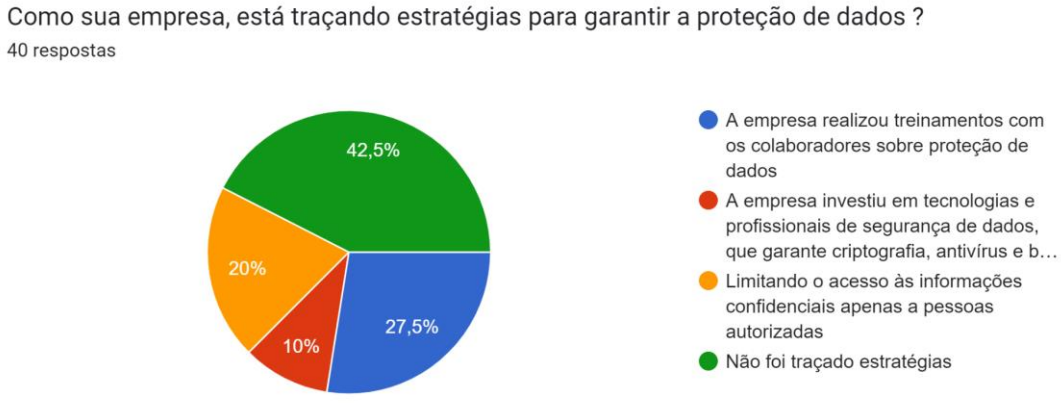
Sua organização oferece periodicamente aos colaboradores o treinamento e conscientização sobre a proteção de dados?

A) Não
B) Sim
C) Estamos em planejamento



Como sua empresa está traçando estratégias para garantir a proteção de dados ?

A) A empresa realizou treinamentos com os colaboradores sobre proteção de dados
B) A empresa investiu em tecnologias e profissionais de segurança de dados, que garante criptografia, antivírus
C) Limitando o acesso às informações confidenciais apenas a pessoas autorizadas
D) Não foi traçado estratégias

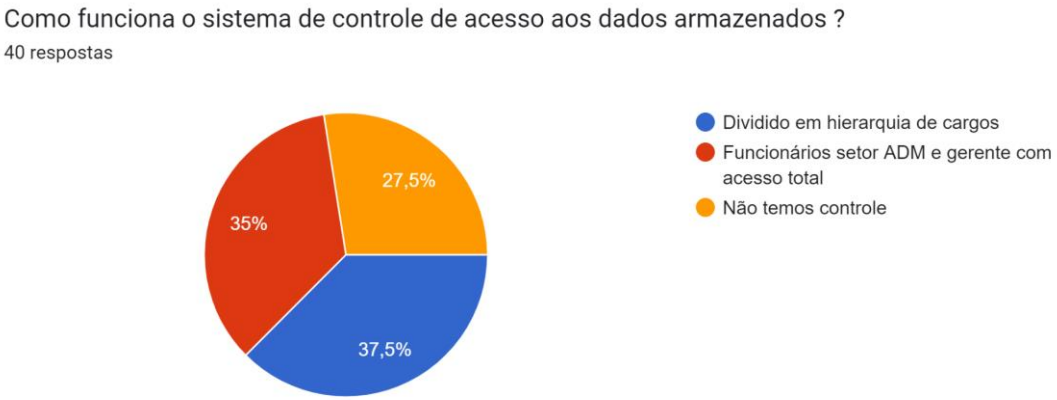


Como sua empresa armazena os dados dos funcionários da instituição ?

A) Drive na rede
B) Memória externa
C) Memória local do computador
D) Arquivos e pastas físicas

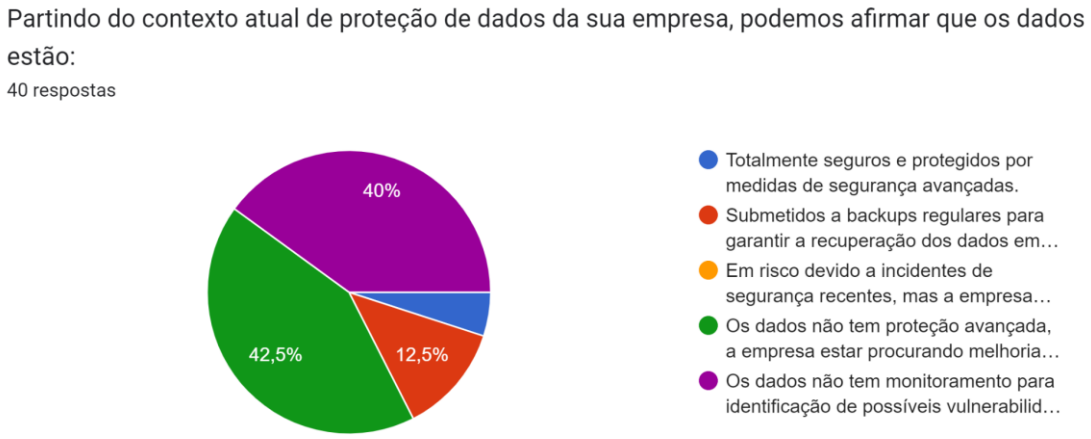
Como funciona o sistema de controle de acesso aos dados armazenados ?

A) Dividido em hierarquia de cargos
B) Funcionários setor ADM e gerente com
C) acesso total
D) Não temos controle



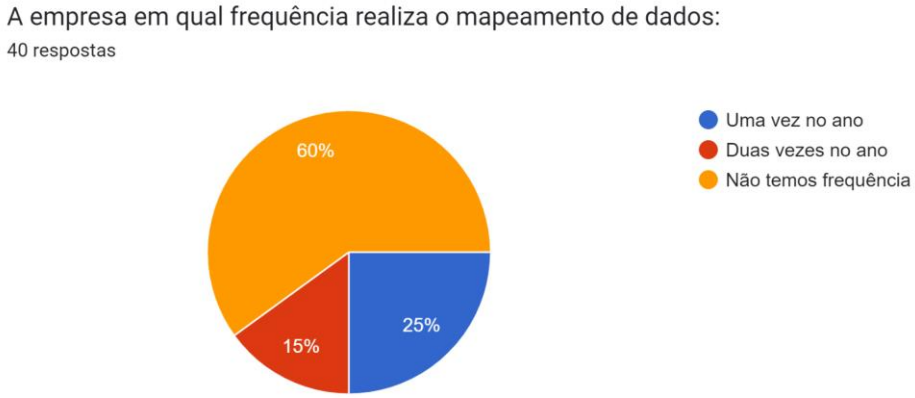
Partindo do contexto atual de proteção de dados da sua empresa, podemos afirmar que os dados estão:

A) Totalmente seguros e protegidos por medidas de segurança avançadas.
B) Os dados não tem proteção avançada, a empresa está procurando melhorias na segurança de dados.
C) Submetidos a backups regulares para garantir a recuperação dos dados em caso de perda ou corrupção.
D) Em risco devido a incidentes de segurança recentes, mas a empresa está tomando medidas para melhorar a proteção de dados.



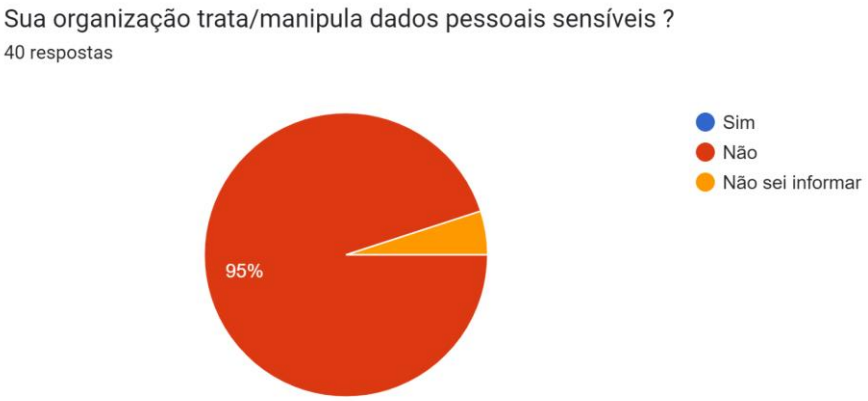
A empresa em qual frequência realiza o mapeamento de dados:

A) Uma vez no ano
B) Duas vezes no ano
C) Não temos frequência



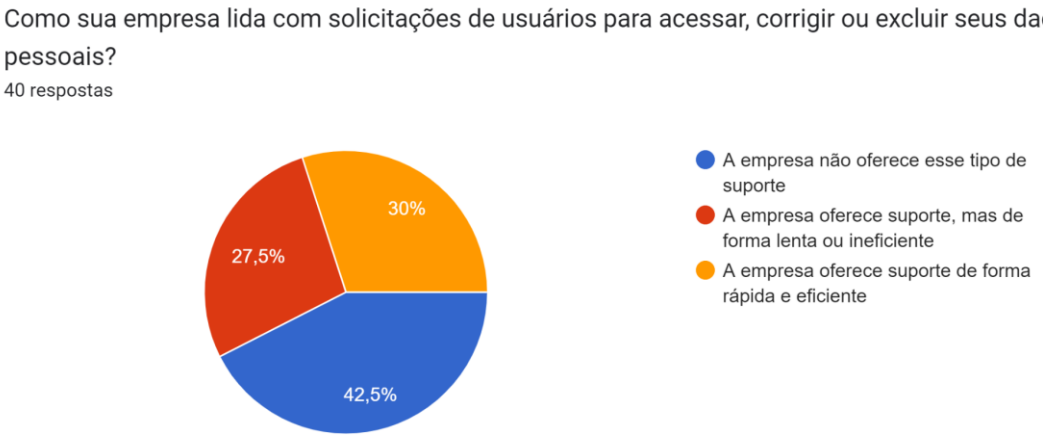
Sua organização trata/manipula dados pessoais sensíveis ?

A) SIM
B) NÃO
C) Não sei informar



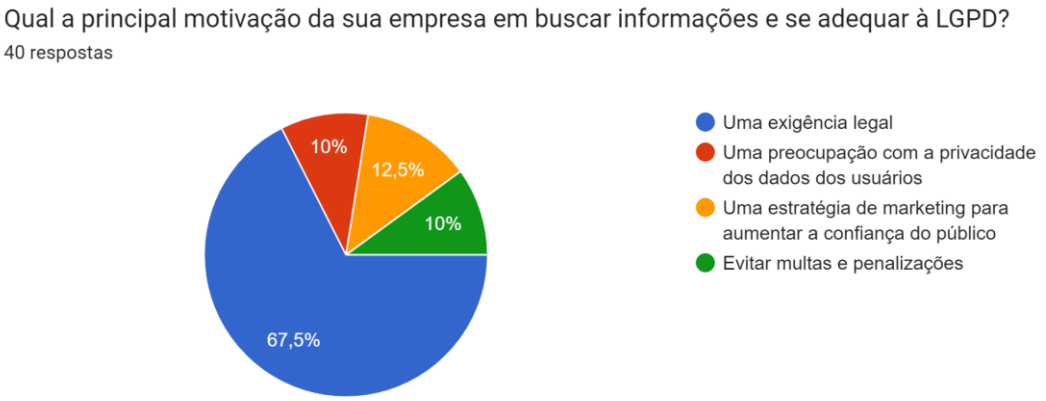
Como sua empresa lida com solicitações de usuários para acessar, corrigir ou excluir seus dados pessoais?

A) A empresa não oferece esse tipo de suporte
B) A empresa oferece suporte, mas de forma lenta ou ineficiente
C) A empresa oferece suporte de forma rápida e eficiente



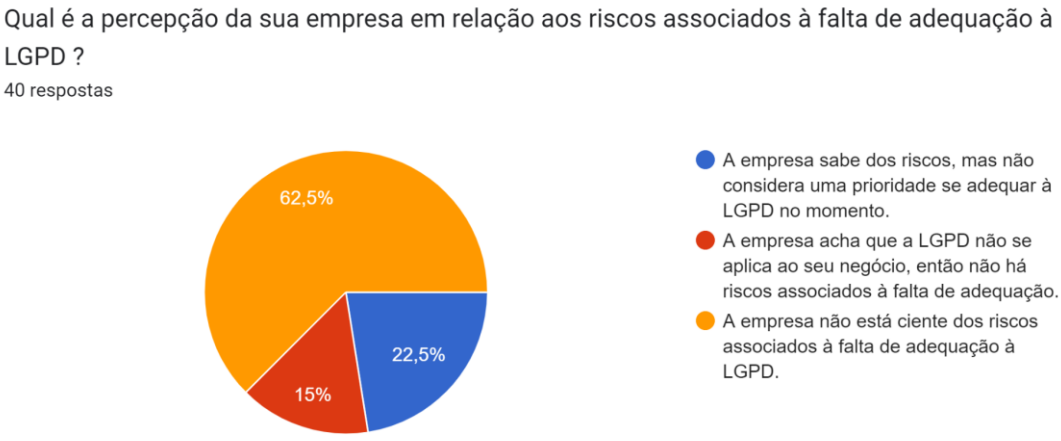
Qual a principal motivação da sua empresa em buscar informações e se adequar à LGPD?

A) Uma exigência legal Uma preocupação com a privacidade dos dados dos usuários
B) Uma estratégia de marketing para aumentar a confiança do público
C) Evitar multas e penalizações



Qual é a percepção da sua empresa em relação aos riscos associados à falta de adequação à LGPD ?

A) A empresa sabe dos riscos, mas não considera uma prioridade se adequar à LGPD no momento.
B) A empresa acha que a LGPD não se aplica ao seu negócio, então não há riscos associados à falta de adequação.
C) A empresa não está ciente dos riscos associados à falta de adequação à LGPD



Sua organização contratou ou pretende contratar uma consultoria para contribuir com a adequação à LGPD ?

A) Pretende contratar
B) Processo de contratação em andamento
C) Contratou e os trabalhos já iniciaram
D) Não será contratada consultoria

Sua organização contratou ou pretende contratar uma consultoria para contribuir com a adequação à LGPD ?

40 respostas