Etec "Profª Anna de Oliveira Ferraz"

GESTÃO DE DOCUMENTAÇÃO: segurança da informação

DOCUMENTATION MANAGEMENT: information security

Ana Beatriz Zanetti Rosas – ana.zanetti.rosas@gmail.com
Ana Julia Santos Fioranelli – juliafioranelli@gmail.com
Camille Leticia dos Santos – camilleleticia32@gmail.com
Rayssa Martinez Cardoso Alves – rayssa.alves.secundario@gmail.com
Tayane Paulino Batista de Souza. – taianepaulino1@gmail.com
ETEC Prof.ª Anna de Oliveira Ferraz – Araraquara – São Paulo -Brasil

Antônio Cláudio Gonçalves da Silva – antonio.silva07@cps.sp.gov.br
Gabriela Messias da Silva – gabriela.silva02@cps.sp.gov.br
ETEC Prof.ª Anna de Oliveira Ferraz – Araraquara – São Paulo -Brasil

RESUMO

O gerenciamento de documentos é um processo essencial para organização, controle, armazenamento e proteção das informações em empresas e instituições. Com a evolução da tecnologia e crescimento da produção de dados, sendo necessário utilizar métodos eficaz para garantir a segurança, agilidade e simplicidade no acesso às informações. Desta maneira, o Trabalho de Conclusão de Curso tem a objetividade de analisar a importância da gestão documental nas organizações, mostrando os seus benefícios para a administração, produtividade e segurança da informação. O método realizado para desenvolver esse trabalho foi com base em artigos científicos, por meio de livros, pesquisas bibliográficas e sites, buscando entender as principais definições, técnicas e práticas relacionadas à gestão de documentos. Ainda por cima, foram abordados temas como arquivamento físico e digital, organização documental, proteção de informações e o efeito da tecnologia na administração de documentos. Os resultados demonstraram que a gestão documental favorece de forma significativa a melhoria dos processos organizacionais, diminuindo perdas de dados, elevando a eficiência administrativa e gerando maior controle e segurança de dados. É possível identificar que a digitalização de documentos e a utilização de sistemas eletrônicos simplificam o acesso ao dados e otimizam o tempo nas atividades das empresas. Como conclusão, a gestão de documentos é relevante para o bom funcionamento das organizações, pois promove a ordenação, eficiência e segurança no gerenciamento das informações. Portanto, investir em ações e tecnologias com o foco na gestão documental se torna um diferencial positivo para as empresas que buscam aprimorar nos seus processos administrativos e garantir maior concorrência no mercado.

Palavras-chave: Documentação. Organização. Arquivamento. Segurança. Digitalização. Administração.

ABSTRACT

Document management is an essential process for organizing, controlling, storing, and protecting information in companies and institutions. With the evolution of technology and the growth of data production, it is necessary to use effective methods to ensure security, speed, and simplicity in accessing information. In this way, the Course Conclusion Project aims to analyze the importance of document management in organizations, showing its benefits for administration, productivity, and information security. The method used to develop this work was based on scientific articles, through books, bibliographic research, and websites, seeking to understand the main definitions, techniques, and practices related to document management. Furthermore, topics such as physical and digital archiving, document organization, information protection, and the effect of technology on document management were addressed. The results demonstrated that document management significantly favors the improvement of organizational processes, reducing data loss, increasing administrative efficiency, and generating greater control and data security. It is possible to identify that the digitization of documents and the use of electronic systems simplify access to data and optimize time in company activities. In conclusion, document management is relevant to the proper functioning of organizations, as it promotes order, efficiency, and security in information management. Therefore, investing in actions and technologies focused on document management becomes a positive differentiator for companies seeking to improve their administrative processes and ensure greater competitiveness in the market.

Keywords: Documentation. Organization. Filing. Security. Digitization. Administration.

1 INTRODUÇÃO

Com o avanço da tecnologia da informação, tornou-se imprescindível repensar a forma como os documentos são gerenciados para a proteção de dados. Tendo de um lado a informação como um bem tão valioso, seja para estratégias e decisões numa empresa, e de outro a era tecnológica, como digitalização de documentos, uso dos mais diversos aplicativos que facilitam e simplificam processos cotidianos empresariais, é de extrema importância uma boa gestão para que esses dados não sejam utilizados de maneira imprópria. Contudo, segundo a Camilo (2025, s/n) "realizar uma correta e completa gestão eletrônica de documentos e, com isso, garantir a segurança de dados é uma tarefa que deve ser encarada como de grande importância no dia a dia empresarial."

No entanto, muitas corporações não têm esse ponto como prioridade, ou buscam se aprofundar e garantir uma boa cautela. Por consequência, muito desse material é manuseado, armazenado e, por fim, descartado de forma incorreta. Nesse sentido, conforme afirma Paiva (2019, s/n.) "Sem uma documentação adequada para a qualidade, não se chega à excelência."

Partindo dessa perspectiva, o objetivo deste trabalho é identificar as formas como algumas empresas armazenam essas documentações, estudar práticas atualizadas e seguras de uma gestão, identificando condutas corretas, falhas comuns e recursos adotados pelas mais diversas empresas.

A relevância do tema se destaca ainda mais quando se observa o cenário nacional: o Brasil é o segundo país com o maior número de crimes cibernéticos, com ataques que envolvem vazamentos de dados, sequestro de informações e ataques que deixam as informações indisponíveis. É de extrema importância que empresas façam investimentos no campo da segurança da informação para que não sejam vítimas desse tipo de perda. Investir nesse tipo de medida dá ao negócio conformidade com os padrões do mercado e leis como a LGPD.

2 FUNDAMENTAÇÃO TEÓRICA

No campo da sociedade empresarial, a partir do final do século XX, informação e dados passaram a ser a nova *commodity* mais preciosa que o cenário corporativo poderia ter, um ativo de grande e alto valor agregado. Nunca foi tão valiosa uma tomada de decisão certeira, precisa e lucrativa baseada nos dados gerados pelas empresas e buscados no mercado.

Cuidar, proteger, tratar, gerir, interpretar, dentre outros verbos, passaram a ser a grande habilidade de lidar com os dados. É o momento em que a tecnologia, a gestão, a governança corporativa e os negócios se aproximam do cenário jurídico e da legislação na velocidade da luz, com isso a agenda global dessa proteção avançou no comércio internacional e passou a ser um critério para se estabelecer negócios com o Brasil; a ferramenta de gestão do *compliance* digital que se revela, então, como uma perspectiva positiva para a padronização da segurança e do cuidado com os dados e a privacidade dessas informações dentro das empresas.

"O Brasil deve investir R$104,6 bilhões em cibersegurança até 2028, segundo projeções da Brasscom (Associação das Empresas de Tecnologia da Informação e Comunicação). O dado faz parte do Relatório de Cibersegurança 2025…"(Febraban Tech, 2025, s/n).

O estudo da Brasscom ressalta que o Brasil conquistou um reconhecimento importante

no cenário internacional. É o único país da América do Sul classificado como Tier 1 no Global Cybersecurity Index (GCI), elaborado pela União Internacional de Telecomunicações (UIT). A posição reflete o compromisso do país com a agenda global de cibersegurança, incluindo a adoção de políticas públicas, marcos regulatórios e cooperação internacional.

Outro ponto abordado pela Brasscom é o mercado de trabalho na área. O número de profissionais que atuam em segurança da informação tem crescido a uma média anual de 16,1% desde 2015. Apenas em 2023, foram registradas 1.849 formações na área, um aumento de 15,3% em relação ao ano anterior. Apesar disso, o déficit de mão de obra ainda é considerado elevado, especialmente diante da complexidade crescente dos sistemas e da sofisticação dos ataques.(Febraban Tech, 2025, s/n)

Desse modo, vale a pena considerar a mudança de paradigma sobre o papel financeiro da tecnologia nas organizações. Se anteriormente a segurança da informação era tratada como um custo passivo, o cenário atual a reposiciona como um investimento de capital essencial para a preservação do valor de mercado e a viabilidade comercial.

Em última análise, a segurança da informação é o seguro de vida das empresas modernas. Ela protege o patrimônio digital, sustenta a confiança do consumidor e assegura a conformidade legal em um ambiente de riscos crescentes.

2.1 O Brasil é o segundo país com maior número de crimes cibernéticos

É um fato que a tecnologia vem sendo bastante acessível à humanidade, mas o maior problema vem sendo as pessoas usando a internet para benefício próprio para concretizar operações ilegais. Segundo o FortiGuard Labs (Global Threat Landscape Report, 2025), o Brasil foi o segundo país mais atacado do mundo em 2025, registrando 315 bilhões de tentativas de ataques cibernéticos apenas no primeiro semestre. Além disso, a América Latina contabilizou 374 bilhões de tentativas de ataques, sendo 84% direcionadas ao Brasil.

O Brasil enfrenta desafios significativos em matéria de segurança cibernética, o que acarretar ataques direcionados a instituições governamentais até ataques de malwares contra empresas privadas. (Santos, 2023).

No cenário atual a segurança da informação, deixou de ser algo normal e se torna algo de extrema relevância, essa informação fortalece que a proteção desses dados não é uma preocupação só para empresas multinacionais. As pequenas e médias empresas também correm

riscos e precisam adotar medidas preventivas. Além de serem difíceis de reconhecer os ataques criminosos roubam dados e os utilizam como moeda de troca para receberem dinheiro.

A legislação obriga que as empresas tenham ações práticas, seguras e administrativas para proteger dados contra acessos não autorizados, vazamentos e desumanidade. Esse grande número de ataques mostra a importância da Lei Geral de Proteção de Dados (LGPD) que está em vigor no Brasil desde 2020 e agora teve suas sanções administrativas valendo a partir de agosto de 2021.

A Autoridade Nacional de Proteção de Dados Pessoais, a ANPD. A instituição também aplica penalidades pelo descumprimento da LGPD, orienta empresas pelo Brasil, além de replicar boas práticas, realizar auditorias e certificar instituições que fazem o uso destes dados.(Santos, 2023).

Os casos de vazamentos de dados tratados com a LGPD merecem a atenção de qualquer tipo de negócio e pode envolver empresas de pequeno, médio e grande porte. Investir em cibersegurança indica estar apto para enfrentar essas dificuldades, reduzir impactos e manter a lealdade de clientes e investidores.

É necessário um esforço do país organizado, com autorizações exigidas por lei, incentivando a norma ISO/IEC 27001 que consiste em fornecer a empresas de qualquer porte e de todos os setores de atividade orientações para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação e a consolidação das políticas públicas e campanhas de educação digital. A cibersegurança que tem como definição o conjunto de ações e tecnologias que tem as funções de proteger redes, sistemas e dados contra a acessos não autorizados e ataques. Essa segurança no setor público é um dos pilares atualmente da governança digital, tem como função proteger redes e sistemas, também os setores de energia, saúde, saneamento e transportes, caso ocorra interrupções pode gerar desmoronamento sociais e econômicos. Essas informações são muitos mais do que dados cadastrais básicos, como nome e data de nascimento, podem incluir dados pessoais, como estado de saúde, acesso a dados bancários e até informações sobre outros familiares.

Embora existam diferentes definições para a Segurança da Informação propostas por diversos autores e pesquisadores, todas elas compartilham como características centrais a preocupação na proteção aos dados, a promoção da continuidade do negócio e a redução dos riscos envolvendo pessoas, equipamentos e processos. (Santos, 2023).

Essa dimensão de informações amplia a oportunidades de particularidades dos golpes,

tornando-os mais efetivos e danosos para os titulares de dados pessoais, população.

A digitalização de documentos públicos, motivada pela inovação digital e pelo crescimento do governo eletrônico, trouxe novas ocasiões para eficácia administrativa e inovação dos serviços públicos. Deste modo, governos inovadores precisam ampliar estruturas de defesa cibernéticas. Embora os avanços, o Brasil continua enfrentando dificuldades. Casos como o ataque cibernético ao Ministério da Saúde (2021) e a invasão de sistemas de prefeituras (2022 – 2023) mostram o enfraquecimento das estruturas digitais públicas.

2.2 Ataques envolvendo vazamentos de dados

O vazamento de dados é uma das principais ameaças digitais da atualidade, com impactos graves para pessoas, empresas e instituições públicas. Casos recentes no Brasil e no mundo expuseram bilhões de registros, incluindo senhas, documentos pessoais e informações financeiras, demonstrando o quanto a segurança da informação se tornou um tema estratégico (FIA, 2025). Por isso, entender como ocorrem os vazamentos e como preveni-los é essencial para todos: profissionais de tecnologia, gestores, consumidores e cidadãos.

"Leva-se 20 anos para construir uma reputação e alguns minutos de um incidente cibernético para arruiná-la." (Nappo, 2018, s/p).

O vazamento de dados acontece quando informações sigilosas são acessadas ou divulgadas por pessoas que não têm autorização. Isso pode acontecer tanto por falhas humanas quanto por ataques cibernéticos feitos por hackers (Microsoft, 2025).

De acordo com pesquisas divulgadas pela NordVPN, o Brasil está em primeiro lugar entre 253 países no ranking mundial de vazamento de cookies, com mais de 7 bilhões de registros expostos (NordVPN, 2026). O estudo também mostrou que muitos desses cookies ainda estão ativos, permitindo que criminosos consigam acessar contas e sistemas sem precisar da senha dos usuários (It Portal, 2025).

Mesmo sendo usados para melhorar a experiência na internet, muitas pessoas não sabem que os cookies também podem ser utilizados por hackers para roubar dados pessoais e invadir sistemas.

Segundo o relatório, entre os dados vazados estão nomes completos, e-mails, senhas e até endereços físicos. Com essas informações, criminosos podem aplicar golpes, cometer fraudes e roubar identidades, colocando em risco a segurança digital de milhões de pessoas.

Levando em consideração todos esses dados, é de extrema importância tratar a gestão eletrônica de documentos (GED) com prioridade. A GED é uma estratégia essencial para as marcas que buscam uma administração mais capacitada de todas as informações sensíveis, principalmente em conformidade com a Lei Geral de Proteção de Dados – LGPD (E-clic, 2025).

Para isso, são utilizadas tecnologias que viabilizam maior segurança no armazenamento em nuvem de tais informações, utilizando servidores confiáveis para evitar qualquer ameaça. Além disso são adotadas estratégias, como o controle de acesso dos usuários, a rastreabilidade dos documentos e criptografia de ponta a ponta. Pois dessa forma, é possível ter a confiança que todas as recomendações da LGPD e de outras Políticas de Privacidade serão seguidas para evitar qualquer situação adversa.

Assim, é possível perceber como o vazamento de dados pode causar diversos impactos negativos e até facilitar outros crimes digitais, como o sequestro de informações, assunto que será abordado no próximo tópico.

2.3 Sequestro de informações

O sequestro de informações em empresas é uma ameaça que vem crescendo e pode resultar em perdas significativas e danos financeiros. As empresas precisam implantar medidas de segurança para proteger seus dados e sistemas contra-ataques de *ransomware*. Isso abrange a execução de *backups* frequentes, o uso de sistemas de detecção de irregularidade e a implantação de políticas de segurança rigorosas. É essencial que as empresas estejam prontas para lidar com incidentes de seguranças e possam agir de forma eficaz em caso de vazamentos de dados.

"O sequestro de informações representa uma das maiores ameaças da era digital, comprometendo dados e causando prejuízos financeiros às organizações" (Pinheiro, 2021, p. 33).

Um dos ataques criminosos mais frequentes e lucrativos é o sequestro de informações, cujo objetivo é roubar dados confidenciais de empresas, instituições ou indivíduos comuns e exigir um pagamento para restaurar o acesso.

Para se ter uma noção, esse tipo de ataque, conhecido também como *ransomware,* registrou um aumento de 13% no Brasil em 2022, de acordo com um relatório da Sophos, empresa especializada em cibersegurança.

Conforme o estudo realizado em 2022, 68% das empresas em funcionamento já foram alvo de algum tipo de ataque cibernético, principalmente devido à fragilidade de seus sistemas.

"Os ataques *ransomware* exploram vulnerabilidades dos sistemas e a ausência de políticas eficazes de proteção de dados" (Sêmola, 2014, p. 15).

Dessa forma, o sequestro de informações no Brasil mostra que há problemas mais profundos do que apenas a ação dos criminosos. Ele revela que nossa cultura de segurança digital ainda é fraca, que os investimentos em proteção tecnológica são insuficientes e que as instituições, tanto públicas quanto privadas, costumam agir de forma mais reativa do que preventiva. Mesmo com leis importantes, como a Lei Geral de Proteção de Dados, ainda encontramos dificuldades para colocar em prática políticas de prevenção, fazer uma fiscalização eficaz e treinar profissionais especializados. Isso tudo mostra que o problema não é só a criminalidade na *internet*, mas também a falta de um planejamento estratégico, de conscientização e de prioridade na segurança da informação no país.

"A segurança da informação deixou de ser apenas uma questão tecnológica e passou a ser uma necessidade estratégica para empresas e instituições" (Peck, 2020, p. 27).

Por fim, o sequestro de informações mostra como a nossa maior dependência da tecnologia deixou empresas e pessoas mais vulneráveis a ataques digitais. Esses ataques podem causar prejuízos financeiros, prejudicar a reputação e levar à perda de dados importantes. A conversa revelou que, com o valor alto dessas informações e o crescimento dos casos de *ransomware*, investir em prevenção, conscientização e boas políticas de segurança não é mais uma opção, mas uma necessidade estratégica para manter as atividades funcionando e proteger a privacidade.

Nesse sentido, o próximo assunto abordará os ataques que deixam as informações indisponíveis, ampliando a compreensão sobre como diferentes práticas cibernéticas podem comprometer o acesso e o funcionamento dos sistemas.

2.3 Ataques que deixam as informações indisponíveis

Tem-se conhecimento de que os ataques cibernéticos são uma preocupação constante das empresas. Afinal, os impactos são devastadores e não se resumem a perdas financeiras, mas também as informações de pessoas indisponíveis têm se tornado cada vez mais comuns no cenário digital atual.

> Os ataques cibernéticos têm se tornado uma ameaça crescente no ciberespaço, afetando indivíduos e organizações públicas e privadas. Segundo pesquisa da Check Point, divulgada pelo portal IT Forum (2024), o Brasil registrou aumento de 67% nos ataques cibernéticos em 2024. Apesar da relevância do tema, a literatura acadêmica ainda o aborda de forma limitada. (Greenberg, 2021; Schneier, 2020).

Quase todos os ataques cibernéticos modernos envolvem algum tipo de *malware*. Os agentes de ameaças usam ataques de malware para obter acesso não autorizado e tornar os sistemas infectados inoperáveis, destruindo dados, roubando informações confidenciais e, até mesmo, apagando arquivos críticos para o sistema operacional.

Um fato relevante relacionado ao tema, pode-se citar o cenário da Empresa Netshoes, que sofreu um incidente de segurança de dados de cerca de 38 milhões usuários, abrangendo: documento de identidade pessoal, localização residencial e histórico de compras, que foram divulgados em fóruns de cibercriminosos. Esse vazamento reacendeu o debate sobre o cumprimento de Lei Geral de Proteção de Dados (LGPD) e os desafios de segurança no *e-commerce*.

No que se refere às principais modalidades de *malware*, incluem – se: O *malware* é um denominação que é usado para qualificar todo software com intenções malignas usado para causar danos, que pode ser até econômico, comprometer sistemas, corromper dados ou causar irritações em usuário, prejudicando tanto computadores como celulares e até redes.

O *ransomware* é um tipo de *malware* que confisca o computador do usuário e reivindica um valor em dinheiro pelo resgate. Esse tipo de vírus age programando os dados do sistema operacional moldando para que o usuário não tenha mais permissão. Um cavalo de troia é um código malicioso que convence as pessoas a baixá-lo, parecendo ser um programa útil ou se escondendo dentro de um software legítimo.

O *spyware* é um *malware* altamente secreto que reúne informações confidenciais, como nomes de usuário, senhas, números de cartão de crédito e outros dados pessoais, e as transmite de volta ao invasor sem que a vítima saiba.

Os *worms* também são um tipo de *malware* que deve ter mais atenção pois se espalha mais rapidamente e surge sem controle do usuário.

Dito isso, senhas fortes, segurança de e-mail e *software* antivírus são todas as primeiras linhas de defesa críticas contra ameaças cibernéticas. No entanto, nenhum sistema de segurança está completo sem recursos de última geração de detecção de ameaças e resposta a incidentes,

para identificar ameaças à cibersegurança em tempo real e ajudar a isolar e corrigir rapidamente as ameaças, para minimizar ou evitar os danos que podem causar.

"Não devemos pedir aos nosso clientes que façam um equilíbrio entre privacidade e segurança. Precisamos oferecer-lhes o melhor de ambos. Em última análise, proteger os dados de outra pessoas é proteger de todos nós" (Cook, 2015).

3 PROCEDIMENTOS METODOLÓGICOS (MATERIAIS E MÉTODOS)

Neste segmento, serão apresentados os procedimentos metodológicos executados para a elaboração da pesquisa referente ao tema Segurança da Informação na Gestão de Documentos, com o intuito de entender a contribuição da proteção e da administração apropriada das informações dentro das empresas. Para construção do procedimento experimental, foi implementado um questionário planejado sendo incluso perguntas especificas vinculadas às praticas de segurança da informação. As respostas foram obtidas e estruturadas para avaliação estatística dos dados. Apresentou-se um levantamento bibliográfico em artigos científicos, livros e sites especializados, visando justificar teoricamente as definições de segurança da informação e gestão de documentos.

Os procedimentos utilizados neste trabalho basearam-se em uma pesquisa de abordagem quantitativa, realizada por meio de um formulário online elaborado na plataforma *Google Forms.* A pesquisa teve como objetivo coletar dados relacionados à Segurança da Informação na gestão de documentos, contando com a participação de 37 pessoas, das quais 27% eram homens e 73% mulheres, que responderam ao questionário de forma virtual. Em relação à faixa etária dos participantes, 10,38% possuíam entre 19 e 25 anos, enquanto 16,62% tinham entre 26 e 60 anos de idade.

A pesquisa foi composta por perguntas objetivas, com o intuito de obter informações referentes ao conhecimento de cada pessoa e as práticas aplicadas em suas rotinas no ambiente de trabalho, relacionadas à segurança da informação e ao gerenciamento de documentos. O levantamento de dados ocorreu no período de 15 de abril de 2026 a 11 de maio de 2026, tendo os resultados organizados em gráficos para uma avaliação de índices.

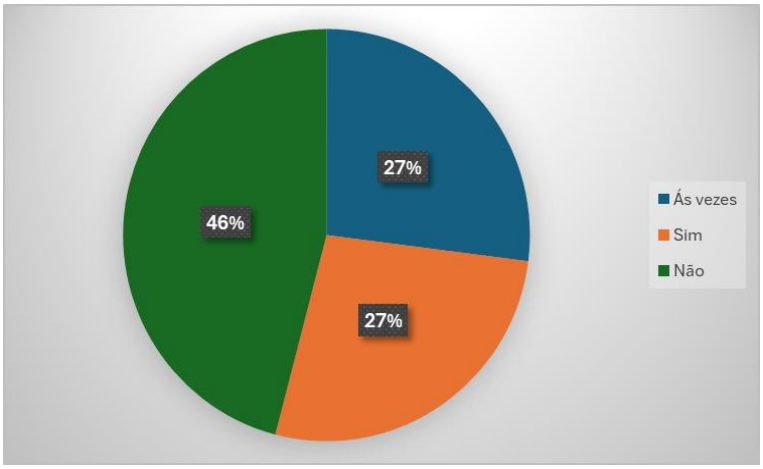
Os questionários foram direcionados a colaboradores e estudantes que possuem conhecimento e contato com documentações em suas rotinas de trabalho. O estudo contou com respostas das pessoas de forma voluntária, que contribuíram por meio do preenchimento do

Google Forms.

4 RESULTADOS E DISCUSSÃO

A partir dos dados obtidos na pesquisa realizada, serão apresentados e analisados os resultados coletados, apresentados em gráficos para melhor visualização e interpretação das respostas dos participantes. Os dados permitem avaliar os métodos de armazenamento de dados e segurança das empresas.

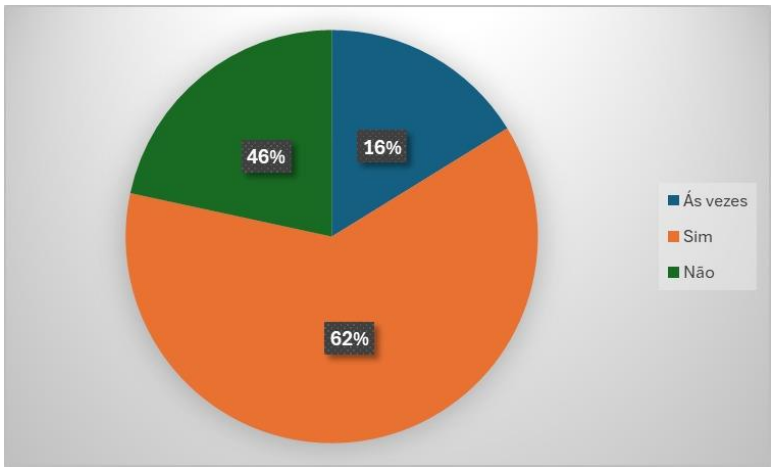
Gráfico 1 – Dificuldade para encontrar documentos na empresa.



Fonte: elaborado pelos autores, Araraquara (2026).

Conforme apresentado no gráfico 1, 27% dos participantes responderam que possuem dificuldades para encontrar documentos na empresa, enquanto 27%, responderam que isso acontece "ás vezes". Por sua vez, 46% dos participantes responderam que não possuem dificuldades para encontrar os documentos na sua instituição.

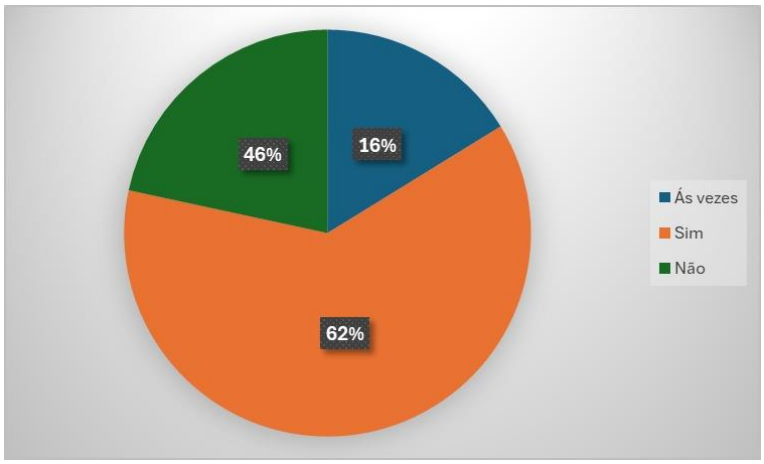
Gráfico 2 – Tempo gasto na procura de arquivos durante as atividades diárias.



Fonte: elaborado pelos autores, Araraquara (2026).

Conforme apresentado no gráfico 2, 27% dos participantes responderam que gastam parte do seu dia procurando arquivos na empresa, enquanto 22% dos participantes da pesquisa, responderam que isso acontece ás vezes. Por sua vez, 46% dos participantes responderam que não possuem dificuldades para procurar os documentos na sua instituição.

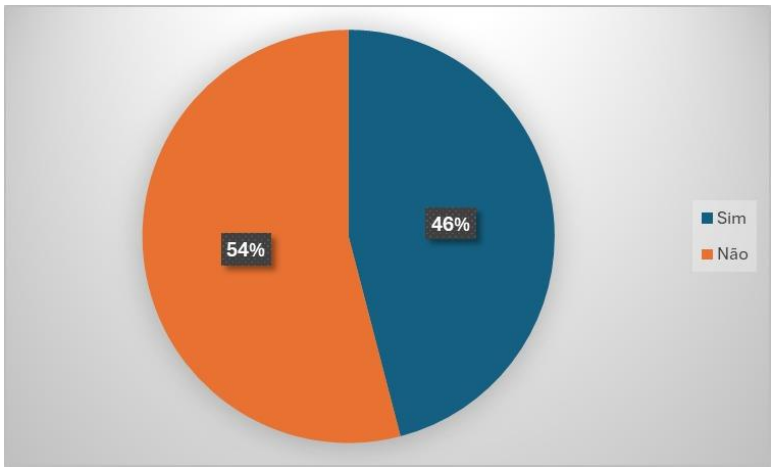
Gráfico 3 – Utilização de pastas físicas para armazenamento de documentos importantes.



Fonte: elaborado pelos autores, Araraquara (2026).

Conforme apresentado no gráfico 3, 62% dos participantes responderam que utilizam pastas físicas para armazenar documentos importantes da empresa, enquanto 16% dos participantes da pesquisa, responderam que isso acontece ás vezes. Por sua vez, 46% dos participantes responderam que não utilizam as pastas físicas.

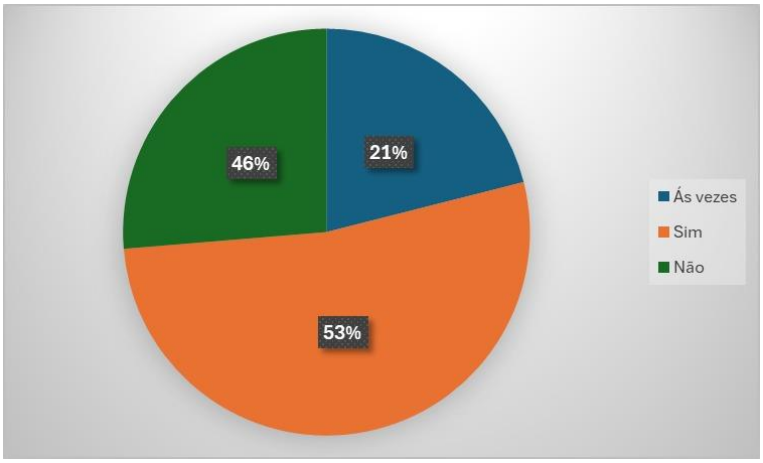
Gráfico 4 – Conhecimento sobre o protocolo de descarte e temporalidade de documentos da empresa.



Fonte: elaborado pelos autores, Araraquara (2026).

Conforme apresentado no gráfico 4, 46% dos participantes responderam que conhecem o protocolo de descarte e temporalidade da empresa, enquanto 54% dos participantes da pesquisa responderam que não conhecem os protocolos e temporalidades.

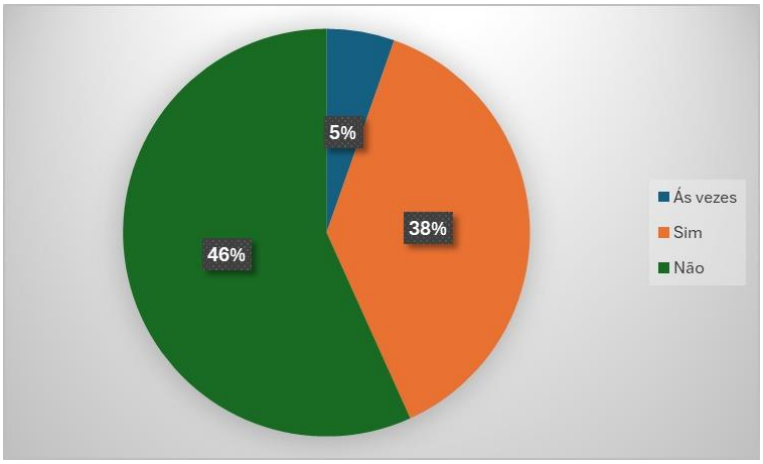
Gráfico 5 - Padrão de nomenclatura para os arquivos digitais no seu setor.



Fonte: elaborado pelos autores, Araraquara (2026).

Conforme apresentado no gráfico 5, 53% dos participantes responderam que existe um padrão de nomenclatura para os arquivos digitais no seu setor, enquanto 21% dos participantes da pesquisa, responderam que isso acontece ás vezes. Por sua vez, 46% dos participantes responderam que não existe um padrão.

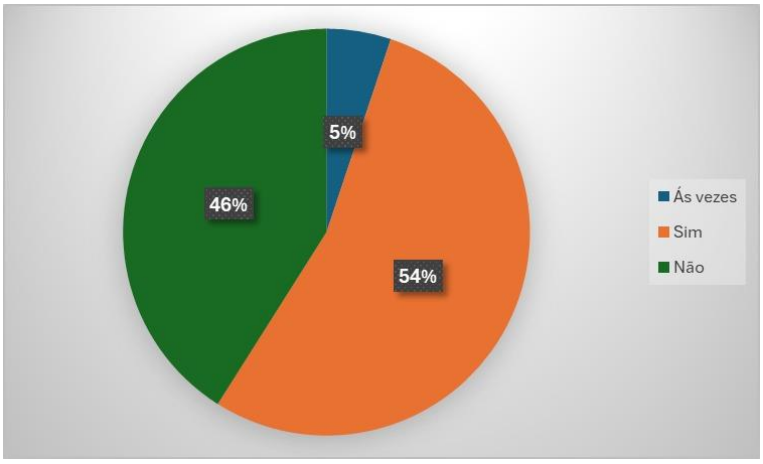
Gráfico 6 – Documentação segura contra perdas.



Fonte: elaborado pelos autores, Araraquara (2026).

Conforme apresentado no gráfico 6, 38% dos participantes responderam que sentem que os documentos da sua área estão seguros contra perdas, enquanto 5% dos participantes da pesquisa, responderam que ás vezes. Por sua vez, 46% dos participantes responderam que não sentem que fiquem seguros.

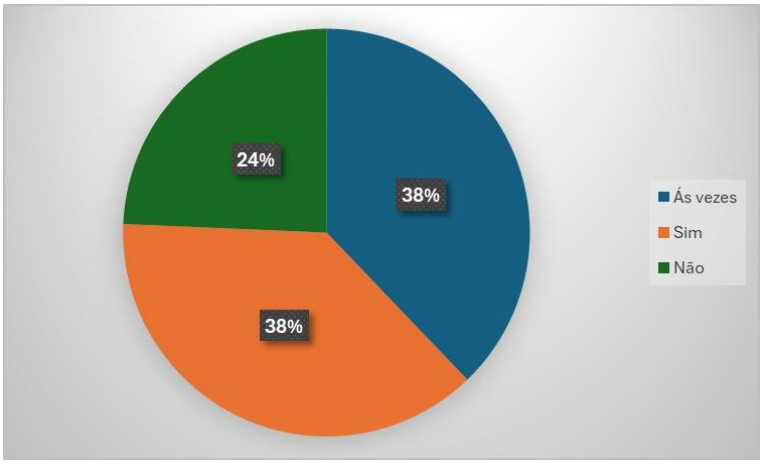
Gráfico 7 – Acesso a todos os documentos necessários de forma remota em seu trabalho.



Fonte: elaborado pelos autores, Araraquara (2026).

Conforme apresentado no gráfico 7, 54% dos participantes responderam que conseguem acessar todos os documentos de forma remota em seu trabalho, enquanto 5% dos participantes da pesquisa, responderam que conseguem ás vezes. Por sua vez, 46% dos participantes responderam que não conseguem acessar.

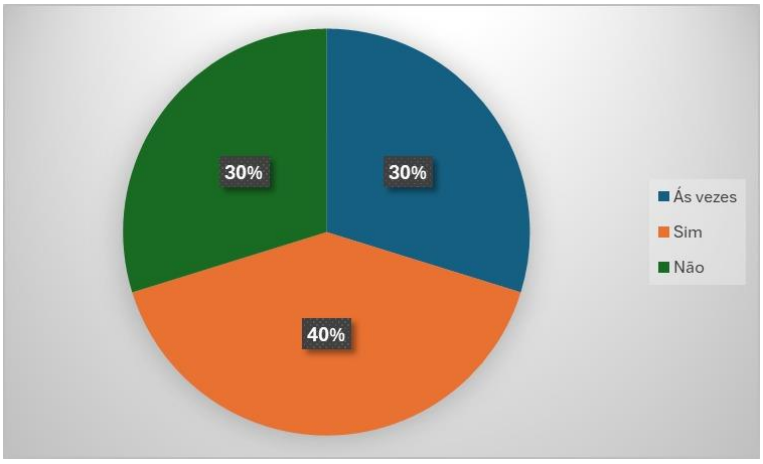
Gráfico 8 – A digitalização de todo o arquivo físico é uma prioridade em sua empresa.



Fonte: elaborado pelos autores, Araraquara (2026).

Conforme apresentado no gráfico 8, 38% dos participantes responderam que a digitalização de todo arquivo físico é uma prioridade em sua empresa, enquanto 38% dos participantes da pesquisa, responderam que ás vezes. Por sua vez, 24% dos participantes responderam que não é uma prioridade.

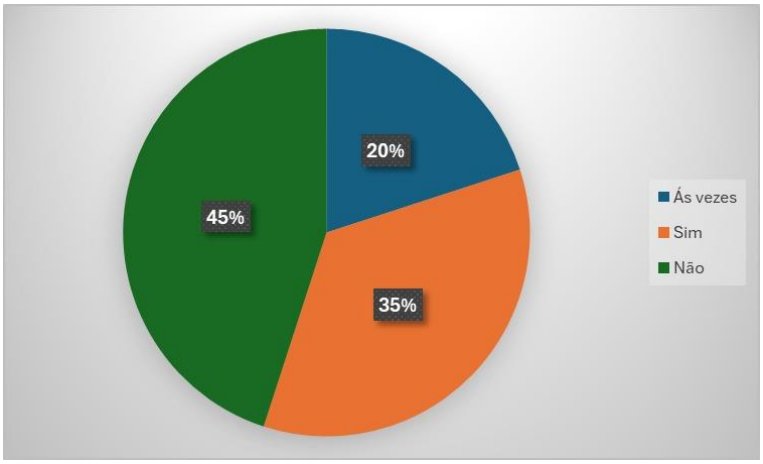
Gráfico 9 - Capacidade de trabalhar com documentos que contêm dados sensíveis, conforme a LGPD.



Fonte: elaborado pelos autores, Araraquara (2026).

Conforme apresentado no gráfico 9, 40% dos participantes responderam que sabem trabalhar com documentos que contém dados sensíveis, enquanto 30% dos participantes da pesquisa, responderam que as vezes. Por sua vez, 30% dos participantes responderam que não sabem trabalhar.

Gráfico 10 - Satisfação com a organização atual dos documentos na empresa.



Fonte: elaborado pelos autores, Araraquara (2026).

Conforme apresentado no gráfico 10, 35% dos participantes responderam que estão satisfeitos com a organização atual dos documentos de sua empresa, enquanto 20% dos participantes da pesquisa, responderam que ás vezes. Por sua vez, 45% dos participantes responderam que estão insatisfeitos.

5 CONSIDERAÇÕES FINAIS

A conclusão deste trabalho tem como foco trazer uma reflexão sobre os resultados obtidos ao longo da pesquisa, ressaltando os principais pontos analisados e a importância do tema abordado. A partir das pesquisas feitas e dados coletados, foi possível compreender o valor da gestão e organização das informações no ambiente de trabalho, como também, o impacto que esses processos realizam na eficiência, segurança e disponibilidade documental. Além disso, o desenvolvimento desse assunto contribuiu para um maior conhecimento do tema, visando o quanto a gestão de documentação é indispensável para garantir o padrão, a conservação adequada e a segurança das informações, diminuindo os erros e simplificando a tomada de decisões

Segundo os resultados obtidos, foi identificado que a maioria das empresas atualmente não estão incluídas na temática Lei Geral de Proteção de Dados Pessoais (LGPD) e da gestão correta. O estudo apresentou dificuldades relacionadas ao descarte correto de documentos,

perdas de arquivos dentro da própria empresa e incapacidade de acessibilidade das informações. Além do mais, a ausência de uma organização documental pode trazer impactos negativos nas rotinas corporativas, como um maior gasto de tempo na busca por documentos, comprometendo a eficiência e a segurança dos processos.

Sugerimos para trabalhos futuros, o aprofundamento de estudos relacionados à implementação da LGPD e aos hábitos de uma gestão documental nas empresas, buscando soluções que contribuam para a organização, segurança e acessibilidade das informações. Tendo em vista que, a utilização de tecnologias e sistemas digitais podem auxiliar em uma melhoria dos processos internos e um gerenciamento correto.

Desta forma, concluímos que a utilização de práticas adequadas de gestão documental e o esclarecimento referente a Lei Geral de Proteção de Dados são essenciais para gerar uma maior segurança, abrangendo organização e eficiência nas empresas.

REFERÊNCIAS

ASCENTY. **Os 15 tipos de ataques cibernéticos mais perigosos para sua empresa.** 2025. Disponível em: https://ascenty.com/blog/artigos/ataques-ciberneticos/. Acesso em: 01 mar. 2026.

CAMILO, Sabrina. **Segurança da informação na gestão de documentos:** como garantir? 2025. Disponível em: https://solides.com.br/blog/seguranca-da-informacao-na-gestao-de-documentos/. Acesso em: 24 out. 2025.

CHRIST, Giovana. **Brasil foi 7º maior alvo de ataques digitais em 2025.** 2026. Disponível em: https://www.cnnbrasil.com.br/tecnologia/brasil-foi-7o-maior-alvo-de-ataques-digitais-em-2025-veja-como-se-proteger/. Acesso em: 02 abr. 2026

COOK, Tim. **As 10 melhores frases de Tim Cook sobre privacidade e segurança 2015.** Disponível em: https://www.kaspersky.com.br/blog/tim-cook-speaks-about-privacy-security/5372/. Acesso em: 09 maio 2026.

CUNHA, Marcella. **Crimes digitais sobem 45% e Senado tem propostas para frear sequestro de dados.** 2025. Disponível em: https://www12.senado.leg.br/radio/1/noticia/2025/01/16/crimes-digitais-sobem-45-e-senado-tem-propostas-para-frear-sequestro-de-dados. Acesso em: 02 abr. 2026.

E-CLIC. **GED com LGPD:** como implementar a gestão eletrônica de documentos. 2025. Disponível em: https://e-clic.net/blog/ged-com-lgpd-como-implementar-a-gestao-de-documentos/. Acesso em: 08 maio 2026.

FEBRABAN TECH. **O Brasil deve investir R$104,6 bilhões em cibersegurança até 2028.** 2025. Disponível em: https://febrabantech.febraban.org.br/temas/seguranca/brasil-deve-investir-r-104-6-bilhoes-em-ciberseguranca-ate-2028. Acesso em: 03 mar. 2025.

FIA – Fundação Instituto de Administração. **Vazamento de dados**: o que é, exemplos reais e como se proteger. 2025. Disponível em: https://fia.com.br/blog/vazamento-de-dados/. Acesso em: 08 maio 2026.

GREENBERG, Andy; SCHNEIER, Bruce**. Abordagens jornalísticas durante o período de ataque cibernético.** 2021. Disponível em: https://www.revistasuninter.com/revistacomunicacao/index.php/revista/article/view/986. Acesso em: 10 maio 2026.

IBM CLOUD. **Tipos de ameaças cibernéticas.** 2025. Disponível em: https://www.ibm.com/br-pt/think/topics/cyberthreats-types. Acesso em: 01 mar. 2026.

IT FORUM**. Brasil é líder global em cookies vazados: 7 bilhões em 2025**. 2025. Disponível em: https://itforum.com.br/cibersegurança/brasil-líder-cookies-vazados/. Acesso em: 27 fev. 2026.

IT PORTAL. **Brasil lidera o roubo de cookies: 7 bilhões de registros**. 2025. Disponível em: https://itportal.com.br/brasil-lidera-o-roubo-de-cookies-7-bilhoes-registros-contabilizados-em-pesquisa-da-nordvpn/. Acesso em: 08 maio 2026.

MICROSOFT. **O que é um vazamento de dados?.** 2025. Disponível em: https://www.microsoft.com/pt-br/security/business/security-101/what-is-a-data-leak. Acesso em: 08 maio 2026.

NAPPO, Stéphane. **O caminho da construção de uma reputação cibernética**. LinkedIn, 2018. Disponível em: <https://www.linkedin.com/pulse/o-caminho-da-constru%C3%A7%C3%A3o-de-uma-reputa%C3%A7%C3%A3o-cibern%C3%A9tica-mitchevis>. Acesso em: 8 maio 2026.

NORD VPN. **Brasil lidera ranking global de vazamento de cookies**. 2026. Disponível em: https://adnews.com.br/post/brasil-lidera-ranking-global-de-vazamento-de-cookies-com-7-bilhoes-de-registros-expostos. Acesso em: 08 maio 2026.

OBLOCK. **10 Ataques cibernéticos mais marcantes de 2024.** 2024. Disponível em: https://www.oblock.com.br/ataques-ciberneticos-2024/#elementor-toc__heading-anchor-1. Acesso em: 10 maio 2026.

PAIVA, Mauricio Ferraz de. **Sem uma documentação adequada para a qualidade, não se chega à excelência.** 2016. Disponível em: https://www.normas.com.br/visualizar/artigo-tecnico/2830/sem-uma-documentacao-adequada-para-a-qualidade-nao-se-chega-a-excelencia?utm_source. Acesso em: 24 out. 2025.

PECK, Patricia. **Direito digital**. 7. ed. São Paulo: Saraiva Educação, 2020.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais:** comentários à Lei Geral de Proteção de Dados Pessoais (LGPD). São Paulo: Saraiva Educação, 2021.

SÊMOLA, Marcos. **Gestão da segurança da informação:** uma visão executiva. 2. ed. Rio de Janeiro: Elsevier, 2014.