UTILIZAÇÃO DA DLP NA PREVENÇÃO A EXPOSIÇÃO E DEFESA DE DADOS SENSÍVEIS EM EMPRESAS DE CONTABILIDADE: UM ESTUDO DE CASO

USE OF DLP TO PREVENT EXPOSURE AND SENSITIVE DATA IN ACCOUNTING FIRMS: A CASE STUDY

Elias Ferreira Carvalho
Faculdade de Tecnologia de Santana de Parnaíba
ecarvalho864@gmail.com

Isabella Fernandes Souza de Morais
Faculdade de Tecnologia de Santana de Parnaíba
isabellafernandes.isaiaslm@gmail.com

Eugenio Eurípedes Bittencourt
Faculdade de Tecnologia de Santana de Parnaíba
eugenio.bittencourt@fatec.sp.gov.br

Resumo

A *Data Loss Prevention – DLP* refere-se a um conjunto de métodos de proteção e análise de comportamento que visa monitorar e controlar o ambiente no qual está inserida, além de mitigar possíveis explorações às vulnerabilidades do ambiente, com diversas opções de ferramentas para configuração e utilização. O artigo possui natureza qualitativa com utilização da metodologia estudo de caso único, apresenta os tipos de ferramentas *DLP* e os possíveis riscos de exposição de dados sensíveis dentro de empresas de Contabilidade. O estudo apresenta os riscos à Segurança da Informação em escritórios de Contabilidade, os tipos de ambientes, ferramentas baseadas em *DLP* e de que forma essas ferramentas podem agregar na proteção de dados no ambiente contábil.

Palavras-chave: *Data Loss Prevention*, Contabilidade, Segurança da Informação.

Abstract

This text refers to a set of methods for protecting and analyzing behavior aimed at monitoring and controlling the environment in which it is applied, as well as mitigating potential exploits of environmental vulnerabilities, with a variety of available tools for configuration and use. The article, using a qualitative methodology based on a single-case study, presents various types of DLP (Data Loss Prevention) tools and the potential risks associated with exposure of sensitive data within accounting firms. The study aims to highlight the risks to information security in accounting offices, the types of environments where these risks may be present, the use of DLP-based tools, and how these tools can enhance data protection in the accounting sector.

Keywords: *Data Loss Prevention, Accounting, Information Security.*

1. Introdução

A contabilidade é a teoria ou prática de registro e cálculo sobre a movimentação dos valores monetários envolvidos em uma atividade em que são trabalhadas e analisadas as questões financeiras como patrimônio e custos de uma organização. Entre esses dados, há alguns que são considerados sensíveis e não devem ser acessíveis e/ou divulgados (TRAVASSOS, 2022).

A era tecnológica apresenta desafios adicionais para contabilidade, especialmente devido à crescente demanda por informações, uma vez que o avanço da tecnologia permitiu que a contabilidade tenha evoluído até o cenário atual deixando de ser uma simples mensuração de dados e fornecimento de informações, tornou-se uma ferramenta de gestão crucial para tomada de decisões, por isso é necessário que se estabeleça procedimentos adequados para exercer um controle e proteção mais eficazes, como a prática e implementação da segurança da informação (RIBEIRO et al., 2020).

Segundo Duarte (2022), a segurança da informação exerce uma função vital para garantir a conformidade, fornecendo diretrizes sólidas e controles técnicos fundamentais para a proteção dos dados em todas as fases da sua existência, desde sua coleta ao descarte. Para este fim, o Brasil aprova em 2018 a Lei de Proteção de Dados (Lei nº 13.709/2018) , que estabelece regulamentações sobre o tratamento de dados pessoais, com objetivo de assegurar que as empresas sigam práticas normatizadas de segurança e privacidade em relação aos dados pessoais, para isso é necessário que as empresas realizem uma série de adaptações, processos e investimentos em segurança da informação.

Diante do cenário apresentado, a *Data Loss Prevention (DLP)* é uma ferramenta de relevância dentro do universo das empresas, uma vez que identifica, monitora e protege contra a perda de dados em tempo real, registrando logs e bloqueando acessos não autorizados contribuindo para a segurança da informação (OLIVEIRA; CAMPOS; MACEDO, 2022a).

Assim, a questão de pesquisa do artigo é: Como a implementação da *DLP* influencia na prevenção de exposição de dados sensíveis em uma empresa de contabilidade? Os objetivos são: (1) Apresentar os tipos de ferramentas *DLP* e (2) Apresentar os possíveis riscos de exposição de dados sensíveis dentro de uma empresa de contabilidade. O artigo está desenvolvido em sete seções, sendo a presente a introdução para o desenvolvimento de pesquisa; a seção 2 apresenta o referencial teórico que traz a base bibliográfica; já a seção 3 traz a metodologia utilizada; a seção 4 traz a questão de pesquisa; a 5 se refere a justificativa e, por fim, a seção 6 apresenta as considerações finais e sugestões para novas pesquisas.

2. Referencial Teórico

Nesta seção, serão apresentados os aspectos teóricos que fundamentam o presente artigo, com destaque para a base teórica da Segurança da Informação, a Lei Geral de Proteção de Dados (LGPD), *DLP* (*Data Loss Prevention*), os tipos de ambiente, a Classificação de dados e a Contabilidade.

2.1. Segurança da Informação

A informação desempenha um papel importante em todas as etapas e processos de negócios de uma empresa. O conceito de segurança da informação refere-se à proteção dos dados de propriedade da empresa garantindo a guarda, através de esforços para mitigar os riscos assegurando a continuidade dos negócios (NEVES et al., 2021).

A segurança da informação, antigamente, era simples, com dados físicos guardados em arquivos em ambientes físicos, com a evolução tecnológica e a sua utilização surgiram controles de acesso lógicos e segurança física, os dados são acessados em vários locais e as ameaças à privacidade e integridade da informação são mais intensas (SANTOS; SILVA, 2021).

Dessa forma, pode-se definir a segurança da informação como medidas destinadas a garantir e proteger a integridade, disponibilidade e confidencialidade. A Integridade visa garantir que não haja alterações da informação protegendo contra alterações indevidas; a Disponibilidade permite que a informação esteja disponível quando necessária; a Confidencialidade refere-se a assegurar que apenas pessoas autorizadas tenham acesso à informação (LIMA; FERREIRA; PEIXOTO, 2022).

Para isso, é necessário que se determine um conjunto apropriado de controles, políticas, processos e procedimento, de forma que se estabeleça diretrizes, implemente-as, realize a monitoração e revisões periódicas, aprimorando-as conforme necessário para assegurar os objetivos de segurança da organização (DUARTE, 2022).

2.2. Lei Geral de Proteção de Dados

A LGPD é o primeiro passo significativo na regulamentação apropriada e aplicável do uso de dados pessoais no Brasil. Aprovada como Lei 13.709 em agosto de 2018 e em aplicação prática em 2020, essa Lei prevê as orientações para a coleta, tratamento, armazenamento e compartilhamento de dados pessoais por entidades públicas e privada (CRUZ; PASSAROTO; JUNIOR, 2021).

Essa lei incide sobre toda e qualquer manipulação de informações pessoais, realizada por indivíduos, entidades públicas ou privadas, sem levar em consideração os métodos, país de origem ou o local onde os dados estejam armazenados (PEITER, ESTER et al, 2022). A LGPD determina a aplicação de punições administrativas conforme estabelece o artigo 52, onde, são previstas: advertência, multa, publicização da infração, bloqueio e/ou eliminação dos dados pessoais relacionados à infração (OLIVEIRA; CAMPOS; MACEDO, 2022b).

De acordo com o artigo 5º os dados pessoais são, então, em princípio, todas as informações caracterizadas por identificar e pela determinar quem é o indivíduo, enquanto os dados sensíveis são aqueles que se tratam sobre a origem racial, étnica, ideais políticos, religiosas, orientação sexual, dados clínicos, dados genéticos e biométricos. Os dados sensíveis são o tipo de informação que pode expor de forma pejorativa ou vexatória quando exposto SARLET; RUARO, 2021).

A LGPD tornou-se um marco regulatório visando garantir os direitos com relação a proteção de dados e estabelecendo diretrizes para o adequado tratamento. Nesse sentido, a *DLP* pode ser uma ferramenta essencial para as organizações (NUNES; SANTOS, 2023), como instrumento para o cumprimento da lei.

2.3. *DLP*

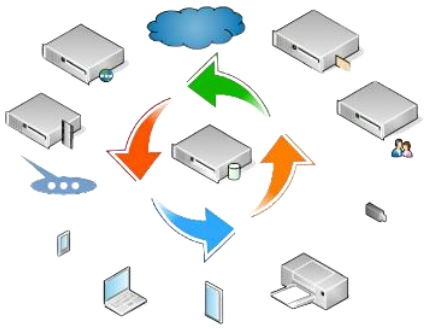
A *DLP* consiste em métodos e processos de proteção que oferecem recursos para prevenir extravios e acessos indevidos, garantindo a segurança da informação, de forma que o sistema realiza a identificação, monitoramento e proteção, registrando as atividades e impedindo acessos não autorizados (OLIVEIRA; CAMPOS; MACEDO, 2022a).

A *DLP* é utilizada na identificação e classificação dos dados, monitorando o tráfego das informações, realizando controle de acesso, prevenção contra vazamento de dados, monitoramento de comportamentos anormais, auditorias e integração com outras soluções de segurança (NUNES; SANTOS, 2023).

Dessa forma, a *DLP* pode ser definida como um conjunto de estratégias, processos e tecnologias para proteger os dados confidenciais contra roubo, perda e uso indevido da informação (IBM, 2024). Ela utiliza recursos como softwares antivírus, inteligência artificial e aprendizado de máquinas para detectar as atividades suspeitas, através das políticas definidas pela empresa (MICROSOFT, 2024).

Segundo Alneyad et al. (2016), as informações sensíveis podem ser compartilhadas em várias plataformas de comunicação em três cenários: (1) em movimento - rede; (2) em uso - *host*; e (3) em repouso - banco de dados. Ainda assim, esses conceitos são amplamente utilizados no ambiente corporativo. A Figura 1 apresenta diversos canais em que é possível ocorrer vazamento de informações:

Figura 1 - Exemplos de canais de vazamento de dados



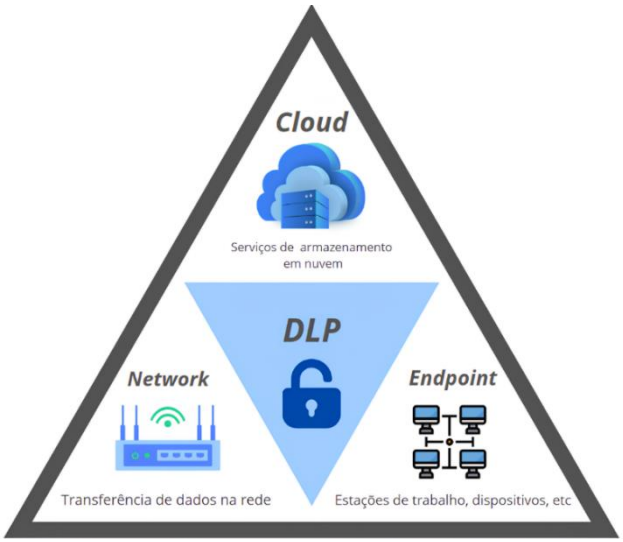
Fonte: Akume, 2022, p.26

A Figura 1 apresenta os principais canais onde pode ocorrer o vazamento de dados sigilosos (AKUME, 2022). Os dados podem vazar de diversas maneiras, tanto físicas - como através de dispositivos usb, laptops, smartphones, tablets - quanto virtuais, como em e-mails, mensagens instantâneas, invasões de servidores ou infecções por vírus.

2.4. Tipos de Ferramentas *DLP*

A *DLP* tem o intuito de reduzir os riscos operacionais, pois ela nos permite o entendimento detalhado sobre como os dados são gerados e reportados em um fluxo de dados. Dessa forma, a *DLP* possui três tipos importantes de soluções: *Network* (rede), *Cloud DLP* (*DLP* na nuvem) e *Endpoint* (Mansikka, 2023), conforme Figura 2 apresentada abaixo.

Figura 2 – Tipos de ferramentas *DLP*



Fonte: Os autores, 2024

A *Network DLP* é uma solução de rede focada na transferência de dados dentro e fora da rede. Normalmente, utiliza-se a inteligência artificial e o machine learning (aprendizado de máquina) para identificar as rotas por onde os dados estão trafegando e assim, detectar e sinalizar o vazamento ou a perda de dados (IBM, 2024).

As soluções baseadas em *Network DLP* são responsáveis pelo processamento de dois tipos de dados: os dados em movimento e os dados em uso. Os dados em movimento são aqueles em que informações são transmitidas por intermédio da rede, já os dados em uso referem-se àqueles que são manipulados pelos usuários (FORCEPOINT, 2020).

A função do *Endpoint DLP* é fornecer ao administrador de redes a oportunidade de monitorar todos os equipamentos que estão conectados na rede, sendo ele um servidor, *smartphone*, *notebook, pc,* ou outro dispositivo. Esse tipo de solução é instalado nos equipamentos utilizados pelos colaboradores como medida preventiva contra o vazamento ou compartilhamento de dados sensíveis (CROWDSTRIKE, 2024).

O *Cloud DLP* é uma ferramenta focada na proteção dos dados que são acessados e armazenados por meio dos serviços em nuvem. Essas ferramentas apresentam a capacidade de analisar, organizar, acompanhar e codificar as informações em plataformas. Além disso, essas ferramentas ajudam na implementação de regras de segurança para usuários específicos e para qualquer serviço *online* que tenham acesso aos dados corporativos. (IBM, 2024).

2.5. Classificação de dados

Segundo Dantas (2011), a classificação de dados diz respeito ao tipo de dados a ser manipulado e sua criticidade e importância para a Organização, dizendo que é possível classificar em quatro tipos:

- Informações públicas, aquelas que têm baixo grau de relevância e em geral não necessitam tanta proteção;
- Informações internas, aquelas que o acesso não autorizado deverá ser evitado, apesar de que, se ocorrer, os impactos não serão dos mais sérios;
- Informações confidenciais, aquelas que devem ser restringidas de acesso externo, preservando a confidencialidade e sendo acessadas somente por pessoas autorizadas, uma vez que podem causar grande impacto na organização prejudicando os lucros ou com perda de competitividade da empresa diante das concorrentes;
- Informações secretas, são as mais críticas, pois são vitais para a existência dos negócios da empresa e, portanto, o acesso deve ser preservado a qualquer custo e restrito a apenas algumas pessoas.

Tipo de informação	Nível de criticidade
Pública	Baixo
Interna	Médio
Confidencial	Alto
Secreta	Muito alto

Fonte: Os autores, 2024

2.6. Contabilidade

A contabilidade possibilita o registro de informações relacionadas a diversas transações realizadas por uma organização, permitindo compreender as consequências dessas operações, oferecendo insights sobre a situação econômico-financeira e disponibilizando dados para que a empresa possa se basear com o passado, fundamentar o presente e planejar o futuro (NGO; PANANGUILA, 2023).

Considerada uma ciência, a contabilidade se dedica a analisar, registrar e compreender os eventos que impactam os ativos (bens e direitos) e passivos (obrigações e patrimônio líquido, por exemplo) de uma organização, por meio da documentação e apresentação dos resultados financeiros gerados, em que seu principal objetivo é oferecer informações valiosas para orientar as decisões, tanto internas quanto externas à empresa, por meio da análise, interpretação, registro e gestão do patrimônio (TADEU; ALMEIDA; GONÇALVES, 2021).

No contexto organizacional, a contabilidade é abastecida diariamente através das operações financeiras, funcionando como um sistema de informação necessário para gestão (NGO; PANANGUILA, 2023). Dessa forma, como fornecedora de informações tanto internas quanto externas, está entre as áreas mais influenciadas pela evolução tecnológica (FRANCO et al., 2021).

A contabilidade tem evoluído juntamente com as inovações tecnológicas e o progresso dos negócios nas empresas. Essas organizações têm se utilizado de sistemas de controle internos, empregando ferramentas tecnológicas que favorecem, simplificam e aceleram todo o processamento contábil (MOREIRA, 2021). Dessa maneira, a utilização da tecnologia na contabilidade permite controles imediatos, fortalecendo os recursos e maximizando o tempo (ANDRADE; MEHLECKE, 2020).

3. Metodologia

A metodologia utilizada foi estudo de caso único (YIN, 2021), que tem como objetivo, entender como a *DLP* atua em informações e dados sensíveis dentro do ramo contábil, através da natureza de pesquisa qualitativa. (THEÓPHILO; MARTINS, 2016).

A coleta dos dados (GIL, 2021) será feita através de análise documental. A empresa para análise será a empresa XYZ, uma empresa do setor contábil, contando com a colaboração de um especialista em segurança da informação que possui conhecimentos na área contábil. A Tabela 1, representa quais são as caraterísticas utilizadas neste trabalho.

Quadro 1 – Metodologia utilizada para o artigo

Item	Descrição	Autor(es)
Natureza	- Qualitativa	Gil (2021)
Metodologia	- Estudo de Caso Único	YIN (2021)
Coleta de Dados	- Entrevista	THEÓPHILO; MARTINS (2016)
	- Análise Documental	THEÓPHILO; MARTINS (2016)
Unidade de Análise	- Empresa XYZ	

Fonte: Os autores, 2024.

3.1 Processos Metodológicos

Para a construção deste estudo, foram realizadas as seguintes etapas:

Passo 1: Definir empresa para estudo: Estabelecer empresa a ser utilizada no estudo de caso, que tenha conhecimento de rotinas do setor contábil e que contribua com uma visão sobre a forma do qual dados sensíveis são classificados, tratados e mitigados.

Passo 2: Definir questões: Elaborar questões que abordem o tema proposto e entendimento para o leitor e que apresentem uma análise qualitativa do ambiente inserido.

Passo 3: Enviar formulário: Envio das questões para o especialista em segurança da informação da empresa que servirá de análise e esclarecimento das dúvidas.

Passo 4: Receber e analisar respostas: Analisar as respostas recebidas e selecionar as

informações que possam contribuir para o entendimento do ambiente contábil.

Passo 5: Apresentar resultados: No artigo, apresentar as respostas analisadas, a atuação das informações no ambiente, o conhecimento técnico em procedimentos de proteção de dados e a familiaridade com ferramentas relacionadas à *DLP* como metodologia. A figura 3 exemplifica o procedimento metodológico e seu passo a passo.

Figura 3 - Procedimentos metodológicos

Fonte: Os autores, 2024.

3.2 Objeto de Estudo

A empresa XYZ é uma empresa fictícia do setor contábil que atua na cidade de Jundiaí, que presta o serviço de contabilidade para empresas de pequeno, médio e grande porte. Essa empresa conta com 40 colaboradores que atualmente atende mais de 50 clientes entre pequenas e médias empresas de vários seguimentos. O objetivo do estudo é entender como a *DLP* pode minimizar os impactos de vazamento de dados e prevenir perdas, e como a mesma pode ser aplicada em um escritório contábil.

3.3 Questionário

Para a realização do estudo de caso, foi criado um questionário para realização da entrevista e levamento das informações. A entrevista se deu através de um questionário enviado por email ao especialista em SI, da qual foi realizada em meados do mês de setembro. Após o retorno das respostas, foi realizada uma análise posterior, conforme exposto no quadro 2.

Questões

1) Como funciona a classificação de dados sensíveis na empresa?

R: Na empresa, os dados são classificados como pessoais, sensíveis ou não pessoais. Depois, recebem selos de circulação: interno, restrito, confidencial ou público. Com essas classificações, aplicamos as diretrizes de uso e cuidados necessários.

2) Já ocorreu algum tipo de vazamento de dados na empresa referente a dados que foram enviados para escritórios concorrentes?

R: Não, devido ao acesso restrito e aos constantes treinamentos sobre o uso consciente dos dados, nunca houve comprometimento. Embora já tenham ocorrido falhas de segurança e identificados pontos vulneráveis, nenhuma dessas situações afetou os dados

3) Como foi resolvido e em que tipo de ambiente ocorreu?

R: As falhas tratavam de credenciais não desativadas após o desligamento do operador no sistema de armazenamento de documentos contábeis. Mas foram tratadas com revisão do processo e inclusão de revisão periódica dos itens por um operador especializado no assunto.

4) Quais tipos de informações, contratos, documentos são considerados sensíveis do ponto de vista contábil?

R: Isso vai depender da política da empresa, mas para dados pessoais ou dados pessoais sensíveis, iremos seguir as diretrizes aplicadas a LEI 13.709. Já nos subníveis temos alguns exemplos como público: cadastro pessoa jurídica junto a receita federal, restrito: folha de pagamento, confidencia: balanços e DRE.

5) Em sua visão, por que é importante não tratar sistemas de segurança de forma isolada, e como isso se aplica especificamente ao contexto de prevenção de perda de dados (DLP)?

R: Não existe no mundo, sistema de informação ou não que funcione isoladamente, assim como os seres humanos, vivem em coletivo e dependem uns dos outros para o bom funcionamento da sociedade, o se aplica para sistemas de informação, a utilização de sistema de informação, como camadas para aumentar a mitigação de riscos a uma informação é a chave para uma melhor prevenção.

6) Quais são as principais limitações de uma solução de DLP? Que outras ferramentas ou procedimentos de segurança da informação são recomendadas para complementar uma DLP e garantir a proteção eficaz dos dados e do ambiente tecnológico como um todo?
R: Escalabilidade inadequada: As soluções tradicionais de DLP podem enfrentar desafios de escalabilidade, tornando-se menos eficazes à medida que a quantidade de dados e dispositivos a serem protegidos aumenta. E tratar exceções nas políticas pode ser custoso gerencialmente e abre portas para riscos desnecessários. Isso pode resultar em lacunas na proteção dos dados sensíveis da empresa.
Limitações na prevenção de vazamentos: As soluções de DLP e EDR muitas vezes não conseguem prevenir efetivamente vazamentos de dados, seja devido a falhas na detecção de comportamentos suspeitos dos usuários, na proteção inadequada dos dispositivos remotos dos funcionários ou no controle insuficiente sobre o acesso e compartilhamento de informações confidenciais.
Necessidade de controle granular: Para garantir a segurança dos dados corporativos, é essencial ter um controle granular sobre quem pode acessar, visualizar, editar e compartilhar informações sensíveis. As soluções tradicionais podem não oferecer esse nível de controle personalizado, o que pode resultar em brechas na proteção dos dados.

7) Como você avalia a combinação de diferentes soluções de segurança, como antivírus, sistemas de prevenção de perda de dados (DLP), Políticas de Segurança da Informação, na construção de um ambiente tecnológico seguro e robusto?
R: É essencial para a real proteção do ambiente e não apenas um gasto de dinheiro, deve ser visto como um investimento. Para o funcionamento adequado, é necessária combinação de várias soluções para a proteção efetivamente.

8) Quais são as melhores práticas recomendadas para empresas de contabilidade que desejam implementar um sistema de segurança integrado, incluindo DLP?
R: O uso de políticas de segurança bem definidas, normas que garantam a melhor forma de tratativa e manipulação de dados, conscientização e treinamentos frequentes a todos os colaboradores que utilizem o sistema da empresa, pois aliados a uma ferramenta baseada em

DLP, a segurança se torna efetiva.

9) Qual seria o passo a passo detalhado para implementação de DLP em uma empresa de contabilidade? Quais dados e documentos precisam ser levantados e a forma para serem tratados?
R: Para se definir corretamente a implementação da DLP, é necessário analisar o porte da empresa, o cenário atual e como a empresa trata suas informações, quais foram as ocorrências de possíveis vazamentos no passado, como foram mitigados e em quais locais a situação ocorreu, para que se possa escolher a melhor ferramenta baseada em DLP juntamente a política de segurança já estruturada e bem definida.

10) Existe alguma cartilha de SegInfo proteção de dados sensíveis específica para a área da contabilidade?
R: Possuímos sim a nossa política de SegInfo, bem como um treinamento para novos funcionários com as boas práticas dentro da ISO 27001, o qual apresentamos e deixamos ao dispor de todos os operadores.

4. Análise e Interpretação dos Resultados

A empresa organiza os dados em três categorias principais: dados pessoais, dados pessoais sensíveis e dados não pessoais. Após essa classificação inicial, aplica-se um sistema adicional de controle, que utiliza selos de circulação para identificar o grau de confidencialidade dos documentos, como interno, restrito, confidencial e público. Essa abordagem dupla de classificação garante a aplicação rigorosa das diretrizes de segurança, proporcionando um controle mais efetivo sobre o acesso e a troca de dados.

Nessa implementação de selos de controle há uma estratégia eficaz para garantir que os documentos sejam manuseados conforme seu nível de sensibilidade, em conformidade com os princípios de segurança da informação estabelecidos pela ISO 27001.

Durante a análise, foi relatado que não ocorreram vazamentos de dados sensíveis, como o envio de informações para concorrentes. Essa situação deve-se ao acesso controlado às informações e a um abrangente programa de capacitação sobre o uso responsável dos dados.

Porém, a empresa admitiu que no passado ocorreram falhas de segurança relacionadas à falta de desativação das credenciais dos empregados que foram desligados.

As principais limitações identificadas para uma solução de *DLP* são: Escalabilidade inadequada, limitações na prevenção dos dados e a necessidade de controle mais detalhado, sendo cada um:

Escalabilidade inadequada: As soluções tradicionais de *DLP* podem enfrentar desafios de escalabilidade, que significa a capacidade de expansão ou regressão de um negócio de acordo com as necessidades daquele momento. Essa escalabilidade pode se tornar menos eficaz à medida que a quantidade de dados e dispositivos a serem protegidos aumenta. Tratar exceções nas políticas pode ser custoso gerencialmente e abre portas para riscos desnecessários. Isso pode resultar em lacunas na proteção dos dados sensíveis da empresa., dessa forma, é necessário que as soluções possam abarcar qualquer tipo de situação prevista.

Limitações na prevenção de vazamentos: Soluções baseadas em DLP nem sempre são ferramentas de prevenção efetivas no combate dos vazamentos de dados, devido as falhas na detecção de procedimentos suspeitos dos usuários, na proteção inadequada dos dispositivos remotos dos funcionários ou no controle insuficiente sobre o acesso e compartilhamento de informações confidenciais. Dessa forma, entende-se a importância de políticas alinhadas com essas soluções ou ferramentas.

Necessidade de controle granular: Para garantir a segurança dos dados corporativos, é essencial ter um controle mais detalhado sobre quem pode acessar, visualizar, editar e compartilhar informações sensíveis. As soluções tradicionais podem não oferecer esse nível de controle personalizado, o que pode ocasionar brechas na proteção dos dados.

No que diz respeito à proteção das informações, a DLP por si não é eficaz para a proteção das informações e prevenção de vazamento ou perda de dados. Para que ela se torne efetiva, é necessário entender o contexto organizacional, porte da empresa, tipos de dados que transitam e por quais departamentos essas informações são manuseadas para que a política de segurança da informação e DLP atuar juntas em cima das informações analisadas e classificadas.

5. Conclusão

Este artigo teve como objetivo entender e analisar como a implementação da *DLP* pode colaborar na prevenção à exposição de dados sensíveis em empresas contábeis, do qual se conclui que são necessários diversos mecanismos aplicados para garantir que a segurança seja efetiva.

Para a construção deste trabalho, entrevistamos um especialista em Segurança da Informação aplicada a Contabilidade que nos forneceu as informações necessárias para esse estudo de caso único. Para isso, buscamos entender sobre diversos fatores como leis que regem a guarda das informações, requisitos e categorias de classificação de dados.

Entretanto, conforme o estudo de caso levantado, a *DLP* por si só não oferece totalidade em proteção, porém requisita mecanismos, procedimentos e políticas de Segurança da Informação combinadas para trazer uma efetividade na proteção das informações. Para isso, é necessário analisar o tamanho da empresa contábil, classificar os dados da forma necessária, rever as políticas atuais e definir a melhor abordagem para a prevenção de perda das informações.

O trabalho pretende contribuir com o conhecimento em *DLP* como uma alternativa para auxiliar nos processos de segurança da informação em ambientes contábeis, devido aos tipos de documentos sensíveis trabalhados por este setor.

Referências

ALNEYADI, S.; SITHIRASENAN, E.; MUTHUKKUMARASAMY, V. A survey on data leakage prevention systems. Journal of Network and Computer Applications, v. 62, p. 137–152, 2016.

AKUME, L. **Yolo DLP: um sistema de prevenção de vazamento de dados de imagens baseado em aprendizado de máquina**. 1. ed. São Paulo: Dialética, 2022.

ANDRADE, C. B. H.; MEHLECKE, Q. T. C. AS INOVAÇÕES TECNOLÓGICAS E A CONTABILIDADE DIGITAL: UM ESTUDO DE CASO SOBRE A ACEITAÇÃO DA CONTABILIDADE DIGITAL NO PROCESSO DE GERAÇÃO DE INFORMAÇÃO CONTÁBIL EM UM ESCRITÓRIO CONTÁBIL DO VALE DO PARANHANA/RS. **Revista Eletrônica de Ciências Contábeis**, v. 9, n. 1, p. 93–122, 3 fev. 2020.

CRUZ, U. L. DA; PASSAROTO, M.; JUNIOR, N. T. O IMPACTO DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD) NOS ESCRITÓRIOS DE CONTABILIDADE. **ConTexto - Contabilidade em Texto**, v. 21, n. 49, p. 30–39, 18 out. 2021.

DANTAS, M. **Segurança da informação: uma abordagem focada em gestão de riscos**. [s.l: s.n.].
DUARTE, E. P. LGPD: MEDIDAS ESSENCIAS DE SEGURANÇA DA INFORMAÇAÇÃO. **FatecSeg - Congresso de Segurança da Informação**, 30 nov. 2022.

EDWARDS, S. Was ist Datenverlustprävention (DLP)? Disponível em: <https://www.crowdstrike.com/de-de/cybersecurity-101/data-protection/data-loss-prevention-dlp/>. Acesso em: 04 maio 2024.

Enterprise DLP (Data Loss Prevention). Disponível em: <https://www.forcepoint.com/pt-br/product/dlp-data-loss-prevention>. Acesso em: 4 maio. 2024.

FRANCO, G. et al. Contabilidade 4.0: análise dos avanços dos sistemas de tecnologia da informação no ambiente contábil. **CAFI**, v. 4, n. 1, p. 55–73, 2021.

GIL, A. C. **Métodos e técnicas de pesquisa social (6a. ed.).** São Paulo: Editora Atlas S.A., 2008.

IBM. **O que é data loss prevention (DLP)? | IBM**. Disponível em: <https://www.ibm.com/br-pt/topics/data-loss-prevention>. Acesso em: 25 abr. 2024.

LIMA, P. R. S.; FERREIRA, L. M. M.; PEIXOTO, A. L. V. DE A. Gestão da segurança da informação: análise de políticas de defesa cibernética e estratégias para a proteção de dados e informações da administração pública brasileira. **P2P E INOVAÇÃO**, v. 9, n. 1, p. 206–221, 29 set. 2022.

MANSIKKA, Jaakko. Data loss prevention: for securing enterprise data integrity. **Centria University of Applied Sciences.** p.44, May 2023.

MICROSOFT. **O que é a DLP (prevenção contra perda de dados)? | Segurança da Microsoft**. Disponível em: <https://www.microsoft.com/pt-br/security/business/security-101/what-is-data-loss-prevention-dlp>. Acesso em: 25 abr. 2024.

MOREIRA, R. G. A Tecnologia da Informação no Avanço da Contabilidade. **Revista FAROL**, v. 13, n. 13, p. 24–39, 2 ago. 2021.

NEVES, D. L. F. et al. A segurança da informação de encontro às conformidades da LGPD. **Revista Processando o Saber**, v. 13, p. 186–198, 9 jun. 2021.

NGO, E. N.; PANANGUILA, M. C. CONTABILIDADE GERAL: A SUA IMPORTÂNCIA COMO SUPORTE DE GESTÃO. **RECIMA21 - Revista Científica Multidisciplinar - ISSN 2675-6218**, v. 4, n. 2, p. e422824, 1 fev. 2023.

NUNES, L. F. P.; SANTOS, J. C. F. DOS. LGPD – Uma visão de tecnologia e agnóstica. **Revista Direito & Paz**, v. 2, n. 49, p. 218–237, 2023.

OLIVEIRA, A.; CAMPOS, B.; MACEDO, A. LGPD - Proposta de implementação de melhorias em um escritório de contabilidade na cidade de Macapá/AP: estudo de caso. **Concilium**, v. 22, n. 6, p. 39–53, 1 nov. 2022a.

OLIVEIRA, A.; CAMPOS, B.; MACEDO, A. LGPD - Proposta de implementação de melhorias em um escritório de contabilidade na cidade de Macapá/AP: estudo de caso. **Concilium**, v. 22, n. 6, p. 39–53,

1 nov. 2022b.

PEITER, ESTER ESCALANTE et al. Lei Geral de Proteção de Dados: Roteiro para Implantação e Adequação em Escritórios de Contabilidade. In: Congresso USP de Iniciação Científica em Contabilidade. São Paulo. 2022. <https://congressousp.fipecafi.org/anais/22UspInternational/ArtigosDownload/3631.pdf>. Acesso em: 23 jun. 2024

RIBEIRO, R. et al. CIBERSEGURANÇA E SEGURANÇA DA INFORMAÇÃO CONTÁBIL: UMA ANÁLISE DA PERCEPÇÃO DO PROFISSIONAL CONTÁBIL. **RAGC**, v. 8, n. 32, 20 abr. 2020.

SANTOS, R. B. DOS; SILVA, T. B. P. E. Gestão da segurança da informação e comunicações: análise ergonômica para avaliação de comportamentos inseguros. **RDBCI: Revista Digital de Biblioteconomia e Ciência da Informação**, v. 19, p. e021024–e021024, 1 out. 2021.

SARLET, Gabrielle Bezerra Sales; RUARO, Regina Linden. A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da Lei Geral de Proteção de Dados (LGPD)–L. 13.709/2018. **Revista Direitos Fundamentais & Democracia**, v. 26, n. 2, p. 81-106, 2021.

TADEU, S.; ALMEIDA, N.; GONÇALVES, A. CONTABILIDADE 4.0, A TECNOLOGIA A FAVOR DOS CONTADORES NA ERA DIGITAL. **Revista Projetos Extensionistas**, v. 1, n. 1, p. 146–153, 6 dez. 2021.

THEÓPHILO, C. R.; MARTINS, G. de A. Metodologia Da Investigação Cientifica (3a). 2016.

Yin RK. Estudo de Caso, planejamento e métodos. 5ª ed. Porto Alegre: Bookman; 2024.