



**UNIVERSIDADE DO ESTADO DA BAHIA (UNEB)
DEPARTAMENTO DE EDUCAÇÃO (DEDC), *CAMPUS XIII***

JOELTON OLIVEIRA DE ARAÚJO

**A RELEVÂNCIA DO *BACKUP* EM ESCRITÓRIO DE PEQUENO PORTE EM
ITABERABA: um estudo de caso**

**ITABERABA
2021**

JOELTON OLIVEIRA DE ARAÚJO

**A RELEVÂNCIA DO *BACKUP* EM ESCRITÓRIO DE PEQUENO PORTE EM
ITABERABA: um estudo de caso**

Trabalho de Conclusão de Curso (TCC), na modalidade monografia, apresentado ao Departamento de Educação (DEDC), *Campus XIII*, da Universidade do Estado da Bahia (UNEB), enquanto requisito para obtenção do título de bacharel em Ciências Contábeis.

Orientador: Professor Dr. Luiz Carlos dos Santos

**ITABERABA
2021**

Ficha Catalográfica

A ser preenchida pela Biblioteca Central da Universidade,
depois de aprovado o TCC

FOLHA DE APROVAÇÃO

A RELEVÂNCIA DO *BACKUP* EM ESCRITÓRIO DE PEQUENO PORTE EM ITABERABA: um estudo de caso

Monografia enquanto Trabalho de Conclusão de Curso (TCC), defendida por **Joenton Oliveira de Araújo** e aprovada em 10 de julho de 2021 pela Banca Examinadora constituída pelos professores abaixo discriminados:

BANCA EXAMINADORA

Professor Doutor – Luiz Carlos dos Santos – Orientador – UMSA e UNIFACS/PPDRU

Universidade do Estado da Bahia (UNEB)

Professor Especialista – Valdir dos Santos Miranda – Examinador – FVC/CEPPEV

Universidade do Estado da Bahia (UNEB)

Professor Mestre Carlos Henrique de Macedo – Examinador – PGDR/UNEB

Universidade do Estado da Bahia (UNEB)

A uma pessoa muito especial, minha querida prima Ludmila Almeida, que foi meu maior incentivo para iniciar esse curso.

AGRADECIMENTOS

Primeiro a Deus, por me proporcionar saúde e coragem para finalizar esse trabalho com sucesso.

À minha mãe, dona Márcia, por sempre confiar em mim e por me incentivar a mais essa jornada.

À minha esposa Caroline, pela paciência em tolerar meus momentos de estresse durante o grande fluxo de atividades, ficando sempre ao meu lado, me apoiando e incentivando em todos os momentos difíceis, mas, gloriosos.

Ao meu mestre, com carinho, Professor Orientador Dr. Luiz Carlos dos Santos, pela paciência, confiança e dedicação, como excelente profissional, que com suas aulas maravilhosas esclareceu muitas dúvidas, para que eu finalmente, concluísse mais essa tarefa.

À professora Edleusa Carvalho, que com seu apoio e atenção me auxiliou na correção desse trabalho.

E, finalmente, meus agradecimentos a meus irmãos, Jailton e Camila, ao meu pai Joselício e a todos os meus familiares que de alguma forma, torceram por mim.

Muito obrigado a todos!

*“A escrita é uma coisa, e o saber, outra.
A escrita é a fotografia do saber, mas não o saber em si.
O saber é uma luz que existe no homem”.*

Tierno Bokar

RESUMO

O presente Trabalho de Conclusão de Curso teve por objetivo evidenciar a relevância do backup em um escritório de contabilidade de pequeno porte. O desenvolvimento desta pesquisa se deu com um estudo de caso sobre o uso do *backup* como ferramenta de trabalho, buscando um maior detalhamento do assunto. Para alcançar o objetivo proposto, este estudo contemplou a seguinte trilha metodológica: método – indutivo; tipologia quanto aos objetivos – exploratória com contornos descritivos; natureza da abordagem – predominantemente qualitativa; tipo de exposição do objeto de pesquisa – teórico-empírico; fontes de pesquisa – bibliográfica, utilizando-se de livros, periódicos e artigos acadêmicos, eletrônicos – *sites* especializados, *e-books* e pesquisa de campo, com aplicação de um questionário. O universo compreendido pela pesquisa foi um escritório de contabilidade da cidade de Itaberaba. Os resultados alcançados apontam que o *backup* se apresenta como uma solução adequada para a guarda e segurança de dados, no entanto, necessita-se de um planejamento estratégico e um plano de contingência bem elaborado; mais de um meio para arquivamento, como o armazenamento em uma empresa especializada e o *backup* em nuvem; além de capacitação de todos os funcionários da empresa para o uso adequado da ferramenta. Concluiu-se, portanto, que o *backup* como cópia de segurança é um instrumento extremamente importante em qualquer ambiente, principalmente no corporativo, pois, a criação de uma política de *backups* é crucial para que a empresa possa ter uma infraestrutura mais confiável, capaz de responder de maneira eficaz e eficiente aos incidentes e desastres, evitando transtornos e trazendo mais segurança, possibilitando a continuidade de negócios da empresa.

Palavras-Chave: *backup*; segurança; planejamento estratégico; armazenamento de dados; ferramenta de informação.

ABSTRACT

The present undergraduate thesis aimed to highlight the relevance of backup in a small accounting office. The development of this research was made with a case study about the use of backup as a work tool, seeking a greater detailing of the subject. To reach the proposed objective, this study contemplated the following methodological path: method - inductive; typology as to the objectives - exploratory with descriptive contours; nature of the approach – predominantly qualitative; type of exposure of the research object – theoretical-empirical; research sources - bibliographic, using books, periodicals and academic articles, electronic - specialized sites, e-books, and field research, with the application of a questionnaire. The universe comprised by the research was an accounting office in the city of Itaberaba. The results achieved point out that the backup presents itself as an adequate solution for data storage and security, however, it requires a strategic planning and a well-designed contingency plan; more than one manner of archiving, such as storing in a specialized company and cloud backup, in addition to training all company employees to use the tool properly. It was concluded, therefore, that backup as a security copy is an extremely important tool in any environment, especially in the corporate one, because the creation of a backup policy is crucial for the company to have a more reliable infrastructure, capable of responding effectively and efficiently to incidents and disasters, avoiding inconvenience and bringing more security, enabling the company's business continuity.

Keywords: *backup; security; strategic planning; data storage; information tool.*

LISTA DE ILUSTRAÇÕES

Figura

Figura 1 – Esquema conceitual.....	16
------------------------------------	----

Gráfico

Gráfico 1 - Principais razões para um plano de <i>backup</i>	30
Gráfico 2 – Participantes do plano de <i>backup</i>	31
Gráfico 3 – Critérios para a escolha de mídias de <i>backup</i>	33
Gráfico 4 – Plano de contingência.....	34

Quadro

Quadro 1 - Relação entre contador e <i>backup</i>	35
---	----

LISTA DE ABREVIATURAS E SIGLAS

ABNT – Associação Brasileira de Normas Técnicas

CD – R – Compact Disc

CEPPEV – Centro de Pós-graduação e Pesquisa Visconde Cairu

CERT- Centro de Estudos para resposta e Tratamento de Incidentes em computadores

COVID-19 – Corona Virus Disease 2019

DVD – Digital Versatile Disc

DEDC – Departamento de Educação

FVC – Faculdade Visconde Cairu

HD – Hard Disk

IA- Inteligência Artificial

NBR – Normas Brasileiras

p. - página

PGDR = Programa de Pós-graduação em Gestão e Desenvolvimento Regional

RW - ReWritable

TCC – Trabalho de Conclusão de Curso

TI – Tecnologia da Informação

UMSA – *Universidad del Museo Social Argentino*

UNEB – Universidade do Estado da Bahia

UNIFACS – Universidade Salvador

SUMÁRIO

1	INTRODUÇÃO.....	13
2	REFERENCIAL TEÓRICO.....	16
2.1	Esquema conceitual.....	16
2.2	<i>Backup</i> : conceituação e objetivo.....	16
2.3	Tipos de Armazenamento de <i>Backup</i>	19
2.4	<i>Backup</i> e contabilidade: uma visão atual.....	20
2.5	<i>Backup</i> como ferramenta de trabalho.....	21
3	METODOLOGIA.....	24
3.1	Método.....	24
3.2	Tipologia quanto aos objetivos.....	24
3.3	Natureza da abordagem.....	25
3.4	Natureza da exposição do objeto.....	25
3.5	Fontes.....	25
3.5.1	Bibliográfica.....	25
3.5.2	Documental.....	26
3.5.3	Eletrônica.....	26
3.6	Universo.....	26
3.7	Amostra.....	26
3.8	Critério Amostral.....	26
3.9	Técnica de coleta de Dados.....	27
3.10	Tabulação e tratamento dos dados.....	27
4	APRESENTAÇÃO, ANÁLISE E INTERPRETAÇÃO DOS RESULTADOS.....	28
5	CONSIDERAÇÕES FINAIS.....	36
	REFERÊNCIAS.....	38
	BIBLIOGRAFIA CONSULTADA.....	40
	APÊNDICE A - Termo de Consentimento Livre Esclarecido.....	41
	APÊNDICE B - Termo de Consentimento – Individual.....	42
	APÊNDICE C - Questionário aplicado a profissionais de TI da AudiConti.....	43

1 INTRODUÇÃO

A segurança dentro de uma empresa sempre foi considerada um dos principais objetivos dos gestores, independentemente do seu tamanho ou da complexidade da sua política de dados, computadores e servidores sempre podem sofrer danos. Seja por meio oscilações e quedas de energia, ataques digitais ou falhas de funcionamento.

Uma empresa seja pequena, média ou grande, pode estar sujeita a perder parte dos seus dados após algum tipo de falha. Nesse cenário, o *backup* para empresas ganha importância pela sua capacidade de manter a integridade de bancos de dados, configurações e arquivos.

Assim, considerando a atual conjuntura e diante de um cenário de mudanças cada vez mais rápidas, consequentes avanços e expansões tecnológicos, existe uma quantidade cada vez maior de dados que precisam ser armazenados, devido a um maior aumento de informações e circulação de dados em diversas empresas. Nesse contexto, os escritórios de contabilidade, torna-se ambientes onde faz-se cada vez mais necessário a manutenção de um *backup* diário, com o objetivo de preservar a segurança dos dados dos clientes.

Em virtude de diversas falhas ou fugas de dados em *backup* por armazenamento em disco rígidos, ou em arquivos de malotes de papeis, tem se criado formas práticas, para possíveis *backups*, de forma mais segura. Diante disso, percebe-se que a segurança digital precisa era disseminada em todas as empresas, e o ato de fazer cópias de arquivos, bancos de dados e sistemas operacionais inteiros, tornou-se uma das principais rotinas.

Os *backups* permitem que gestores tenham a confiança de que, caso algum hardware falhe ou algum sistema fique corrompido, os seus registros e arquivos sejam recuperados facilmente. É uma ferramenta de extrema relevância em qualquer empresa e especificamente nos escritórios de contabilidade, onde é considerado um importante aliado na gestão da segurança. É por meio dele que se recuperam arquivos essenciais, permitindo que as empresas tenham uma infraestrutura confiável, capaz de suportar problemas e que permitam a recuperação de dados estratégicos a qualquer momento, evitando prejuízos.

O processo de armazenamento nos escritórios de contabilidade consiste em preservar informações e dados, mantendo-as seguras e acessíveis a qualquer momento, para isso, é de fundamental importância que sejam executadas ações de *backups* diários, evitando, com isso, risco de perda de qualquer informação obtida durante o dia, deixando em segurança as empresas contratadas. Dessa forma, caso ocorra algum problema, de forma ágil, a empresa poderá retomar as suas operações, evitando perda de produtividade ou de arquivos que possam comprometer as suas operações a médio e longo prazos.

As informações são cada vez mais importantes no dia a dia de todas as pessoas e empresas, e essas informações têm de estar à disposição das pessoas de forma segura e rápida, sem que esteja corrompida ou inutilizável, e para isso são utilizadas algumas ferramentas como o *backup*. Segundo Lento (2014), antecipar-se aos possíveis incidentes e desastres é um dos maiores diferenciais para o sucesso das organizações. A capacidade de se responder de maneira eficaz e eficiente aos incidentes e desastres é alcançada implementando-se ferramentas que possam trazer mais segurança e continuidade de negócios da empresa.

Diante da importância e da necessidade cada vez maior do uso da ferramenta chamada *backup* para a segurança nos escritórios de contabilidade, tendo em vista um *backup* mais seguro e prático para evitar fugas ou perdas de dados, tem-se como enunciado investigativo, o seguinte questionamento: **qual a relevância do *backup* em um escritório de pequeno porte em Itaberaba?**

Em decorrência de tal enunciado, levantou-se as seguintes norteadoras:

- Como surgiu o *backup*?
- Qual a relação do Contador com os *backups* dentro dos escritórios de contabilidade?
- Quais as principais formas de manter os *backups* mais seguros no escritório de contabilidade?

O presente artigo tem como objetivo geral evidenciar a relevância do *backup* nos registros contábeis em uma empresa de pequeno porte na cidade de Itaberaba. Para tanto realizou-se a mensuração do uso do *backup*, apontando as vantagens em fazer *backup* de arquivos mais importantes no dia a dia das empresas. E para que

esse objetivo seja alcançado necessário se faz estabelecer os objetivos específicos, adiante descritos:

- Identificar como eram armazenadas as informações em *backup* dos escritórios de contabilidade.
- Mostrar os avanços ocorridos nos *backups* com a chegada da era digital.
- Analisar as formas como o Contador mantém seus *backups* atualizados e seguros nos dias atuais.

A importância científica desse estudo, reside no fato de que poderá servir de fonte para futuras pesquisas em torno da temática referente a *backups* como uma forma de segurança digital, além de contribuir de forma significativa para que leitores e pesquisadores tenham uma maior consciência da importância do *backup* enquanto ferramenta do trabalho diário, evitando prejuízos futuros.

Para este pesquisador a motivação do estudo decorreu do fato de o mesmo estar inserido na área de Tecnologia da Informação (TI), fazendo parte o *backup* de sua rotina diária de trabalho, sem deixar de considerar também que o setor de contabilidade de qualquer empresa depende de sistemas, sejam de segurança ou não. Além disso, o conhecimento adquirido durante a pesquisa poderá subsidiar uma mudança na carreira profissional.

A presente pesquisa possui natureza teórico-empírica, ou seja, além de expor uma discussão em âmbito teórico acerca da temática abordada, incluiu, também, uma pesquisa de campo. A metodologia utilizada para a realização do trabalho encontra-se detalhada no terceiro capítulo.

Este artigo é composto por cinco capítulos: o primeiro, refere-se a esta introdução; o segundo, aborda-se o referencial teórico acerca do tema em foco; o terceiro, enquadra-se a metodologia utilizada no estudo; o quarto, exibe-se, a apresentação, análise e interpretação dos resultados da pesquisa de campo; finalmente, o quinto capítulo, expõe-se as considerações finais na perspectiva do alcance dos propósitos desta inicial.

Espera-se que esse estudo possa trazer novas contribuições para futuros pesquisadores e sirva de subsídio para outras pesquisas sobre o tema.

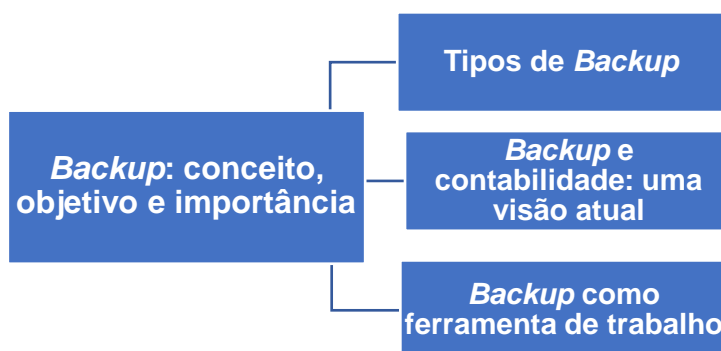
2 REFERENCIAL TEÓRICO

As seções deste capítulo, a partir do esquema conceitual, visam trazer à tona as bases teórico-epistemológicas capazes de elucidar a problemática da pesquisa, responder as questões norteadoras do objeto investigativo e alcançar os objetivos fixados na introdução.

2.1 Esquema conceitual

A figura 1, a seguir, ilustra o esquema conceitual do objeto de estudo:

Figura 1 – Esquema conceitual



Fonte: Elaborado pelo autor

2.2 Backup: conceito, objetivo e importância

O termo americano *backup* significa “cópia de segurança”, e corresponde a criação e armazenamento de cópias de arquivos digitais importantes, de modo que seja possível realizar sua restauração em caso de perda dos arquivos originais.

De acordo com Mulato Neto *et al* (2012, p. 2) o *backup* pode ser definido como “cópia de segurança dos dados de determinado dispositivo de armazenamento que pode ser espelhado em outro dispositivo de forma a garantir a estabilidade dos arquivos e afastar a possibilidade de surpresas como a perda desses dados”. Conforme Reis (2005), *backup* é uma cópia exata de um programa e/ou arquivo para salvaguardar as informações.

Portanto, o conceito de *backup* refere-se basicamente a soluções que têm como propósito produzir cópias das informações mais relevantes da empresa. Tem

papel fundamental para garantir restauração dos dados perdidos após simples alterações mal feitas ou apagamentos acidentais até desastres com perda de 100% do conteúdo original armazenado.

De acordo com a NetApp (2019) empresa americana que cria produtos inovadores de software, sistemas de storage para ajudar clientes do mundo inteiro, o objetivo do *backup* é criar uma cópia dos dados que podem ser recuperados no caso de uma falha nos dados primários. As falhas primárias de dados podem ser o resultado de falha de *hardware* ou *software*, corrupção de dados ou um evento causado por humanos, como um ataque malicioso (*vírus* ou *malware*) ou exclusão acidental de dados. As cópias de *backup* permitem que os dados sejam restaurados a partir de um momento anterior para ajudar a empresa a se recuperar de um evento não planejado.

Backups podem ser utilizados não só para a restauração de dados ou sistemas na ocorrência de desastres ou outros incidentes de segurança, mas também, para a recuperação de versões anteriores de dados, ou ainda para o arquivamento de dados ainda necessários, mas raramente acessados (CERT.br, 2012).

Sendo assim, o objetivo de um *backup* é permitir que dados possam ser acessados mesmo que os locais em que foram armazenados estejam inacessíveis. E as razões para que isso ocorra podem ser muitas: desastres naturais, como vendavais e alagamentos; incêndio ou dano elétrico no *data center*; invasão cibernética ou problema técnico no *hardware* em que os dados estão salvos.

Uma vez entendida a necessidade do *backup* e a importância dos dados para sobrevivência do sistema, a empresa deve ter a capacidade de decidir e fazer a gestão das cópias de segurança de seu ambiente. Diante deste cenário de crescimento de informações digitais, cada vez mais a segurança destes dados se torna alvo de atenção e o *backup* se torna imprescindível.

Ainda segundo a NetApp (2019) para obter melhores resultados, as cópias de *backup* devem ser feitas de maneira consistente e regular para minimizar a quantidade de dados perdidos entre os *backups*. Quanto mais tempo passa entre as cópias de *backup*, maior o potencial de perda de dados ao se recuperar de um

backup. A retenção de várias cópias de dados fornece o seguro e a flexibilidade para restaurar em um ponto no tempo não afetado por corrupção de dados ou ataques maliciosos.

De acordo com Penso Tecnologia (2019) um escritório de contabilidade deve atender a uma série de normas para operar em conformidade com a legislação brasileira, e a maneira como a contabilidade trata, armazena e a assegura as informações dos clientes requer uma atenção especial.

Segundo Almeida (2007), na definição das estratégias de *backup* deve-se levar em conta os seguintes fatores:

- Capacidade de recuperação em caso de *crash* total do sistema;
- Verificação dos *backups* periodicamente;
- O meio de armazenamento pode não ser totalmente confiável. Um conjunto de fitas muito grande é totalmente inútil se os dados neles contidos não puderem ser restaurados;
- Elaborar uma política de retenção de fitas;
- Determinar um ciclo para reutilização de fitas. Não se deve, entretanto, reutilizar todas as suas fitas. Às vezes transcorre meses antes que algum usuário sinta a necessidade de restaurar algum arquivo importante que tenha sido apagado por engano. Devido a isto *backups* antigos, dentro de certos limites, devem ser mantidos;
- Um *backup* efetuado a partir de um sistema de arquivos corrompido pode ser inútil. Antes de efetuar *backups* é aconselhável verificar a integridade dos sistemas de arquivos;
- Fazer *backups* em horários em que o sistema se encontre em estado de mínima (ou nenhuma) atividade;
- Fazer preferencialmente mais de um, *backup* antes de efetuar alterações substanciais no sistema. É sempre aconselhável fazer um *backup* antes de efetuar mudanças de porte no sistema operacional, instalação de correções, mudanças significativas em programas aplicativos, enfim, tudo o que possa representar uma ameaça ao funcionamento normal do sistema.

O processo de recuperar dados do *backup* realizado é conhecido como

restauração e, mais importante que manter as cópias de segurança atualizadas, conseguir restaurá-las em caso de desastre é imprescindível. Sendo assim, a política de *backup* tem a função de garantir que a equipe de Tecnologia da Informação da empresa esteja preparada para reagir caso as informações da empresa sejam afetadas por qualquer tipo de imprevisto. Nesse processo, são definidos métodos, responsabilidades e as ferramentas necessárias para garantir a segurança dos dados da empresa, porque o objetivo maior é reduzir os riscos e aumentar a segurança dos dados, evitando prejuízos.

2.3 Tipos Armazenamento de *Backups*

Os primeiros vestígios de *backup* foram na era dos cartões perfurando, que, com o decorrer do tempo tem evoluído com outros diversos meios de *backups*, como:

- Fitas magnéticas: um rolo de fita magnética, conseguia armazenar dados tanto quanto 10000 cartões perfurados;
- Disco rígido;
- Disquetes;
- CD-R / RW E DVD;
- *Pen drive* e HD externo;
- *Backup* na nuvem.

Segundo Andriotti (2016) as primeiras tradições e estratégias de *backup* começaram a surgir no início de 1960. Os *backups* de fitas foram os mais difundidos, devido à confiabilidade, escalabilidade e baixo custo da unidade de fita.

Há alguns anos segundo Penso Tecnologia (2019) os escritórios armazenavam a papelada em arquivos de metal fechados com chave, dentro de salas igualmente fechadas à chave. Como obrigatoriedade, muitos documentos ficam armazenados por anos, até décadas, e isso fazia com que os escritórios tivessem custos cada vez maiores com estrutura física para armazenar tudo. A segurança era bem baixa e os arquivos estavam vulneráveis à um incêndio, enchente ou assalto.

As primeiras formas de armazenamento em cópias digitais foram os discos rígidos, CDs, DVDs, depois vieram os *pens drives* e mais recente os HDs externos. Mas todas essas opções são físicas, ou seja, embora seja uma forma de garantia ter

duas ou mais cópias dos arquivos, como são físicas, podem ser perdidas ou danificadas também.

Com a evolução dos meios de armazenamento, as empresas foram se adequando e modernizando seus meios de *backup* de acordo a uma análise compensatória onde visa avaliar, custos, flexibilidade de armazenamento, tamanho da memória, segurança e praticidade ao executá-lo.

As vulnerabilidades a que estão sujeitas as empresas como erros humanos ou de *software*, corrupção de dados, falha de *hardware*, invasões virtuais, furtos e eventos como enchentes ou incêndios precisam ser mensuradas antes de definir qual será o melhor plano de *backup* para cada situação.

A maioria dos *softwares* hoje, possuem recursos para diminuir o tempo com essa operação, seja copiando dados de uma agenda de um celular ou um banco de dados corporativos. Apesar de grande parte dos usuários acharem que todos os dados são copiados a cada operação de backup realizada, isso quase nunca acontece. A maioria dos *softwares* de *backup* monitoram as atualizações das informações e copiam somente os dados alterados. Isso significa menor tempo de cópia, consumo de energia e espaço utilizado, reduzindo assim diversos custos.

2.4 Backup e contabilidade: uma visão atual

Atualmente muito se discute a questão da segurança da informação, pois, com o processo de globalização, as informações chegam em tempo real, há um imenso aumento do fluxo dessas informações dentro das empresas contábeis, e, conseqüentemente, aumentam também as ameaças e incidência de erros, que podem levar à perda de dados.

Os prejuízos com a perda de dados e informações das empresas de contabilidade são muito grandes e colocam em risco a saúde dessas empresas, que podem perder clientes e a credibilidade. Portanto, a segurança dos dados é de extrema relevância nesse ambiente, justificando a implantação de medidas de segurança que possa garantir a guarda de dados dessas empresas sob seus cuidados.

Com o avanço da tecnologia, as informações/dados guardadas em inúmeros armários catalogados foi gradativamente ficando no passado. Os arquivos contábeis que precisam ser mantidos por muitos anos devido a questões legais, só aumentam a necessidade de espaço e os gastos com estrutura física. Portanto, a questão de armazenamento de documentos é crucial numa empresa, pois existe uma necessidade real de arquivamento.

A contabilidade, assim como qualquer outra área, está sendo remodelada rapidamente pela digitalização. Poucos negócios lidam com tantos documentos e demandam tanta organização quanto os escritórios de contabilidade. Dentre as ações sob responsabilidade dos escritórios contábeis, temos as que visam catalogar, armazenar e manter as informações em segurança, o que é mais do que fundamental.

Sendo assim, as inovações tecnológicas como o *backup* fornecem subsídios para soluções mais ágeis, mesmo para problemas complexos, facilitando os processos dentro dos escritórios contábeis, mantendo as informações em segurança, como modo de prevenir situações catastróficas ou perdas de dados, e como economia de espaço físico. Segundo Coelho (2005, p. 1):

O empresário e a sociedade empresária devem ter mecanismos que permitam ao contabilista adotar sistemas de *backup*, visando garantir a segurança quanto à disponibilidade da escrituração contábil digital em casos de extravio e desastre computacional.

Portanto, o *backup* é a primeira providência que deve ser feita para evitar que haja o comprometimento de dados e a descontinuidade da produção. O desenvolvimento da rotina de *backup* começa com uma análise profunda das necessidades de cada empresa, considerando a dimensão do fluxo de dados. O planejamento do processo é fundamental para implantação da rotina e frequência, conforme necessidade da empresa. É necessário também a criação de um protocolo de segurança ou a criação de políticas internas sobre a responsabilidade das rotinas, para que todos os funcionários reconheçam a necessidade de *backup* e cumpram com estas determinações.

2.5 Backup como ferramenta de trabalho

Há muito tempo a informação, os dados, se tornou um dos patrimônios mais importantes para as empresas, e como tudo que apresente valor, ela precisa ser protegida. Antigamente, com o grande uso de mídias impressas, a segurança estava na parte física, voltada para quem teria acesso ao local que contém a informação. Todavia, com a evolução das tecnologias, cada vez mais temos as informações salvas de forma digital.

A tecnologia tem se tornado cada vez mais valiosa para os contadores. Isso porque a utilização das ferramentas tecnológicas pode fazer um grande diferencial na produtividade e nos resultados de um escritório ou setor contábil. As rotinas contábeis estão se modernizando, assim como as atribuições dos contadores, que deverão ser cada vez mais estratégicas. Essas tecnologias não tornam redundante o fator e a criatividade humana, ou seja, apenas fornecem melhores subsídios para seu trabalho.

Segundo Moreira (2008) para uma eficaz segurança da informação dentro de uma organização é necessário ficar atentos para algumas questões como uma boa análise de riscos, a definição da Política de Segurança e por fim um plano de contingência. Segundo Médice (2013), o *primeiro passo a ser observado é que não existe risco zero*. Sendo assim, os dados veiculados pela internet, estão acessíveis a todo mundo e quando não ocorre o devido tratamento da segurança dessas informações, podem ocorrer fraudes, causando prejuízos.

Para melhor compreendermos o que devemos buscar em uma solução, deve-se entender que não existe uma única ferramenta. Existem diversos recursos que podem ser utilizados. Assim, tecnologias como computação em nuvem, inteligência artificial (IA) e *blockchain* têm capacitado cada vez mais o trabalho dos contadores. Se por um lado a tecnologia reduz as tarefas de entrada de dados manuais, por outro lado, ela melhora a velocidade, precisão e qualidade dos dados.

Segundo Pulia (2016), *backup* é uma apólice de seguro contra a perda de dados. Devido ao grande número de fatores que podem, de algum modo corromper a informações, seja através de vírus, falhas humanas como alteração indevida do arquivo ou exclusão acidental, queda de energia ao salvar o arquivo. Uma empresa depende das informações para sobreviver com seus negócios.

Portanto, o propósito do *backup* é criar uma cópia do dado em uma mídia secundária. Esta cópia será armazenada e guardada para uso futuro caso o dado original tenha sido perdido, destruído, corrompido, atacado por vírus ou até mesmo sequestrado. A perda dessa informação pode levar a multas, perda de clientes e até ao fechamento do negócio, dependendo de sua relevância.

Algumas empresas de pequeno e médio porte, apresentam preconceito e indisposição, contra medidas de *backup*, devido a sua natureza de ser criada, com a intenção de nunca usar. Criando um gasto não compreendido em um orçamento pequeno.

Ainda de acordo com Mulato Neto *et al* (2012) a prática rotineira de *backup* é vista como algo chato para muitos. Por isso, muitos gestores de sistemas estão trabalhando na tarefa de simplificar e automatizar a tarefa de realização do *backup*, para minimizar o tempo gasto. Com o *backup* em caso de acidentes, é possível continuar com as atividades da empresa seja qual for o seu tamanho ou segmento, quase que instantaneamente, dependendo dos recursos disponíveis.

3 METODOLOGIA

O presente trabalho foi elaborado baseado em uma pesquisa teórica com o uso de bibliografia relevante, consubstanciada por uma pesquisa de campo com o intuito de identificar a relevância da utilização do *backup* em empresas de contabilidade como ferramenta de segurança da informação. Para tanto se elaborou um questionário composto de 14 questões, sendo 4 fechadas e 10 abertas. Após a análise da resposta do questionário é possível conhecer os resultados. É necessário esclarecer que a escolha da empresa se deu pelo critério de acessibilidade.

Para Fonseca (2002), metodologia é o estudo da organização, dos caminhos a serem percorridos, para se realizar uma pesquisa, estudo, ou para fazer ciência. A pesquisa, como relata Gil (2007), desenvolve-se por um processo constituído de várias fases, desde a formulação do problema até a apresentação e discussão dos resultados.

Portanto, este capítulo tem como finalidade apresentar os métodos e técnicas empregados para a realização da pesquisa, sendo dividida em método e tipo de pesquisa, tipologia quanto aos objetivos, natureza da abordagem, natureza da exposição do objeto, fontes bibliográficas, documentais, eletrônicas, universo da pesquisa, amostra, critério amostral, técnica de coleta de dados, tabulação e análise de dados.

3.1 Método

Adotou-se o método indutivo que, segundo Descartes *apud* Ferreira (1998), parte de premissa maior, a generalidade para se chegar à especificação. No caso em foco, dos princípios que norteiam a utilização de *backup* para aplicabilidade em escritório de contabilidade, visando à segurança e guarda de dados das empresas sob sua responsabilidade.

3.2 Tipologia quanto aos objetivos do estudo

Utilizou-se a tipologia exploratória, que de acordo com Gil (2011), além de ampliar a literatura na área do objeto de estudo, pode servir como fonte para futuras pesquisas em torno da temática. No campo contábil, o uso da ferramenta *backup* é indiscutível, todavia, observa-se escassez de obras versando sobre o assunto.

3.3 Natureza de abordagem

Baseou-se na abordagem qualitativa, na medida em que foram levantadas percepções do público-alvo da pesquisa acerca da realidade quanto à utilização de *backup* em escritório contábil, ou seja, na área de Tecnologia da Informação (TI) da empresa de contabilidade AudiConti. Goldenberg (2007), diz que a pesquisa qualitativa não se preocupa com representatividade numérica, mas, sim, com o aprofundamento da compreensão de um grupo social ou de uma organização.

A pesquisa qualitativa preocupa-se, portanto, com aspectos da realidade que não podem ser quantificados, centrando-se na compreensão e na explicação da dinâmica das relações sociais. (MINAYO, 2007).

3.4 Natureza da exposição do objeto investigativo

Quanto aos procedimentos foi feito um estudo de caso sobre o uso do *backup* como ferramenta de trabalho, buscando um maior detalhamento do assunto. Esse tipo de pesquisa é amplamente usado nas ciências biomédicas e sociais, visto que tem o foco em conhecer com profundidade o como e o porquê de uma determinada situação que se supõe ser única em muitos aspectos. Para a autora Alves-Mazzotti (2006, p.640):

Os exemplos mais comuns para esse tipo de estudo são os que focalizam apenas uma unidade: um indivíduo (como os casos clínicos descritos por Freud), um pequeno grupo (como o estudo de Paul Willis sobre um grupo de rapazes da classe trabalhadora inglesa), uma instituição (como uma escola, um hospital), um programa (como o Bolsa Família) ou um evento (a eleição do diretor de uma escola).

Assim, a presente investigação científica enquadra-se na tipologia teórico-empírica, porque utiliza a literatura na área e complementa a pesquisa de campo (SANTOS, 2020).

3.5 Fontes

Para a consecução dos objetivos e resultados da pesquisa, fez-se uso concomitante de diversas fontes de pesquisa tais como: bibliográficas, documentais e eletrônicas.

3.5.1 Bibliográficas

É bibliográfica porque como citam Marconi e Lakatos (1999, p. 57), “[...] a pesquisa bibliográfica, ou de fontes secundárias, abrange toda a bibliografia já tornada pública em relação ao tema de estudo [...]”, assim, foram consultados os temas voltados para o uso do *backup* como ferramenta de segurança e guarda de dados de informação, como artigos, trabalhos de conclusão de curso, dissertações, periódicos etc. em formato impresso.

3.5.2 Documentais

A pesquisa documental tem objetivos específicos e pode ser um complemento à pesquisa bibliográfica e permite fazer análises qualitativas sobre determinado fenômeno. A pesquisa documental como expõe Kahlmeyer-Mertens, *et al.* (2007), é feita quando se faz necessária a análise de documentos existentes que possam contribuir para a realização da pesquisa. Com isso, foi realizada a leitura e análise dos principais temas consultados e selecionados os de maior relevância para o presente trabalho, levando em consideração os objetivos propostos a esta pesquisa.

3.5.3 Eletrônicas

Para ao aprofundamento do conteúdo estudado foi utilizado materiais encontrados de forma *online* ou eletrônica, como livros, revistas especializadas ou artigos publicados em formato digital, incluindo a temática sobre tecnologia da informação. Esta classificação levou em conta os ensinamentos de Boaventura (2017).

3.6 Universo

O universo da pesquisa delimitou-se a empresa de contabilidade AudiConti, empresa de pequeno porte, situada na cidade de Itaberaba.

3.7 Amostra

A amostra desta pesquisa de campo confunde-se com o universo ou população. Escolheu-se a empresa AudiConti. Desta entidade colheu-se a percepção dos profissionais, responsáveis pela realização de *backups* como ferramenta de segurança e de guarda de dados.

3.8 Critério Amostral

O critério amostral escolhido foi o não probabilístico, levando-se em consideração: disponibilidade de acesso à informação; circunstância da pandemia da COVID-19; prazo estabelecido para a entrega do TCC, entre outros.

3.9 Técnica de coleta de Dados

A coleta de dados é um processo que visa reunir os dados para uso secundário por meio de técnicas específicas de pesquisa. Neste caso específico, a coleta dos dados foi feita por meio da ferramenta questionário, o qual é definido Segundo Marconi e Lakatos (1999, p.100), como: “Um instrumento desenvolvido cientificamente, composto de um conjunto de perguntas ordenadas de acordo com um critério predeterminado, respondido sem a presença do entrevistador”. O questionário é composto de 14 perguntas semiestruturadas, de respostas curtas e objetivas, (Apêndice C) estabelecendo um contato mais direto, recolhendo as percepções acerca do tema objeto desse estudo.

3.10 Tabulação e tratamento dos dados

As respostas oriundas das questões fechadas, constantes do questionário aplicado aos profissionais do setor de TI do escritório contábil em foco, tiveram tratamento estatístico, apropriado – números absolutos e relativos -, os quais encontram-se dispostos no capítulo seguinte, por meio de gráficos e tabelas. No que concerne às questões abertas do mencionado instrumento de coleta de dados, aplicou-se a lógica interpretativa no trato das respostas, organizadas em quadro único, contendo três colunas: a primeira, refere-se à pergunta do instrumento; a segunda, codifica-se os pesquisados que responderam de igual teor; e, a terceira, translada-se a súmula de cada resposta por grupo de informante.

4 APRESENTAÇÃO, ANÁLISE E INTERPRETAÇÃO DOS RESULTADOS

A empresa de contabilidade AudiConti é especializada na execução e elaboração de serviços contábeis para pessoas físicas ou jurídicas de pequeno, médio e grande porte, optantes do simples, lucro real, lucro presumido e entidades sem fins lucrativos da cidade de Itaberaba e região.

Atua no ramo contábil há mais de 20 anos, possui oito funcionários e desde o começo utiliza a contabilidade tradicional como principal forma de atender seus clientes.

Na contabilidade tradicional todo trabalho é realizado dentro do escritório, também se faz o uso da tecnologia, mas apenas por profissionais específicos de cada departamento e não pelo empreendedor do negócio. Aqui se faz uso de vários meios para atender seu cliente, inclusive o presencial. (PIGATTI, 2018, p. 1)

O avanço das novas tecnologias fez com que os escritórios contábeis tivessem a oportunidade de adotar o modelo digital de contabilidade, para que as empresas pudessem inovar e se reinventar no mercado, buscando sempre melhores resultados, pois, a tecnologia tem um papel extremamente importante no processo de implantação da contabilidade digital. Mas, junto com as novas tecnologias, surgem novos problemas que devem ter soluções, e, a segurança dos dados é uma preocupação constante na era digital em que vivemos.

Sendo assim, pensando na integração e segurança dos dados dos clientes, a empresa AudiConti decidiu buscar no mercado uma ferramenta capaz de auxiliar na guarda dos dados e movimentações de seus clientes. O programa escolhido foi o *Netspeed*, para fornecer essa ferramenta de segurança, além desse programa, o *backup* diário na nuvem também é utilizado.

Com a tecnologia e a inclusão do computador, o contador está mais para um analista de contabilidade. Isso porque os softwares fazem de tudo dentro do departamento de contabilidade, dentro de uma empresa ou em um escritório de contabilidade. Assim o profissional dedica mais tempo à análise da área contábil e consegue efetuar mais precisamente e com mais segurança o seu trabalho em pouco tempo (SIMAS; ALVES; CABRAL, 2011 *apud* OLIVEIRA; MALINOWSKI, 2017, p. 9).

Portanto, com a contabilidade digital, os escritórios passaram a ter um aumento na produtividade de seus colaboradores e ter uma melhoria nos serviços, estimulando os profissionais a estarem sempre inovando para que não fiquem para trás.

O principal objetivo do *backup* é prover a recuperação segura e rápida dos dados quando necessário, pois a segurança da informação é algo a ser tratado com muito cuidado para que não existam falhas que comprometam um todo, principalmente quando se trata de banco de dados, onde estão armazenadas todas as informações da empresa e dos clientes, assim o uso de uma ferramenta adequada é essencial.

O resultado principal obtido ao longo da presente pesquisa foi estruturado em etapas seguidas conforme o projeto de pesquisa. O estudo foi baseado em normas, padrões e recomendações da literatura e profissionais da área de contabilidade, com um questionário aplicado a cinco profissionais da empresa AudiConti que trabalham diretamente com a guarda de dados.

A maioria dos respondentes disse que o questionário estava bem completo, não tendo muito a acrescentar. Também consideraram que a sequência das perguntas permitiu um bom entendimento dos objetivos da pesquisa.

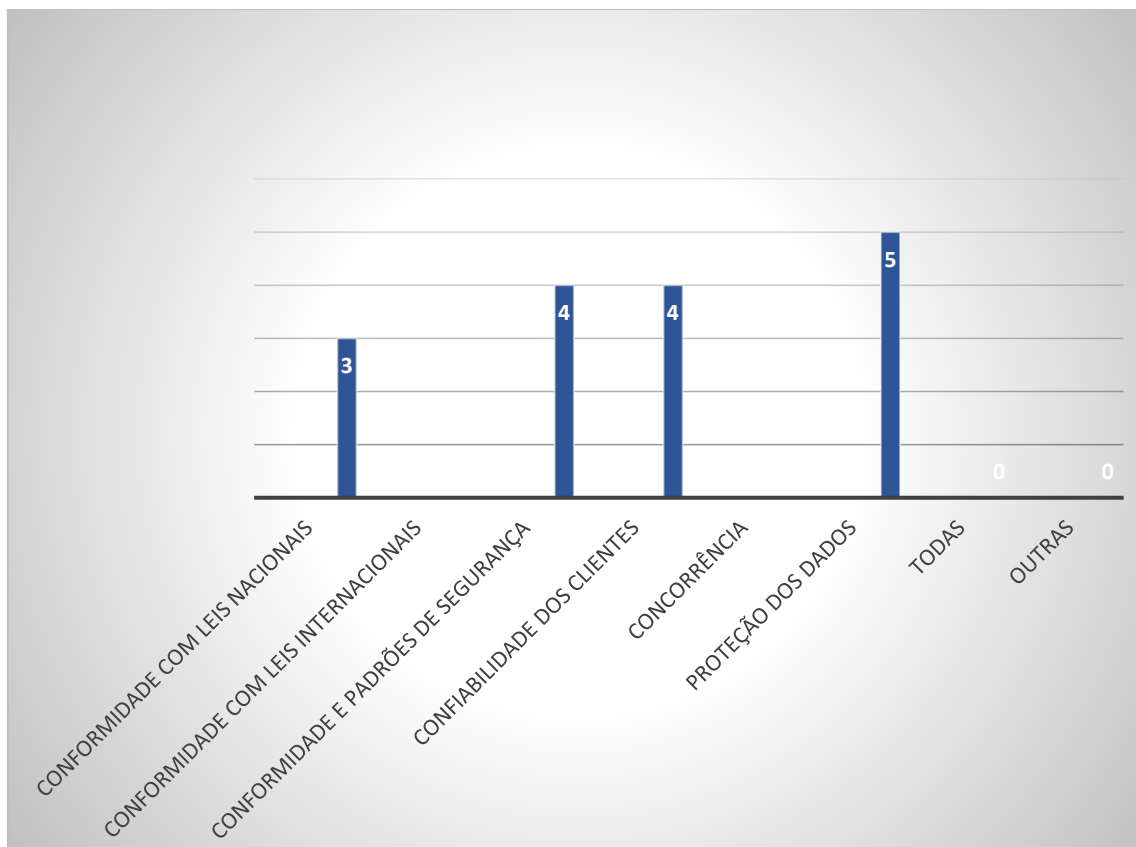
Para chegar ao resultado principal da forma como apresentado, teoricamente coerente com a literatura revista e estudada, foi feita a consolidação das respostas, destacando e discutindo os pontos mais importantes do questionário, explanados a seguir:

A primeira pergunta teve o propósito de saber há quanto tempo a empresa faz *backup* de dados e os entrevistados responderam que a cerca de quatro anos fazem *backup* diário.

A segunda pergunta do questionário objetivava saber se a empresa possui dados considerados críticos e que precisam ser mantidos em arquivo por dois anos ou mais, já que as empresas de contabilidade de modo geral, precisam ter esses dados guardados para uma eventual fiscalização e prestação de contas ao fisco e todos os respondentes disseram que sim, que possuem dados críticos que precisam ser guardados por tempo determinado, para eventuais consultas.

Em relação à questão número três sobre quais razões podemos considerar para se ter um plano de *backup* de dados, produziu-se o seguinte gráfico:

Gráfico 1 - Principais razões para um plano de *backup*



Fonte: Elaborado pelo autor, 2021.

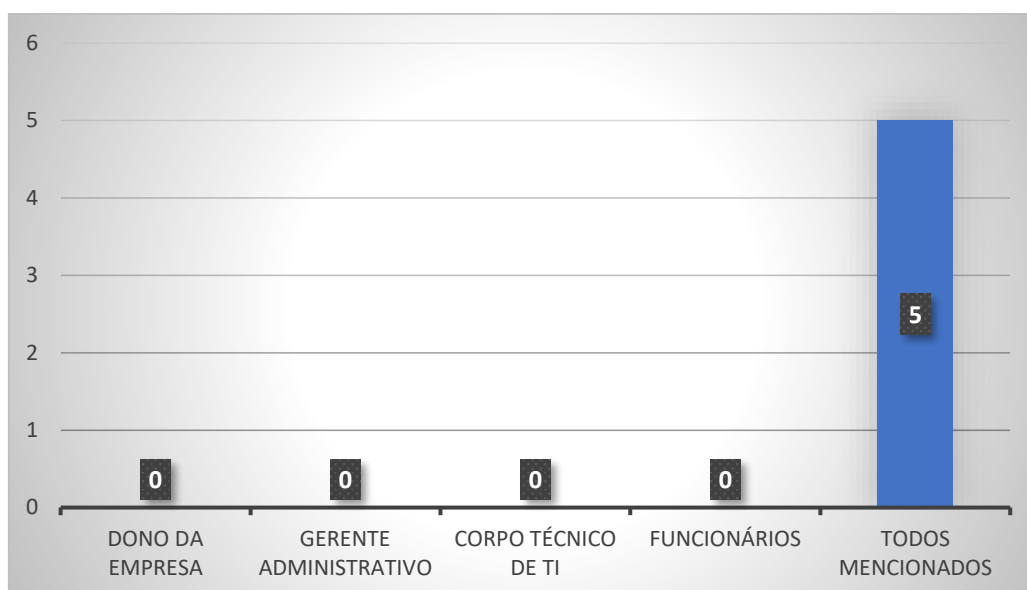
Portanto, baseado no gráfico 1 acima pode-se observar que as principais razões para que a empresa tenha um plano de *backup* é em primeiro lugar pela segurança e proteção dos dados, em seguida está pela confiança e credibilidade em relação ao cliente, seguido de padrões de conformidade exigidos pelos órgãos fiscalizadores nacionais.

Na questão quatro e cinco perguntou-se qual o tipo de *backup* é realizado pela empresa e qual a periodicidade desse *backup*, e todos os entrevistados disseram que a empresa realiza diariamente o *backup* em nuvem, visto que é uma segurança a mais para a guarda de dados. O *backup* em nuvem é muito utilizado, é uma tendência o seu uso, pela sua praticidade e segurança.

Segundo os entrevistados o *backup* diário é uma necessidade, pois os dados mudam constantemente o dia todo e necessitam de uma periodicidade diária, a fim de minimizar possíveis problemas relacionados à segurança da informação.

A questão número seis foi perguntado quem os entrevistados achavam que deveria participar do desenvolvimento do Plano de *Backup* de Dados, de acordo com o que foi respondido produziu-se o seguinte gráfico (2):

Gráfico 2 – Participantes do Plano de *Backup*



Fonte: Elaborado pelo autor, 2021.

Pelo que se pode observar no gráfico 2, todos os entrevistados acham que todos que trabalham na empresa, sem exceção, devem participar da elaboração do plano de *backup*, pois, todos tem algo a contribuir.

Em relação a questão número sete que busca saber se a equipe de trabalho já participou de algum treinamento direcionado a correta utilização do *backup* e sua importância, todos os respondentes disseram que nunca participaram de treinamento algum, isso evidencia que apesar de reconhecerem a importância da guarda adequada de dados da empresa, os gestores não vêem necessidade de capacitar seus funcionários para a tal.

Perguntados se existe um profissional específico para tratar os dados que serão objeto de *backup*, todo responderam que não, que todos os dados são tratados

de forma automática pelo sistema. Outra importância do *backup* em nuvem em empresas é que ele pode acabar evitando custos adicionais com funcionários ou dispositivos extras. Consequentemente faz com que a produtividade aumente, já que se houverem erros, não precisará ser perdido tempo refazendo todo o trabalho novamente.

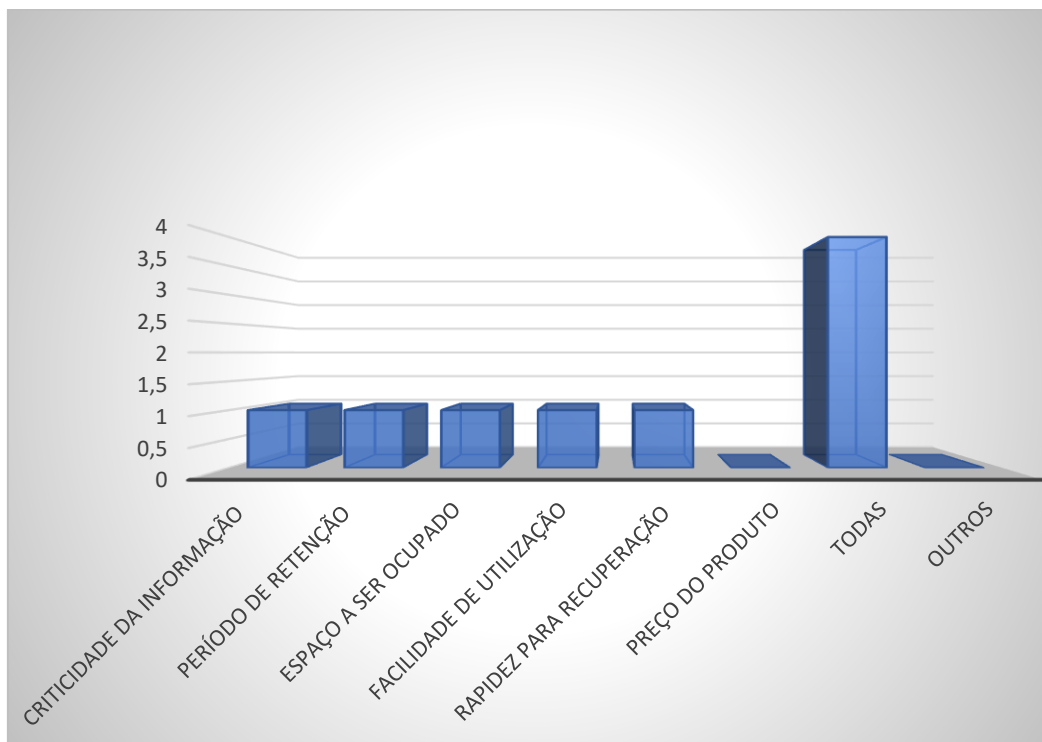
Questionados então sobre se a empresa dispõe de um contrato com *backup* remoto, além do *backup* na nuvem, responderam que sim, que possuem um contrato com uma empresa que disponibiliza um *backup* diário, que após sofrerem um ataque virtual, e tendo seus dados todos perdidos o escritório adquiriu uma forma de *backup* mais seguro onde teria mais segurança e com o backup remoto facilitaria o acesso, caso fosse necessário fazer a recuperação de dados.

O programa contratado pela empresa chamado *Netspeed*, se responsabiliza pela guarda dos dados produzidos pela empresa, como uma segunda opção em caso de problemas com o *backup* na nuvem.

Muitas empresas utilizam o *backup* em nuvem, tendo em mente a praticidade e segurança gerada por esse meio, mas ainda assim, são necessários outros meios, ou outros programas para o caso da nuvem apresentar alguma falha.

Na questão número onze do questionário em anexo, perguntou-se o que deve-se considerar necessário para a escolha de mídias de *backup*, as respostas estão descritas no gráfico (3) a seguir:

Gráfico 3 – Critérios para a escolha de mídias de *backup*



Fonte: Elaborado pelo autor, 2021.

Como pode-se observar no gráfico 3, os entrevistados em sua grande maioria acreditam que todos os fatores elencados são de grande importância na escolha de mídias de segurança, sendo que o preço é o fator considerado por todos menos relevante, pois, a confiabilidade e segurança está acima de qualquer outra coisa. Não adianta ter um produto acessível em relação ao preço se não facilita o trabalho e não traz segurança ao usuário.

O método de *backup* em nuvem tem um dos melhores custo-benefício do mercado, além de ser muito prático e consideravelmente rápido. Ele funciona de forma parecida com o método de *backup* em servidor interno, onde os arquivos ficam armazenados em um servidor que se situa em uma sala separada de todo o resto, mantendo a segurança física do mesmo.

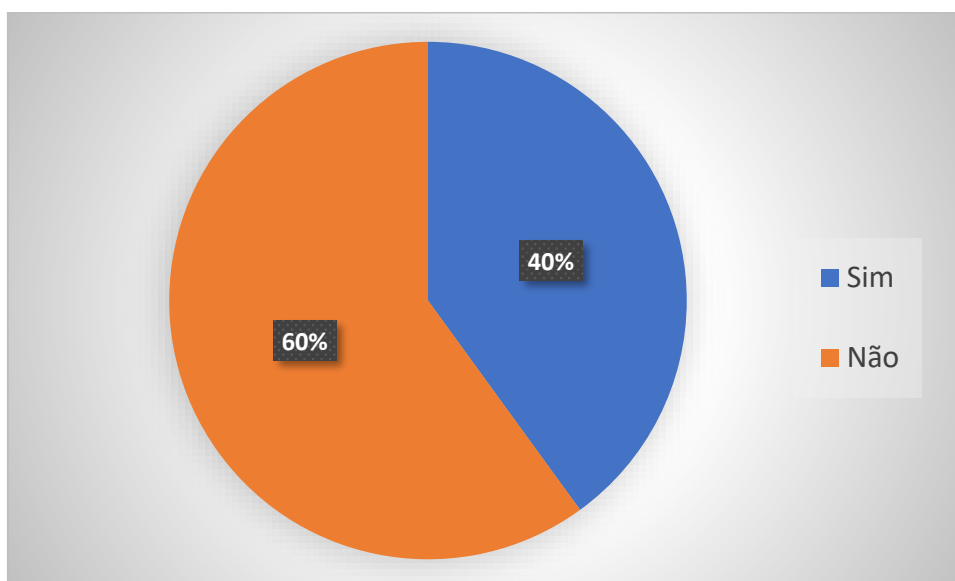
A principal diferença entre o *backup* em nuvem e o de fita magnética é que no *backup* em nuvem, um servidor de alguma empresa especializada é alugado para os arquivos serem armazenados de forma mais segura.

Algumas empresas utilizam de *backup* em fitas magnéticas, com um sistema automatizado para troca e organização das fitas. Esse método também tem um dos

melhores custo-benefício do mercado, mas também oferece grandes riscos quando organizado por humanos e não é automatizado.

Em relação à questão doze do questionário de pesquisa, perguntado aos entrevistados se a empresa possui um plano de contingência para o caso de perda de dados, obteve-se de acordo com o gráfico (4) abaixo, as seguintes respostas:

Gráfico 4 – Plano de contingência



Fonte: Elaborado pelo autor, 2021.

Pelo que pode-se deduzir no gráfico 4, cerca de 40% dos funcionários responderam afirmativamente e 60% dos funcionários responderam que não, esses dados refletem a questão da participação dos funcionários na elaboração do plano de contingência e no processo todo de segurança de dados, visto que o esperado era que todos respondessem sim ou não, as respostas obtidas nos deixa claro a falta de informação entre os funcionários da empresa, que não possuem o conhecimento esperado nessa área, reflexo de ausência de cursos de capacitação.

A pergunta da questão treze indagou aos entrevistados se já ocorreu a perda de dados de algum cliente importante da empresa, e qual providência foi tomada em relação ao ocorrido. Todos os entrevistados foram unânimes em dizer que sim, já aconteceu de perder dados de cliente e a providência tomada foi acionar o suporte do sistema de Tecnologia da Informação (TI) para tentar corrigir o problema e recuperar

os dados perdidos o mais rapidamente possível. Tudo isso, traz um grande transtorno para a empresa e seus usuários, que necessitam dos dados arquivados todos os dias, com segurança e rapidez.

E, finalizando, o questionário foi indagado aos entrevistados qual a sua percepção acerca da relação do contador com o *backup*, os dados coletados estão expressos no quadro abaixo:

Quadro 1 – Relação entre contador e *backup*

Entrevistado 1	O contador trabalha com documentos e arquivos contábeis que precisam estar armazenados e de fácil acesso.
Entrevistado 2	Existe sim uma relação muito importante entre o contador e o <i>backup</i> , pois tem dados sigilosos de várias empresas, e precisamos muito dessas informações em armazenamento.
Entrevistado 3	o contador trabalha com documentos e arquivos importantes. Nada como ter a segurança para armazenar as informações. Essa segurança também pode ser chamada de <i>backup</i> . Essa relação é imprescindível, uma vez que os documentos contábeis precisam estar armazenados e de fácil acesso sempre que necessário.
Entrevistado 4	não respondeu
Entrevistado 5	O <i>backup</i> é de extrema importância para o contador, visando sua capacidade de complementar as suas atividades, fazendo sua parte de armazenamento e segurança das informações criadas e acessadas pelo profissional.

Fonte: Elaborado pelo autor, 2021.

Pelo que pode-se analisar, quase todos responderam que existe uma relação muito estreita entre o contador e o *backup*, pois, o contador trabalha diariamente com documentos alheios, documentos importantes de clientes que precisam estar a mão, de fácil acesso, para serem manuseados, analisados e posteriormente guardados para uma eventual necessidade futura de fiscalização ou até mesmo de consulta, sem o *backup*, esse trabalho do contador se tornaria mais penoso e menos confiável, visto que a segurança e a guarda desses documentos são essenciais para um bom desempenho e credibilidade. Portanto, essa relação é hoje imprescindível, em qualquer setor da economia e no setor contábil então, é primordial e de grande relevância.

5 CONSIDERAÇÕES FINAIS

O presente TCC intitulado: “*A relevância do backup em escritório de pequeno porte em Itaberaba: um estudo de caso*”, teve a seguinte retrospectiva teórica: iniciou-se os estudos trazendo o conceito e importância do *backup* para as empresas de contabilidade e especialmente a AudiConti, localizada no município de Itaberaba, após estudos dos autores referenciados, concluiu-se que o mundo contemporâneo é digital e a tecnologia já faz parte da maioria das empresas do mercado, de modo que ter conhecimento sobre diferentes recursos é essencial. O *backup* é um deles, e possui uma importância indiscutível na segurança e no registro de dados de qualquer negócio e especialmente no mundo contábil.

Verificou-se que o *backup* se apresenta como uma solução adequada para a guarda e segurança de dados, no entanto, necessita-se de mais de um meio para arquivamento, como o armazenamento em uma empresa especializada e também o *backup* em nuvem, para mais segurança. Em relação à periodicidade constatou-se que ela necessariamente deve ser diária, visto que os dados sofrem mudanças a todo momento. Essa rotina diária pode ser programada para ser executada de forma automática, guardando cópias dos dados e arquivos e armazená-los de maneira segura em ambiente de datacenter.

Portanto, depreende-se que a maneira como os escritórios de contabilidade realiza seus *backups* pode ser fator decisivo na escolha de uma empresa. O risco de perda, inaccessibilidade ou acesso não autorizado aos dados mantidos nos computadores devido às ameaças, aumenta a preocupação em se manter a disponibilidade, confidencialidade e integridade das informações para a continuidade dos negócios.

No entanto, para segurança dos dados, além de outras medidas, é necessário que as estratégias para *backup* de dados sejam aplicadas, testadas e analisadas continuamente para serem válidas, mesmo com mudanças no ambiente de negócios.

Através deste trabalho, pode-se concluir que com planejamento e estratégias, segundo as melhores práticas podem ser decisivos em uma organização, tendo em mente que cada organização terá estratégias de *backup* de dados personalizadas de acordo com as características de cada negócio.

Na revisão da literatura, ficou claro a importância de uso de estratégias de *backup* de dados para garantir a segurança das informações e a gestão correta do plano de contingência, para o caso de acontecer perda de dados, pois acidentes acontecem em qualquer setor.

Na aplicação do questionário de pesquisa, verificou-se que nem todas as estratégias indicadas pela literatura são aplicadas dentro da empresa como a capacitação dos profissionais que trabalham diretamente com a guarda de dados. Apesar de todos os respondentes serem responsáveis por informações críticas que precisam de segurança, as opiniões sobre *backup* de dados divergem bastante. Esse fato pode ser explicado pela falta de guias e/ou cursos específicos para o planejamento de *backup* de dados.

Um dos benefícios deste trabalho foi mostrar que o processo de *backup* de dados deve ser estratégico, pois engloba toda a organização, desde a parte técnica, que deve conhecer o funcionamento das tecnologias, até a parte administrativa, que deve, além de liberar os recursos, auxiliar na classificação das informações e em outros procedimentos necessários ao plano de *backup* de dados.

Em relação as limitações deste estudo, a principal delas refere-se ao tipo de amostragem, a qual foi não probabilística por conveniência, e desse modo, os resultados e conclusões não podem ser generalizados. Para investigações futuras sugere-se a ampliação deste estudo para uma amostra maior, considerando diferentes tipos de negócio em um contexto mais abrangente.

REFERÊNCIAS

- ALVES-MAZZOTTI, A. J.; GEWANDSZNAJDER, F. **O método nas ciências naturais e sociais**: pesquisa quantitativa e qualitativa. São Paulo: Pioneira, 2006.
- ANDRIOTT, Guilherme. **A história do backup de dados**. 21 dez. 2016. Disponível em: <http://nfeexpert.com.br/blog/a-historia-do-backup-de-dados/>. Acesso em 05 abr. 2021.
- CERT.br. **Ransomware**: saiba como se prevenir desse código malicioso com as orientações do CERT.br. 2012. Disponível em: <https://www.tiespecialistas.com.br/review/ransomware-saiba-como-se-prevenir-desse-codigo-malicioso-com-as-orientacoes-do-cert-br/>. Acesso em: 07 abr. 2021.
- COELHO, José Martonio Alves. Resolução Conselho Federal de Contabilidade – CFC Nº 1.061 de 09.12.2005. **Portal de Contabilidade**, Curitiba, 27 dez. 2005. Disponível em: http://www.portaldecontabilidade.com.br/legislacao/cfc1061_2005.htm. Acesso em: 09 abr. 2021.
- FERREIRA, Rosilda Arruda. **A pesquisa científica nas ciências sociais**: caracterização e procedimentos. Recife: EDUFPE, 1998.
- FONSECA, João José Saraiva da. **Metodologia da pesquisa científica**. Fortaleza: UEC, 2002.
- GIL, Antônio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. São Paulo: Atlas, 2011.
- GOLDENBERG, Miriam. **A arte de pesquisar**: como fazer pesquisa qualitativa em Ciências Sociais. 8. ed. Rio de Janeiro: Record, 2007.
- LENTO, Luiz Otávio Botelho; LUZ, Théo Augustus. **Gestão de Continuidade do Negócio** – Livro Digital. Unisul Virtual, 2014. Disponível em: <https://www.riuni.unisul.br/bitstream/handle/12345/7045/MelhoresPraticasBackupEmNuvem.pdf?sequence=1&isAllowed=y>. Acesso em: 10 abr. 2021.
- MÉDICE, Roney. **A importância da Segurança da Informação** – Visão Corporativa Disponível em: <https://www.profissionaisti.com.br/2013/07/a-importancia-da-seguranca-da-informacao-visao-corporativa/>. Acesso em: 07 abr. 2021.
- MINAYO, Maria Cecília de Souza. **O desafio do conhecimento**: pesquisa qualitativa em saúde. São Paulo: HUCITEC, 2007.
- MOREIRA, Ademilson. **A importância da segurança da informação**. Disponível em: https://www.oficinadanet.com.br/artigo/1124/a_importancia_da_seguranca_da_informacao. Acesso em: 07 abril. 2021.
- MULATO NETO, Guilherme. O que é e como conseguir um certificado digital. **Techtudo**, Rio de Janeiro, 26 jul. 2012. Disponível em:

<http://www.techtudo.com.br/artigos/noticia/2012/07/o-que-e-e-como-conseguir-umcertificado-digital.html>. Acesso em: 10 abr. 2021.

PIGATTI, Fernando. Contabilidade online e contabilidade tradicional. **Rede Jornal Contábil**, Araguari – MG, 31 maio. 2018. Disponível em: <<https://www.jornalcontabil.com.br/contabilidade-online-e-contabilidadetradicional/#.W7Z5RXtKjIU>>. Acesso em: 05 abr. 2021.

PULIA, André. **Entendendo uma solução de backup**. Revista TIEspecialista. 4 agosto, 2016. Disponível em: <https://www.tiespecialistas.com.br/entendendo-uma-solucao-de-backup/#:~:text=BACKUP%20%C3%A9%20uma%20ap%C3%B3lice%20de,Word%2C%20Excel%2C%20PDF>). Acesso em 10 de abr. 2021.

SANTOS, Luiz Carlos dos. **Como elaborar projeto de pesquisa, artigo técnico-científico e monografia**. Belo Horizonte: Dialética, 2020.

Como recuperar dados no storage **NETAPP**. Controle net, 2019. Disponível em: <https://www.controle.net/buscas/como-recuperar-dados-no-storage-netapp>. Acesso em: 20 mar. 2021.

BIBLIOGRAFIA CONSULTADA

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 6023** - informação e documentação - referências - elaboração. 2. ed. Rio de Janeiro: ABNT, 2018.

_____. **NBR 6022** - informação e documentação – artigo técnico-científico - apresentação. Rio de Janeiro: ABNT, 2018.

_____. **NBR 6027** - informação e documentação - sumário - apresentação. Rio de Janeiro: ABNT, 2012.

_____. **NBR 6024** - informação e documentação - numeração progressiva das seções de um documento - apresentação. Rio de Janeiro: ABNT, 2012.

_____. **NBR 15287** - informação e documentação - projeto de pesquisa - apresentação. Rio de Janeiro: ABNT, 2011.

_____. **NBR 14724** - informação e documentação - trabalhos acadêmicos - apresentação. Rio de Janeiro: ABNT, 2011.

_____. **NBR 6028** - informação e documentação - resumo - apresentação. Rio de Janeiro: ABNT, 2021.

_____. **NBR 10520** - informação e documentação - citações - apresentação. Rio de Janeiro: ABNT, 2002.

APÊNDICE A - TERMO DE CONSENTIMENTO LIVRE E ESCLARECIDO

Você está sendo convidado para participar, como voluntário, em uma pesquisa. Após ser esclarecido(a) sobre as informações a seguir, no caso de aceitar fazer parte do estudo, assine ao final deste documento, elaborado em duas vias de um só teor. Uma delas é sua e a outra é do pesquisador responsável. Em caso de recusa você não será penalizado (a) de forma alguma.

Informações sobre a pesquisa:

Título do Projeto: Relevância do *Backup* em Escritório de Pequeno Porte em Itaberaba: um estudo de caso.

Pesquisador Responsável: Joelton Oliveira de Araújo - **e-mail:** ojoelton@yahoo.com.; **telefone para contato:** (75) 99841-1275.

Professor orientador: Dr. Luiz Carlos dos Santos

Esta pesquisa tem como objetivo geral - evidenciar a relevância do *backup* nos registros contábeis em uma empresa de pequeno porte na cidade de Itaberaba.

Nesta etapa do trabalho o pesquisador busca colher a percepção do público-alvo da pesquisa, no sentido de complementar o arcabouço teórico acerca da temática, ou seja, a prática sobre a importância do *backup* de dados em escritórios de contabilidade, situados em Itaberaba e ao mesmo tempo, auxiliando os profissionais da área de Segurança da Informação no Planejamento de *Backup* de Dados. Os respondentes são os responsáveis pela empresa e funcionários que convivem dia a dia com dados das empresas de clientes, que precisam ser mantidos por, no mínimo, dois anos.

Garante-se que não há riscos de qualquer natureza para os participantes desta pesquisa. Os respondentes são livres para recusarem-se a participar, retirarem seu consentimento ou interromper a participação a qualquer momento. A participação é voluntária e a recusa em participar não irá acarretar qualquer penalidade.

As respostas serão consideradas confidenciais, com finalidade estritamente acadêmica, e utilizadas apenas para fins de pesquisa. Assim, não serão, sob qualquer hipótese, repassados a outras pessoas ou instituições, ou utilizadas para outros fins. Os resultados consolidados da pesquisa serão divulgados posteriormente, especialmente aos colaboradores, mas isso será feito sem apontar as respostas específicas de qualquer respondente.

Estas respostas obtidas serão analisadas e consolidadas em um relatório, identificando o que é utilizado e indicado, pelos profissionais que atuam nos escritórios de contabilidade, como principais estratégias para gestão e planejamento de *backup* de dados e sua relevância para os mesmos. Ressalta-se que isso não é um teste, onde deveriam ser dadas as “respostas exatas”, mas sim um instrumento de coleta de dados. Para esclarecimento de eventuais dúvidas, contate o pesquisador responsável.

Itaberaba, maio de 2021.

Joelton Oliveira de Araújo

APÊNDICE B – Termo de Consentimento - Individual
Consentimento da participação da pessoa como sujeito

Eu, _____, RG _____, abaixo assinado, concordo em participar do estudo “Relevância do *Backup* em Escritório de Pequeno Porte em Itaberaba: um estudo de caso”, como sujeito de pesquisa. Fui devidamente informado (a) e esclarecido (a) pelo pesquisador Joelton Oliveira de Araújo, sobre a pesquisa, os procedimentos nela envolvidos, assim como os possíveis riscos e benefícios decorrentes de minha participação. Foi-me garantido (a) que posso retirar meu consentimento a qualquer momento, sem que isto leve a qualquer penalidade.

Itaberaba, ____/____/_____

Nome: _____

Assinatura: _____

APÊNDICE C – Questionário sobre a pesquisa empírica, intitulada “A relevância do *backup* em escritório de pequeno porte em Itaberaba: um estudo de caso”

QUESTÕES:

1- Há quanto tempo a empresa faz *backup* de dados?

2- A empresa possui dados críticos, que precisam ser mantidos por dois anos ou mais?

() sim () não

3- O que você considera como principais razões para se ter um Plano de *Backup* de Dados?

- () Conformidade com leis e regulamentos nacionais
- () Conformidade com leis e regulamentos internacionais
- () Conformidade com padrões de segurança, mesmo que não obrigatórios
- () Confiabilidade e crédito de clientes
- () Concorrência
- () Proteção dos Dados
- () Todas
- () Outras, quais?

4- Qual o tipo de *backup* é feito na empresa?

5 - Qual a periodicidade do *backup*?

6- Quem você acha que deve participar do desenvolvimento do Plano de *Backup* de Dados?

- () Dono da empresa
- () Gerente administrativo
- () Corpo técnico de TI
- () Funcionários
- () Todos mencionados

7- A equipe de trabalho já participou de algum treinamento sobre a importância do *backup* e sua correta utilização?

8- Existe um profissional responsável pelo *backup*?

Sim Não

9- A empresa dispõe de um contrato com *backup* remoto? Justifique

Sim Não

10- Foi necessário a aquisição de recursos tecnológicos para conseguir as tecnologias de *hardware*, *software* e mídias para *backup*? Justifique

Sim Não

11- O que você considera necessário para escolher mídias para *backup* de Dados?

- Criticidade da informação classificada
 - Período de retenção dos dados
 - Espaço a ser ocupado pelos dados
 - Facilidade de utilização
 - Rapidez para o *backup* e Recuperação dos dados
 - Preço do produto
 - Todas
 - Outros? Cite.
-
-

12- Existe um plano de contingência para o caso de perda de dados?

Sim Não

13- Já aconteceu de perder algum dado importante de clientes, em caso positivo qual providência foi tomada?

Sim Não
