

## A IMPORTÂNCIA DO *BACKUP* EM PEQUENAS EMPRESAS: o *backup* em empresas de contabilidade de Americana

Sergio Mitsunaga<sup>1</sup>  
Thiago Ramos Nunes Pereira<sup>2</sup>  
Edson Roberto Gaseta<sup>3</sup>

### RESUMO

A Tecnologia da Informação – TI, permanece sendo o principal fator de continuidade dos negócios das empresas cujos alicerces estão fundamentados no valor da informação. Toda informação de valor representa parte ou todo o sucesso e permanência da empresa no cenário na qual ela se insere; e assim como artistas de elevadíssimo nível, colocam em seguradoras seus instrumentos, e em alguns casos até parte de seus membros, as empresas que tratam a informação como ativo intangível, considerando inestimável seu valor, recorrem às melhores tecnologias para a preservação, manutenção e recuperação destas informações. Neste cenário se incluem as pequenas empresas que prestam serviços para outras maiores, que terceirizam seus serviços administrativos, tais como atividades de departamento pessoal e fiscal; tratando assim, informações confidenciais e estratégicas destes clientes. Esta pesquisa pretende corroborar que o processo de guarda, arquivamento, cópia segura da informação (*backup*) é fator fundamental para empresas do segmento contábil, tendo impacto direto em médias e grandes empresas, pela corresponsabilidade sobre a confidencialidade, integridade e disponibilidade das informações de valor.

**Palavras-chave:** Cópia de Segurança. Segurança da Informação. Dados contábeis.

### ABSTRACT

*Technology of Information – IT, remains the main business continuity factor for companies whose foundations are based on the value of information. All invaluable information represents part or all success and company life into the market scenario, and such as very high-level artists provides insurance to their instruments and some case even part of their members, companies that treat such information, as an intangible asset, considering it invaluable, are looking for the best technologies for preservation, maintenance and recovery of that information. In that scenario are included small companies that work for big others, through administrative services, such as personnel and finance departments; therefore, treating confidential and strategic information of them. This research intends to corroborate that the process of safekeeping, archiving, and safe copy of information (backup) is a fundamental factor for accounting company's business, having direct impact on medium sized and big enterprises, about great responsibility on confidentiality, integrity, and availability of invaluable information.*

**Keywords:** Backup. Information Security. Accounting data.

### 1 INTRODUÇÃO

Após o advento da era da informática, e, mais recentemente a era da informação, a dependência por recursos de informática para manter confiáveis e recuperáveis dados armazenados em computadores, tem-se a necessidade de procedimentos seguros denominado de *backup*, termo inglês que tem o significado de **cópia de segurança**.

É o caso das pequenas empresas de contabilidade, cujo número tem se expandido cada vez mais, pois a livre iniciativa de profissionais liberais empreendedores num mercado cada vez mais competitivo, no qual as grandes empresas terceirizam os serviços para reduzir os custos internos, vê-

---

<sup>1</sup> Graduado em Tecnologia Mecânica pela Fatec-SP e Universidade Metodista de Piracicaba, Graduando em Tecnologia de Segurança da Informação pela Faculdade de Tecnologia de Americana. E-mail: smitsunaga59@gmail.com

<sup>2</sup> Bacharel em Ciência da Computação, Especialista em Tecnologia da Informação para Estratégia de Negócios, Graduando em Tecnologia de Segurança da Informação pela Faculdade de Tecnologia de Americana. E-mail: thiagoramos@gmail.com

<sup>3</sup> Graduado em Tecnologia em Processamento de Dados, Especialista em Redes de Computadores, MBA em Gestão Empresarial, Mestre em Gestão de Redes de Telecomunicações pela Pontifícia Universidade Católica de Campinas. Docente da Faculdade de Tecnologia de Americana, E-mail: gaseta@gmail.com

se o surgimento deste segmento que impulsiona a economia tanto quanto empresas de médio e grande porte.

É nesse cenário que as informações se tornam o patrimônio intelectual, comercial e profissional para o desempenho de cada segmento nesse mercado competitivo, e a segurança da informação através de recursos e procedimentos de *backup*, garante a integridade dos dados e informações, por exemplo: de pessoas físicas, jurídicas, mantendo sua confidencialidade com alto grau de ética profissional que o segmento deve oferecer.

Por isso, estudar a importância do *backup* neste segmento de serviço torna-se uma relevante medida para que se diminuam os riscos com a perda das informações, podendo ser determinante para a continuidade do negócio, diminuindo os possíveis prejuízos oriundos da falta de cópia de segurança – *backup*.

O objetivo principal desta pesquisa se concentra em analisar as consequências da perda de dados e informações no meio empresarial, em destaque, o universo de empresas da área contabilidade, na cidade de Americana/SP.

Com efeito, pretende-se evidenciar as consequências financeiras em termos de prejuízos relativos à confiabilidade na recuperação de dados nas empresas de contabilidade, investigando as causas da perda de dados e informações nestas empresas.

## 1.1 METODOLOGIA DE PESQUISA

O método científico de pesquisa utilizado é do tipo exploratória baseando-se em entrevistas e dados coletados junto às empresas de contabilidade da cidade de Americana /SP. Os critérios envolvidos nos questionários serão relativos ao sistema de *backup* utilizado, os incidentes ocorridos durante um período determinado, os custos envolvidos – suporte, multas e aquisições. Os dados serão compilados ocultando os nomes das empresas. Por motivo ético serão referenciados através de numeração e os resultados apresentados em forma de gráficos quantitativos e qualitativos.

## 2 REVISÃO DE LITERATURA

A cópia de segurança da base de dados de um sistema informatizado, mundialmente denominada de *backup*, permite a restauração em caso de perda dos dados originais. Essas perdas podem ocorrer de forma acidental, por corrupção de dados, ou mesmo por acessos não autorizados.

As boas práticas de administração de sistemas informatizados sugerem a implementação de um procedimento robusto de *backup*, que é considerada uma importante tarefa devido sua complexidade e benefício; relaciona-se diretamente a restauração de arquivos que estão relacionados à confiabilidade, integridade e proteção de dados (LEÃO, 2010).

A continuidade de um negócio, a consolidação da carreira de um profissional de TI – Tecnologia da Informação, além do sucesso de seus clientes, pode estar representada na eficácia de um bom sistema de recuperação de dados. Desta forma, um processo confiável de *backup* é sem dúvida uma questão essencial para a sobrevivência de uma empresa e todos aqueles que fazem parte do processo, preservando inclusive os ativos intangíveis, que comumente são “esquecidos”, tais como a reputação e a imagem da organização (SCHNEIDER, 2003).

O Código de prática para a gestão de segurança da informação, segundo a NBR diz que:

“O valor da informação vai além das palavras escritas, números e imagens: conhecimento, conceitos, idéias e marcas são exemplos de formas intangíveis da informação. Em um mundo interconectado, a informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações, são informações que, como outros ativos importantes, tem valor para o negócio da organização e, conseqüentemente, requer proteção contra vários riscos” (ABNT, 2013, pag. 4).

O *backup*, portanto, deve estar ligado à questão econômica, dentro da estratégia de negócio de uma empresa, mesmo sendo de pequeno porte, segmento abordado por esta pesquisa, pois a perda

dos dados e informações, seja qual for a causa e o motivo, vai impactar na sua sobrevivência nesse mercado tão competitivo.

A contribuição dos textos referenciais será de notória relevância nesta pesquisa principalmente considerando a abordagem minuciosa dada aos problemas oriundos da negligência das gestões empresariais no tocante aos investimentos nos serviços de *backup* dos dados e informações.

## 2.1 SOBRE A NATUREZA DA PESQUISA

Em relação a natureza da pesquisa, Gil (2008), afirma que:

### 2.1.1 Pesquisa Básica:

Objetiva gerar conhecimentos novos úteis para o avanço da ciência sem aplicação prática prevista. Envolve verdades e interesses universais;

### 2.1.2 Pesquisa Aplicada:

Objetiva gerar conhecimentos para aplicação prática, dirigidos à solução de problemas específicos. Envolve verdades e interesses locais.

A pesquisa sobre o tema será desenvolvida conforme a definição de Pesquisa Aplicada, pois o objetivo proposto é a solução de problemas de interesse local – empresas de contabilidade de Americana.

## 2.2 SOBRE O TIPO DA PESQUISA

Em relação ao tipo de pesquisa a ser realizada, algumas definições se fazem necessárias:

### 2.2.1 Pesquisa Qualitativa

É traduzida por aquilo que não pode ser mensurável, pois a realidade e o sujeito são elementos indissociáveis. Assim sendo, quando se trata do sujeito, levam-se em consideração seus traços subjetivos e suas particularidades. Tais pormenores não podem ser traduzidos em números quantificáveis. (DUARTE, 2011).

### 2.2.2 Pesquisa Quantitativa

Diferente da Pesquisa Qualitativa, este método busca por resultados que possam ser quantificados por meio da coleta de dados sem instrumentos formais e estruturados de uma maneira mais organizada e intuitiva (DUARTE, 2011).

O tema da pesquisa a ser desenvolvida abordará uma problemática que abrange não só o universo das médias e grandes empresas, mas principalmente das pequenas, onde a maioria dos empreendedores são profissionais liberais; portanto, a pesquisa será direcionada às modalidades qualitativa e quantitativa, que serão retratadas por meio de relatórios, comentários e opiniões do público envolvido, além de dados numéricos coletados nas empresas de contabilidade de Americana.

## 2.3 PROCEDIMENTO PARA A PESQUISA

### 2.3.1 Pesquisa Bibliográfica

Segundo Lakatos e Marconi (1987, p. 66), a pesquisa bibliográfica trata-se do levantamento, seleção e documentação de toda bibliografia já publicada sobre o assunto que está sendo pesquisados em livros, revistas, jornais, boletins, monografias, teses, dissertações, material cartográfico, com o objetivo de colocar o pesquisador em contato direto com todo o material já escrito sobre o mesmo.

Segundo Cervo e Bervian (1976, p. 69), qualquer tipo de pesquisa em qualquer área do conhecimento, supõe e exige pesquisa bibliográfica prévia, quer para o levantamento da situação em

questão, quer para a fundamentação teórica ou ainda para justificar os limites e contribuições da própria pesquisa.

Assim, afirmam que a pesquisa bibliográfica é um excelente meio de formação e juntamente com a técnica do resumo de assunto ou revisão de literatura, constitui geralmente o primeiro passo de toda a pesquisa científica. Por isso, os universitários devem ser incentivados a usarem métodos e técnicas científicas para realiza-la, tanto independente, quanto como parte complementar de uma pesquisa descritiva ou de uma experimental. (DA SILVA, 2012).

### **2.3.2 Pesquisa de Campo**

É a pesquisa em que se observa e coleta os dados diretamente no próprio local em que se deu o fato em estudo, caracterizando-se pelo contato direto com o mesmo, sem interferência do pesquisador, pois os dados são observados e coletados tal como ocorrem espontaneamente. (LAKATOS; MARCONI, 1996, p. 75).

Baseado nas definições e no material coletado inicialmente será adotado primordialmente o procedimento de pesquisa bibliográfica, porém consonante com a pesquisa de campo, cujas informações complementarão o objetivo da pesquisa.

## **3 PESQUISA DE CAMPO E ENTREVISTA**

Em complemento a pesquisa bibliográfica, foi realizada uma pesquisa de campo em visita a empresas de contabilidade na cidade de Americana, interior do estado de São Paulo.

As Figuras 1 e 2, mostram o questionário que foi apresentado a representantes destas empresas, buscando levantar dados sobre o ambiente informático no qual estão inseridos para o desempenho de suas atividades profissionais e demais itens relevantes ao assunto dessa pesquisa.

Figura 1 - Pesquisa de Campo - Questionário pag.1





---

**FACULDADE DE TECNOLOGIA DE AMERICANA**  
**Curso Superior de Tecnologia em Segurança da Informação**

Artigo Científico: "A Importância do Backup em Pequenas Empresas: o backup em empresas de contabilidade".

Alunos: Sergio Seidji Mitsunaga e Thiago Ramos Nunes Pereira

**Pesquisa de Campo** (Confidencial)

1) Número de funcionários da empresa:  
a- [ ] Até 10                      b- [ ] Mais de 10 a 30                      c- [ ] Mais de 30

2) Quais as soluções existentes para estabelecer a segurança da informação em sua empresa? (pode assinalar mais do que uma).  
a- [ ] Plano de Backup (cópia de segurança de dados);  
b- [ ] Redundância / Recurso em Nuvem - (Meio de salvaguarda de dados);  
c- [ ] Programa de Antivírus;  
d- [ ] Firewall (Programa que ajuda a impedir o acesso indevido à rede da empresa);  
e- [ ] Equipe/Profissional responsável pela administração permanente da rede/dados;  
f- [ ] Equipe/Profissional responsável pela resposta a incidentes;  
g- [ ] Outras: \_\_\_\_\_

3) Quais os Tipos de problemas enfrentados?

a) Perda de dados por meio desconhecido:  
1- [ ] Sem perda de dados    2- [ ] Até 5 vezes em 1 ano    3- [ ] Até 5 vezes em 5 anos    4- [ ] Mais vezes

b) Perda de dados por Ransomware (vírus que sequestra dados e resgate pago):  
1- [ ] Sem perda de dados    2- [ ] Até 5 vezes em 1 ano    3- [ ] Até 5 vezes em 5 anos    4- [ ] Mais vezes

c) Perda de dados por outro tipo de software malicioso (phishing, vírus, etc):  
1- [ ] Sem perda de dados    2- [ ] Até 5 vezes em 1 ano    3- [ ] Até 5 vezes em 5 anos    4- [ ] Mais vezes

d) Perda de dados por Ataque cibernético (invasão por hackers):  
1- [ ] Sem perda de dados    2- [ ] Até 5 vezes em 1 ano    3- [ ] Até 5 vezes em 5 anos    4- [ ] Mais vezes

e) Perda de dados por Falha de Software (Sistema Operacional ou Aplicativo):  
1- [ ] Sem perda de dados    2- [ ] Até 5 vezes em 1 ano    3- [ ] Até 5 vezes em 5 anos    4- [ ] Mais vezes

Fonte: Elaborado pelos autores

**Figura 2 - Pesquisa de Campo - Questionário pag.2**

f) Perda de dados por Falha de Hardware (Computador, Servidor, ou periférico):  
 1- [ ] Sem perda de dados    2- [ ] Até 5 vezes em 1 ano    3- [ ] Até 5 vezes em 5 anos    4- [ ] Mais vezes

g) Perda de dados por Falha Humana (erro operacional):  
 1- [ ] Sem perda de dados    2- [ ] Até 5 vezes em 1 ano    3- [ ] Até 5 vezes em 5 anos    4- [ ] Mais vezes

h) Perda de dados por Falta de Backup (cópia de segurança de dados):  
 1- [ ] Sem perda de dados    2- [ ] Até 5 vezes em 1 ano    3- [ ] Até 5 vezes em 5 anos    4- [ ] Mais vezes

4) Prejuízos financeiros por perda de dados no último ano:  
 1- [ ] Sem prejuízo    2- [ ] Até R\$5.000,00    3- [ ] R\$5.000,00 a R\$50.000,00    4- [ ] Mais de R\$50.000,00

5) Prejuízos financeiros por perda de dados nos últimos 5 anos:  
 1- [ ] Sem prejuízo    2- [ ] Até R\$5.000,00    3- [ ] R\$5.000,00 a R\$50.000,00    4- [ ] Mais de R\$50.000,00

6) Investimentos financeiros em T.I. no último ano:  
 1- [ ] Sem    2- [ ] Até R\$5.000,00    3- [ ] R\$5.000,00 a R\$50.000,00    4- [ ] Mais de R\$50.000,00

7) Investimentos financeiros em T.I. nos últimos 5 anos:  
 1- [ ] Sem    2- [ ] Até R\$5.000,00    3- [ ] R\$5.000,00 a R\$50.000,00    4- [ ] Mais de R\$50.000,00

8) Previsão de Investimentos em T.I. nos próximos 5 anos (financeiro e pessoal):  
 1- [ ] Sem    2- [ ] Até R\$5.000,00    3- [ ] R\$5.000,00 a R\$50.000,00    4- [ ] Mais de R\$50.000,00

9) Sobre software para GED (Gestão Eletrônica de Documentos – digitalização, cadastro, workflow, integração, gerenciamento):  
 1- [ ] Não conheço    2- [ ] Conheço, mas não uso. Qual? \_\_\_\_\_    3- [ ] Conheço, e uso. Qual? \_\_\_\_\_

10) O quanto se considera satisfeito com a estrutura atual da empresa, na perspectiva de Segurança da Informação:  
 1- [ ] Pouco satisfeito    2- [ ] Satisfeito    3- [ ] Muito satisfeito    4- [ ] Prefiro não responder.

Fonte: Elaborado pelos autores

#### 4 APRESENTAÇÃO DOS DADOS

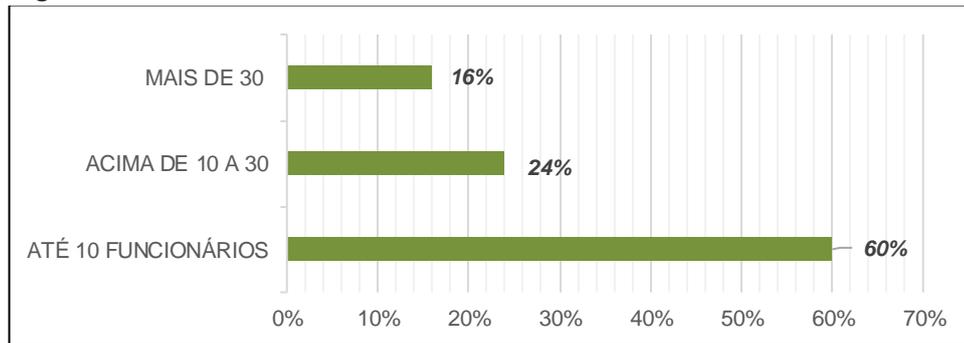
Após visita e realização da pesquisa à empresas de contabilidade de Americana, tendo entrevistado profissionais locais sobre seu ambiente de trabalho, conhecimento em informática, *software* e aplicativos relacionados ao negócio, dificuldades e limitações em relação aos sistemas computacionais que faz uso, também falhas decorrentes do fator humano, foi possível tabular os seguintes resultados:

##### 4.1 NÚMERO DE FUNCIONÁRIOS NA EMPRESA

Observa-se, no gráfico da figura 3, que mais da metade das empresas entrevistadas são pequenas empresas com no máximo 10 funcionários, com percentual de 60%, seguido de empresas

com até 30 funcionários – 24%, e apenas 4 empresas, ou seja 16%, com mais de 30 funcionários. Nestas últimas percebe-se uma evolução mais profunda em termos de recursos materiais e humanos, demonstrados nas instalações, mobiliário, uniformes dos funcionários e posicionamento do departamento de TI. Mais adiante demonstra-se que tais empresas, representando uma quantificação modesta, detêm uma significativa qualificação em termos de tecnologia da informação, percebida no atendimento prestado pelos seus responsáveis de TI, demonstrando conhecimento de causa através de sua formação acadêmica e profissional.

**Figura 3 – Gráfico Nº de funcionários**

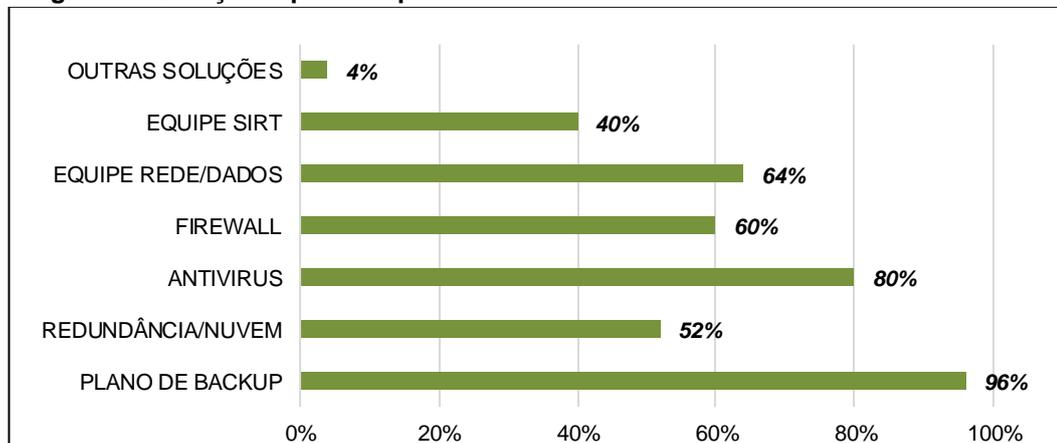


Fonte: Elaborado pelos autores.

#### 4.2 QUAIS AS SOLUÇÕES QUE AS EMPRESAS ADOTAM PARA SEGURANÇA DA INFORMAÇÃO

Neste segundo bloco de questões foram abordadas algumas soluções que são adotadas pelas empresas entrevistadas. Os resultados são demonstrados na figura 4, e será referência para os itens que se seguem, relativas às soluções e respectivos comentários.

**Figura 4 - Soluções que a empresas adotam.**



Fonte: Elaborado pelos autores.

##### 4.2.1 Plano de *Backup*

Nota-se, no gráfico da figura 4, que a maioria (96%) das empresas entrevistadas contam com um plano de *backup*; apenas uma delas informou que não necessita do plano, pois nunca ocorreu perda de dados. Neste aspecto, não abordamos os detalhes com relação a tempo de existência no mercado, ou outros fatores que certamente afetariam as decisões acerca da questão. Também não entramos em detalhes, em relação as outras que detêm um plano de *backup*, como item de uma política ou se apenas existe uma rotina de procedimentos e responsáveis pela efetivação do plano.

#### 4.2.2 Redundância<sup>4</sup>/ Recurso em Nuvem<sup>5</sup>

A figura 4 demonstra o gráfico representando o percentual de empresas (52%) que têm processo de redundância para o processo de *backup* local ou em nuvem. Praticamente se dividem igualmente, neste requisito; evidenciando que há a preocupação com a preservação de dados com um plano de *backup*, mas não com a mesma importância quando se trata de redundância, quando ocorrer algum problema que impede a recuperação de dados em sua fonte primária.

#### 4.2.3 Programa de antivírus

Evidencia-se na figura 4, que 80% das empresas, utilizam programa antivírus, corroborando a crescente preocupação com a proteção contra vírus, que provocam perdas significativas em termos financeiros, principalmente pelo valor das informações, mas também nas ações de formatação e recuperação de dados.

#### 4.2.4 Programa de Firewall

Em termos de prevenção de ataques e acessos indevidos, percebe-se que, 60% das empresas entrevistadas possuem programa de *Firewall*, instalado em sua rede de computadores. Entretanto em 40% delas há a vulnerabilidade de sua rede não possuir o programa para defesa de ameaças e acessos indevidos.

#### 4.2.5 Equipe responsável pela rede e dados

Em termos de equipe responsável por redes e dados, o gráfico da figura 4 demonstra que 64% das empresas entrevistadas, possuem uma equipe responsável por este quesito. Somente 36% não mantem essa equipe.

#### 4.2.6 Equipe responsável SIRT – Security Incident Response Team

Em contraposição ao resultado demonstrado pela figura 4, onde a maioria possui responsável pela administração da rede e dados, o gráfico demonstra que 60% das empresas entrevistadas, não possuem uma equipe *SIRT* responsável por resposta a incidentes de segurança. Somente 40% mantem um time para atender esse quesito.

#### 4.2.7 Outras soluções

Em termos percentuais, apenas 4% das empresas entrevistadas tem outras soluções em TI – *software* de gestão, A maioria informou não ter nenhuma outra solução para a área de TI, conforme pode-se observar na figura 4.

### 4.3 QUAIS OS TIPOS DE PROBLEMAS ENFRENTADOS PELA EMPRESA?

Neste item são apresentados os resultados obtidos no questionário apresentado às empresas acerca dos vários problemas por elas enfrentados. Os problemas foram dispostos em perguntas diretas sem a necessidade de detalhar o objeto da perda de dados. Entenda-se por detalhamento do objeto, a especificação do nome e outras características intrínsecas que levaram a perda de dados; assunto a ser abordado em tópico pertinente.

---

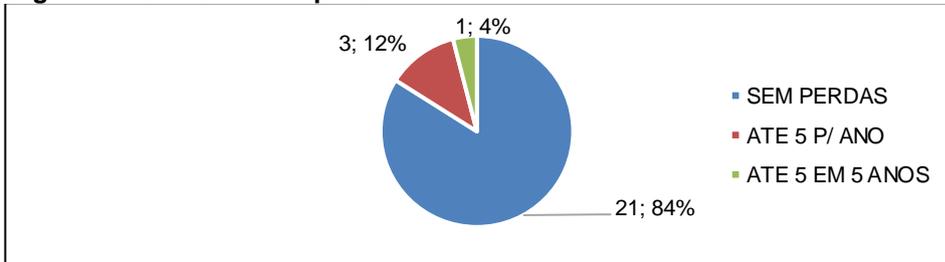
<sup>4</sup> (Informática)- Meio para suportar perda de dados e manter alta disponibilidade. Disponível em: <<https://aws.amazon.com/s3/reduced-redundancy/>> Acesso em 15 out. 2018.

<sup>5</sup> Capacidade de armazenamento de dados em servidores disponibilizados em internet por provedores. Disponível em :< <https://aws.amazon.com/pt/what-is-cloud-storage/>> Acesso em 15 out. 2018.

#### 4.3.1 Perda de dados por meios desconhecidos

Constata-se na figura 5, que a maioria das empresas – 84%, não tiveram perdas de dados. O mesmo não ocorreu para 12% delas, onde tiveram até 5 incidentes envolvendo perda de dados num período de até 1 ano, e em 4%, com até 5 incidentes em 5 anos, por meios desconhecidos.

**Figura 5 - Gráfico Nº empresas - Perda de dados**

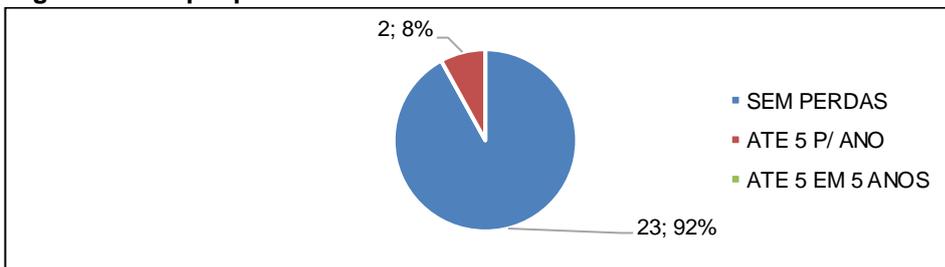


Fonte: Elaborado pelos autores.

#### 4.3.2 Perda de dados por *Ransomware* – *malware* que sequestra dados

Os resultados demonstrados na figura 6 indicam que poucas empresas - 8%, sofreram ataques de *Ransomware*, um tipo de *malware* que sequestra dados exigindo quantias, geralmente depositadas em conta, em troca da liberação dos dados criptografados. O número de ataques foram de até 5 por ano.

**Figura 6 - Ataque por *Ransomware***

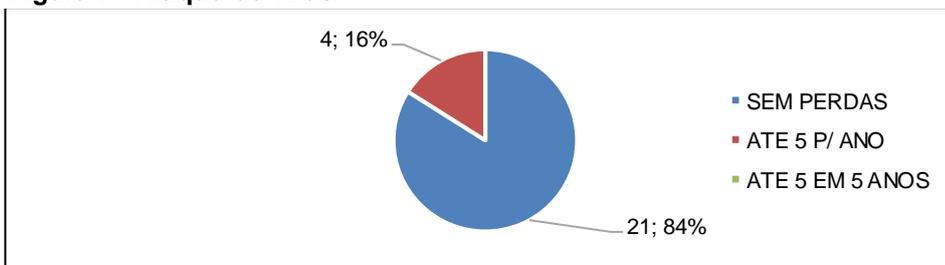


Fonte: Elaborado pelos autores.

#### 4.3.3 Perda de dados por ataque de vírus

As empresas que sofreram ataques de vírus somam 16%, com pelo menos 5 ataques por ano. A maioria - 84%, não tiveram esse problema. Resultado muito coerente com o item 4.2.3, da figura 4, na qual se destaca que 80% utilizam programa de *firewall*.

**Figura 7 - Ataque de vírus.**

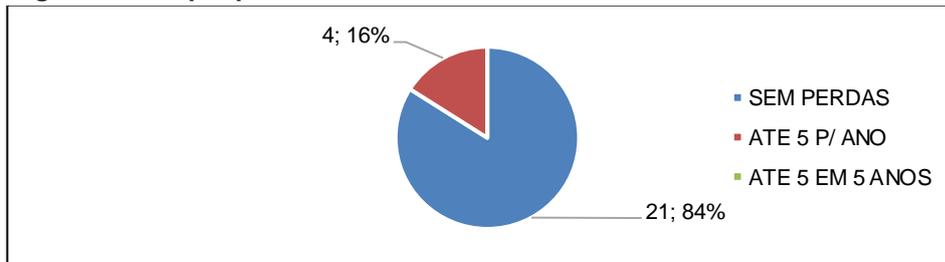


Fonte: Elaborado pelos autores.

#### 4.3.4 Perda de dados por ataque de *Hacker*

Os resultados do gráfico da figura 8 parecem similares ao do item 4.3.3, figura 7. em termos percentuais, porém os incidentes não ocorreram nas mesmas empresas. Fato este, interessante, pois em análise mais criteriosa, pode-se destacar que as empresas atacadas não pertencem àquelas que estão no percentual que informaram adotarem programa de *firewall*, conforme apresentado no item 4.2.4.

**Figura 8 - Ataque por *Hacker*.**

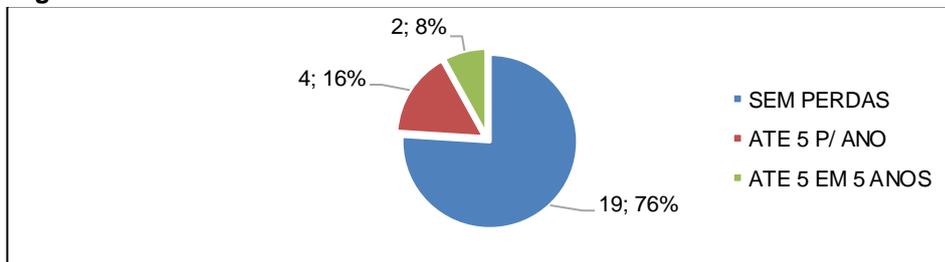


Fonte: Elaborado pelos autores.

#### 4.3.5 Perda de dados por falha de *Software* (sistema operacional, aplicativos)

Pode-se distinguir pelo gráfico da figura 9, que as perdas de dados ocasionadas por falha de *software* atingiram 24% das empresas, sendo 16% com até 5 falhas em um ano e 8% com 5 falhas em 5 anos. Não foram especificados os tipos de *software*, porém de uma forma geral, a empresas indicaram que as falhas ocorreram no sistema operacional.

**Figura 9 - Falha de *Software*.**

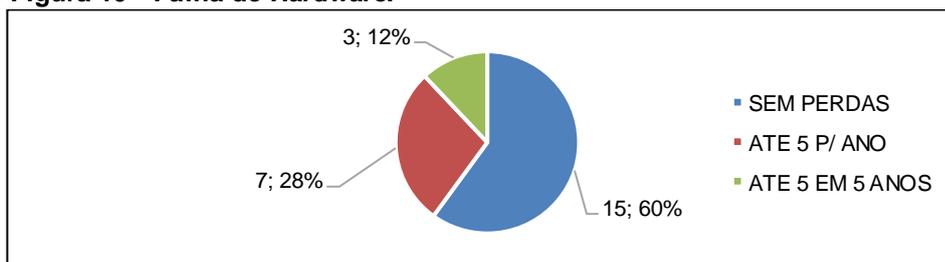


Fonte: Elaborado pelos autores.

#### 4.3.6 Perda de dados por falha de *hardware* (computador, servidor, outros)

Um dos maiores índices de perda de dados dentre as empresas entrevistadas foi a falha de *hardware* - 40%, conforme mostra a figura 10. Este dado não está vinculado a questão da recuperação de dados pelo *backup*, mas diretamente relacionado ao incidente ocorrido. É um assunto com potencial de exploração em futuros trabalhos.

**Figura 10 - Falha de *Hardware*.**

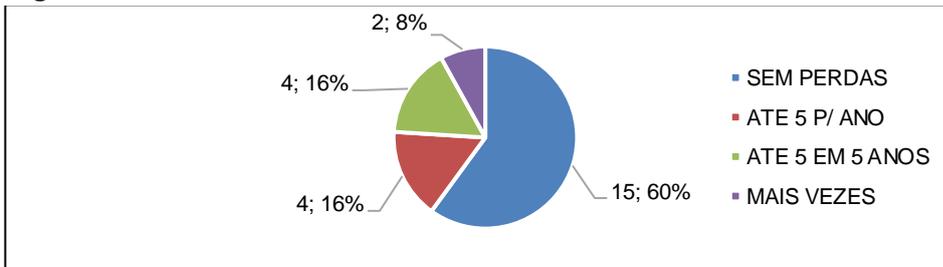


Fonte: Elaborado pelos autores.

**4.3.7 Perda de dados por falha humana**

Este é outro índice com maior incidência nas empresas; conforme figura 11, são 40% das empresas onde a falha humana tem grande impacto; indicando que apesar dos treinamentos, metodologias, procedimentos, balizados por uma política (quando efetivados), não se consegue reduzir o número de incidentes relacionados a condição operacional humana. Assunto com grande potencial de exploração em futuros trabalhos.

**Figura 11 - Falha Humana.**

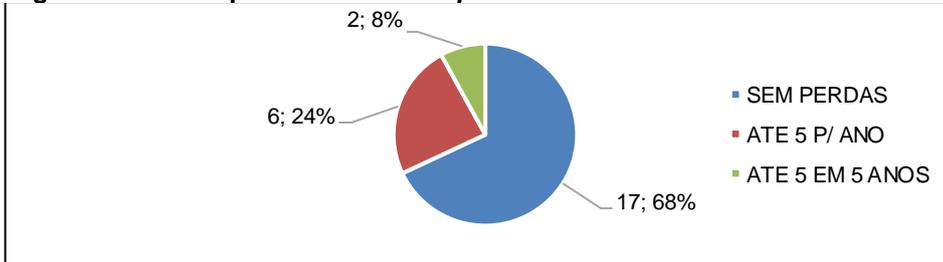


Fonte: Elaborado pelos autores.

**4.3.8 Perda de dados por falta de backup**

Mesmo não se situando entre os maiores índices de perda de dados, a figura 12 demonstra que o resultado é preocupante, pois um percentual de 32% das empresas teve problemas com a falta de *backup*, mesmo com 96% delas, conforme figura 4, do item 4.2.1, possuírem um plano de *backup*, o percentual total de empresas com perdas indica que podem haver falhas operacionais, ou mesmo deficiências na metodologia aplicada, sugerindo que o assunto tem potencial de abordagem em futuros trabalhos.

**Figura 12 - Falha por falta de backup**

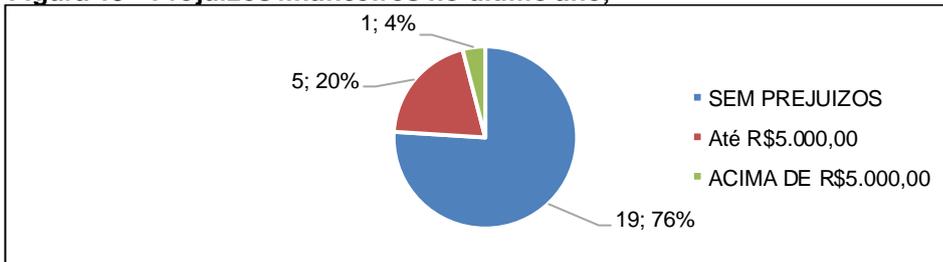


Fonte: Elaborado pelos autores.

**4.4 PREJUÍZOS FINANCEIROS POR PERDA DE DADOS NO ÚLTIMO ANO**

Os prejuízos até R\$5.000,00 ocorreram em 20% das empresas, e acima de R\$5.000,00, em 4%. A maioria das empresas – 76% não tiveram prejuízos neste período. Nota-se que um total de 24% de empresas teve prejuízos financeiros; observa-se na figura 13 uma relação próxima com o resultado da figura 4, item 4.2.3.

**Figura 13 - Prejuízos financeiros no último ano,**

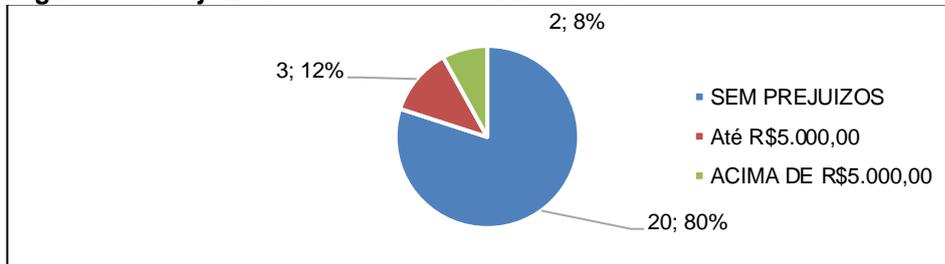


Fonte: Elaborado pelos autores.

#### 4.5 PREJUÍZOS FINANCEIROS POR PERDA DE DADOS NOS ÚLTIMOS 5 ANOS

O percentual de empresas com prejuízos no período de 5 anos, mostrado na figura 14 abaixo: 20%, é menor que o mostrado no item 4.4; sugerindo que os incidentes tendem a diminuir num tempo acima de um ano, sinalizando a eficiência dos recursos com relação as invasões.

**Figura 14 - Prejuízos financeiros nos últimos 5 anos.**

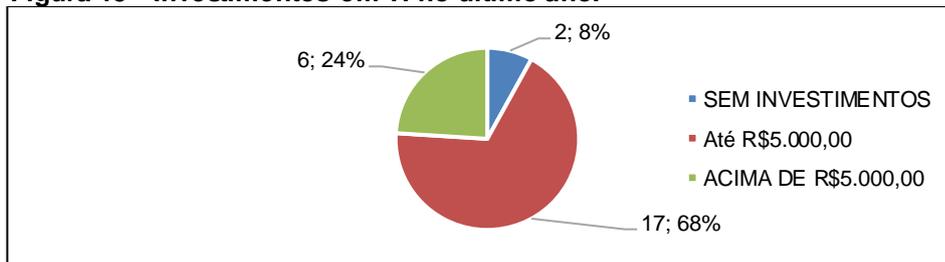


Fonte: Elaborado pelos autores.

#### 4.6 INVESTIMENTOS EM TI NO ÚLTIMO ANO

Os investimentos em TI no último ano, como indicado na figura 15, somam 92% das empresas, demonstrando que apesar do investimento significativo, o número de empresas com perdas, em determinados tipos de incidentes, não tem uma relação proporcional, ou seja, nem sempre o resultado esperado é alcançado.

**Figura 15 - Investimentos em TI no último ano.**

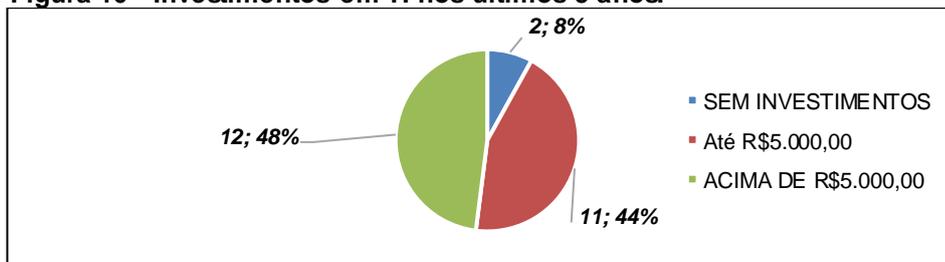


Fonte: Elaborado pelos autores.

#### 4.7 INVESTIMENTOS EM TI NOS ÚLTIMOS 5 ANOS

O resultado demonstrado na figura 16, indica inicialmente um grande percentual de empresas que investiram valores acima de R\$5.000,00 nos últimos 5 anos, porém há de se esclarecer que tais investimentos são relativos ao mesmo investimento anual aplicado em 5 anos, resultando num montante maior. Fica claro que grande parte das empresas (44%), mantiveram os mesmos investimentos.

**Figura 16 - Investimentos em TI nos últimos 5 anos.**

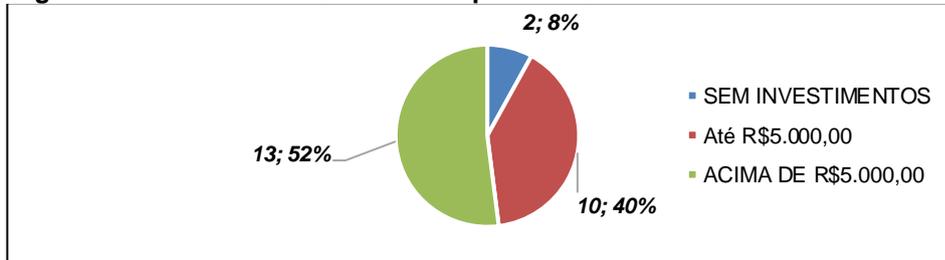


Fonte: Elaborado pelos autores.

#### 4.8 INVESTIMENTOS EM TI NOS PRÓXIMOS 5 ANOS

Nesta figura 17, pode-se verificar que o número de empresas com investimentos acima de R\$5.000,00, teve um sensível aumento, de 48% para 52%, indicando que os investimentos em TI ainda são muito tímidos neste segmento empresarial.

**Figura 17 - Investimentos em TI nos próximos 5 anos.**

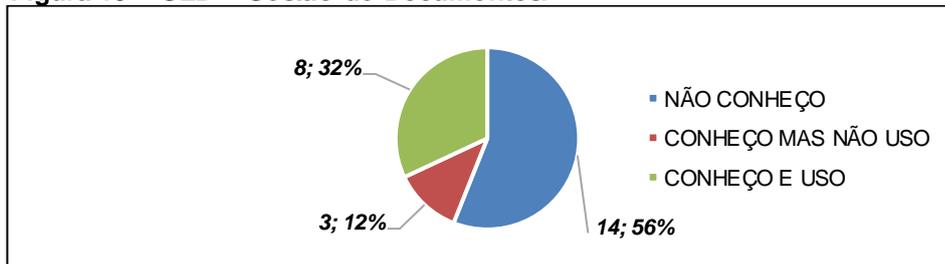


Fonte: Elaborado pelos autores.

#### 4.9 GED - GESTÃO DE DOCUMENTOS

Um resultado surpreendente neste segmento de empresas é evidenciado neste gráfico da figura 18, onde 68% das empresas entrevistadas não usam nenhum tipo de gerenciamento de documentação. É antagônico uma empresa cujo negócio principal é o manuseio e tratamento de documentação, não utilizar uma solução de gestão de documentos.

**Figura 18 – GED – Gestão de Documentos.**

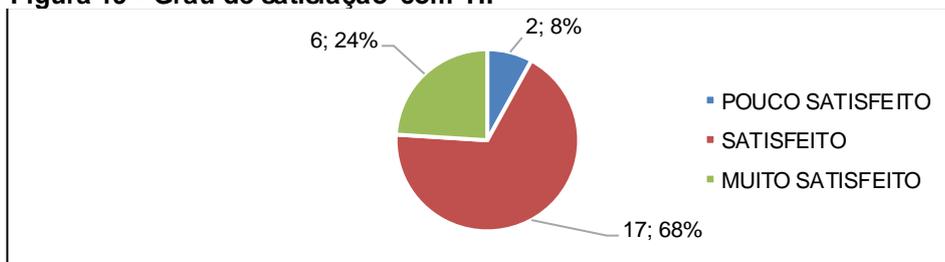


Fonte: Elaborado pelos autores.

#### 4.10 SATISFAÇÃO COM TI NA EMPRESA

Considerando-se o grau de satisfação que as empresas manifestaram sobre a área de TI, pode-se constatar pela figura 19, que a maioria está satisfeita – 68%, e 24% muito satisfeita; conclui-se que quase a totalidade das empresas estão considerando a área de TI como satisfatória; apenas 8% das empresas estão pouco satisfeitas.

**Figura 19 - Grau de satisfação com TI.**



Fonte: Elaborado pelos autores.

## 5 PROPOSTAS DE MELHORIAS

Resultados promissores para área de segurança da informação, pois atualmente as atividades inerentes à tecnologia da informação está voltada aos assuntos relativos a soluções – *software*, e a *hardware* – equipamentos e dispositivos para o funcionamento desta área. Os requisitos relacionados a segurança da informação ainda estão em evolução tímida no que se refere a sua aplicação, portanto uma área propensa a investimentos de médio a longo prazo; a conscientização da relação investimento/benefício ainda não está bem difundida neste segmento. É, portanto, uma oportunidade para os profissionais que estão se formando em segurança da informação atuar no sentido de divulgar as vantagens de se investir nessa área, por exemplo elaborando Políticas de Segurança da Informação, levantamento de ativos e análise de riscos, implantação Gerenciamento Eletrônico de Documentos (GED), haja vista os resultados deste trabalho.

### 5.1 POLÍTICA DE *BACKUP*

Os resultados da pesquisa indicam que a maioria entende que é necessário um plano de *backup*, porém o cuidado na definição da infraestrutura e recursos humanos e metodológicos, parece que ainda está longe de ser alcançada, para muitas empresas da área contábil, pois as perdas de dados são significativas. É um assunto intrínseco à área de segurança da informação.

### 5.2 INVESTIMENTOS EM PESSOAL

O ser humano ainda é um dos principais fatores no cenário de incidentes e perdas de dados. Daí a necessidade de investimentos não somente na contratação de profissionais competentes na área de segurança da informação, mas também que possam transmitir a cultura aos demais colaboradores. A conscientização acerca de uma política de segurança da informação eficaz é o diferencial que pode manter a sobrevivência da empresa, principalmente quando seu negócio depende de informação de valor.

### 5.3 INVESTIMENTOS EM *HARDWARE*

*Hardware* é outro fator que está entre aqueles em que os níveis de incidentes são os mais elevados, provocando perda de dados. Investir em *hardware* somente e não manter uma política de segurança voltada a prevenção de incidentes com o parque informático de uma empresa, é tornar o investimento em despesas futuras, pois sem uma análise de risco e um bom plano de continuidade de negócios, certamente, as perdas continuarão a ocorrer.

### 5.4 INVESTIMENTOS EM *SOFTWARE*

Assim como os investimentos em recursos humanos e em *hardware*, os investimentos em *software* não são menos importantes e necessários, pois a tecnologia está sempre em evolução: novos algoritmos, novos equipamentos para suportá-los e novos conhecimentos para administrá-los. Os resultados desta pesquisa corroboram essa necessidade, pois as perdas de dados decorrentes de falha em *software*, principalmente sistemas operacionais, justificam plenamente os investimentos. Aliado a isso é fundamental uma política de segurança que aborde também a gestão desses *software*, para a prevenção de incidentes, que certamente provocarão perdas financeiras.

## 6 CONCLUSÕES

Face aos resultados da pesquisa de campo, cuja produção de dados e sua origem, fundamentados em metodologias reconhecidas e aplicadas ao trabalho ora apresentado, pode-se afirmar com substancial propriedade que este representativo número de empresas de contabilidade da cidade de Americana, forneceu dados para um mapeamento de toda a região circunvizinha. Foi aplicado o questionário de perguntas objetivas e diretas, sem especificidade nos detalhes, para produzir

resultados práticos e rápidos, evitando interromper os pesquisados em suas atividades diárias por mais que 10 minutos respondendo o questionário.

Os resultados foram surpreendentes em relação às soluções em TI que as empresas adotam; grande parte delas se enquadram em 5 dos 7 itens pesquisados. Observa-se que existe pela maior parte, a preocupação com preservação dos dados, porém comprova-se que gradativamente há uma queda em relação ao arsenal de soluções apresentadas, que fazem parte da manutenção e preservação dos ativos tangíveis e intangíveis da empresa.

As respostas do questionário, vem a corroborar o parágrafo anterior no que se refere à perda de dados. Percebe-se que mesmo com um plano de *backup*, as perdas de dados pela falta deste, falha de *hardware*, falha de software e falha humana, são significativas. A situação indica a necessidade de uma ação rápida para mitigar os incidentes gerados por esses fatores comprovadamente de risco.

No bloco de questões voltadas predominantemente ao contexto financeiro dessas empresas, a preocupação com as perdas de dados, é claramente percebida pelas respostas, onde a maioria das empresas ainda investem e pretendem continuar os investimentos nos próximos anos.

Finalizando o questionário, em relação a GED, nota-se que poucas empresas conhecem e usam o recurso; a maioria desconhece, e afirmam usar soluções caseiras, desconhecendo também os riscos que tais soluções potencializam.

Em termos de satisfação com TI na empresa, a grande maioria se mostrou satisfeitos a muito satisfeitos.

As questões levantadas indicam possibilidades a se explorarem no sentido de quantificar e qualificar o tratamento de informações de valor nesse ramo, podendo estender à empresas de outras áreas, em trabalhos futuros; implementar a quantidade de empresas na pesquisa, estender o nível da pesquisa abordando mais profundamente os aspectos das atividades relacionadas neste trabalho, elaboração de roteiro para levantamento dos riscos de segurança dessas empresas, envolvendo os recursos materiais e humanos, gestão de investimentos e também produzir material instrucional que, fazendo uso dos conhecimentos aqui elencados, resulte numa lista de requisitos que devam ser atendidos, ponderados conforme sua criticidade em relação ao processo inerente dentro de cada empresa do setor.

## 7 AGRADECIMENTOS

Os autores agradecem ao Centro Paula Souza e em especial à FATEC Americana pelos subsídios acadêmicos à pesquisa. Também agradecem aos entrevistados na pesquisa de campo pela disponibilização dos dados, e ao orientador Professor Me. Edson Roberto Gaseta pelos preciosos comentários e direcionamentos, que foram de grande valia para a evolução do presente trabalho.

## 8 REFERÊNCIAS

ABNT – NBR ISO/IEC 27002:2013 **Tecnologia da Informação** – Técnicas de segurança – Código de prática para a gestão de segurança da informação. Disponível em: <<http://abntcatalogo.com.br/norma.aspx?ID=215545813>> Acesso em: 16 maio 2018;

BACULA SYSTEMS. **Enterprise backup and support**. Disponível em: <<http://www.bacula.com>>. Acesso em: 14 jun. 2018;

CERVO, Amado Luiz; BEVIAN, Pedro Alcino. A pesquisa: noções gerais. **Metodologia científica: para uso dos estudantes universitários**. São Paulo: Mc Graw-Hill do Brasil. 1976, Cap.3, p. 65-70;

COMPUTER ASSOCIATES, Inc. **Data protection solutions** – *backup, disk to disk, replications, high availability*. Disponível em: <<http://arcserve.com/us>>. Acesso em: 25 maio 2018;

DA SILVA, Eder Janeo. **Tipos de pesquisa** – conceitos Disponível em: <<https://pt.scribd.com/doc/73499641/Tipos-de-Pesquisa-Conceitos>>. Acesso em: 8 maio 2018;

DEL-BUONO, Regina C. **O que é pesquisa básica ou científica?** Artigo publicado em 03/05/2015. Disponível em: <<http://www.abntouvancouver.com.br/2015/05/o-que-e-pesquisa-basica-ou-aplicada.html>>. Acesso em: 14 maio 2018;

DUARTE, Vania M. Nascimento. **Pesquisa Quantitativa e Qualitativa**. Disponível em: <<http://monografias/brasilecola.uol.com.br/regrasabnt/pesquisa-quantitativa-qualitativa.htm>>. Acesso em: 10 jun. 2018;

E-MASTERS INFORMÁTICA & TECNOLOGIA. **A importância do backup**, 2013. Disponível em: <[www.emastertecnologia.com.br](http://www.emastertecnologia.com.br)>. Acesso em: 22 ago. 2018;

GIL, A.C. **Métodos e técnicas de pesquisa social**. 6 ed. São Paulo: Atlas, 2008;

LAKATOS, E. Maria; MARCONI, M. de Andrade – **Fundamentos de metodologia científica** – SP, 7 ed., Atlas, 2010;

LEÃO, Itagiba C. Carneiro – **Estudo de viabilidade de com enfoque experimental para a implantação de sistema de backup open source em ambiente corporativo**. Disponível em: <[tcc.ecomp.poli.br/20102/TCC\\_Itagiba\\_Final.pdf](http://tcc.ecomp.poli.br/20102/TCC_Itagiba_Final.pdf)> Acesso em: 15 ago. 2018;

MICROSOFT TECHNET. **Conceitos de backup**. Disponível em: <<http://technet.microsoft.com/pt>>. Acesso em: 24 set. 2018;

PRESTON, W. Curtis. **Backup central**. Disponível em: <<http://www.backupcentral.com>>. Acesso em: 16 set. 2018;

PRESTON, W. Curtis. **Backup & recovery**. Sebastopol, Ca: O'Reilly Media, Inc., 2006. Disponível em: <<http://books.google.com?id=6-w4fXbBlnC&>>. Acesso em: 17 set 2018;

SCHNEIDER, Charles. **Desmistificando a continuidade do negócio** - uma análise do cenário brasileiro. São Paulo, 2 out. 2003. Disponível em: <[axurblog.blogspot.com/2003](http://axurblog.blogspot.com/2003)> Acesso em: 18 maio 2018.

**INDICE DE FIGURAS**

Figura 1 - Pesquisa de Campo - Questionário pag.1 .....	5
Figura 2 - Pesquisa de Campo - Questionário pag.2 .....	6
Figura 3 – Gráfico Nº de funcionários .....	7
Figura 4 - Soluções que a empresas adotam .....	7
Figura 5 - Gráfico Nº empresas - Perda de dados .....	9
Figura 6 - Ataque por <i>Ransomware</i> .....	9
Figura 7 - Ataque de vírus. ....	9
Figura 8 - Ataque por <i>Hacker</i> . ....	10
Figura 9 - Falha de <i>Software</i> . ....	10
Figura 10 - Falha de <i>Hardware</i> . ....	10
Figura 11 - Falha Humana. ....	11
Figura 12 - Falha por falta de <i>backup</i> .....	11
Figura 13 - Prejuízos financeiros no último ano, .....	11
Figura 14 - Prejuízos financeiros nos últimos 5 anos. ....	12
Figura 15 - Investimentos em TI no último ano. ....	12
Figura 16 - Investimentos em TI nos últimos 5 anos.....	12
Figura 17 - Investimentos em TI nos próximos 5 anos. ....	13
Figura 18 – GED – Gestão de Documentos.....	13
Figura 19 - Grau de satisfação com TI.....	13



---

**Faculdade de Tecnologia de Americana**

Sergio Seidji Mitsunaga  
Thiago Ramos Nunes Pereira

**A IMPORTÂNCIA DO BACKUP EM PEQUENAS EMPRESAS:  
o backup em empresas de contabilidade de Americana**

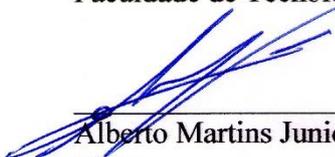
Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo Centro Paula Souza – FATEC Faculdade de Tecnologia de Americana.  
Área de concentração: Informática.

Americana, 08 de dezembro de 2018.

**Banca Examinadora:**

  
\_\_\_\_\_  
Edson Roberto Gasetta (Presidente)  
Especialista  
Faculdade de Tecnologia de Americana

  
\_\_\_\_\_  
Maria Cristina Aranda (Membro)  
Doutora  
Faculdade de Tecnologia de Americana

  
\_\_\_\_\_  
Alberto Martins Junior (Membro)  
Mestre  
Faculdade de Tecnologia de Americana