

**UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL  
ESCOLA DE ADMINISTRAÇÃO  
DEPARTAMENTO DE CIÊNCIAS ADMINISTRATIVAS**

**Carlos Barum Velloso da Silveira**

**UM ESTUDO DAS NECESSIDADES DAS  
MICROEMPRESAS EM GARANTIR A INTEGRIDADE  
DOS SEUS DADOS DIGITAIS**

**Porto Alegre  
2010**

**Carlos Barum Velloso da Silveira**

**UM ESTUDO DAS NECESSIDADES DAS  
MICROEMPRESAS EM GARANTIR A INTEGRIDADE  
DOS SEUS DADOS DIGITAIS**

Trabalho de conclusão do curso de graduação apresentado ao Departamento de Ciências Administrativas da Universidade Federal do Rio Grande do Sul, como requisito parcial para a obtenção do grau de Bacharel em Administração.

Orientador: Prof. José Carlos Fiorioli

**Porto Alegre  
2010**

**CARLOS BARUM VELLOSO DA SILVEIRA**

**UM ESTUDO DAS NECESSIDADES DAS MICROEMPRESAS EM  
GARANTIR A INTEGRIDADE DOS SEUS DADOS DIGITAIS**

Trabalho de conclusão do curso de graduação apresentado ao Departamento de Ciências Administrativas da Universidade Federal do Rio Grande do Sul, como requisito parcial para a obtenção do grau de Bacharel em Administração.

Conceito final.....

Aprovado em.....de.....de.....

**BANCA EXAMINADORA**

---

Prof. Hugo Fridolino Müller Neto - UFRGS

---

Orientador – Prof. José Carlos Fiorioli – UFRGS

## RESUMO

A utilização da Tecnologia da Informação (TI) vem sendo cada vez mais presente no cotidiano das microempresas. Adotada inicialmente como ferramenta de apoio às atividades empresariais, inovações tecnológicas fizeram da TI um elemento crítico no processo produtivo de algumas microempresas. Entretanto, a disponibilidade destes recursos enfrenta riscos já amplamente discutidos na literatura. A fim de conhecer detalhes sobre a utilização da Tecnologia da Informação por parte das microempresas, realizou-se uma pesquisa exploratória utilizando o método de entrevistas semi-estruturadas com profissionais ligados ao tema. Entre os principais resultados obtidos, destacam-se necessidades fundamentais relacionadas à manutenção da integridade dos dados digitais das microempresas, como: *hardware* confiável, *software* antivírus, conhecimento técnico por parte dos usuários e serviços de manutenção.

Palavras-chave: Microempresas; Segurança de dados; Tecnologia da Informação.

# Agradecimentos

À UFRGS e todos os seus profissionais que proporcionam a nós, estudantes, um ambiente saudável e favorável à construção do conhecimento. Dentre estes profissionais, um agradecimento especial aos trabalhadores das bibliotecas, cujo suporte tem sido essencial aos nossos estudos.

Aos nossos professores, que ficarão na minha memória como amigos.

Ao meu professor orientador José Carlos Fiorioli, por seu inestimável apoio à conclusão deste trabalho.

Aos profissionais e empresas que colaboraram com este estudo, entre eles Alexandre Santos, André Möller, Henrique Mendes, Digimer, Soma e CGK.

À minha família, cujos exemplos sempre influenciaram positivamente a minha vida.

## LISTA DE ILUSTRAÇÕES

Quadro 1 - Classificação das Micro e Pequenas Empresas.....	12
Gráfico 1 - Evolução do PIB da Regional Metropolitana de Porto Alegre.....	21
Quadro 2 – Necessidades relacionadas à segurança dos dados digitais.....	32
Quadro 3 – Programa geral de ações.....	33

## LISTA DE TABELAS

Tabela 1 - Distribuição das empresas por setor da economia.....	21
Tabela 2 – Distribuição de empregos por setor da economia.....	22

## SUMÁRIO

<b>1</b>	<b>INTRODUÇÃO .....</b>	<b>10</b>
1.1	CENÁRIO .....	10
1.2	AS MICROEMPRESAS.....	11
<b>2</b>	<b>DELIMITAÇÃO DO PROBLEMA.....</b>	<b>13</b>
<b>3</b>	<b>JUSTIFICATIVA.....</b>	<b>14</b>
<b>4</b>	<b>OBJETIVOS.....</b>	<b>16</b>
4,1	OBJETIVO GERAL .....	16
4.2	OBJETIVOS ESPECÍFICOS .....	16
<b>5</b>	<b>REVISÃO TEÓRICA .....</b>	<b>17</b>
5.1	OS RISCOS À INTEGRIDADE DOS DADOS DIGITAIS.....	17
5.2	A IMPORTÂNCIA DAS MICROEMPRESAS .....	20
<b>6</b>	<b>MÉTODO .....</b>	<b>23</b>
<b>7</b>	<b>OBTENÇÃO E APRESENTAÇÃO DOS DADOS COLETADOS .....</b>	<b>25</b>
7.1	<i>HARDWARE</i> .....	26
7.2	<i>SOFTWARE</i> .....	27
7.3	FATOR HUMANO .....	28
7.4	OS SERVIÇOS DE MANUTENÇÃO .....	28
<b>8</b>	<b>ANÁLISE DE DADOS E RESULTADOS OBTIDOS .....</b>	<b>30</b>
8.1	A UTILIZAÇÃO DA TI POR PARTE DAS MICROEMPRESAS .....	30

8.2	PRINCIPAIS AMEAÇAS À SEGURANÇA DOS DADOS DIGITAIS DAS MICROEMPRESAS.....	31
8.3	NECESSIDADES DAS MICROEMPRESAS EM GARANTIR A INTEGRIDADE DOS SEUS DADOS DIGITAIS .....	31
8.4	ALTERNATIVAS PARA DESENVOLVEDORES DE SOLUÇÕES DE SEGURANÇA.....	34
<b>9</b>	<b>CONSIDERAÇÕES FINAIS .....</b>	<b>35</b>
	<b>REFERÊNCIAS.....</b>	<b>36</b>
	<b>APÊNDICE A – ROTEIRO DA ENTREVISTA AO ESPECIALISTA EM REDES.....</b>	<b>39</b>
	<b>APÊNDICE B – ROTEIRO DAS ENTREVISTAS AOS EMPRESÁRIOS ..</b>	<b>40</b>
	<b>APÊNDICE C – ROTEIRO DA ENTREVISTA AO ESPECIALISTA EM TI.....</b>	<b>41</b>
	<b>APÊNDICE D – ROTEIRO DA ENTREVISTA AOS FORNECEDORES ..</b>	<b>42</b>
	<b>ANEXO A – CONTRATO DE MANUTENÇÃO .....</b>	<b>43</b>
	<b>GLOSSÁRIO.....</b>	<b>44</b>

## 1 INTRODUÇÃO

Vivemos uma época em que os computadores estão cada vez mais presentes em nossas vidas, seja para uso pessoal ou profissional. Hoje em dia, a Tecnologia da Informação (TI), conceituada por TURBAN *et al* (2009) como a soma de todos os sistemas de computação usados por uma empresa, tornou-se uma ferramenta praticamente indispensável às suas atividades.

À parte os benefícios oriundos deste novo paradigma, o uso de computadores envolve alguns cuidados que podem não ser observados pela totalidade dos seus adeptos. Uma das propostas deste trabalho é reunir e analisar informações pertinentes a esta situação.

### 1.1 CENÁRIO

Criados para realizar cálculos numéricos precisos e em tempo reduzido, os computadores foram ganhando mais versatilidade ao longo dos anos, incorporando inovações proporcionais ao crescente desenvolvimento tecnológico. Estas inovações tornaram os computadores capazes de armazenar e processar um volume cada vez maior de dados. Convertidos para o chamado formato digital, estes dados são representados apenas pelos símbolos 0 e 1 (GALLO; HANCOCK, 2003). Dada sua natureza, para fins deste estudo, estes dados serão chamados dados digitais, independentemente do seu volume ou conteúdo.

A importância destas considerações iniciais recai no advento do uso de computadores pessoais para realizar inúmeras tarefas, tais como: transações financeiras, sejam elas bancárias ou mesmo compra de bens e serviços; comunicação, por exemplo, através de *e-mails*; armazenamento de dados, sejam eles pessoais ou comerciais (CERT.br, 2005). Estas tarefas também estão

presentes no cotidiano das empresas, e muitas delas têm significado crucial nos seus processos. O risco de destruição, roubo ou até mesmo desorganização dos dados digitais faz da sua integridade motivo de justificado interesse.

Como exemplo do que se considera integridade dos dados digitais, segue definição encontrada na Cartilha de Segurança para Internet - Parte I: Conceitos de Segurança (CERT.br, 2005, p.3): “Um computador (ou sistema computacional) é dito seguro se este atende a três requisitos básicos relacionados aos recursos que o compõem: confidencialidade, integridade e disponibilidade”.

Para melhor entendimento destes requisitos, a mesma obra apresenta uma breve explicação (CERT.br, 2005, p.3):

A confidencialidade diz que a informação só está disponível para aqueles devidamente autorizados; a integridade diz que a informação não é destruída ou corrompida e o sistema tem um desempenho correto, e a disponibilidade diz que os serviços/recursos do sistema estão disponíveis sempre que forem necessários.

Empresas de grande porte dispõem de recursos para investir em tecnologia e contratar profissionais especializados, possibilitando manter as ameaças à integridade dos seus dados digitais em um nível muito reduzido. Porém, uma vez que as empresas de pequeno porte não têm a mesma capacidade de investimento, quais fatores lhes permitiriam enfrentar com eficácia estas ameaças? Coletar e organizar informações relevantes ao tema faz parte do esforço em responder a este questionamento.

## 1.2 AS MICROEMPRESAS

Temos, no Brasil, uma classificação das empresas em função de seu faturamento. A LEI COMPLEMENTAR Nº 123, de 14 de Dezembro de 2006 (BRASIL, 2006) considera Microempresa:

a sociedade empresária, a sociedade simples e o empresário devidamente registrados no Registro de Empresas Mercantis ou no Registro Civil de Pessoas Jurídicas, conforme o caso, que aufera, em cada ano-calendário, receita bruta igual ou inferior a R\$ 240.000,00.

Em comparação às pequenas empresas, a classificação por faturamento bruto, estabelecida pela Lei Geral da Micro e Pequena Empresa, é apresentada no Quadro 1 (SEBRAE, 2007).

Porte	Faturamento
Microempresa	Até R\$ 240.000,00
Pequena empresa	De R\$ 240.000,00 a R\$ 2.400.000,00

**Quadro 1 – Classificação das Micro e Pequenas Empresas**

Fonte: SEBRAE

Esta breve comparação nos permite imaginar o quão reduzida pode ser a capacidade da microempresa de investir em infra-estrutura de TI. Ainda assim, quanto mais importantes forem os dados digitais da empresa, mais necessário será garantir sua integridade.

## 2 DELIMITAÇÃO DO PROBLEMA

É provável que empresas de maior porte tenham um departamento de TI com equipamentos de qualidade e profissionais especializados, contratados para garantir o bom funcionamento deste setor.

Reconhecendo que a capacidade de investimento em infra-estrutura da microempresa não chega a este nível pode-se imaginar que a sua utilização da Tecnologia da Informação também seja bem diferente. No entanto, os benefícios do uso de computadores na gestão da microempresa são cada vez mais interessantes, à medida que a tecnologia incorpora novas possibilidades à TI. Além disso, a TI pode ser usada não somente como um apoio à gestão, mas também como parte do produto oferecido pela microempresa ao seu cliente. Por exemplo, uma empresa que tem um cadastro de clientes armazenado em computador fica dependente destes dados digitais para obter informações de seus clientes. Diferentemente, uma empresa que trabalha com criação de conteúdo para *internet*, utiliza computadores de forma mais intensa, e será incapaz de entregar a seus clientes o produto final se perder a capacidade de acessar os dados digitais correspondentes ao seu trabalho. Neste sentido, este estudo é focado nas necessidades apresentadas por microempresas cuja integridade dos seus dados digitais é tão importante que pode comprometer as atividades essenciais e normais para as quais a empresa se constituiu.

### 3 JUSTIFICATIVA

Tomando como pressuposto que a integridade dos dados digitais de algumas microempresas é condição fundamental para o seu funcionamento, surgiu um questionamento a respeito de como elas lidam com esta questão. Afinal, existem várias ameaças que podem inutilizar dados digitais, e elas só evoluem com o passar do tempo. Shipley (2008), afirma: “[...] estão se expandindo em um ritmo inexorável e voltar no tempo não é uma opção”.

Se é verdade que existem produtos desenvolvidos com o intuito de oferecer segurança disponíveis no mercado, também é verdade que as ameaças aos dados digitais fazem vítimas, apesar de tudo. “Nossos adversários passaram de *hackers* que invadiam computadores como um passatempo a criminosos organizados” (SHIPLEY, 2008). Faz-se necessário o desenvolvimento de novas soluções, que acompanhem a evolução da tecnologia e das dificuldades que estão a surgir.

A questão da integridade dos dados digitais se torna mais intrigante ao observarmos que as microempresas, apesar de não terem a mesma capacidade das grandes empresas, também precisam investir em segurança. Sob esta ótica, parece fazer sentido considerá-la como um segmento diferenciado, dotado de suas próprias necessidades. Porém, quais são estas necessidades, e o que as determina?

Projetar e entregar produtos que satisfaçam estas necessidades é uma tarefa que tem como foco primário o consumidor (FERREL; HARTLINE, 2005). Estudar sua realidade é de grande importância. “O profissional de marketing precisa tentar compreender as necessidades do mercado-alvo, seus desejos e suas demandas” (KOTLER 2000, p.33).

Considerando que não há evidências de muitos estudos voltados ao tema específico das necessidades relativas à integridade dos dados digitais das

microempresas, surge a proposta deste trabalho, que consiste em obter e organizar informações que levem na direção da satisfação deste segmento de mercado.

## 4 OBJETIVOS

A seguir são apresentados os objetivos que orientam este estudo.

### 4.1 OBJETIVO GERAL

Desenvolver um programa geral de ações de manutenção da segurança dos dados digitais de microempresas com baixa capacidade de investimentos em Tecnologia da Informação.

### 4.2 OBJETIVOS ESPECÍFICOS

- Caracterizar a utilização da TI por parte das microempresas;
- Identificar as principais ameaças à segurança dos dados digitais das microempresas (situações de vulnerabilidade);
- Identificar necessidades deste nicho consumidor de produtos voltados à segurança de dados digitais;
- Sugerir alternativas para desenvolvedores de soluções de segurança, interessados em oferecer produtos mais adequados às microempresas.

## 5 REVISÃO TEÓRICA

Segundo Ferrel e Hartline (2005), uma das partes básicas do marketing, o produto e as decisões em torno dele estão entre os aspectos mais importantes da estratégia de marketing. Essa importância depende da conexão entre o produto e as necessidades do consumidor. “A decisão do consumidor de comprar um produto ou conjunto de produtos em vez de outro é antes de tudo uma função do quanto essa escolha satisfará suas necessidades e desejos” (FERREL; HARTLINE, 2005, p. 10).

O papel desempenhado pelo marketing na sociedade envolve atividades que provém satisfação aos consumidores (KOTLER, 2000). Para isto, é necessário reconhecer e compreender as necessidades e desejos dos consumidores (SCHEWUE; SMITH, 1982).

Porém, segundo Kotler (2000) “Compreender as necessidades e os desejos dos clientes nem sempre é uma tarefa fácil. Alguns consumidores têm necessidades das quais não têm plena consciência. Ou não conseguem articular essas necessidades”. Dadas estas dificuldades, muitas vezes é necessário que haja um conhecimento prévio da realidade do mercado-alvo, bem como a identificação de necessidades que possam ser satisfeitas através de um produto.

Entre outros aspectos, as necessidades apresentadas pelas microempresas em relação à integridade dos seus dados digitais são pautadas pelos tipos de riscos aos quais eles estão expostos. Atender a estas necessidades envolve, entre outras coisas, conhecer quais são estes riscos.

### 5.1 OS RISCOS À INTEGRIDADE DOS DADOS DIGITAIS

Os computadores atuais armazenam estes dados em diferentes tipos de dispositivos, internos ou externos, para posterior referência e processamento. Um

dispositivo muito comum de armazenamento é o disco rígido: meio magnético de armazenamento de dados (JUNIOR, 2008), encontrado nos computadores pessoais. Pode ser ligado ao computador externamente como um meio portátil.

Vale ressaltar que os recursos digitais são recursos eletrônicos, que só estarão disponíveis se houver disponibilidade de energia elétrica. Tanto a interrupção no fornecimento de energia elétrica quanto sua estabilidade são cruciais à disponibilidade dos dados e à sua integridade, uma vez que, sobrecargas elétricas podem danificar equipamentos eletrônicos. Além disso, incêndios, enchentes, ou outros desastres naturais podem prejudicar sistemas computacionais (LAUDON; LAUDON, 2007). Também por estes motivos o local de armazenamento do meio que contém dados importantes deve ser cuidadosamente escolhido (CERT.br, 2005).

É importante observar também que dispositivos eletrônicos têm uma vida útil. Os termos de garantia de cada um deles pode ser uma forma de estimar sua durabilidade.

A *internet* também é uma fonte de ataques que podem comprometer a integridade dos dados digitais. Para Laudon e Laudon (2007) a vulnerabilidade decorre da abertura a praticamente qualquer um, e, quando há abusos, pode resultar em prejuízos de enormes proporções. O uso disseminado de *e-mail* faz parte deste tipo de ameaça oriunda da *internet* pois permite anexar conteúdo que possibilita a ação de *softwares* mal-intencionados ou acesso não autorizado a sistemas corporativos internos (LAUDON; LAUDON, 2007; CERT.br, 2005). Este tipo de *software*, chamado *malware*, pode incluir uma variedade de ameaças, tais como vírus de computador, *worms* e cavalos de Tróia. Vírus de computador é um tipo de programa de *software* espúrio que infecta outros programas de *software* ou arquivos de dados a fim de ser executado, geralmente sem conhecimento nem permissão do usuário. *Worms* são programas de computador independentes que copiam a si próprios, dependendo menos do comportamento humano para se disseminar. Diferentemente dos vírus, eles podem funcionar sozinhos, sem a necessidade de se anexar a outros arquivos de programa. Os *worms* destroem dados e programas, assim como prejudicam e até interrompem o funcionamento de redes de computadores. O cavalo de Tróia em si não é um vírus, mas sua função envolve criar uma abertura no sistema para que vírus ou outros códigos mal-

intencionados entrem no sistema de computador, permitindo até mesmo que a pessoa que originou o ataque assuma controle sobre o sistema em questão (LAUDON; LAUDON, 2007; TURBAN *et al*, 2009).

Para evitar ameaças deste tipo, os computadores devem utilizar programas antivírus. Estes programas devem ser atualizados periodicamente, caso contrário poderão não detectar os vírus mais recentes (CERT.br, 2005).

Quando pensamos em ameaças à segurança de uma empresa, tendemos a pensar em algo que se origina fora da organização. Mas, segundo Laudon e Laudon (2007) pesquisas concluíram que a falta de conhecimento dos usuários é a maior causa isolada de falhas na segurança de redes. Danificação, por uso impróprio ou atividades criminosas, ou configuração inapropriada também fazem com que os sistemas não funcionem como deveriam (LAUDON; LAUDON, 2007; TURBAN *et al*, 2009). Usuários podem causar danos ao introduzir erros ou ao acessar sistemas sem autorização (LAUDON; LAUDON, 2007; TURBAN *et al*, 2009). No caso de uma empresa que conta com um departamento de Tecnologia da Informação, Turban *et al* (2009) consideram extremamente importante o bom relacionamento entre os técnicos deste departamento e o usuário final, mas considera esta uma tarefa difícil, já que estes tem personalidades, estilo cognitivo e nível de conhecimento técnico diferentes. Dentre as alternativas para compensar esta situação, Turban *et al* (2009) sugerem promover o treinamento dos usuários e desenvolver um plano de recuperação de falhas para cada uma das unidades usuárias, de modo a reduzir as interferências em seu trabalho quando um sistema falha.

Neste sentido, garantir a segurança destas informações é um objetivo que envolve diferentes tomadas de decisão e consequentes iniciativas. Para Laudon e Laudon (2007, p. 210), o termo segurança: "...abarca as políticas, procedimentos e medidas usados para impedir acesso não autorizado, alteração, roubo ou danos físicos a sistemas de informação".

É preciso que o gestor da empresa saiba quais são as informações, na forma de dados digitais, que exigem proteção e em que medida são vulneráveis. Além disso, determinar quais usuários produz, controla e manipula essas informações, quais políticas de segurança já estão em curso para proteger essas informações e qual nível de risco a administração está disposta a aceitar para cada um dos ativos é

fundamental para criar um programa voltado à proteção dos dados mais importantes da empresa (LAUDON; LAUDON, 2007; TURBAN *et al*, 2009). Os administradores da empresa, com o apoio de especialistas em sistemas de informação, podem determinar o valor dos ativos de informação e quanto custará atingir um nível de risco aceitável, os pontos de vulnerabilidade, a frequência provável de um problema e seu prejuízo potencial. Com base nestas informações torna-se possível estabelecer uma hierarquia para os riscos e identificar metas de segurança aceitáveis para lidar com estes riscos (LAUDON; LAUDON, 2007).

Investir em segurança não tem relação direta com aumento de receita. Mas pode ser crucial ao funcionamento da empresa. Quando os recursos de TI ficam indisponíveis algumas empresas podem sofrer perdas totais de negócios. Neste contexto, ao gerir uma empresa que utiliza TI, é preciso pensar em segurança e controle como prioridades (LAUDON; LAUDON, 2007).

## 5.2 A IMPORTÂNCIA DAS MICROEMPRESAS

Foco deste estudo, as microempresas foram alvo de um levantamento do SEBRAE/RS, realizado em 2009, que dá indícios da sua importância para a economia brasileira.

O estudo do SEBRAE/RS (2009) explica que:

No Brasil, as informações sobre as micro e pequenas empresas (MPEs) ainda são pouco disponíveis por órgãos oficiais, comparadas à importância deste segmento na economia do País. Tal fato resulta uma carência de conhecimento sobre os pequenos negócios e dificulta o direcionamento adequado dos recursos disponíveis para a promoção deste segmento.

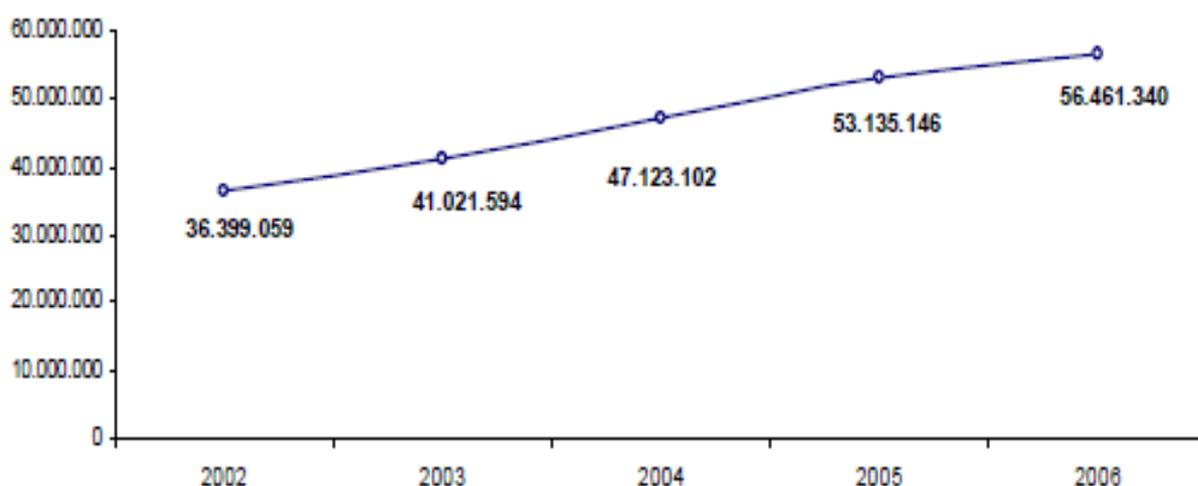
No entanto, há interessantes dados disponíveis em relação às micro e pequenas empresas da Região Metropolitana de Porto Alegre, cidade onde foi realizado o presente estudo.

No ano de 2007 existiam no Brasil 6,9 milhões de empresas formais

No Rio Grande do Sul, que participava com 6,6% do PIB nacional neste período, 99,3% das empresas eram micro e pequenas empresas.

Na regional Metropolitana de Porto Alegre estavam localizadas 193.200 empresas, 99% das quais eram micro e pequenas empresas (SEBRAE/RS, 2009).

A região metropolitana de Porto Alegre responde por 35% do PIB gaúcho (SEBRAE/RS, 2009). Em 2006, o PIB da Regional era de R\$ 56.461.340, tendo apresentado um crescimento de 6% em relação ao ano de 2005, conforme o Gráfico 1 (SEBRAE/RS, 2009).



**Gráfico 1 – Evolução do PIB da Regional Metropolitana de Porto Alegre**

Fonte: SEBRAE/RS

Ainda no ano de 2007, foi mapeada a participação de cada estrato nos setores de atividade econômica. Os resultados podem ser observados na Tabela 1 (SEBRAE/RS, 2009).

**Tabela 1 – Distribuição das empresas por setor da economia**

Setor	Agropecuária		Comércio		Indústria		Serviços		Total	
	Nº de estab	%	Nº de estab	%	Nº de estab	%	Nº de estab	%	Nº de estab	%
Micro	1.820	1	77.223	42	22.419	12	82.819	45	184.281	100
Pequeno	56	1	2.747	37	948	13	3.603	49	7.354	100
Médio	13	1	317	25	224	18	708	56	1262	100
Grande	0	0	34	11	42	14	227	75	303	100
Total	1.889	1	80.321	42	23.633	12	87.357	45	193.200	100

Fonte: SEBRAE/RS

A Tabela 1 ilustra a grande quantidade de microempresas estabelecidas na Região Metropolitana de Porto Alegre. O reflexo desta situação na sociedade pode ser observado na Tabela 2, onde está mapeada a distribuição de empregos por setor e porte empresarial (SEBRAE, 2009).

**Tabela 2 – Distribuição de empregos por setor da economia**

Setor	Agropecuária		Comércio		Indústria		Serviços		Total	
	Nº de empregados	%	Nº de empregados	%	Nº de empregados	%	Nº de empregados	%	Nº de empregados	%
Micro	1.988	1	49.934	36	30.300	22	56.827	41	139.049	100
Pequeno	1.308	1	49.477	31	38.898	24	71.631	44	161.314	100
Médio	912	1	30.186	20	45.790	31	71.080	48	147.968	100
Grande	0	0	15.676	4	46.450	11	369.230	86	431.356	100
Total	4.208	0,5	145.273	16,5	161.438	18	568.768	65	879.687	100

Fonte: SEBRAE/RS

## 6 MÉTODO

A fim de atingir os objetivos já definidos é fundamental seguir um procedimento sistemático para realizar o estudo. Assim, faz-se necessário escolher um método eficaz que permita solucionar o problema proposto.

Conforme Malhotra (2001), a pesquisa de marketing é a ferramenta capaz de fornecer informações precisas que reflitam fielmente uma situação. Neste trabalho, o uso da pesquisa pode colaborar para que os objetivos propostos sejam alcançados.

Segundo Ferrel e Hartline (2005, p. 13): “Os profissionais de marketing estão acostumados a fazer e analisar pesquisas, especialmente com respeito às necessidades, opiniões e atitudes de seus consumidores”.

Para Mattar (1996), pesquisa de marketing caracteriza-se como:

investigação sistemática, controlada, empírica e crítica de dados com o objetivo de descobrir e (ou) descrever fatos e (ou) de verificar a existência de relações presumidas entre fatos (ou variáveis) referentes ao marketing de bens, serviços, idéias ao marketing como área de conhecimento de administração.

Inicialmente, é fundamental a delimitação da questão a ser respondida, tomando-se o cuidado em não limitar, nem tornar o estudo amplo demais (KOTLER, 2000). Para Malhotra (2001): “Somente depois da definição clara do problema é que a pesquisa pode ser concebida e realizada de forma adequada”. Neste estudo, conforme os objetivos já relacionados, a questão central refere-se a quais necessidades devem ser atendidas para a manutenção da integridade dos dados digitais das microempresas.

Complementarmente, a respeito da pesquisa de marketing, Malhotra (2001, p.105) afirma que a mesma “pode ser classificada de forma ampla como exploratória ou conclusiva”.

Enquanto a pesquisa conclusiva utiliza procedimentos formais e estruturados, a pesquisa exploratória é caracterizada por flexibilidade. Raramente envolve

questionários estruturados, grandes amostras e planos de amostragem por probabilidade (MALHOTRA, 2001).

A pesquisa exploratória coleta dados secundários e dados primários. Dados secundários são aqueles coletados originalmente para fins diferentes do problema em pauta (MALHOTRA, 2001).

Dados primários são originados pelo pesquisador para a finalidade específica de solucionar o problema em pauta (MALHOTRA, 2001).

Conforme Malhotra (2001, p. 128) existe uma regra geral que colabora fortemente para a pesquisa de marketing:

O exame dos dados secundários disponíveis é um pré-requisito para a coleta de dados primários. Comece com dados secundários, prossiga até os dados primários somente quando as fontes de dados secundários estiverem esgotadas ou produzam retornos apenas marginais.

Com relação à obtenção dos dados, Aaker (2007), Malhotra (2001), Mattar (1996) e Zikmund (2006) identificam as entrevistas individuais em profundidade como método comum de coleta de dados.

Ao se construir as conclusões acerca das informações obtidas, faz-se a análise dos dados obtidos baseada nas etapas anteriores do processo, nas características conhecidas dos dados, em propriedades de técnicas estatísticas e na formação e filosofia do pesquisador (MALHOTRA 2001).

Para Zikmund (2006), a análise é uma aplicação da lógica para o entendimento dos dados obtidos. Envolve a determinação de padrões consistentes e resume detalhes relevantes revelados na investigação.

Como última etapa, o pesquisador apresenta suas conclusões. Deve apresentar conclusões importantes, que sejam relevantes para as principais decisões de marketing relativas à organização (KOTLER, 2000). Malhotra (2001) recomenda que "...em lugar de simplesmente resumir os dados estatísticos, o pesquisador deve apresentá-los de maneira a que possam ser usados diretamente como dados orientadores na tomada de decisão".

## 7 OBTENÇÃO E APRESENTAÇÃO DOS DADOS COLETADOS

Levando-se em consideração o caráter incipiente do tema em estudo, foi realizada uma pesquisa exploratória, a fim de prover critérios e compreensão a respeito da utilização da TI por parte das microempresas (MALHOTRA, 2001).

Inicialmente, procurou-se fontes de dados secundários. Levou-se em consideração 25 anos da experiência pessoal do autor no uso de computadores, consultas a *sites* e livros especializados em TI, participação no 3º Fórum Internacional de TI Banrisul, (realizado em 05 e 06 de abril de 2010). Os dados obtidos serviram para fornecer uma idéia mais concreta a respeito das ameaças conhecidas à integridade de dados digitais.

Numa segunda etapa foi elaborada uma relação de pessoas que, por terem algum tipo de contato com microempresas, pudessem prover dados relevantes à pesquisa. Deste universo foram selecionadas 13 pessoas para entrevistas semi-estruturadas:

- 3 especialistas em TI;
- 1 fornecedor de *hardware* para armazenamento de dados e de *softwares* voltados à proteção de dados;
- 1 fornecedor de equipamentos para computadores Macintosh;
- 1 fornecedor de softwares voltados à proteção de dados;
- 3 microempresários
- Funcionários das empresas participantes.

Por motivos de segurança o nome das empresas não podem ser revelados (neste trabalho, as mesmas serão denominadas A, B e C por solicitação dos responsáveis).

A empresa A tem por atividade manutenção de equipamentos eletrônicos, contando com uma extensa base de dados armazenada no formato digital. Perder estas informações comprometeria gravemente sua produção.

A empresa B vive uma situação semelhante, sendo que possui informações de clientes e prestadores de serviços na sua base de dados. Da mesma forma, teria suas atividades comprometidas em caso de perda dos dados digitais.

A empresa C utiliza seus computadores para produzir imagens para fins publicitários. Em caso de perda destes dados, fica impossibilitada de entregar seus produtos aos seus clientes.

A fim de tornar mais clara a análise das entrevistas, as respostas foram agrupadas por tópicos.

## 7.1 HARDWARE

As entrevistas com especialistas, microempresários e revendedores apontaram o disco rígido como principal dispositivo de armazenamento de dados digitais utilizados pelas microempresas. No entanto, o entrevistado da empresa A opinou sobre a conveniência de utilizar serviço de armazenamento de dados à distância (*cloud computing*): “Não estou totalmente satisfeito da maneira que eu trabalho. O ideal pra mim seria ter o *backup* todo em FTP. Todo um protocolo de transferência em outro lugar”.

André Möller, especialista em TI também aponta o serviço de *cloud computing* como um alternativa, porém exige confiança no prestador de serviço:

[...] essa empresa tem que ser uma empresa que tenha um certo respaldo, uma certa tradição no mercado [...] na prática, se alguém na empresa não é sério, ela pode pegar esses teus dados e vazar, e divulgar pra outras, pra concorrência.

Segundo Alexandre Santos, especialista em redes de computadores da UFRGS, as microempresas optam por comprar um computador pessoal para

armazenar seus dados digitais ao invés de um servidor, o que seria mais recomendável, por escassez de recursos financeiros. Ele observa diferença da qualidade entre as marcas ofertadas, em termos de qualidade.

Para garantir a disponibilidade dos dados digitais nas empresas entrevistadas, todas elas usam *no-break*, dispositivo capaz de manter os equipamentos funcionando em caso de falta no fornecimento de energia elétrica, por, no mínimo 20 minutos. É uma das recomendações do engenheiro Emerson Tormann, especialista em TI.

## 7.2 SOFTWARE

Em todas as microempresas estudadas existe o procedimento de *backup* dos dados digitais considerados essenciais, sendo que em duas delas este processo é feito automaticamente, por *software* desenvolvido para esta tarefa. Para Alexandre Santos este procedimento é indispensável: “[...] não pode deixar de ter uma rotina de backup, bem feita, testada”.

André Möller recomenda também o *backup* para prevenção contra perda dos dados digitais: “É essencial”.

Todos os entrevistados reconhecem a importância dos *softwares* antivírus. Estão presentes em todas as microempresas entrevistadas. Alexandre Santos diz que: “[...] uma empresa não pode deixar de ter antivírus”. No entanto, os revendedores demonstraram que a maioria dos seus clientes parece achar que a simples instalação do antivírus é suficiente para fornecer segurança. Esta mesma idéia é reforçada por Alexandre Santos: “Eles acham que estão totalmente protegidos com aquele *software*”.

Com relação a diferentes sistemas operacionais, Alexandre Santos recomenda os mesmos cuidados a todos, independentemente do sistema utilizado. Em contrapartida, outros entrevistados indicaram que usuários de computadores Macintosh imaginam não estarem expostos às mesmas ameaças.

Em todas as empresas estudadas já houve, em algum momento, a detecção de vírus de computador. Porém, em nenhum caso houve prejuízo decorrente deste fato. Os entrevistados atribuem à constante atualização dos *softwares* antivírus e sistemas operacionais esta possibilidade de se defender das ameaças mais recentes.

### 7.3 O FATOR HUMANO

Nenhuma das pessoas entrevistadas relatou algum caso de danos causados intencionalmente por algum usuário. Apenas a empresa C já teve algum problema causado por erro não intencional na manipulação de seus arquivos digitais, o que lhes causou prejuízo.

O nível de conhecimento a respeito das ameaças à integridade dos dados digitais parece ser razoável entre as pessoas entrevistadas. Conhecem a seriedade da situação e as atitudes mais básicas para evitar falhas. Os funcionários indagados demonstraram interesse em adquirir mais conhecimento a respeito das ameaças à integridade dos dados digitais. No entanto não têm interesse em participar de algum curso sobre o assunto.

Os especialistas entrevistados observaram que, nas empresas de maior porte, os usuários possuem níveis diferenciados de acesso aos dados digitais. Embora esse recurso seja uma medida importante, dificilmente pode ser empregado em microempresas, devido ao seu custo.

### 7.4 OS SERVIÇOS DE MANUTENÇÃO

Conforme observado pelos especialistas, para manter-se prevenido contra as ameaças que evoluem a cada dia, os *softwares* utilizados pela TI devem ser atualizados constantemente. Estes serviços devem estar disponíveis às empresas por parte dos desenvolvedores ou fornecedores de *software*. Neste sentido, Alexandre Santos observa que: “Antivírus gratuito é gratuito para uso caseiro. Se tu

traz (sic) o antivírus gratuito pra dentro de uma empresa, ele é ilegal. Teria que comprar a licença, e toda a questão de licenciamento de *software*".

Duas das empresas entrevistadas recebem semanalmente a visita de um técnico especializado que lhes presta serviço de manutenção. Alexandre Santos recomenda a contratação deste serviço por duas razões: o serviço é especializado e evita que algum funcionário da empresa perca eficiência por acumular tarefas.

Na empresa A é o proprietário que realiza todo serviço de manutenção necessário à sua estrutura de TI, em função da sua capacidade técnica e redução de custos.

## 8 ANÁLISE DE DADOS E RESULTADOS OBTIDOS

O estudo realizado foi satisfatório no que se refere a alcançar os objetivos pré-estabelecidos. As entrevistas realizadas revelaram dados suficientes para se obter as informações desejadas.

### 8.1 A UTILIZAÇÃO DA TI POR PARTE DAS MICROEMPRESAS

Com base nas entrevistas realizadas foi possível estabelecer critérios a respeito de como as microempresas utilizam os recursos da Tecnologia da Informação.

Seus dados digitais mais importantes são armazenados em discos rígidos, sejam dos computadores utilizados nas atividades da empresa, ou em discos para onde cópias de segurança são copiadas.

Utilizam *softwares* antivírus para se defender das principais ameaças à integridade dos seus dados digitais.

Contam com serviço de suporte técnico de um profissional.

Apresentam um conhecimento razoável sobre o que são ameaças à integridade dos seus dados digitais, mas em geral, todos os trabalhadores da empresa se mostram interessados em adquirir conhecimento mais avançado.

## 8.2 PRINCIPAIS AMEAÇAS À SEGURANÇA DOS DADOS DIGITAIS DAS MICROEMPRESAS

As principais situações de vulnerabilidade que as microempresas estudadas poderiam apresentar parecem sob controle. Não houve manifestação grande preocupação com a integridade dos dados digitais por parte dos entrevistados. O uso de equipamento moderno e a prática de *backup* periódico as afasta da possibilidade de ocorrência de danos irreparáveis a seus dados digitais. Além disso, a presença de um profissional com bom nível de conhecimento nas empresas, ainda que semanalmente colabora para que qualquer situação de risco não evolua a um nível irreversível.

Uma vulnerabilidade que poderia acarretar algum problema no futuro seria se os recursos humanos das microempresas deixassem de se atualizar com relação às novas ameaças que surgem de tempos em tempos. Até hoje, por não terem enfrentado uma situação grave, tem-se a impressão de que o conhecimento das pessoas que trabalham nestas empresas tem sido suficiente para evitar que alguma situação evolua para um quadro mais grave.

Mas cabe observar, conforme indica a revisão teórica, que as empresas estudadas, ao utilizarem recursos para se precaverem de falhas na integridade dos seus dados digitais, levam em consideração situações como: pane no disco rígido, falta de energia elétrica, desastres naturais, vírus de computador e outros tipos de *malware* e manipulação irresponsável dos dados digitais por parte dos usuários.

## 8.3 NECESSIDADES DAS MICROEMPRESAS EM GARANTIR A INTEGRIDADE DOS SEUS DADOS DIGITAIS

As necessidades reveladas pelas empresas através deste estudo se dividem em quatro categorias: *hardware*, *software*, serviço de manutenção e conhecimento técnico.

O Quadro 2 lista e explora cada uma destas necessidades.

<p style="text-align: center;"><b>Hardware</b></p>	<p>A fim de ter sempre disponível seus dados digitais, é necessário que o equipamento em que são armazenados seja de boa qualidade, e substituído periodicamente por equipamentos novos.</p> <p>Para evitar a indisponibilidade dos dados digitais recomenda-se o uso de <i>no-break</i>.</p>
<p style="text-align: center;"><b>Software</b></p>	<p>Para manter seus dados livres das constantes ameaças, é necessário utilizar <i>software</i> antivírus de boa reputação, e manter este <i>software</i> e o sistema operacional dos computadores constantemente atualizado.</p>
<p style="text-align: center;"><b>Conhecimento técnico</b></p>	<p>Conhecimento atualizado em relação a presentes e novas ameaças é indispensável à manutenção da integridade dos dados digitais.</p>
<p style="text-align: center;"><b>Serviço de manutenção</b></p>	<p>Por trás de cada um dos esforços anteriores deve haver uma prestação de serviço adequada, seja ela de manutenção de <i>hardware</i>, atualização dos <i>softwares</i> antivírus ou atualização dos conhecimentos por parte das fontes de informação conhecidas.</p>

**Quadro 2 – Necessidades relacionadas à segurança dos dados digitais**

Fonte: Elaborado pelo autor

Com base nas informações obtidas, o Quadro 3 contém um programa geral de ações, como proposta às microempresas que se preocupam em manter a integridade dos seus dados digitais, levando em conta um orçamento bastante enxuto:

Necessidade	Recomendações	Valor estimado
<i>Hardware</i>	Comprar um disco rígido externo para <i>backup</i>	R\$ 200,00
	Comprar um <i>no-break</i>	R\$ 250,00
<i>Software</i>	Comprar um <i>software</i> antivírus	R\$ 75,00
	Obter um <i>software</i> de <i>backup</i> gratuito	disponível na <i>internet</i> gratuitamente
Conhecimento técnico	Consultar cartilha de segurança do CERT.br	disponível na <i>internet</i> gratuitamente
Serviço de manutenção	Contratar um técnico especializado	R\$ 40,00 a R\$ 60,00 a visita

### Quadro 3 – Programa geral de ações

Fonte: Elaborado pelo autor

Além das ações listadas, recomenda-se:

- Evitar que o *hardware* utilizado sofra choques mecânicos ou seja molhado;
- Nunca abrir arquivos de computador sem antes verificá-los com o antivírus;
- Não utilizar senhas fáceis de adivinhar, nem divulgá-las a outras pessoas;
- Não confiar em *e-mails* que pedem para digitar uma senha ou acessar um endereço da *internet*;
- Verificar sempre a procedência da mensagem e se o fato sendo descrito é verídico;

- Armazenar as cópias de segurança dos dados digitais importantes em local acondicionado, de acesso restrito e com segurança física, preferencialmente em lugar diferente de onde está o computador.

#### 8.4 ALTERNATIVAS PARA DESENVOLVEDORES DE SOLUÇÕES DE SEGURANÇA

Ao propor soluções de segurança a uma empresa é importante levar em consideração suas necessidades e recursos disponíveis. No caso das microempresas, seu nível de investimento em infra-estrutura e recursos humanos faz com que suas necessidades sejam bem diferentes das empresas de maior porte. Levando em consideração esta característica, foi proposto um programa de ações que prevê investimentos próximos dos níveis mais baixos possíveis. Mas mesmo dentro deste segmento de mercado haverá microempresas com necessidades diferentes, e mais disponibilidade de recursos. Um exemplo desta diversidade é a solução adotada por uma microempresa de Porto Alegre, presente no Anexo A deste trabalho. Trata-se de uma proposta mais onerosa do que o programa de ações apresentado na seção 8.3, mas que provavelmente atende melhor às suas necessidades específicas de segurança. Neste sentido, é importante que os desenvolvedores levem em consideração as características do segmento de mercado que estão dispostos a atender, bem como inovações, tanto em termos de ameaças como em termos de ferramentas para combatê-las

## 9 CONSIDERAÇÕES FINAIS

A experiência profissional na área de TI resulta traz um acúmulo de conhecimento empírico e científico. Porém, há momentos em que, a fim de estender as fronteiras deste conhecimento, faz-se necessário esquecer um pouco o que já foi aprendido, e se lançar em direção a novas descobertas. O questionamento a respeito das necessidades das microempresas em garantir a integridade dos seus dados digitais surgiu a partir da observação de fatos, e da suposição de que poderia haver descobertas a serem feitas ao explorar este tema. Neste sentido, o conhecimento adquirido serviu de base para a pesquisa exploratória. A partir deste ponto, as experiências dos entrevistados revelaram um pouco mais a respeito de uma realidade que ainda não estava bem esclarecida.

Os resultados obtidos através deste trabalho, ainda que considerados satisfatórios, podem levar a novos questionamentos. Além disso, o dinamismo que caracteriza o universo da Tecnologia da Informação está para revelar novos paradigmas, novas necessidades, a serem identificadas pelos profissionais de marketing. Espera-se que este cenário estimule a realização de outras pesquisas, que continuem a explorar as questões referentes à utilização da TI por parte das empresas.

## REFERÊNCIAS

AAKER, David A; KUMAR, V; DAY, George S. **Pesquisa de marketing**. 2. ed. São Paulo: Atlas, 2007.

BRASIL. Presidência da República. **Lei Complementar Nº 123, de 14 de Dezembro de 2006**. Brasília, 2006.

Disponível em: [http://www.planalto.gov.br/ccivil\\_03/Leis/LCP/Lcp123.htm](http://www.planalto.gov.br/ccivil_03/Leis/LCP/Lcp123.htm). Acesso em 23/06/2010

CERT.br – CENTRO DE ESTUDOS, RESPOSTA E TRATAMENTO DE INCIDENTES DE SEGURANÇA NO BRASIL. **Cartilha de Segurança para Internet - Parte I: Conceitos de Segurança**. Versão 3.0, Setembro de 2005.

Disponível em: <http://www.dominiopublico.gov.br/download/texto/ct000001.pdf>. Acesso em: 14/10/2009

CGI.br - COMITÊ GESTOR DA INTERNET NO BRASIL. **Pesquisa sobre o Uso das Tecnologias da Informação e da Comunicação no Brasil : TIC Domicílios e TIC Empresas 2009**. São Paulo, 2010.

Disponível em: <http://www.cetic.br>. Acesso em: 12/05/2010

FERREL, O. C; HARTLINE, Michael D. **Estratégia de Marketing**. São Paulo: Pioneira Thomson Learning, 2005.

FORUM INTERNACIONAL DE TI BANRISUL, 3. 2010, Porto Alegre, RS.

Disponível em: [http://www.forumtibanrisul.com.br/mod\\_certificado.php](http://www.forumtibanrisul.com.br/mod_certificado.php). Acesso em: 23/06/2010

GALLO, Michael A; HANCOCK, William M. **Comunicação entre Computadores e Tecnologias de Rede**. São Paulo: Thompson, 2003.

JUNIOR, Cícero C. **Informática,internet e aplicativos**. São Paulo: Ibpex, 2008.

KOTLER, Philip. **Administração de marketing**. 10. ed. São Paulo: Pearson Prentice Hall, 2000.

LAUDON, Kenneth C; LAUDON, Jane P.; **Sistemas de Informações Gerenciais**. 7. ed. São Paulo: Pearson Prentice Hall, 2007.

MALHOTRA, Naresh. **Pesquisa de marketing: uma orientação aplicada**. Porto Alegre: Bookman, 2001.

MATTAR, Fauze Najib. **Pesquisa de marketing: edição compacta**. 3. ed. São Paulo: Atlas, 2001.

McDONALD, Malcolm. **Planos de marketing: Planejamento e gestão estratégica: como criar e implementar**. Rio de Janeiro: Elsevier, 2004.

SCHEWUE, Charles D; SMITH, Reuben M. **Marketing: conceitos, casos e aplicações**. São Paulo: McGraw-Hill do Brasil, 1982.

SEBRAE/RS – SERVIÇO BRASILEIRO DE APOIO ÀS MICRO E PEQUENAS EMPRESAS RIO GRANDE DO SUL. **Ambiente Empresarial das Micro e Pequenas Empresas Gaúchas – Quantas são? Onde se localizam? Quanto agregam na economia e no emprego?** Porto Alegre: SEBRAE/RS, 2009.

SEBRAE – SERVIÇO BRASILEIRO DE APOIO ÀS MICRO E PEQUENAS EMPRESAS. **Lei Geral da Micro e Pequena Empresa**. Brasília: 2007

Disponível em: <http://www.abinee.org.br/informac/arquivos/lgeral.pdf>. Acesso em: 21/06/2010

SHIPLEY, Greg. **Deixe de ser reativo na gestão da segurança de TI**. São Paulo, 2008.

Disponível em: <http://www.itweb.com.br/noticias/index.asp?cod=49328>.

Acesso em: 10/06/2010.

TURBAN, Efraim; LEIDNER, Dorothy; MCLEAN, Ephraim; WETHERBE, James. **Tecnologia da Informação para Gestão – transformando os negócios na economia digital**. 6. ed. Porto Alegre: Bookman, 2009.

WESTWOOD, John. **O plano de Marketing**. 2. ed. São Paulo: Makron Books, 1996.

ZIKMUND, William G.; **Princípios da Pesquisa de Marketing**. São Paulo: Thomson, 2006.

## APÊNDICE A – ROTEIRO DA ENTREVISTA AO ESPECIALISTA EM REDES

---

<b>1. PERFIL DO ENTREVISTADO</b>
<b>2. QUESTÕES RELATIVAS A HARDWARE</b>
<p>Quais os principais dispositivos utilizados para armazenamento de dados digitais?</p> <p>Existem marcas mais confiáveis?</p> <p>Existe diferença no risco nas plataformas PC e Mac?</p>
<b>3. QUESTÕES RELATIVAS A SOFTWARE</b>
<p>As ameaças estão evoluindo com o tempo?</p> <p>Há softwares que não se deve usar na empresa?</p> <p>Que softwares são indispensáveis a uma empresa, em termos de segurança?</p> <p>O que seria ideal nos aplicativos? E nos softwares?</p> <p>Softwares customizados são mais seguros?</p> <p>Linux é mais seguro?</p> <p>Proxy e máquinas virtuais são eficazes?</p>
<b>4. QUESTÕES RELATIVAS AO FATOR HUMANO</b>
<p>O usuário compreende os recursos dos softwares modernos?</p> <p>Quais as maiores dificuldades em manter a segurança?</p> <p>Recomendações aos usuários?</p>

**APÊNDICE B – ROTEIRO DAS ENTREVISTAS AOS EMPRESÁRIOS**

---

<b>1. PERFIL DO ENTREVISTADO</b>
<b>2. QUESTÕES RELATIVAS A HARDWARE</b>
Quais dispositivos utilizados para armazenamento de dados digitais na empresa? Ocorreu alguma falha grave? Que situação comprometeria o funcionamento da empresa?
<b>3. QUESTÕES RELATIVAS A SOFTWARE</b>
Como se defende dos riscos? Quais aplicativos? O que é desejável nos aplicativos? Utiliza softwares customizados? Ocorreu alguma falha grave? Que situação comprometeria o funcionamento da empresa?
<b>4. QUESTÕES RELATIVAS AO FATOR HUMANO</b>
Necessidade de compreensão dos riscos à integridade dos dados digitais? Necessidade de treinamento? Confiança nos colaboradores? Quem provê suporte à TI?

**APÊNDICE C – ROTEIRO DA ENTREVISTA AO ESPECIALISTA EM TI**

---

<b>1. PERFIL DO ENTREVISTADO</b>
<b>2. QUESTÕES RELATIVAS A HARDWARE</b>
Quais os principais dispositivos utilizados para armazenamento de dados digitais? Falhas provocadas por usuário? Como prevenir?
<b>3. QUESTÕES RELATIVAS A SOFTWARE</b>
Como se defende dos riscos? Quais aplicativos? O que é desejável nos aplicativos? Utiliza softwares customizados? Ocorreu alguma falha grave? Que situação comprometeria o funcionamento da empresa?
<b>4. QUESTÕES RELATIVAS AO FATOR HUMANO</b>
O usuário compreende os recursos dos softwares modernos? Quais as maiores dificuldades em manter a segurança? Recomendações aos usuários?

**APÊNDICE D – ROTEIRO DA ENTREVISTA AOS FORNECEDORES**

---

<b>1. PERFIL DO ENTREVISTADO</b>
<b>2. QUESTÕES RELATIVAS AO PRODUTO</b>
Quais os principais produtos? A quais necessidades os produtos atendem? Quais seus atributos?
<b>3. QUESTÕES RELATIVAS AO FATOR HUMANO</b>
O cliente compreende os recursos dos produtos? Apresenta necessidade de mais conhecimento a respeito dos produtos? Dificuldades apresentadas pelos usuários?

**ANEXO A – CONTRATO DE MANUTENÇÃO**

<b>1. IMPLANTAÇÃO</b>
<b>EQUIPAMENTO</b>
Servidor <i>No-break</i> (2 horas de autonomia)
Custo: R\$ 4000,00
<b>2. SERVIÇO DE MANUTENÇÃO</b>
Custo: R\$ 35,00 por computador Inclui uma visita semanal do técnico à empresa Adicional de 10% do valor do contrato para visita técnica extra

## GLOSSÁRIO

**Antivírus:** Programa ou *software* especificamente desenvolvido para detectar, anular e eliminar vírus e outros tipos de programas maliciosos de um computador.

**Aplicativo:** Programa de computador cuja finalidade é facilitar a realização de um trabalho específico pelas pessoas.

**Ataque de vírus:** Tentativa, bem ou mal sucedida, de acesso ou uso não autorizado a um programa ou computador.

**Atualização automática:** Atualização do programa ou *software* antivírus ou sistema operacional sem necessidade de ação do usuário.

**Backup:** cópia de dados digitais de um dispositivo para outro, com o objetivo de recuperá-los posteriormente caso haja necessidade ou algum problema com os dados originais.

**Cavalo de Tróia:** Programa que simula uma ação desejável, porém tem como real função facilitar o acesso não-autorizado a um computador, sem o conhecimento do usuário.

**Cloud computing:** Serviço de armazenamento de dados digitais via internet, prestado por terceiros.

**E-mail:** caixa postal para trocar mensagens pela Internet.

**FTP:** Protocolo de transferência de dados.

**Hardware:** A parte física, material, do computador.

**No-break:** sistemas responsáveis pelo fornecimento de energia elétrica, mesmo durante interrupção por parte das concessionárias.

**Linux:** Sistema operacional da família Unix, de código aberto, desenvolvido inicialmente por Linus Torvalds.

**Macintosh:** Marca de computadores pessoais fabricados e comercializados pela Apple Inc., que utilizam seu próprio sistema operacional.

**Servidor:** É um computador que fornece acesso a dados a dispositivos e computadores ligados remotamente.

**Sistema operacional:** Conjunto de programas e aplicativos que servem de interface entre o usuário e o computador.

**Software:** Qualquer programa de computador.

**Spyware:** Tipo de programas cujo objetivo é monitorar atividades de um sistema e enviar as informações coletadas para outras pessoas.

**TIC:** Tecnologias de Informação e Comunicação.

**Vírus:** Programa malicioso de computador criando cópias de si mesmo e se tornando parte de outros programas e arquivos de um computador.

**Worm** – Programa capaz de se propagar automaticamente através de redes, enviando cópias de si mesmo de computador para outro.

