



UNISUL

UNIVERSIDADE DO SUL DE SANTA CATARINA

MARCIO HOERLLE LOPES

**BACKUP PARA PEQUENAS EMPRESAS
ESTRATÉGIAS DE IMPLEMENTAÇÃO**

Porto Alegre

2019

MARCIO HOERLLE LOPES

**BACKUP PARA PEQUENAS EMPRESAS
ESTRATÉGIAS DE IMPLEMENTAÇÃO**

Relatório apresentado ao Curso **Tecnólogo em Gestão da Tecnologia da Informação**, da Universidade do Sul de Santa Catarina, como requisito parcial à aprovação na unidade de aprendizagem de Estudo de Caso.

Orientador: Me. Nilce Miranda Ayres

Porto Alegre
2019

MARCIO HOERLLE LOPES

**BACKUP PARA PEQUENAS EMPRESAS
ESTRATÉGIAS DE IMPLEMENTAÇÃO**

Este trabalho de pesquisa na modalidade de Estudo de Caso foi julgado adequado à obtenção do grau de Tecnólogo em Gestão da Tecnologia da Informação e aprovado, em sua forma final, pelo Curso Superior de Tecnologia em Gestão da Tecnologia da Informação, da Universidade do Sul de Santa Catarina.

Porto Alegre, 15 de outubro de 2019.

Prof. e orientador Me. Nilce Miranda Ayes
Universidade do Sul de Santa Catarina

AGRADECIMENTOS

Agradeço a meus pais, Judith e Milton, Meu irmão Alexsander e minha esposa Fernanda que me apoiou na busca da minha formação acadêmica e foi fundamental para que este trabalho fosse realizado.

RESUMO

Este trabalho responde à questão: “Quais as causas da não adoção de backups em pequenas empresas e como apresentar uma opção viável para sanar esta deficiência?”. Para tal, demonstra de forma concisa, um breve levantamento das causas que levam gestores de pequenas empresas a correrem riscos desnecessários por não manterem cópias de segurança de seus dados no seu dia a dia. Também demonstra a consequência financeira da continuidade deste comportamento no evento de uma perda catastrófica de dados e auxilia na percepção dos gestores sobre como é executada a implementação de uma solução de backup, bem como as respectivas demandas financeiras e organizacionais deste processo. Além do exposto, também apresenta um breve comparativo das soluções mais comuns de backup, desde servidores locais a soluções de armazenamento em nuvem, com suas particularidades, prós e contras. O trabalho conclui sua missão ao apresentar soluções viáveis econômica e cronologicamente, alinhados com a situação financeira da empresa, também levando em consideração a urgência na solução da questão.

Palavras-chave: backup.estratégia.análise.

SUMÁRIO

1 INTRODUÇÃO	7
2 TEMA	9
3 OBJETIVOS	10
3.1 OBJETIVO GERAL	10
3.2 Erro! Indicador não definido.	
4 PROCEDIMENTOS METODOLÓGICOS	11
4.1 CAMPO DE ESTUDO	11
4.2 INSTRUMENTOS DE COLETA DE DADOS	11
5 APRESENTAÇÃO E ANÁLISE DA REALIDADE OBSERVADA	12
5.1 ESTRUTURA DA ORGANIZAÇÃO	12
5.2 DESCRIÇÃO E ANÁLISE DA REALIDADE OBSERVADA	13
5.2.1 AMBIENTE DE TI	17
5.2.2 AMBIENTE ATUAL DE BACKUP	18
5.2.3 CRITICIDADE DOS DADOS	18
5.2.4 NECESSIDADES DA EMPRESA	19
6 PROPOSTA DE SOLUÇÃO DA SITUAÇÃO-PROBLEMA	21
6.1 PROPOSTA DE MELHORIA PARA A REALIDADE ESTUDADA	21
6.1.1 PRIMEIRA ETAPA	21
6.1.2 SEGUNDA ETAPA	27
6.1.3 TERCEIRA ETAPA	28
6.1.4 QUARTA ETAPA	28
6.2 RESULTADOS ESPERADOS	29
6.3 VIABILIDADE DA PROPOSTA	30
6.3.1 VALORES	30
6.3.2 CRONOGRAMA	32
7 CONSIDERAÇÕES FINAIS	32
REFERÊNCIAS	34
APÊNDICES	36

1 INTRODUÇÃO

Este trabalho baseia-se em uma pequena empresa de Porto Alegre e busca identificar os motivos que levam pequenas empresas a não adotarem políticas de backup, apresentando as causas e possíveis soluções para correção do problema.

Justifica-se este trabalho com a intenção de fornecer um comparativo e base para consultas, auxiliando os profissionais da área a terem sucesso no tratamento de casos similares, já que esta é uma ocorrência bastante comum neste segmento.

A metodologia utilizada compreende um conjunto de ferramentas como pesquisas na internet, questionários e tabelas para identificação e tabulação dos resultados, além de gráficos para facilitar o entendimento dos dados levantados, resultando em uma pesquisa descritiva-explicativa já que identifica causas, apresenta justificativas e explica fatos para um determinado comportamento, além de demonstrar um processo de correção das deficiências encontradas.

2 TEMA

O processo de efetuar cópias de segurança - mais conhecido em inglês como “Backup” é tão antigo quanto os primeiros computadores, sendo que os primeiros backups de que se tem notícia foram feitos ainda em cartões perfurados nos anos 50. Desde então, sua importância tem sido cada vez mais reconhecida e levada em consideração no momento de planejar a infraestrutura de TI de uma empresa e até mesmo como garantia de segurança de dados pessoais.

Hoje em dia, efetuar backups das informações críticas de uma empresa deixou de ser considerado um luxo, mas uma necessidade para garantir não só a tranquilidade e segurança dos profissionais de TI, mas principalmente como parte integral de qualquer plano de continuidade de negócio e a primeira linha de defesa contra perdas catastróficas de dados. Conforme relatado por FARIA (2014), a inacessibilidade aos dados pode ocorrer por falhas de software, hardware, erros humanos, desastres naturais, invasões e vírus, entre outros. Estas situações são analisadas por outros autores em concordância com as políticas de segurança da informação como menciona MOREIRA (2008) para uma segurança da informação eficaz dentro de uma organização deve-se ficar atento para algumas questões como uma boa análise de riscos, a definição da política de segurança e por fim um plano de contingência. Já MÉDICE (2013) declara que o primeiro passo a ser observado é que não existe risco zero e medidas precisam ser tomadas para evitar o desastre.

Apesar da importância e criticidade da implementação de processos de backup, há uma grande maioria de empresas de pequeno porte que não aderem à esta prática por diversas razões, que nem sempre fazem sentido quando em face da perda irrecuperável de informações e riscos associados quando isto ocorre. Dito isto, o problema em questão é: qual o motivo que impede uma empresa de adotar uma política de backup e como determinar a melhor solução de backup que seja de aplicação simples e rápida para atender a demanda de segurança da informação?

Neste contexto, este trabalho tem como tema a identificação das causas que levam pequenas empresas a não adotarem políticas de backup e apresentar o processo de implementação de uma ferramenta e processos para corrigir o problema.

Espera-se que este trabalho possa servir de argumentação para futuros casos de implementação de backups em empresas de pequeno porte, apresentando os benefícios da adoção desta prática e desmistificando o assunto de forma clara e abrangente.

3 OBJETIVOS

3.1 OBJETIVO GERAL

Analisar as causas da não adoção de políticas de segurança da informação e apresentar procedimentos de implantação em conjunto com análise das ferramentas existentes mais apropriadas.

3.1 OBJETIVOS ESPECÍFICOS

Identificar as causas da não adoção de políticas de backup;

Identificar as soluções de backup disponíveis e políticas de segurança da informação aplicáveis;

Avaliar comparativamente os custos envolvidos na implementação, suporte e operação;

Analisar os pontos positivos e negativos das soluções identificadas, considerando fatores como: disponibilidade, facilidade de uso, tempo de implementação e velocidade de operação;

Propor a melhor solução de backup para pequenas empresas no cenário atual;

A partir da definição da melhor solução, apresentar um procedimento de implementação da solução e criação do processo de uso da mesma.

4 PROCEDIMENTOS METODOLÓGICOS

4.1 CAMPO DE ESTUDO

A pesquisa terá um formato explicativo conforme disposto por GIL (2002), já que tem como preocupação identificar motivos para ocorrência dos fatos. Terá como campo de estudo uma pequena empresa de Porto Alegre (que solicitou sigilo em relação a sua identidade real e será citada como a Empresa “ACME”). Dado o tamanho reduzido da empresa (8 funcionários), serão colhidos depoimentos dos key users, respectivamente Diretor e Gerente financeiro, como amostras através de questionário padronizado para uma melhor compreensão dos motivos relevantes para a não adoção de uma política de backup até o momento. Em paralelo, serão coletados dados técnicos das soluções e procedimentos de implementação de backup mais comuns no mercado para delimitar a solução mais abrangente em relação às necessidades identificadas.

4.2 INSTRUMENTOS DE COLETA DE DADOS

Os instrumentos de coleta de dados adotados neste trabalho são:

Quadro 1 – Instrumento de coleta de dados

Instrumento de coleta de dados	Universo pesquisado	Finalidade do Instrumento
Entrevista e Formulário	Entrevista com os diretores da empresa com preenchimento de formulário para obtenção de dados.	Avaliar a importância do backup na empresa e motivos da falta de adoção de políticas preventivas.
Observação direta	A observação será feita nas dependências da empresa semanalmente.	Identificar problemas causados pela falta de uma política de backup.
Documentos	<ul style="list-style-type: none">• Documentação das soluções disponíveis no mercado;• Relatório do sistema de arquivos utilizado.	<ul style="list-style-type: none">• Identificar o cenário atual de backup na empresa;• Montagem de tabela comparativa de soluções;• Identificar políticas de backup compatíveis com a empresa.

Fonte: Do autor.

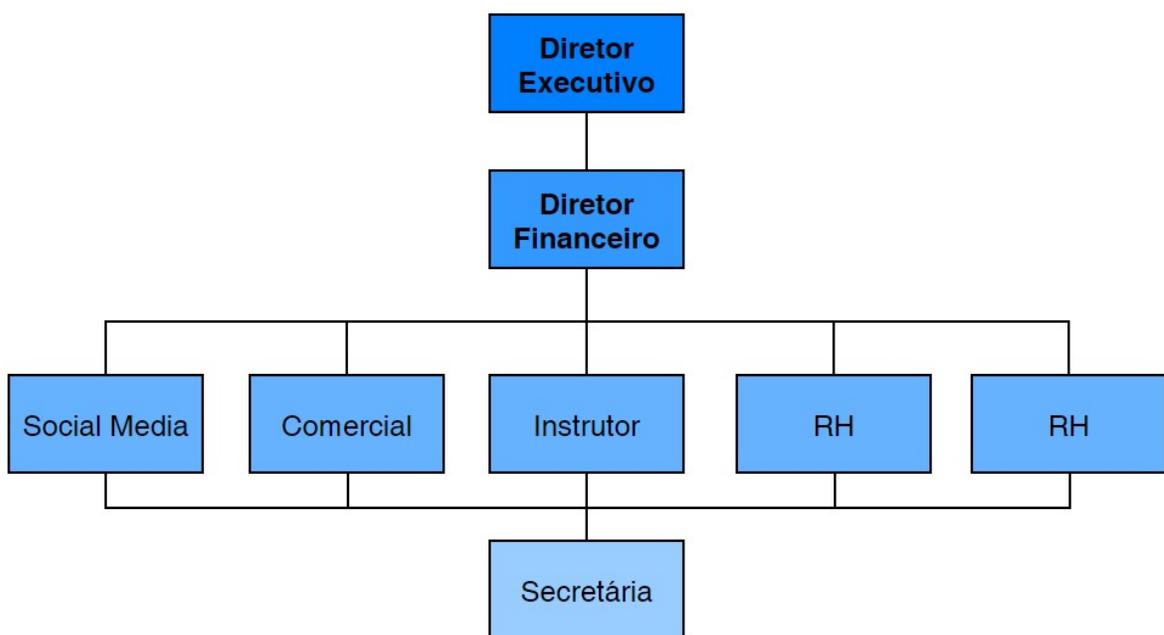
5. APRESENTAÇÃO E ANÁLISE DA REALIDADE OBSERVADA

4.1 ESTRUTURA DA ORGANIZAÇÃO

Para apresentar a realidade estudada, seguem algumas informações contextuais sobre a empresa ACME: fundada em 1977, trata-se de uma ONG registrada como pequena empresa especializada em fomentar treinamentos na linguagem LIBRAS para deficientes auditivos e outros interessados, além de prestar o serviço de agência de empregos para deficientes e promover a defesa de políticas, educação e cultura em favor da comunidade deficiente auditiva. Este trabalho trata do escritório local com uma estrutura de 8 pessoas localizado no centro de Porto Alegre, RS. A empresa não possui departamento ou funcionários dedicados para gestão ou operação de TI.

A estrutura organizacional da empresa é demonstrada no quadro abaixo:

Figura 1 – Estrutura Organizacional:



Fonte: Do autor

Dada a pequena estrutura disponível, a empresa começa a perceber a necessidade de organizar seu parque de TI e profissionalizar sua operação, sob pena de ter perdas de dados e consequentes perdas financeiras, porém não dispõe de recursos financeiros para contratação

efetiva de pessoal especializado, optando por serviços técnicos com contratação terceirizada em atendimentos pontuais, considerado como um cenário de “TI reativa” como descrito por RAFAEL (2014). Mesmo assim, até o momento do trabalho não havia sido cogitada uma implementação qualquer solução de backup dos dados da empresa.

5.2 DESCRIÇÃO E ANÁLISE DA REALIDADE OBSERVADA

Neste cenário, a fim de identificar mais claramente os motivos da falta de uma política de TI para sanar o problema e em concordância com o processo de análise da dados qualitativos demonstrado por FREITAS (2000), foi efetuada uma entrevista com o preenchimento de um questionário com os key users, respectivamente o diretor executivo e diretor financeiro da ACME. Os entrevistados deveriam elencar os motivos em ordem de importância pelos quais não havia uma política de backup implementada até o momento, buscando apresentar pontos chave relacionados com o tema, em concordância com FLICK (2009):

Quadro 2 – Pontuação de dados coletados

Peso	Importância
5	Muito importante
4	Importante
3	Normal
2	Baixa prioridade
1	Nenhuma prioridade

Fonte: Do autor

Respostas dos entrevistados:

Quadro 3 – Tabela de coleta de dados

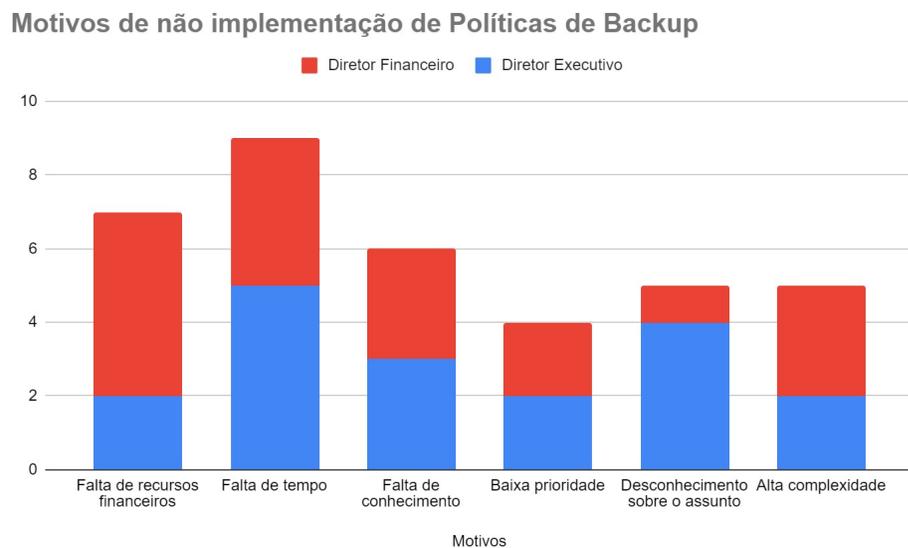
Diretor Executivo			
Motivos	Concordância com a afirmação	Comentários	Importância
Falta de recursos financeiros	Não	Não temos valores para considerar no momento.	2
Falta de tempo	Sim	Não tivemos tempo para considerar uma solução .	5
Falta de	Sim	Não temos pessoal com	3

conhecimento		conhecimento na área na empresa.	
Baixa prioridade	Sim	Não houveram crises de perda de dados até o momento.	2
Desconhecimento sobre o assunto	Sim	Precisamos de mais informações para tomar uma decisão.	4
Alta complexidade	Sim	Soluções de TI demandam alto conhecimento técnico.	2
Diretor Financeiro			
Motivos	Concordância com a afirmação	Comentários	Importância
Falta de recursos financeiros	Sim	Não há previsão orçamentária para esta necessidade no ano fiscal.	5
Falta de tempo	Sim	Nossa estrutura não permite deslocamento de recursos pessoais para a tarefa.	4
Falta de conhecimento	Sim	Não temos pessoal com conhecimento na área na empresa	3
Baixa prioridade	Não	A perda de dados pode comprometer a gestão financeira da empresa.	2
Desconhecimento sobre o assunto	Sim	Tenho ideia do funcionamento e a que se destina.	1
Alta complexidade	Sim	Não temos conhecimento interno para implementar.	3

Fonte: Do autor

Abaixo o gráfico elencando as respostas do questionário para uma identificação visual dos motivos de não implementarem uma política de backup até onde se identifica o pouco (ou nenhum) tempo dedicado ao assunto, seguido da percepção de que não há recursos financeiros para implementar uma solução e falta de conhecimento sobre o assunto.

Gráfico 1 – Causas de não implementação



Fonte: Do autor.

Na segunda parte do formulário, foi questionado o interesse da empresa em solucionar o problema e a urgência para implementação de uma solução.

Quadro 4 – Tabela índice de níveis de interesse e urgência

Nível de interesse	Nível de urgência
Alto	Alta (peso 3)
Normal	Normal (peso 2)
Baixo	Baixa (peso 1)

Fonte: Do autor.

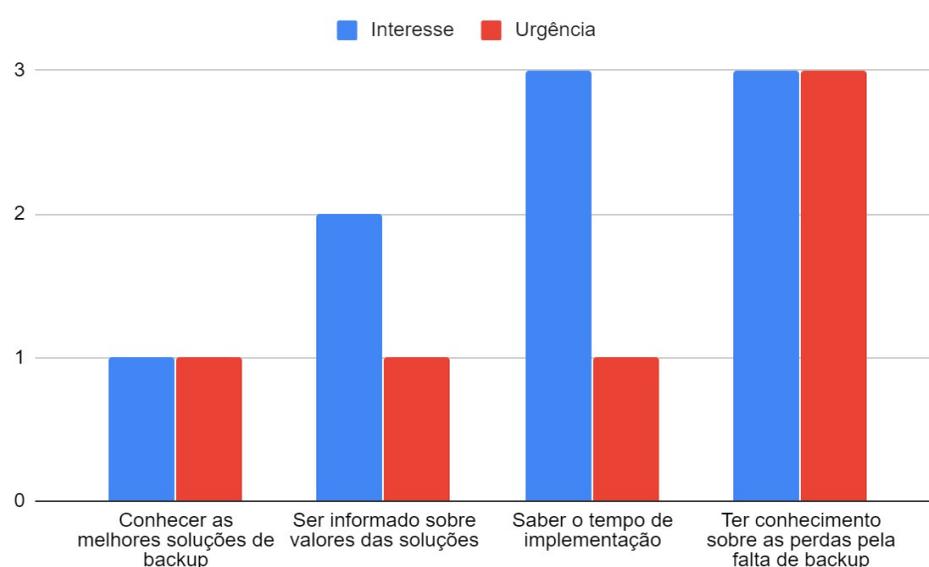
Quadro 5 – Tabela de coleta de níveis de interesse e urgência

Diretor Executivo	Interesse	Urgência
Conhecer as melhores soluções de backup	Baixo	Baixa
Ser informado sobre valores das soluções	Normal	Alta
Saber o tempo de implementação	Alto	Baixa
Ter conhecimento sobre as perdas pela falta de backup	Alto	Alta
Diretor Financeiro	Interesse	Urgência
Conhecer as melhores soluções de backup	Alto	Baixa
Ser informado sobre valores das soluções	Alto	Alta
Saber o tempo de implementação	Normal	Normal
Ter conhecimento sobre as perdas pela falta de backup	Alto	Normal

Fonte: Do autor.

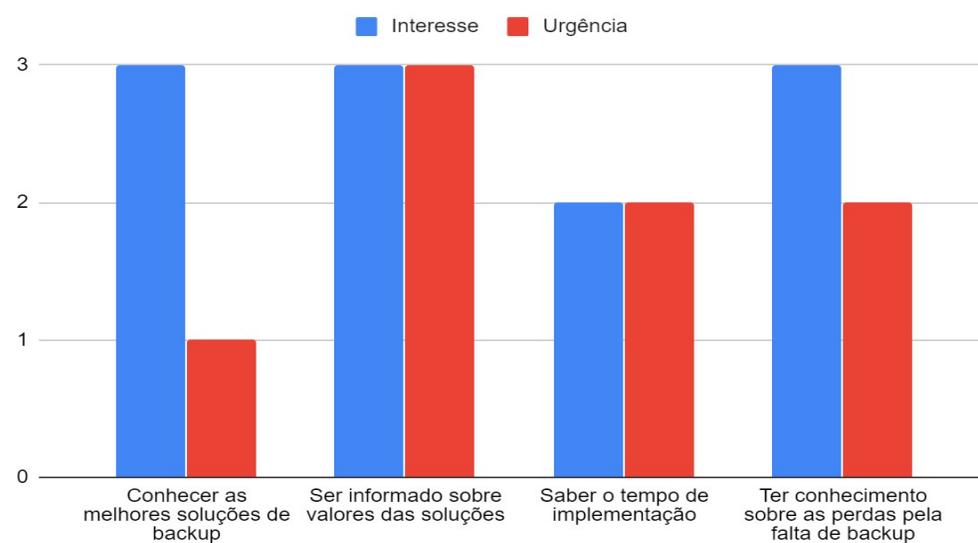
A seguir, o gráfico elencando as respostas para uma identificação visual a matriz de interesse x urgência para os entrevistados, onde se identifica o interesse no conhecimento sobre perdas e valores das soluções disponíveis, claramente demonstrando a necessidade da empresa de um comparativo entre custos de implementação e perdas financeiras:

Gráfico 2 – Motivos para interesse em uma solução de backup por parte do Diretor executivo:



Fonte: Do autor.

Gráfico 3 – Motivos para interesse em uma solução de backup por parte do Diretor financeiro:



Fonte: Do autor.

Baseado nas respostas fornecidas, identifica-se que os principais interesses são obter conhecimento sobre as perdas causadas pela falta de backup e ter conhecimento sobre valores das soluções disponíveis.

5.2.1 AMBIENTE DE TI

Nas visitas realizadas à empresa, foi identificado o parque de TI composto da seguinte forma:

Diretor Administrativo:

Notebook Dell Inspiron I15-3567-D15P

Disco Rígido: 1TB

Diretor financeiro:

Notebook Dell Inspiron I15-3567-D15P

Disco Rígido: 1TB

Demais funcionários:

6x Desktop Inspiron 3647-D20, Intel Core i3, 4GB RAM, HD 1TB

Link de acesso à internet: (relevante para identificação de soluções em nuvem):

1x Link ADSL 25mbps (25mpbs de download x 1mbps de upload)

Rede Local:

O escritório possui 9 pontos de acesso com cabeamento não estruturado no padrão CAT5e conectados a um switch Encore 16 portas.

Periféricos adicionais:

1x HD externo genérico para cópias pontuais e 2 Pen drives de 16Gb para eventuais transportes de arquivos, eventualmente utilizado como um armazenamento de cópias de arquivos sem qualquer frequência regular ou procedimento específico.

1x Impressora laser Kyocera em regime de outsourcing de impressão com empresa terceirizada.

5.2.2 AMBIENTE ATUAL DE BACKUP

Em conversas com os diretores, identificou-se que não há qualquer prática de backup em uso e foi citada a necessidade de cópias de segurança dos seguintes itens:

- Arquivos de trabalho (documentos, planilhas, apresentações);
- Arquivos de mídia (vídeos, fotos, arquivos de áudio);
- E-mails e Bases de dados dos programas em uso (programa ponto, sistema de agendamento, sistema educacional).

Foi definido que arquivos pessoais dos funcionários não devem ser alvo dos backups e deverão ser removidos dos computadores da empresa pelos mesmos em um período de 1 (uma) semana antes da nova solução de backup ser implementada. Arquivos pessoais encontrados após esse período serão deletados.

Atualmente, cada computador tem arquivos salvos de forma aleatória em pastas e subpastas que por vezes são salvas de forma duplicada em locais diferentes do sistema, dada a falta de um procedimento e padrão de organização dos arquivos na empresa. Foi declarado também que um local único de acesso a todos para salvar os arquivos seria ideal, para evitar perda ou duplicidade de arquivos e retrabalho.

Sobre a perda de dados já existentes, foi declarado que houveram pequenas perdas com pen drives defeituosos, mas os mesmos arquivos foram localizados depois de algumas horas de procura nos computadores. Esta situação serviu como alerta para a empresa evitar problemas futuros com perdas maiores. Neste contexto, os funcionários relataram em conversa informal suas experiências em empresas anteriores, com perdas catastróficas de dados e como foram sanadas ou evitadas com o uso de políticas de segurança da informação e recuperação de dados a partir de backups.

5.2.3 CRITICIDADE DOS DADOS

Os arquivos e bases de dados atualmente em uso tem como conteúdo dados vitais como:

- Cadastro dos funcionários e folha de pagamento;
- Contratos de terceirização de recursos;
- Contratos com fornecedores;
- Histórico do sistema de ponto eletrônico;

- Apresentações e material didático dos cursos de LIBRAS;
- E-mails;
- Planilhas com movimentação financeira da empresa.

A perda permanente dos arquivos descritos pode resultar nos seguintes problemas (entre outros):

- Atraso no pagamento de funcionários e fornecedores;
- Perda de oportunidades comerciais;
- Cancelamento de cursos de LIBRAS;
- Interrupção das comunicações via mídias sociais;
- Inadimplência com tributos fiscais;
- Impossibilidade de emissão de notas fiscais e subsequente perda de receita.

5.2.4 NECESSIDADES DA EMPRESA

Após reuniões com os diretores, foram listadas as características mais atraentes em uma solução de backup para a empresa:

- Acesso fácil aos dados de backup em caso de perda;
- Baixo custo de aquisição e manutenção;
- Garantia de privacidade dos dados armazenados;
- Baixa complexidade de operação;
- Facilidade de expansão do espaço de backup caso necessário;
- Possibilidade de acesso remoto aos dados.

Dadas as informações expostas até o momento, percebe-se a vulnerabilidade do sistema de dados e grande possibilidade de perdas financeiras, algo crítico em pequenas empresas que precisam de uma recuperação rápida em caso de perda de dados, como exposto por OLIVEIRA (2015). Além do exposto, identifica-se claramente um caso de reatividade na gestão de TI, onde problemas são solucionados após sua ocorrência e não há qualquer procedimento ou política de prevenção. Vale citar o exposto por RONNENBERG (2015):

The value of data stored on a computer, often far exceeds the value of the computer! Hardware can be quickly and easily replaced, but data cannot! Companies often insure their computer

hardware against theft and loss, but fail to backup their data, which is far more precious!

Ou seja, o valor dos dados armazenados em um sistema computacional frequentemente ultrapassa o valor do próprio sistema, pois equipamentos podem ser substituídos facilmente, mas os dados não, algo sem lógica uma vez que empresas tendem a ter um seguro contra roubo e perdas de equipamentos, porém frequentemente falham na tarefa de resguardar seus dados, algo extremamente valioso. Esta afirmação reforça a importância da necessidade de uma política de segurança da informação como parte integral de qualquer plano de continuidade de negócios.

Dito isto, resta apresentar uma proposta de implementação de política de backup com uma análise comparativa das soluções disponíveis mais aderentes às necessidades do cliente, sem, no entanto, comprometer os princípios de segurança da informação, conforme expostos na norma NBR ISO/IEC 27002 ABNT (2005).

Abaixo, apresenta-se o quadro com pontos fortes e fracos gerados como resultado de observações na empresa, entrevistas, conversas informais e avaliação dos questionários aplicados (Apêndice 1):

Quadro 6 – Tabela de pontos fortes e fracos

Problema	Pontos fortes	Pontos fracos	Justificativa
qual o motivo que impede uma empresa de adotar uma política de backup e como	A empresa reconhece a necessidade de ter backups de dados.	Falta de qualquer procedimento de backup atualmente.	A empresa cita falta de tempo, conhecimento e recursos para implementação.
determinar a melhor solução de backup que seja de aplicação simples e rápida para atender a demanda de segurança da	A empresa tem conhecimento que podem ocorrer perdas financeiras em caso de perda de dados.	Perdas podem ocorrer não só por falha de equipamentos, mas também pela falta de organização dos dados armazenados.	Perdas financeiras resultantes da perda de dados podem comprometer a continuidade do negócio.
informação?	Apesar de desorganizados, os arquivos têm cópias em diversos PCs.	Falta de um local centralizado para armazenamento dos dados em uso.	A desorganização gera retrabalho e alto risco de conflito de dados.

Fonte: Do autor

6 PROPOSTA DE SOLUÇÃO DA SITUAÇÃO-PROBLEMA

6.1 PROPOSTA DE MELHORIA PARA A REALIDADE ESTUDADA

Dada a criticidade deste trabalho, é importante citar que o objetivo do mesmo é identificar causas da não implementação de uma política de backup e apresentar opções e processos para que a empresa estudada possa alinhar-se com as normas de segurança da informação, objetivando evitar ou minimizar as perdas de dados e seu consequente impacto negativo dentro do âmbito de um plano de continuidade de negócios. Dito isto, a proposta de melhoria é apresentada nas seguintes etapas:

6.1.1 Primeira etapa – apresentar respostas para as necessidades da gestão da empresa

Com o resultado do questionário sobre quais as necessidades identificadas pela empresa e o nível de interesse apresentado, percepção de necessidade e importância com resultados nos gráficos 2 e 3, as mesmas devem ser atendidas através do levantamento dos dados necessários e apresentados na ordem de importância identificada:

- **Ser informado sobre valores das soluções**

Antes de informar o valor das soluções, será necessário efetuar um levantamento das soluções de backup disponíveis no mercado conforme as características do parque de TI.

Avaliando a estrutura de TI atual, identifica-se que não há estrutura para instalação de um servidor local da forma correta, com um rack, nobreak e cabeamento estruturado com switch gigabit e controle de tráfego de dados (QoS) para evitar que as sessões de backup local não criem um “gargalo” no tráfego local e degradem a performance dos demais serviços como impressão via rede, acesso à internet e comunicação entre as estações de trabalho.

Dito isso, cabe citar as possíveis soluções e seus custos aproximados (todos os valores informados foram resultados de cotações simples):

1. Backup em armazenamento em servidor na rede local:

Quadro 7 – Tabela de custos de implementação de servidor local

item	descrição	valor (R\$)
1	Rack de Piso, fechado 20U x 1070mm de profundidade	\$1,140.00
2	Nobreak APC Smart UPS 3kva para rack	\$4,405.00
3	Switch HP Office Connect gerenciavel 24 portas Gigabit	\$1,591.00
4	Serviço de cabeamento estruturado e adequação de ambiente	\$8,990.00
5	Licença Microsoft Windows Server 2019 Essentials Open NL	\$2,200.00
6	Storage server Lenovo SR630	\$14,562.00
	Total	\$32,888.00

Fonte: Do autor

Esta solução pretende fornecer um backup diretamente na rede local, contemplando a estrutura necessária para instalação e operação de um servidor de armazenamento de dados (storage) escalável que servirá como servidor de arquivos local com discos rígidos com políticas de espelhamento RAID, garantido a duplicidade dos dados das estações. Os prós e contras desta solução são listados abaixo:

Prós:

- Sem custo mensal fixo;
- Rapidez no acesso às informações;
- Escalabilidade dependente da quantidade de discos instalados;
- Possibilidade de realocação do servidor sem custos.

Contras:

- Alto custo inicial ;
- Possibilidade de falha no equipamento;
- Requer mão de obra especializada para instalação e manutenção;
- Possível necessidade de atualizações de software futuras com custos adicionais.

2. Backup local em um dispositivo de armazenamento ligado à rede (NAS).

Quadro 8 – Tabela de custos de implementação de um armazenamento NAS

item	descrição	valor (R\$)
1	WD 4TB My Cloud EX2 Ultra	\$2,500.00
2	Nobreak APC SMC1500-BR 1440VA (900W) 120V, senoidal	\$2,757.00
	Total	\$5,257.00

Fonte: Do autor.

Esta solução é considerada uma versão de baixo custo de um servidor local, fornecendo um armazenamento de 4TB nativo ligado diretamente à rede, com um sistema de RAID entre 2 discos rígidos internos (espelhamento) onde o primeiro disco é utilizado como armazenamento dos arquivos da empresa e o segundo disco gera um espelhamento (backup) dos dados em tempo real. Pode também ser utilizado para armazenar backups dos computadores locais. Os prós e contras desta solução são listados abaixo:

Prós:

- Sem custo mensal fixo;
- Não requer um rack para armazenamento;
- Rapidez no acesso às informações;
- Escalabilidade parcial, dependendo da troca dos discos internos por modelos de maior capacidade ou com a adição de mais unidades do mesmo modelo;
- Possibilidade de realocação do servidor sem custos;
- Não requer mão de obra especializada;
- Menor custo em relação a um servidor.

Contras:

- Alto custo inicial quando comparado com soluções em nuvem;
- Possibilidade de falha no equipamento e ponto crítico de falha, pois em caso de problemas no equipamento, os discos podem ser inutilizados;
- Poderá necessitar atualizações de software futuras com custos adicionais.

3. Backup em nuvem.

Quadro 9 – Tabela de custos de para armazenamento em nuvem

Serviço	Fornecedor	Descrição de funcionalidades	custo	
			1 usuário/mês	para 10 usuários/ano
DropBox	Dropbox	3Tb de armazenamento em nuvem; cliente integrado para desktops; compartilhamento externo de arquivos; criptografia e gerenciamento de permissões; versionamento de arquivos e recuperação de versões anteriores; controle de acesso e autenticação em 2 fatores; ferramentas de produtividade;	R\$ 50,00	R\$ 6.000
Google Drive	Google	armazenamento em nuvem ilimitado ; cliente integrado para desktops; compartilhamento externo de arquivos; criptografia e gerenciamento de permissões; versionamento de arquivos e recuperação de versões anteriores; controle de acesso e autenticação em 2 fatores; ferramentas de produtividade; inclui acesso ao pacote de ferramentas g-suite (docs,sheets e outros); edição de arquivos nativos em formato colaborativo;	R\$ 45,90	R\$ 5.508
Onedrive For Business	Microsoft	armazenamento em nuvem ilimitado no total, 25Tb por usuário ; cliente integrado para desktops; compartilhamento externo de arquivos; criptografia e gerenciamento de permissões; versionamento de arquivos e recuperação de versões anteriores;	R\$ 43.30	R\$ 5.196

Fonte: Do autor.

Estas soluções podem ser consideradas as mais baratas quando partindo-se do princípio que não são suscetíveis a problemas de equipamentos locais, sinistros e outros, fornecendo opções de espaço de armazenamento diversificado e altamente customizável. Pode tanto serem usados estritamente como backups como também como um servidor remoto de arquivos. Os prós e contras desta solução são listados abaixo:

Prós:

- Sem custo fixo inicial;
- Não requer um rack para armazenamento;
- Custos podem ser fracionados e escalonados conforme a necessidade;
- Não requer futuros investimentos com atualizações de equipamentos ou licenciamento de software;

- Dados podem ser acessados de qualquer lugar com acesso à internet;
- Não requer mão de obra altamente especializada;
- Menor custo em relação às outras soluções apresentadas.

Contras:

- Custo mensal variável, sujeito a reajustes imprevistos;
- Possibilidade de perda de acesso aos dados caso ocorram problemas de acesso à internet.
- Apesar de não ser obrigatório, pode requerer um gestor com conhecimento da ferramenta para aproveitar todo seu potencial.

- **Ter conhecimento sobre as perdas pela falta de backup**

Para identificar as perdas pela falta de backup, especialmente em pequenas empresas, deve-se utilizar um cálculo básico da renda média mensal da empresa para que se estipule um valor/dia e/ou valor/hora para que se considere um índice de lucro cessante, e ao mesmo podem ser somados custos eventuais.

No caso da empresa ACME, foram fornecidos os seguintes valores médios, baseados em dados históricos:

Quadro 10 – Tabela de receitas

receita mensal	receita diária	receita horária
\$37,216.00	\$1,691.64	\$211.46

Fonte: Do Autor

O cálculo utilizado foi: receita diária = receita mensal / 22 (dias úteis) e receita horária = receita diária / 8h.

Baseado no quadro acima, identificam se as perdas diretas (custos tangíveis) baseadas nos valores informados, desconsiderando custos eventuais como juros sobre pagamentos que eventualmente atrasem devido a uma parada no ambiente de TI dada uma falha que acarrete em perda dos dados essenciais da empresa.

Vale citar que, como exposto por CABRAL e CAPRINO (2015), a análise de impacto nos negócios deve sempre estar de acordo com as perdas aceitáveis pelo negócio, porém cálculos mais detalhados podem aumentar significativamente as perdas tangíveis indicadas ao serem somadas na linha do tempo durante um episódio de parada, como juros, multas e taxas extras pelo não cumprimento das obrigações fiscais da empresa em tempo hábil. Vale também lembrar que em um segundo momento podem ser considerados os custos intangíveis, tais como perda de reputação, perda de mercado, desvalorização da marca e outros.

- **Conhecer as melhores soluções de backup**

É importante apresentar de forma clara e organizada à empresa um comparativo dos prós, contras e detalhamento de cada tipo de serviço para que possa se obter uma decisão em conjunto entre os responsáveis da empresa e quem está auxiliando no processo de implementação para que se chegue a um meio termo entre o menor custo e implementação mais rápida e a rigidez das normas e melhores práticas de TI em busca da excelência na implementação de TI.

- **Saber o tempo de implementação**

Tempos de implementação das soluções são importantes quando se está correndo contra o relógio e seu concorrente é um desastre de perda de dados que ainda não ocorreu. Nesse sentido, quanto menor o tempo de implementação, melhores as chances de se evitar um problema durante o processo. Percebe-se claramente que a solução de armazenamento em nuvem tem os menores prazos de implantação, mesmo quando se adicionam prazos de implementação. No quadro abaixo podem ser verificados os tempos médios para as soluções citadas no início desta etapa:

Quadro 11 – Tabela de prazos de contratação e implantação – em dias úteis

Servidor local				
Itens	contratação / compra	envio	configuração	total
Storage server Lenovo SR630	5	30	5	40
Rack 20U	1	7	1	9
Switch gigabit	1	7	1	9
Cabeamento	1	7	3	11
Nobreak	1	7	1	9
Licenciamento Microsoft	2	5	3	10
	total			88
Armazenamento em rede (NAS)				
Itens	contratação / compra	envio	configuração	total
WD 4TB My Cloud EX2 Ultra	1	15	5	21
Nobreak 1.4Kva	1	5	1	7
	total			28
Armazenamento em nuvem				
Itens	contratação / compra	envio	configuração	total
Dropbox	1	1	5	7
Google Drive	1	1	10	12
Onedrive for Business	1	1	10	12

Fonte: Do autor

6.1.2 Segunda etapa – Implementação de práticas de backup e procedimentos organizacionais

Uma vez apresentadas as melhores opções de backup, prazos de implementação das soluções e possíveis perdas em caso de paradas por perda de dados, é importante apresentar um plano de melhoria nos processos organizacionais para que a empresa não apenas tenha uma ferramenta confiável de backup mas também adote práticas de segurança da informação, para garantir que a mesma seja utilizada em toda sua extensão e capacidade, além de colaborar para a organização da empresa como um todo. De contra partida, é importante citar que pequenas empresas normalmente não têm recursos financeiros ou de pessoal para implementar uma política detalhada de processos organizacionais. Partindo deste princípio e mantendo o foco em

soluções de backup, podemos apresentar uma sugestão básica de processos organizacionais diretamente relacionados com a necessidade e regularidade da execução de backups.

Usando como base e incrementando o que mencionou PADLIPSKAS, o processo de implementação de novos procedimentos organizacionais do ponto de vista da segurança da informação com foco no backup da dados passa pelas seguintes etapas:

- a. Catalogar dados e sistemas a serem armazenados;
- b. Efetuar levantamento de prioridades de armazenamento e disponibilidade dos dados;
- c. Definir frequências de execução do backup;
- d. Elaboração da agenda de execução de backups;
- e. Definição dos tempos de recuperação de dados;
- f. Documentação dos processos e novas políticas;
- g. Aplicação dos procedimentos e treinamento da equipe.

6.1.3 Terceira etapa – Sensibilização dos colaboradores

É importante citar que parte essencial do processo de implementação dos procedimentos passa obrigatoriamente pela sensibilização dos funcionários para que compreendam o motivo da mudança ou início do uso de procedimentos de backup. Nenhum processo, por mais perfeito que seja, sobreviverá a uma equipe reativa que não compreende a lógica por trás das novas funções. Cabe à gestão da empresa apoiar a apresentação das perdas e danos recorrentes da não execução com os colaboradores, juntamente com um plano estruturado de treinamento na nova ferramenta e nas mudanças de paradigmas da empresa, sempre reforçando a importância da participação ativa de cada funcionário no processo e demonstrando as vantagens ao serem aderentes com o programa. Conforme OLIVEIRA (2009), No âmbito de pequenas e médias empresas, apesar desta tarefa não requerer grande esforço, deve ser projetada e aplicada com atenção e, sempre que possível, permitindo a participação dos funcionários no processo como forma de engajamento.

6.1.4 Quarta etapa – Sanitização dos dados

É de conhecimento de todos os profissionais de TI que dados desorganizados de uma empresa tendem a ser armazenados juntamente com dados pessoais dos funcionários. Em um

ambiente de pequena empresa esta prática é ainda mais comum. Conforme citado por CRUZ (2008) a “Desorganização Informacional (DoI)” ou seja, a perda de controle sobre meios de armazenamento é uma doença crônica e deve ser combatida antes de se tornar um peso a ser carregado pela organização, gerando custos desnecessários com armazenamento e desgaste de recursos. Isto posto, é fundamental que ocorra um processo de “faxina” dos arquivos pessoais dos colaboradores juntamente com a definição de regras de armazenamento. Esta limpeza deve ser feita em 3 partes:

- comunicação aos usuários:

Todos os colaboradores devem ser comunicados sobre a definição de uma nova política de armazenamento e devem receber um prazo determinado para que possam remover ou apagar arquivos pessoais, com o alerta de que após o prazo, qualquer arquivo identificado como não relacionado com o escopo de seu trabalho será removido permanentemente;

- Manutenção do processo:

Após a primeira rodada de limpeza de dados desnecessários, deve ser definido um “dia de faxina” onde um funcionário responsável ou terceirizado fará verificações por novos arquivos e removerá os mesmos sem prévio aviso. Em casos de reincidência, o colaborador ofensor poderá ser convidado a participar de um processo de reeducação;

- Revisão da política de armazenamento:

Em período a ser determinado, (normalmente uma vez ao ano) as políticas de armazenamento poderão ser revisadas e adequadas conforme a necessidade da empresa.

6.2 RESULTADOS ESPERADOS

Dados os fatos expostos na realidade observada e suas contrapartidas na proposta de melhoria, espera-se demonstrar de forma clara e concisa alguns dos motivos que levam pequenas empresas a não adotarem políticas de backup, apontar processos e soluções de hardware e software para sanar o problema, garantindo a segurança, acessibilidade e confiabilidade dos dados, além de uma melhora nos processos organizacionais, aumentando a performance da empresa e contribuindo para a continuidade do negócio.

A identificação das causas e subsequente esclarecimento das dúvidas apresentadas no decorrer deste trabalho permitirão que os gestores possam reconhecer a urgência em definir como implementar um procedimento de backup de forma mais segura e aderente às necessidades da empresa.

A apresentação de opções de backup local ou remoto com seus respectivos prós e contras, também elencando suas funcionalidades, servirá como uma base de conhecimento para

escolha da melhor plataforma a ser implementada e em paralelo, fomentar uma possível melhora nos sistemas em uso atualmente com a opção de migração para ferramentas em nuvem, resultando na modernização dos softwares utilizados.

Uma vez implementada a nova ferramenta e iniciado o processo de mudança organizacional no âmbito que tange os processos de backup, há a intenção de que o início das mudanças processuais possa fomentar o desenvolvimento de novos processos em outras áreas da empresa, aproveitando o engajamento da equipe.

Por fim, com a solução implementada e a equipe treinada nos novos processos, o objetivo final esperado é que a empresa, apesar de pequena, tenha uma garantia de segurança de seus dados e, em parte um princípio de plano de continuidade de negócios, dando maior tranquilidade aos gestores e mais segurança aos funcionários.

6.3 VIABILIDADE DA PROPOSTA

Identificou-se que após este trabalho, os gestores da empresa ACME foram conscientizados da necessidade, importância e urgência na implantação de um processo e ferramenta de backup. Partindo desta premissa, e levando em consideração a viabilidade financeira com foco em contratação de serviços em detrimento da compra de equipamentos, é apresentado abaixo um demonstrativo de viabilidade financeira:

6.3.1 Valores

Dada a necessidade urgente e definição da empresa em contratar uma solução no menor tempo possível, e com o menor custo inicial, foram descartadas as opções de servidor local e de armazenamento conectado à rede (NAS). Portanto, apresentamos as informações para implementação de armazenamento em nuvem com os seguintes valores:

- Pacote Google Drive para dez usuários: R\$ 5.508,00 pagos anualmente, contemplando armazenamento ilimitado, acesso ao pacote de ferramentas Gsuite;
- Serviço de instalação e configuração da ferramenta por empresa terceirizada local: R\$ 2.500,00 em 5 prestações, com possibilidade de contratação de serviços mensais de gestão por R\$ 500,00 em pacote de 10 horas, incluindo consultoria para upgrade do link de acesso à internet para comportar esta modalidade de armazenamento em nuvem;

- Treinamento na ferramenta ministrado por empresa terceirizada com ênfase na redefinição de processos organizacionais relacionados, por R\$ 2.000,00 em 4 prestações de R\$ 500,00 com duração de 10 horas, incluindo treinamento com prática diretamente no ambiente de produção.

Quadro 12 – Tabela de viabilidade

Viabilidade financeira			
Serviço	Valor unitário	10 usuários	Valor anual
Contratação do serviço Google Drive	R\$ 45,90	R\$ 459,00	R\$ 5.508,00
Total serviços			R\$ 5.508,00
Serviços locais			Valor total
Configuração nas estações e no servidor remoto			R\$ 2.500,00
Treinamento			R\$ 2.000,00
Total serviços			R\$ 4.500,00
Total geral			R\$ 10.008,00

Fonte: Do autor

Levando em consideração a rapidez na implantação, a alta disponibilidade e facilidade no uso da ferramenta e seu valor agregado, aliada à possibilidade de diluição dos custos recorrentes da contratação deste Software como serviço (SaaS), o valor investido total de aproximadamente R\$ 10.000,00 é o equivalente a 5 dias úteis de receita perdida (vide Quadro 10) em caso de uma perda de dados da empresa. Vale ressaltar que sem qualquer backup atualmente, uma perda total de dados tomaria muito mais tempo para ser recuperada.

6.3.2 Cronograma

Quadro 13 – Cronograma de implantação

Cronograma de implantação			
Serviço	contratação	entrega	prazo total
Contratação do serviço Google Drive	1	1	2
Configuração nas estações e no servidor remoto	1	10	11
Treinamento	1	10	11
		Total	24 dias úteis

Fonte: Do autor

No quadro acima, apresentamos uma previsão de cronograma de implementação e início de uso da nova solução de backup, a ser considerada como entregue em até 24 dias da data de aceite da proposta de viabilidade. Ressalta-se que o período de treinamento e início dos trabalhos pode sofrer atrasos eventuais se solicitado pela gestão da empresa para não impactar o período entre 5 dias antes e 5 dias após o final de mês dada a criticidade da disponibilidade dos funcionários para a conclusão de processos administrativos com pagamento de impostos, folha de pagamento e outros compromissos financeiros.

7 CONSIDERAÇÕES FINAIS

Durante o processo de criação desta trabalho, buscou-se apresentar um cenário real de pequenas empresas que ainda não consideram ou valorizam soluções de backup, sendo apresentado o caso da empresa ACME, demonstrando os motivos pelos quais ainda não tinham optado por sanar esta deficiência e, partindo destas informações, conscientizar os gestores sobre as possíveis perdas financeiras tangíveis resultantes da inatividade em relação ao problema apresentado. No mesmo âmbito, foram apresentadas soluções para sanar o déficit na segurança de dados em busca de regularizar o ambiente de TI e subsequentemente, demonstrar os benefícios da prática de backups.

Entende-se que ao analisar e levar em consideração as informações apresentadas, a empresa em questão tenha dados concretos e conclusivos para a tomada de decisão sobre o assunto e regularize seu ambiente de TI, adotando práticas atualizadas de segurança de dados e em paralelo, fomentando o início de mudanças organizacionais que resultarão em um ambiente de TI e processos mais sólidos, seguros e confiáveis, além de contribuir para a estruturação dos dados armazenados atualmente.

Os obstáculos encontrados durante o processo de confecção deste documento foram uma certa resistência da empresa no quesito financeiro, não tendo interesse inicial na participação por temores de haver algum custo no processo. Afora isto, o desafio deste projeto foi encontrar um meio termo entre uma abordagem por demais casual e uma abordagem extremamente técnica e rígida, algo que não é possível quando se trata de pequenas empresas sem recursos financeiros ou de pessoal para acomodar os requisitos de normas técnicas aplicáveis à grandes empresas com departamentos de TI dedicados.

REFERÊNCIAS

- ABNT. ABNT NBR ISSO/IEC 27002: Código de prática para gestão da segurança da informação.** Disponível em: < http://www.fieb.org.br/download/senai/NBR_ISO_27002.pdf> Acessado em: 12/09/2019.
- CABRAL, Carlos e CAPRINO, William. Trilhas em Segurança da Informação: Caminhos e ideias para a proteção de dados.** Editora: Brasport. ISBN 9788574526867. 2015. pgs. 398-402.
- CRUZ, Tadeu. BPM & BPMS - Business Process Management & Business Process Management Systems.** Editora: Brasport. ISBN 9788574523774. 2008. p. 52.
- FARIA, Medrado de; HEITOR. Bacula - Ferramenta Livre de Backup.** Segunda Edição. Editora: Brasport. ISBN 8574526894. 208 Pgs. 2014.
- FLICK, Uwe. Qualidade na pesquisa Qualitativa.** Segunda Edição. Editora: Bookman. ISBN 9780761949824 2009. pgs. 153,175.
- FREITAS (H.). Análise de dados qualitativos: aplicações e as tendências mundiais em Sistemas de Informação.** São Paulo/SP: Revista de Administração da USP, RAUSP, v. 35, nr. 4, Out-Dez. 2000, p.84-102
- MÉDICE, Roney. A importância da Segurança da Informação – Visão Corporativa** Disponível em: <<https://www.profissionaisiti.com.br/2013/07/a-importancia-da-seguranca-da-informacao-visao-corporativa/>>.Acessado em: 15/08/2019.
- GIL AC. Como classificar as pesquisas.** Disponível em <<http://www.madani.adv.br/aula/Frederico/GIL.pdf>> Acessado em 01/09/2019.
- MACHADO, Cristiane Salvan et al. Trabalhos acadêmicos na Unisul: apresentação gráfica.** Palhoça: Ed. Unisul, 2012.
- MOREIRA, Ademilson. A importância da segurança da informação.** Disponível em: <https://www.oficinadanet.com.br/artigo/1124/a_importancia_da_seguranca_da_informacao>.Acessado em: 15/08/2019.
- OLIVEIRA, André. Falta de backup: Problemas e consequências para sua empresa.** Disponível em: < <http://www.strati.com.br/falta-de-backup-problemas-e-consequencias-para-sua-empresa/>> Acessado em: 10/09/2019.
- OLIVEIRA, Fátima. TECNOLOGIA DA INFORMAÇÃO E DA COMUNICAÇÃO Articulando processos, métodos e aplicações.** Editora: E-papers. ISBN 9788576501944. 2009. p. 117-118.
- PADLIPSKAS, Sálvio. Desenvolvendo uma estratégia eficiente de Backup & Restore em ambientes transacionais.** Disponível em: < <https://bit.ly/2P0a0KZ>> Acessado em: 11/10/2019.

RAFAEL, Gustavo. A realidade de ambientes de TI em Micro e Pequenas Empresas (MPE). Disponível em < <https://www.profissionaisti.com.br/2014/02/a-realidade-de-ambientes-de-ti-em-micro-e-pequenas-empresas-mpe/>> Acessado em 08/09/2019.

RAUEN, Fábio José. Roteiros de investigação científica. Tubarão: Unisul, 2002.

RONNENBERG, T.E. Backup Quotes. 2015 Disponível em: < <http://www.backup.info/quotes/value-data>> Acessado em: 10/09/2019.

APÊNDICE

Questionário utilizado na coleta de dados

QUESTIONÁRIO:

Você está participando de um questionário que ajudará a identificar as causas da não implementação de uma política de segurança de dados (backup) em sua empresa, basta que responda as questões citadas abaixo:

1. Enumere em ordem de prioridade de 1 a 5 , conforme o quadro abaixo, quão importante são as afirmações sobre os motivos da falta de implementação de um processo de backup em sua empresa. Logo após, preencha com sim ou não se você concorda com a afirmação e justifique sua resposta no campo comentários:

Peso	Importância
5	Muito importante
4	Importante
3	Normal
2	Baixa prioridade
1	Nenhuma prioridade

Motivos	Importância (1-5)	Concordância com a afirmação	Comentários
Falta de recursos financeiros			
Falta de tempo			
Falta de conhecimento			
Baixa prioridade			
Desconhecimento sobre o assunto			
Alta complexidade			

2. Para identificarmos os seus níveis pessoais de interesse e urgência em relação à implementação de um sistema de backup na empresa, preencha a tabela abaixo conforme sua opinião:

Informações prévias para implementação de backup	Interesse	Urgência
Conhecer as melhores soluções de backup		
Ser informado sobre valores das soluções		
Saber o tempo de implementação		
Ter conhecimento sobre as perdas pela falta de backup		