



Importância da Segurança da Informação e *Backup*

Eduardo Longhi Scopel, Breno Carra Fiorese, Natan Susin Cervinski, Guilherme Cavalheiro Carlesso, Nicolas Lamb Xavier, Priscila Bresolin Tissot, Gabriela Zanandrea, Eduardo Robini da Silva, Maria Emilia Camargo

RESUMO

O objetivo deste estudo foi mostrar a importância da segurança da informação, tanto para empresas de grande e pequeno porte quanto para cidadãos comuns. Também mostrar políticas de segurança da informação quanto aos meios virtuais. Para tanto, foram utilizadas abordagens qualitativa e quantitativa. A pesquisa realizada visando resultados qualitativos ocorreu com a realização de entrevistas semi-estruturadas. A pesquisa quantitativa consistiu na entrevista de alunos de escolas públicas, visando descobrir principalmente a frequência de utilização de uma ferramenta muito simples de proteção à informação, o *backup*. Os resultados qualitativos apontam que, mesmo sendo o método mais utilizado por empresas e indivíduos, o *backup* em nuvem não é completamente confiável, apresentando alguns erros e limitações aos usuários em algumas situações. Apesar disso, é de fácil manutenção, gerando economia para as empresas. Os resultados quantitativos observados a partir da pesquisa com estudantes comprovaram que apesar da importância da realização de cópia de segurança dos dados bem como da utilização de ferramentas de proteção, ainda há a falta de conscientização para esta questão, o que favorece a perda de informações.

Palavras-chave: Segurança da informação. *Backup*. Políticas de Segurança.

1 INTRODUÇÃO

As informações são cada vez mais importantes no dia-a-dia de todas as pessoas e empresas, e essas informações têm de aparecer para a pessoa certa na hora certa, sem que esteja corrompida ou inutilizável, e para isso são utilizadas algumas ferramentas como o *backup* (FONTES, 2012). Para as empresas, os usuários dos sistemas são uma das vulnerabilidades que a informação pode ter em alguns casos passando suas senhas a estranhos, permitindo a eles que acessem as informações da empresa (WORKMAN; BOMMER; STRAUB, 2008).

Outra vulnerabilidade são os incidentes físicos que podem ocorrer com a empresa, sendo eles: incêndio, infiltrações, roubo de mídias, queima de equipamento, etc., gerando perdas de informação, algumas vezes de valor inimaginável para a empresa. Por esses motivos, quase todas as empresas têm um sistema de *backup* para assegurar a integridade de suas informações, para que em caso de incidentes de perda de informações seja possível recuperá-las, de forma eficiente e rápida, para que a perda em dinheiro que a empresa poderia estar ganhando nesse período sem a informação seja o mínimo possível.

Este artigo teve por objetivo geral mostrar a importância da segurança da informação, tanto para empresas de grande e pequeno porte quanto para cidadãos comuns. Também mostrar políticas de segurança da informação quanto aos meios virtuais. Para tanto realizou-se a mensuração do uso do *backup* em empresas de grande/médio porte e no dia-a-dia das pessoas, bem como, foram apontadas as vantagens em fazer *backup* de arquivos mais importantes no dia-a-dia das pessoas.

Além desta seção introdutória, o artigo apresenta Referencial Teórico acerca dos temas propostos, seguidos pela Metodologia, Discussão dos Resultados e Considerações Finais.



2 REFERENCIAL TEÓRICO

2.1 SEGURANÇA DA INFORMAÇÃO

Para Espírito Santo (2018) a segurança da informação é uma arma e também vital para as empresas. A segurança da informação tem como finalidade fazer a proteção e gerir a informação.

De acordo com Fontes (2012, p.6), “A informação é um recurso essencial para toda e qualquer organização, independentemente do seu porte e segmento de atuação no mercado”. Isso se dá, pois, todas as empresas, para suas decisões, crescimento e planejamento, necessitam de muitas informações, principalmente as atuais, o que gera uma grande busca por informações diariamente.

Segundo Castilhos (2013, p.55) “a segurança da informação é obtida a partir da implementação de um conjunto de políticas processos e procedimentos e estruturas”. Uma empresa, para sobreviver, precisa guardar muito bem suas informações. E uma eficaz segurança da informação só poderá ser obtida com um conjunto de controles adequados, sendo um deles uma política de segurança de informação, fiscalizando o que for necessário para obter êxito.

Para Knapp et al. (2009) o primeiro e mais importante passo é fazer um conjunto de políticas de segurança da informação para deixar a organização preparada contra-ataques, tanto internos quanto externos. Segundo Workman, Bommer e Straub, (2008), a falta de conscientização dos usuários é uma das principais ameaças à segurança, pois existem muitas medidas de segurança disponíveis, mas os usuários não dão muita importância, facilitando ataques e violações à segurança das informações nas organizações.

A preservação digital é composta por dois tipos de procedimentos: os de ordem estrutural que dizem respeito a definições de normas, adoção de padrões e a infraestrutura; e os de ordem operacional que são as atividades aplicadas para a preservação física, lógica e intelectual dos documentos digitais (THOMAZ, 2004; MÁRDERO; ARELLANO, 2004). Neste momento questiona-se a natureza do *backup*: ele é um procedimento estrutural ou operacional? Segundo Franch (2008) o *backup* consiste na replicação idêntica dos dados que integram um documento, esta é uma técnica comum em qualquer contexto tecnológico, que se tornou necessária devido as experiências de perdas em nível mundial.

2.2 BACKUP

Segundo Neto et al (2012, p.2) o *backup* pode ser definido como “cópia de segurança dos dados de determinado dispositivo de armazenamento que pode ser espelhado em outro dispositivo de forma a garantir a estabilidade dos arquivos e afastar a possibilidade de surpresas como a perda desses dados.” Ainda de acordo com Neto et al (2012) a prática rotineira de *backup* é vista como algo chato para muitos. Por isso muitos gestores de sistemas estão trabalhando na tarefa de simplificar e automatizar a tarefa de realização e *backup*, para minimizar o tempo gasto.

De acordo com Jesus e Schimiguel (2018, p.23) “para *backup* de pequeno e médio porte a solução de *backup* em nuvem apresenta grandes vantagens, devido ao fato de seu tamanho ser pequeno. Além da vantagem de utilização do *backup* em nuvem, que permite a inexistência de um local para armazenamento, e a escalabilidade, aumentando gradualmente o tamanho do *backup* de acordo com a necessidade, não requer um custo inicial”.

2.3 POLÍTICAS DA SEGURANÇA DA INFORMAÇÃO



As políticas da segurança da informação têm como objetivo fornecer aos usuários da informação nas empresas um conjunto de regras, que por sua vez tem como objetivo manter as informações da empresa em um nível minimamente seguras. Cabe à direção estabelecer as políticas, mas o mais importante é que os usuários que devem se conscientizar e seguir esse determinado conjunto de regras. (SANTANA, 2016).

A maioria das empresas criam suas próprias políticas de segurança, adequando a política à empresa, o que é uma prática que por si só já ajuda a proteger ainda mais a informação. No entanto essas políticas sempre são baseadas em um modelo.

Um exemplo de modelo bastante utilizado é o que Freitas (2016) descreve em seu trabalho, que se baseia principalmente na política de senhas, política de e-mails e política de internet, que são políticas que tem como finalidade fazer com que os usuários evitem contrair vírus e *malwares*.

No que diz respeito à política de senhas, observa-se que:

- a) a senha deve conter no mínimo 6 caracteres alfanuméricos (números e letras);
- b) a senha deverá nunca ser passada para outras pessoas, caso o usuário ache que a senha não está totalmente segura ele deverá trocá-la;
- c) tudo que for executado com sua senha será de responsabilidade do usuário, então é necessário tomar precauções para manter a senha segura.

Já no que tange à política de e-mails, ressalta-se que não se deve utilizar o e-mail da empresa para uso pessoal; deve-se evitar anexos muito grandes; e não reenviar correntes, aviso de vírus, criança desaparecida, criança doente. A política de internet diz que:

- a) o uso recreativo da internet não deverá se dar no horário do expediente;
- b) proibido usar aplicativos de mensagem instantânea não autorizada pela equipe de segurança;
- c) o acesso a site de jogos, pornográficos, apostas, bate-papo e semelhantes serão bloqueados e monitorados.

2.4 PERDAS EM RELAÇÃO A SEGURANÇA DA INFORMAÇÃO

São três as possíveis perdas relacionadas diretamente à segurança da informação: (i) perda de confidencialidade; (ii) perda de integridade e; (iii) perda de disponibilidade. A perda de confidencialidade ocorre quando documentos, planilhas, senhas, ou qualquer tipo de arquivo importante e altamente restrito sofre uma quebra de sigilo, sendo perdido ou podendo parar em mãos erradas, que podem causar grandes prejuízos à empresa (ARAUJO, 2008)

Já a perda de integridade acontece quando os arquivos da empresa ficam expostos e podem ser manuseados por pessoas sem autorização, que podem causar alterações não aprovadas e que não estão sob controle do atual dono da informação. No que diz respeito à perda de disponibilidade, esta ocorre quando os arquivos deixam de estarem acessíveis por quem necessitaria deles, como a perda de comunicação com alguns sistemas importantes da empresa (ARAUJO, 2008)

No caso de ameaças a sistemas e/ou redes de computadores, podem ser causados pelos *crackers* (agentes maliciosos), que são motivados a tais atos por muitos motivos, sendo eles a autoestima, tentar ganhar dinheiro vendendo aos verdadeiros donos, vingança por ser demitido ou simplesmente para mostrar a público sobre o atual plano da empresa. (ARAUJO, 2008)

3 PROCEDIMENTOS METODOLÓGICOS

Para a realização da pesquisa e obtenção dos resultados foram utilizadas abordagens



qualitativa e quantitativa. A pesquisa realizada visando resultados qualitativos ocorreu com a realização de entrevistas semi-estruturadas. As entrevistas ocorreram em forma de conversa, tendo como base um questionário pré-formulado, que foi aplicado a profissionais da área de TI de diferentes empresas, visando saber as diferenças e semelhanças mais marcantes entre a forma de proteger as informações das empresas. As entrevistas foram gravadas e transcritas, visando obter resultados com base nas semelhanças e diferenças das respostas obtidas.

A pesquisa quantitativa consistiu na entrevista de alunos de escolas públicas, visando descobrir principalmente a frequência de utilização de uma ferramenta muito simples de proteção à informação, o *backup*. A pesquisa consistiu na aplicação de um questionário com 10 perguntas para 55 alunos de 3 escolas públicas diferentes de uma cidade chamada Antônio Prado. Os dados coletados foram tabulados pelos próprios autores do artigo, sem que fosse preciso qualquer *software* para a tabulação, e foram distribuídos em forma de tabelas.

4 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

4.1 RESULTADOS QUALITATIVOS

A segurança da informação é algo a ser tratado com muito cuidado para que não existam falhas que comprometam um todo, principalmente quando se trata de banco de dados, onde estão armazenadas a maior parte das informações da empresa, assim como disse o entrevistado N°1. Ressalta-se que o entrevistado N°2 concorda com a afirmação de que o banco de dados é o item mais importante para manter seguro, como pode-se observar nos trechos a seguir:

[...] O mais importante é o Banco de Dados, [...] dentro desse Banco de Dados estão todas as informações da empresa, então na verdade assim, planilhas de Excel, esse tipo de coisa, esse tipo de arquivo a gente consegue voltar, mas um Banco de Dados que tem informações tipo de notas fiscais e tal ele é um pouco mais delicado. (ENTREVISTADO 1)

[...] tipos de arquivos que constam em FS ou Bases de dados são os mais importantes (ENTREVISTADO 2)

Muitas empresas já utilizam o *backup* em nuvem, tendo em mente a praticidade e segurança gerada por esse meio, mas ainda são usados os meios físicos para o caso da nuvem apresentar alguma falha, assim como diz o entrevistado N°3.

Na nuvem pela praticidade e segurança, e o HD externo é mais para ter um *backup* do *backup*, caso um falhe tem o outro. (ENTREVISTADO 3)

O *backup* em nuvem é muito usado pelas pessoas ligadas com a tecnologia, e é também uma tendência que todos passem a usá-lo, pela sua praticidade e segurança, como disse o entrevistado N°1.

[...] a migração para esta estratégia na nuvem é uma tendência não só para *backup*, a questão de nuvem [...] que é onde você aluga um espaço fora em um servidor em qualquer parte do planeta você pode jogar todo o seu sistema para lá, não só o *backup* então isso é uma tendência uma tecnologia nova. (ENTREVISTADO 1)

Mesmo parecendo inseguro, quem usa a nuvem tem bastante confiança no meio, pois mantendo práticas de segurança, como botar senhas difíceis e trocá-las constantemente aumenta em muito a segurança, como disse o entrevistado N°1.

[...], mas o risco de isso acontecer hoje é muito baixo. [...] seguindo algumas políticas de



segurança como senha diferente é muito improvável que aconteça. (ENTREVISTADO 1)

O *backup* nas empresas é extremamente importante, pois garante muita segurança a todo tipo de informação da empresa. Com ele é possível recuperar os danos de algum problema ocorrido com os servidores ou as máquinas dos funcionários. O Entrevistado N°1 diz:

A gente faz um *backup* diário dentro de umas fitas, tá, essas fitas são externas e são tiradas da empresa, além dessa fita é feito um *backup* para uma outra parte aqui da empresa, e além disso eu faço um *backup* online que é feito a cada 10, 15 minutos. Se eu tiver um funcionário com uma planilha de Excel e ele me disser, “cara, minha planilha sumiu”, eu consigo voltar ela até 15 minutos atrás, e isso a gente tá agora melhorando e a ideia é fazer com que fique 5 minutos só. (ENTREVISTADO 1)

Outra importância do *backup* em nuvem em empresas é que ele pode acabar evitando custos adicionais com funcionários ou dispositivos extras. Consequentemente faz com que a produtividade aumente, já que se houverem erros, não precisará ser perdido tempo refazendo todo o trabalho novamente. O entrevistado N°1 conta:

Em 16 anos nós tivemos um incidente só, esse incidente foi um problema no Banco de Dados, onde a gente perdeu aí, 2 horas de trabalho, quase menos, mas isso faz bastante tempo. (ENTREVISTADO 1)

O método de *backup* em nuvem tem um dos melhores custo-benefício do mercado, além de ser muito prático e consideravelmente rápido. Ele funciona de forma parecida com o método de *backup* em servidor interno, onde os arquivos ficam armazenados em um servidor que se situa em uma sala separada de todo o resto, mantendo a segurança física do mesmo. A diferença é que no *backup* em nuvem, um servidor de alguma empresa especializada é alugado para os arquivos serem armazenados de forma mais segura.

Temos de exemplo também a empresa do entrevistado N°1, que utiliza de *backup* em fitas magnéticas, com um sistema automatizado para troca e organização das fitas. Esse método também tem um dos melhores custo-benefício do mercado, mas também oferece grandes riscos quando organizado por humanos e não é automatizado. O entrevistado N°1 afirma:

Os arquivos são enviados pra uma fita magnética, uma fita LTO, as nossas fitas tem 8 *terabytes* de capacidade em cada uma, e a gente usa um robô, a gente chama de robô mas não é exatamente um robô e ele fica fazendo o rodizio entre as fitas, ele bota 36 fitas dentro e fica fazendo um rodizio das fitas, tem todo um mecanismo pra não usar sempre a mesma fita, é enviado pra essa fita e é enviado pra um servidor fora da sala principal. (ENTREVISTADO 1)

4.2 RESULTADOS QUANTITATIVOS

A pesquisa contou com a colaboração de cinquenta e cinco estudantes de escolas públicas de ensino médio de uma cidade situada na Serra Gaúcha. A pesquisa foi feita em três escolas diferentes dessa cidade. Desses cinquenta e cinco estudantes que responderam à pesquisa foi possível perceber que a maioria dos entrevistados nas escolas tem entre 15 e 16 anos de idade (Tabela 1).

Tabela 1 – Faixa etária dos respondentes

Faixa etária	Escola 1	Escola 2	Escola 3	Total
14	0	0	0	0
15	11	9	3	23
16	3	10	15	28



17	2	1	0	3
18 ou +	0	1	0	1
Total	16	21	18	55

Fonte: Elaborado pelos autores (2018).

Foi questionado aos participantes a frequência com que utilizavam *backup*, os resultados evidenciam que a maioria (17 respondentes) não utilizam *backup*, seguido por indivíduos que realizam tal procedimento quinzenalmente (13 respondentes) e semanalmente (10 respondentes), conforme apresentado na Tabela 2.

Tabela 2 – Frequência de utilização do *Backup*

Utilização de <i>backup</i>	Escola 1	Escola 2	Escola 3	Total
Nunca	8	9	0	17
Diariamente	2	7	0	9
Semanalmente	3	2	5	10
Quinzenalmente	2	2	9	13
Mensalmente	1	1	4	6
Bimestralmente	0	0	0	0
Total	16	21	18	55

Fonte: Elaborado pelos autores (2018).

Estes resultados indicam que muitos dos respondentes não utilizam o *backup*, que é uma ferramenta muito importante nos dias atuais, já que possibilita a proteção contra diferentes falhas de *hardware*, de *software*, entre outros (FIALHO, 2007). Esse resultado é corroborado por Guisso (2017) onde também verificaram a baixa realização de *backups* entre alunos do ensino médio de algumas escolas da Serra Gaúcha. O autor enfatiza que efetuar *backups* representa uma das melhores práticas para proteger os dados de um sistema.

Há diferentes meios de realizar a cópia de segurança dos dados, dentre as mais utilizadas citam-se os discos rígidos externos, pen drive, CD/DVD/Blu-Ray, e os *backups* na nuvem (GUISO, 2017). Assim, foi questionado quais ferramentas utilizariam para realização do *backup*. Vale ressaltar que os participantes podiam indicar mais de uma das alternativas propostas. Desse modo, os resultados apontam que a maioria dos entrevistados tem preferência em fazer *backup* em *pendrives* ou armazenar em seus arquivos em nuvem, pois é mais prático e seguro, já que é possível acessar a nuvem de quase qualquer lugar, e, no caso do *pendrive*, é possível leva-lo para qualquer lugar, no entanto é possível observar que os CDs já não são mais tão utilizados pelos jovens como forma de *backup*.

Tabela 3 – Meios utilizados para o *Backup*

Meios para <i>backup</i>	Escola 1	Escola 2	Escola 3	Total
<i>Pendrive</i>	13	10	16	39
Nuvem	10	15	7	32
HDs	3	1	2	6
CDs	0	0	0	0

Fonte: Elaborado pelos autores (2018).

Sob este aspecto, Jesus e Kafure (2010) afirmam que as estratégias adotadas para a preservação dos dados podem possuir vantagens e desvantagens, por isso, devem ser verificadas, haja vista que possibilitam a preservação de acervos e coleções, permitindo o acesso futuro às referidas informações.



Em seguida, foi questionado aos respondentes quais os principais tipos de arquivos salvos em *backup*. De acordo com a pesquisa feita, é possível ver que os tipos de informações mais salvos em *backup* são fotos, músicas e mensagens, pois são dados pessoais e a maioria dos adolescentes nas idades de 15 a 16 anos usa constantemente esse tipo de dado. As redes sociais têm uma grande influência nisso, pois esse tipo de informação (fotos, músicas e mensagens) é muito compartilhada e usada.

Tabela 4 – Principais tipos de arquivos salvos em *Backup*

Tipos de arquivos salvos	Escola 1	Escola 2	Escola 3	Total
Fotos	14	17	8	39
Músicas	14	16	2	32
Mensagens	11	14	3	28
Vídeos	7	5	0	12
Trabalhos	2	1	3	6
Documentos	1	3	2	6

Fonte: Elaborado pelos autores (2018).

Em relação à preferência dos meios físico ou nuvem, essa pesquisa revelou que ambos, tanto armazenamento físico quanto nuvem, são usados, praticamente, na mesma quantidade, pois ambos são práticos e acessíveis. Nesse ponto, Ingizza (2017) revelou que apesar da grande difusão dos sistemas de armazenamento digital, há indivíduos que ainda optam pelo meio física, cuja vantagem principal reside na disponibilidade e segurança deste.

Tabela 5 – Preferencia de meios entre físico e nuvem

Preferência de meios	Escola 1	Escola 2	Escola 3	Total
Físico	7	10	12	29
Nuvem	11	9	6	26

Fonte: Elaborado pelos autores (2018).

Na sequência verificou-se que quanto ao número de aparelhos, onde concluiu -se que na maioria das residências dos entrevistados estão presentes entre 3 e 4 dispositivos.

Tabela 6 – Número de aparelhos na casa dos entrevistados

Número de aparelhos	Escola 1	Escola 2	Escola 3	Total
1	0	0	5	5
2	3	3	0	6
3	4	4	5	13
4	5	5	4	14
5	4	5	0	9
6 ou +	0	4	4	8

Fonte: Elaborado pelos autores (2018).

Guisso (2017) afirma que o avanço tecnológico permitiu o acesso à internet a partir de diferentes dispositivos, onde constata que em 2015 os telefones celulares ultrapassaram a proporção de computadores que acessam a internet. Apesar disso, quando questionados sobre os dispositivos onde o *backup* é realizado, os entrevistados afirmaram que o uso de



computador para *backup* é melhor pois é no computador que as coisas mais importantes como documentos importantes e trabalhos estão salvos.

Tabela 7 – Dispositivos em que o *Backup* é utilizado

Dispositivos	Escola 1	Escola 2	Escola 3	Total
Computador	13	16	14	43
Celular	10	12	12	34
Tablet	2	0	3	5

Fonte: Elaborado pelos autores (2018).

Assim, destaca-se a necessidade de se abordar meios que promovam a segurança dos dados. Deve-se, portanto, estabelecer mecanismos de prevenção dentre eles destaca-se os antivírus, caracterizado como item básico de segurança. Assim, quando questionados sobre a utilização do antivírus para a segurança da informação, a maior parte dos entrevistados acham importante a sua utilização, mas há também uma parte significativa que não acha importante a utilização dos mesmos.

Tabela 8 – Utilização do antivírus para a segurança da informação

Tipos de arquivos salvos	Escola 1	Escola 2	Escola 3	Total
Irrelevante	0	1	4	5
Pouco relevante	2	6	3	11
Indiferente	3	4	3	10
Importante	5	6	4	15
Muito importante	6	4	4	14

Fonte: Elaborado pelos autores (2018).

Esse resultado contraria os achados de Pimenta e Quaresma (2016), onde constataram em seu estudo com trabalhadores de Portugal que a grande maioria possuía algum software antivírus instalado em seus dispositivos. A pesquisa concluiu que alguns dos entrevistados acham que é importante manter seus softwares sempre atualizados para manter seus documentos sempre intactos.

Tabela 9 – Utilização para a correção de falhas de segurança

Tipos de arquivos salvos	Escola 1	Escola 2	Escola 3	Total
Irrelevante	0	2	0	2
Pouco relevante	1	2	3	6
Indiferente	5	7	0	12
Importante	10	2	8	20
Muito importante	0	8	7	15

Fonte: Elaborado pelos autores (2018).

A pesquisa concluiu que a maior parte dos entrevistados acham a utilização do *backup* muito importante em suas vidas pessoais e profissionais, mas também há uma significativa quantidade de pessoas que acredita que o *backup* é irrelevante.

Tabela 10 – Utilização do *backup*

Tipos de arquivos	Escola 1	Escola 2	Escola 3	Total
-------------------	----------	----------	----------	-------



salvos				
Irrelevante	0	1	0	1
Pouco relevante	2	3	1	6
Indiferente	8	7	2	17
Importante	3	5	4	12
Muito importante	3	5	11	19

Fonte: Elaborado pelos autores (2018).

Pimenta e Quaresma (2016) destacam a importância da conscientização dos usuários em realizarem com regularidade as cópias de segurança.

5 CONSIDERAÇÕES FINAIS

Os resultados qualitativos deste estudo feito com empresas de variados ramos apontam que, mesmo sendo o método mais utilizado por empresas e indivíduos, o backup em nuvem não é completamente confiável, apresentando alguns erros e limitações aos usuários em algumas situações, muitas vezes em relação ao custo, que se apresenta elevado no caso de precisar de um *restore*, mas apresenta bastante segurança quando utilizado da maneira correta, com senhas difíceis e trocadas frequentemente.

Outra vantagem do *backup* em nuvem para empresas é sua fácil manutenção, que acaba economizando gastos extras com manutenção ou até mesmo substituição de equipamentos. Também foi descoberto que um método de *backup* que ainda é muito utilizado pelas empresas é o *backup* em fitas magnéticas ou fitas LTO, por terem um custo muito baixo, possibilitando uma fácil substituição caso necessário.

Os resultados quantitativos observados a partir da pesquisa com estudantes comprovaram que apesar da importância da realização de cópia de segurança dos dados bem como da utilização de ferramentas de proteção, nessa pesquisa ainda há a falta de conscientização para esta questão. Estas atitudes permitem que ataques e violações à segurança de suas informações ocorram.

Em relação as limitações deste estudo, a principal delas refere-se ao tipo de amostragem, a qual foi não probabilística por conveniência, e desse modo, os resultados e conclusões não podem ser generalizados. Para investigações futuras sugere-se a ampliação deste estudo para uma amostra maior, considerando diferentes faixas etárias e gênero dos respondentes, buscando verificar a existência ou não de diferenças em função destas variáveis.

6 AGRADECIMENTOS

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

REFERÊNCIAS

ARAUJO, Nonata Silva. **Segurança da Informação (TI)**. 2008. Disponível em: <<http://www.administradores.com.br/artigos/tecnologia/seguranca-da-informacao-ti/23933/>>. Acesso em: 06 jul. 2018.

CARDOSO NETO, Celso et al. BACKUP. REVISTA DE TRABALHOS ACADÊMICOS, 2014.



DO ESPÍRITO SANTO, Adrielle Fernanda Silva. **SEGURANÇA DA INFORMAÇÃO**.

FIALHO Jr., M. **Guia essencial do backup**. São Paulo: Digerati Books, 2007. Disponível em: <https://books.google.com.br/books?id=RP8R90IysJQC&printsec=frontcover&hl=pt-BR&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false>. Acesso em: 14 jul. 2018.

GUISSO, L. **Segurança digital: avaliação do nível de conhecimento da população sobre os riscos de segurança atrelados ao uso da internet na região de Bento Gonçalves**. 84 p. 2017. Trabalho de Conclusão de Curso (Curso de Sistemas de Informação), Campus Universitário da Região dos Vinhedos, Universidade de Caxias do Sul, Bento Gonçalves, 2017.

INGIZZA, C. **Nuvem ou HD externo: qual o melhor tipo de backup?** Estadão. 19 de jul. 2017. Disponível em: <<https://link.estadao.com.br/noticias/geral,nuvem-ou-hd-externo-qual-o-melhor-tipo-de-backup,70001895307>>. Acesso em 16 jul. 2018.

JESUS, J. D. P; KAFURE, I. Preservação da informação em objetos digitais. **Biblionline**, v. 6, n. 2, 2011.

JESUS, Guilherme Bindi Alencar; SCHIMIGUEL, Juliano. **IMPLEMENTAÇÃO DE BACKUP COMO PROCESSO DE SEGURANÇA DA INFORMAÇÃO**. **Atlante: Cuadernos de Educación y Desarrollo**, Málaga, v. 00, n. 00, p.1-28, fev. 2018.

MÁRDERO ARELLANO, Miguel Ángel. Preservação de documentos digitais, *Ci. Inf.*, Brasília, v. 33, n. 2, p. 15-27, maio/ago. 2004. Disponível em: <<http://www.scielo.br/pdf/ci/v33n2/a02v33n2.pdf>> Acesso em: 25 mar. 2014.

PALMA, Fernando. **Exemplo de Política da Segurança da Informação**. 2001. Disponível em: <<https://www.portalgsti.com.br/2011/06/exemplo-de-politica-da-seguranca-da-informacao.html>>. Acesso em: 06 jul. 2018.

PIMENTA, A. M. S.; QUARESMA, R. F. C. A segurança dos sistemas de informação e o comportamento dos usuários. **JISTEM-Journal of Information Systems and Technology Management**, v. 13, n. 3, p. 533-552, 2016.

SANTANA, Wallace Rodrigues de. **POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO**. 2016. Disponível em: <http://www.neutronica.com.br/wp-content/uploads/PSI-Material-v1.0-Parte_II.pdf>. Acesso em: 06 jul. 2018.

SANTARENO PIMENTA, Alexandre Manuel; CERQUEIRA QUARESMA, Rui Filipe. A segurança dos sistemas de informação e o comportamento dos usuários. **JISTEM: Journal of Information Systems and Technology Management**, v. 13, n. 3, 2016.

THOMAZ, Kátia de Pádua. A preservação de documentos eletrônicos de caráter arquivístico: novos desafios, velhos problemas. 389f. Tese (Doutorado em Ciência da Informação). Escola de Ciência da Informação. Universidade Federal de Minas Gerais, 2004.