Especificação de um Guia para a Elaboração da Política de Segurança nas Empresas

Eduardo George Henriques Paranhos Garcia[1], Romualdo Monteiro de Resende Costa[2]

[1]Bacherelado de Sistemas de Informação – Centro de Ensino Superior de Juiz de Fora (CES/JF) – Juiz de Fora – MG – Brasil

[2]Centro de Ensino Superior de Juiz de Fora (CES/JF) – Juiz de Fora – MG – Brasil

eduardogeorge@live.com, romualdomrc@gmail.com

Abstract. *One of the mandatory tools in the prevention of security incidents is the specification of a Security Policy, which establishes, among other aspects, the limits of employee actions and punishments arising from actions that may harm the security of the organization's information resources. The preparation of this document is not fixed, on the contrary, it must meet the particular requirements of each company, in order not to disturb the activities of the business. However, in order to meet security requirements, it is necessary for an appropriate Security Policy to take into account current attacks and security standards. In order to establish the minimum requirements for the elaboration of a Security Policy, this work has the purpose of analyzing several documents and establishing, in accordance with the current norms, main points that can later be extended by the organizations, in order to facilitate the implementation of security.*

Resumo. *Uma das ferramentas obrigatórias na prevenção aos incidentes de segurança é a especificação de uma Política de Segurança que estabeleça, entre outros aspectos, os limites das ações dos colaboradores e as punições decorrentes de ações que possam atentar contra a segurança dos recursos de informática da organização. A elaboração desse documento não é fixa, ao contrário, deve atender aos requisitos particulares de cada empresa, a fim de não atrapalhar as atividades próprias do negócio. No entanto, a fim de atender aos requisitos de segurança, é necessário que uma Política de Segurança adequada leve em consideração os atuais ataques e normas de segurança. A fim de estabelecer os requisitos mínimos para a elaboração de uma Política de Segurança, este trabalho tem por finalidade analisar diversos documentos e estabelecer, seguindo as normas vigentes, pontos principais que, posteriormente, poderão ser estendidos pelas organizações, com o objetivo de facilitar a implementação da segurança.*

1. Introdução

Gerenciar e manter um ambiente de tecnologia da informação (TI) seguro tem sido um desafio para organizações de médio e grande porte atualmente. Mesmo com o avanço das ferramentas de gerenciamento e da invenção de novas tecnologias, ainda sim os recursos da empresa estão sempre expostos aos riscos. A preservação da integridade, da confidencialidade e da disponibilidade dos dados são fatores primordiais para a proteção dos ativos da organização, por isso o gerenciamento de riscos é de suma

importância nesse cenário. A segurança da informação protege a informação contra vulnerabilidades no intuito de garantir a continuidade dos processos, minimizar os impactos e maximizar os investimentos e oportunidades do negócio (JÚNIOR, 2008).

Um dos documentos mais importantes para minimizar o risco das empresas é a Política de Segurança (FONTES, 2012), um documento que estabeleça, entre outros aspectos, os limites das ações dos colaboradores e as punições decorrentes de ações que possam atentar contra a segurança dos recursos de informática da organização.

Existe uma grande quantidade de políticas relacionadas à segurança, mas apenas algumas serão aceitas sem muita resistência por um gestor sem que haja a necessidade de uma explicação mais detalhada por um profissional de segurança.

A Política de Segurança é, por definição, uma série de recomendações relacionadas à segurança da informação, que são fornecidas por um profissional da área. Segundo Bayuk (BAYUK, 2012), um profissional de segurança cujo trabalho é compor a Política de Segurança deve assumir o papel de esponja e escriba para a gerência executiva. Uma esponja é um bom ouvinte que é capaz de absorver facilmente o conteúdo da conversa de cada pessoa, independentemente da diversidade do grupo no que diz respeito às habilidades de comunicação e cultura. Um escriba documenta esse conteúdo fielmente sem embelezamento ou anotação. Uma boa esponja e escriba será capaz de capturar temas comuns a partir de entrevistas gerenciais e preparar uma declaração positiva sobre como a organização como um todo quer que sua informação seja protegida. O tempo e o esforço gastos para obter consenso executivo sobre a política compensará na autoridade que empresta ao processo de aplicação da política.

Assim, longe de ser um documento fixo, a Política de Segurança, ao contrário, deve atender aos requisitos particulares de cada empresa, a fim de não atrapalhar as atividades próprias do negócio. E, ao ser elaborada de forma interativa, com a participação da estrutura gerencial da empresa, pode se tornar mais eficiente a implementação das ações especificadas nesse documento.

Apesar da necessidade de uma Política de Segurança que atenda especificamente as características de uma organização, a fim de atender aos requisitos de segurança, é necessário que uma política adequada leve em consideração, ao menos, a possibilidade dos riscos atuais e as normas de segurança existentes. Assim, a proposta deste trabalho é estabelecer quais poderiam ser os requisitos mínimos para a elaboração de uma Política de Segurança a partir da análise de Políticas de Segurança existentes, bem como normas de segurança importantes, como a família de normas 27000[1] (ABNT, 2015) (ABNT, 2018). De posse desse documento inicial referente à Política de Segurança, um profissional da área poderia refiná-lo, em um processo que envolveria maior interação com a área gerencial da empresa. Dessa forma, o profissional da segurança teria um documento inicial que comtemplaria itens amplamente utilizados para ações de segurança das empresas e que poderia ser adaptado, em maiores detalhes, às particularidades da empresa.

Para o desenvolvimento do trabalho, a próxima seção apresenta uma análise de diversas Políticas de Segurança encontradas em empresas onde itens que poderiam fazer parte de uma política foram coletados. A seguir, a terceira seção apresenta uma análise das normas 27000 que complementam os itens de segurança relevantes que deveriam, eventualmente, fazer parte de uma Política de Segurança. A partir dos itens selecionados,

[1]https://standards.iso.org/ittf/PubliclyAvailableStandards/c073906_ISO_IEC_27000_2018_E.zip

a Seção 4 apresenta uma sugestão de elaboração de documentos utilizando ferramentas do Google Docs[2]. Por fim, a última seção apresenta as conclusões e alguns possíveis trabalhos futuros.

2. Políticas de Segurança

Segundo Campos (CAMPOS, 2007) "A informação é o elemento essencial para todos os processos de negócio da organização, sendo, portanto, um bem ou ativo de grande valor". A partir dessa definição pode-se afirmar que a informação se tornou uma parte valiosa das organizações sendo, com isso, alvo de uma série de ameaças que tentam explorar as vulnerabilidades, causando prejuízos. Existe, portanto, a necessidade de implementar políticas de segurança da informação, que visem reduzir as chances de fraudes ou mesmo de perda de informações.

Diferentes autores (JUNIOR, 2008) (ARAÚJO, 2008) (BAYUK, 2012) (DANTAS, 2011) descrevem necessidades diversas de segurança que devem ser implementadas nas políticas. Apesar de serem propostas em momentos diversos, por diferentes autores e do tema relacionado à segurança ser amplo, é possível encontrar pontos em comum presentes nos artigos analisados, principalmente a preocupação com a confidencialidade, com a integridade e com a disponibilidade (BAYUK, 2012).

Em relação à preservação da informação, seja qual for a forma de armazenamento ou transmissão da informação, a informação precisa estar resguardada das ameaças existentes. Evidentemente, um significante aumento da interconectividade faz com que a informação esteja exposta a várias ameaças.

Muitas vezes, as informações presentes nos sistemas são confidenciais. Esse conceito define que a informação seja acessível apenas a pessoas autorizadas. O acesso às informações por pessoas não autorizadas, faz com que haja uma quebra na segurança e, com isso, pode acarretar prejuízos financeiros ou então a divulgação de projetos confidenciais. Toda e qualquer informação, cujo comprometimento possa causar perda de vantagem competitiva, pode gerar um dano ou prejuízo ao negócio ou a imagem da organização (ARAÚJO, 2008).

A integridade nada mais é do que a garantia da informação não ter sido alterada, ou seja, a proteção à precisão e a completude dos ativos de informação, garantindo que a informação só será alterada de forma autorizada e não acidental. Por fim, a disponibilidade é a garantia que o usuário tenha acesso a informação e aos dados correspondentes sempre que houver necessidade. Quando não houver a possibilidade de acessar a informação, isso configura uma quebra de disponibilidade (DANTAS, 2011).

Assim, embora uma política de segurança não seja algo pronto, que possa ser implementado diretamente em toda e qualquer organização, é inegável que essas políticas terão vários pontos em comum, que derivam, justamente, das preocupações comuns de segurança que incluem, como citado, a preservação da informação, com aspectos de disponibilidade, integridade e confidencialidade (JÚNIOR, 2008).

Para tentar identificar aspectos mais precisos de itens comuns em diferentes políticas de segurança foram analisando planos sobre as políticas de segurança da

[2] https://docs.google.com

informação de grandes e pequenas empresas, escolhidas aleatoriamente. A Tabela 1 apresenta o nome da organização e o endereço (URL) de 23 diferentes políticas de segurança de organizações dos mais diferentes segmentos, que incluem ensino, tecnologia, empresas de investimento, energia, administração pública, entre outras.

Tabela 1. Empresas escolhidas para o levantamento dos itens existentes nas políticas de segurança (do autor)

Área	Organização	Política de Segurança
Financeiro	RIO BRAVO INVESTIMENTOS	URL[3]
	BOVESPA	URL[4]
	VINCI PARTNERS	URL[5]
	SERPROS	URL[6]
	SANTANDER	URL[7]
	Modal	URL[8]
Hospitalar	GHC	URL[9]
Telecomunicações	OI	URL[10]
Energia	RAÍZEN	URL[11]
Educação	EMESCAM	URL[12]
	SENAC	URL[13]
	UFCE	URL[14]
	IFCE	URL[15]
	IFAM	URL[16]
	TOTVS	URL[17]
Tecnologia	ITEAM	URL[18]
	SESI	URL[19]
Indústria	FIEB	URL[20]
	Cia Docas do Pará	URL[21]
Administração Pública	INMETRO	URL[22]

[3]https://www.riobravo.com.br/RioBravo/Compliance/PGC_07_Pol%C3%ADtica%20de%20Segurança%20da%20Informação%20e%20Segurança%20Cibernética.pdf

[4]http://ri.bmfbovespa.com.br/fck_temp/26_107/file/Pol%C3%ADtica%20de%20Seguran%C3%A7a%20da%20Informa%C3%A7%C3%A3o%2020160513.pdf

[5] https://www.vincipartners.com/uploads/114079371.pdf

[6] http://serpros.com.br/wp-content/uploads/2019/03/Politica_de_Seguranca_da_Informacao_v2019.pdf

[7] https://www.santander.com.br/document/wps/politica_seguranca_informacao_fev_13.pdf

[8] https://www.modaldtvm.com.br/wp-content/uploads/2014/06/Politica-Seguranca-Informacao.pdf

[9] https://www.ghc.com.br/files/PSI_GHC.pdf

[10] https://www.oi.com.br/oi/sobre-a-oi/empresa/informacoes/politica-de-seguranca-informacao/

[11] https://www.raizen.com.br/sites/default/files/fornecedores_seguranca_da_informacao.pdf

[12] http://www.emescam.br/informatica/arquivos/politicas-seguranca-informacao-v1.pdf

[13] http://www.sp.senac.br/normasadministrativas/psi_normas_administrativas.pdf

[14] http://www.seginfo.ufc.br/wp-content/uploads/2019/02/posic-rev.05-dseg.pdf

[15] https://ifce.edu.br/dgti/governanca/arquivo/023-17-aprova-a-politica-de-seguranca-da-informacao-do-ifce.pdf

[16] http://www.ifam.edu.br/portal/images/file/PSI_autorizada.pdf

[17] http://www.pe.sesi.org.br/Documents/Manual%20de%20Seguranca%20da%20Informacao.pdf

[18] https://it-eam.com/psi2018.pdf

[19] http://www.pe.sesi.org.br/Documents/Manual%20de%20Seguranca%20da%20Informacao.pdf

[20] http://www.fieb.org.br/Adm/FCKimagens/file/FIEB/2014/PSI%20.pdf

[21] https://www.cdp.com.br//documents/10180/bba74dae-cc38-459f-850c-5b3b6c7cb30e

[22] http://www4.inmetro.gov.br/sites/default/files/media/file/politica-de-seguranca-da-informacao-e-comunicacoes-inmetro-2015.pdf

	IPHAN	URL[23]
	IBGE	URL[24]
	TCU	URL[25]
	FUNPRESP	URL[26]
	EBSERH	URL[27]
	INFRAERO	URL[28]
	SANEAGO	URL[29]

A partir da leitura cuidadosa das políticas de segurança das organizações listadas na Tabela 1 foram identificados 19 itens que compõem essas políticas na sua totalidade. Entre esses itens estão o "Tratamento da Informação" onde são definidas medidas sobre o ciclo de vida da informação, desde a sua aquisição ou produção, até a sua eliminação.

Também são encontrados itens referentes a utilização de serviços, como o "Controle de Acesso" onde são definidas as regras gerais para utilização dos serviços, bem como, eventualmente, o uso de senhas. Serviços mais específicos também são eventualmente especificados, de acordo com a sua importância, incluindo, por exemplo, o "Correio Eletrônico", "Backup", "Acesso à Internet", "Mensagens Instantâneas", "Conteúdo Multimídia", como rádio, TV, streaming de vídeo, "Uso de Redes Sociais" e "Uso de Dispositivos Móveis".

Algumas políticas fazem menção aos ativos, sejam equipamentos físicos que foram identificados através do item "Ativos de Informação", sejam informações, que foram identificados através do item "Ativos de Tecnologia da Informação". Nas políticas também é possível encontrar restrições em relação ao "Data Center" e a outras instalações, identificadas através do item "Controle de Acesso Físico". Algumas políticas detalham elementos referentes ao desenvolvimento e aquisição de sistemas ("Desenvolvimento e Aquisição de Sistemas").

Itens específicos de segurança de informação foram encontrados nas políticas analisadas, incluindo a "Gestão de Continuidade", que trata das medidas para preservar o funcionamento, ou ao menos minimizar os efeitos adversos de ataques sobre os ativos, a "Gestão de Riscos", que trata da análise de potenciais problemas, a verificação de atendimento às normas, através do item "Conformidade". Foram encontrados também itens relacionados a tarefa de verificação das proposições com o que foi, de fato, implementado, através de itens como a "Auditoria do Ambiente" e "Auditoria".

A distribuição dos itens mencionados nas políticas de cada organização é detalhada nas Tabelas 2, 3, 4, 5 e 6.

[23] http://portal.iphan.gov.br/uploads/ckfinder/arquivos/Pol%C3%ADtica%20de%20Seguran%C3%A7a%20da%20Informa%C3%A7%C3%A3o.pdf

[24] https://ww2.ibge.gov.br/home/disseminacao/eventos/missao/Politica_de_Seguranca_da_Informacao_e_Comunicacoes_2016.pdf

[25] http://www4.planalto.gov.br/cgd/assuntos/publicacoes/2511466.pdf

[26] http://www.funprespjud.com.br/wp-content/uploads/2017/01/Politica-de-Seguranca-da-Informacao-Funpresp-Jud_2016.pdf

[27] http://www2.ebserh.gov.br/documents/16824/0/Pol%C3%ADtica+de+Segurança+da+Informação/0468172b-9e8e-4d30-8e36-38334521d341

[28] https://www4.infraero.gov.br/media/674039/politica-de-seguranca-da-informacao-e-comunicacoes-posic.pdf

[29] http://www.saneago.com.br/2016/investidores/politica/PL04.0006.00.pdf

Tabela 2. Itens encontrados nas políticas de segurança das empresas (do autor)

Empresa/Item Considerado	RIO BRAVO INVEST.	ITEAM	VINCI PARTNERS	SANEAGO	EBSERH	RAÍZEN
Tratamento da informação	✗	✗	✗	✗	☑	✗
Controle de acesso	✗	☑	☑	☑	☑	☑
Correio eletrônico	☑	☑	☑	☑	☑	☑
Serviço de backup	✗	☑	☑	☑	✗	☑
Data center	✗	✗	✗	✗	✗	✗
Auditoria do ambiente	✗	✗	✗	✗	✗	✗
Acesso à Internet	☑	✗	☑	☑	✗	☑
Gestão de riscos	✗	✗	✗	☑	☑	✗
Gestão de continuidade	✗	✗	✗	✗	☑	✗
Tratamento de incidentes em redes computacionais	✗	✗	✗	☑	☑	✗
Ativos da informação	✗	✗	✗	✗	✗	✗
Ativos de tecnologia da informação	✗	✗	✗	✗	✗	✗
Controle de acesso físico a equipamentos	✗	✗	✗	☑	✗	☑
Conformidade	✗	✗	✗	✗	☑	✗
Auditoria	✗	✗	✗	✗	☑	✗
Desenvolvimento e aquisição de sistemas	✗	✗	✗	☑	☑	✗
Sistema de Mensagens	☑	✗	✗	✗	✗	☑
Uso de redes sociais	✗	✗	✗	✗	☑	✗
Uso de dispositivos móveis	✗	☑	☑	☑	☑	✗

Tabela 3. Itens encontrados nas políticas de segurança das empresas (do autor)

Empresa/Item Considerado	IFCE	INFRAERO	BOVESPA	EMESCAM	SENAC
Tratamento da informação	☑	☑	☑	☑	☑
Controle de acesso	✗	☑	☑	✗	✗
Correio eletrônico	✗	✗	✗	☑	☑
Serviço de backup	✗	✗	✗	☑	☑
Data center	✗	✗	✗	✗	☑
Monitoramento e auditoria do ambiente	✗	✗	☑	☑	☑
Uso e acesso a internet	☑	✗	✗	☑	☑
Gestão de riscos	☑	☑	✗	✗	☑
Gestão de continuidade	☑	☑	✗	✗	✗
Tratamento de incidentes em redes computacionais	☑	☑	☑	✗	☑
Ativos da informação	☑	✗	✗	✗	✗
Ativos de tecnologia da informação	✗	✗	✗	✗	✗
Controle de acesso físico a equipamentos	☑	✗	✗	☑	☑
Conformidade	✗	✗	✗	✗	✗
Auditoria	✗	✗	✗	✗	✗

Desenvolvimento e aquisição de sistemas	☑	☑	✗	✗	✗
Sistema de Mensageria	✗	✗	✗	✗	✗
Uso de redes sociais	☑	✗	✗	✗	☑
Uso de dispositivos móveis	✗	✗	✗	☑	☑

Tabela 4. Itens encontrados nas políticas de segurança das empresas (do autor)

Empresa/Item Considerado	**UFCE**	**OI**	**IFAM**	**Cia Docas PA**	**SERPROS**
Tratamento da informação	✗	☑	☑	✗	☑
Controle de acesso	☑	☑	☑	☑	☑
Correio eletrônico	✗	✗	☑	☑	✗
Serviço de backup	✗	✗	☑	☑	✗
Data center	✗	✗	✗	✗	✗
Monitoramento e auditoria do ambiente	✗	☑	✗	✗	✗
Uso e acesso à internet	✗	✗	✗	☑	✗
Gestão de riscos	☑	☑	✗	✗	✗
Gestão de continuidade	☑	✗	✗	☑	☑
Tratamento de incidentes em redes computacionais	✗	✗	☑	✗	☑
Ativos da informação	☑	✗	✗	✗	✗
Ativos de tecnologia da informação	✗	✗	✗	✗	☑
Controle de acesso físico a equipamentos	✗	✗	✗	✗	✗
Conformidade	☑	✗	✗	✗	✗
Auditoria	☑	☑	✗	✗	✗
Desenvolvimento e aquisição de sistemas	✗	✗	✗	☑	✗
Sistema de Mensageria	✗	✗	✗	✗	✗
Uso de redes sociais	✗	✗	✗	✗	✗
Uso de dispositivos móveis	✗	✗	✗	☑	✗

Tabela 5. Itens encontrados nas políticas de segurança das empresas (do autor)

Empresa/Item Considerado	**FIEB**	**SANTANDER**	**INMETRO**	**IPHAN**	**IBGE**
Tratamento da informação	☑	☑	☑	☑	☑
Controle de acesso	☑	☑	☑	☑	☑
Correio eletrônico	☑	✗	☑	☑	✗
Serviço de backup	☑	✗	✗	☑	✗
Data center	✗	✗	✗	☑	✗
Monitoramento e auditoria do ambiente	✗	✗	✗	☑	✗
Uso e acesso à internet	☑	☑	☑	☑	☑
Gestão de riscos	✗	✗	✗	☑	☑
Gestão de continuidade	✗	✗	☑	☑	✗

Tratamento de incidentes em redes computacionais	☑	×	☑	☑	☑
Ativos da informação	×	×	☑	×	☑
Ativos de tecnologia da informação	×	×	×	×	☑
Controle de acesso físico a equipamentos	☑	×	☑	×	☑
Conformidade	×	×	☑	×	☑
Auditoria	×	×	☑	×	☑
Desenvolvimento e aquisição de sistemas	☑	×	×	×	☑
Sistema de Mensageria	×	×	×	×	☑
Uso de redes sociais	☑	×	☑	×	×
Uso de dispositivos móveis	☑	×	☑	×	×

Tabela 6. Itens encontrados nas políticas de segurança das empresas (do autor)

Empresa/Item Considerado	**MODAL**	**GHC**	**TOTVS**	**SESI**	**TCU**	**FUNPRESP**
Tratamento da informação	☑	☑	☑	×	☑	☑
Controle de acesso	☑	☑	☑	×	×	☑
Correio eletrônico	☑	×	×	☑		☑
Serviço de backup	☑	☑	×	×	×	×
Data center	☑	×	☑	×	×	☑
Monitoramento e auditoria do ambiente	☑	☑	×	☑	×	×
Uso e acesso à internet	☑	☑	×	☑	×	☑
Gestão de riscos	☑	☑	☑	×	☑	×
Gestão de continuidade	☑	☑	☑	×	☑	☑
Tratamento de incidentes em redes computacionais	☑	☑	×	×	☑	×
Ativos da informação	×	×	×	×	×	×
Ativos de tecnologia da informação	×	☑	×	×	×	☑
Controle de acesso físico a equipamentos	☑	☑	☑	×	×	☑
Conformidade	☑	☑	×	×	×	×
Auditoria	×	×	☑	×	×	×
Desenvolvimento e aquisição de sistemas	☑	×	×	×	×	×
Sistema de Mensageria	×	×	×	×	×	×
Uso de redes sociais	×	×	×	×	×	☑
Uso de dispositivos móveis	☑	×	×	×	×	☑

A partir da análise das Tabela 2, 3, 4, 5 e 6 não foi possível identificar uma hegemonia no conteúdo das Políticas de Segurança da Informação, independente do nicho da empresa e do tamanho dela. Para proporcionar uma melhor visualização em relação aos 19 itens catalogados, esses itens foram representados como gráficos com valores percentuais relativos a sua ocorrência nas políticas de segurança das empresas. A Figura 1 apresenta três desses gráficos, que representam a participação dos itens

“Tratamento da Informação”, “Controle de Acesso” e “Ativos da Informação”, nas políticas analisadas.

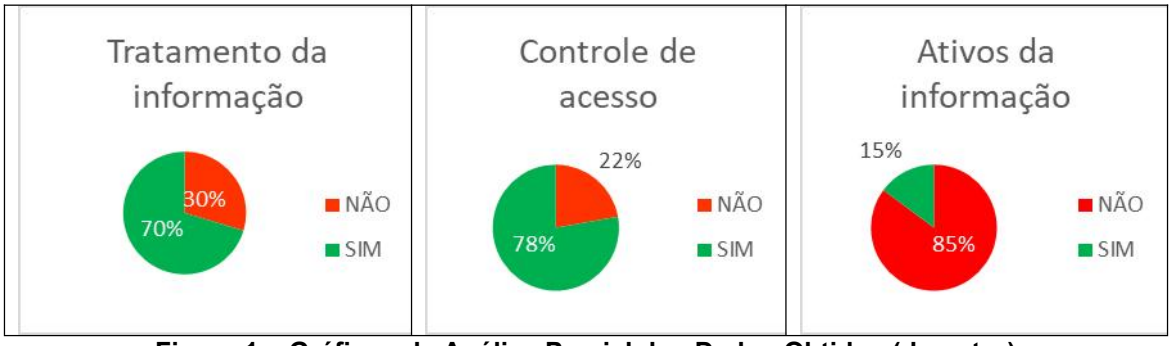


Figura 1 – Gráficos da Análise Parcial dos Dados Obtidos (do autor)

Conforme observado na Figura 1, a maioria das empresas, cerca de 70%, definem regras para o item “Tratamento da Informação”, o total de 78% das empresas analisadas trata do item “Controle de Acesso”, onde são definidas as regras gerais para utilização dos serviços, bem como, eventualmente, o uso de senhas. O controle de acesso está presente na quase totalidade das empresas pesquisas. Esse fato é importante porque, embora não elimine totalmente os riscos à segurança da informação, diminui, em muito, a possibilidade de que ocorram incidentes que prejudiquem a continuidade das atividades da empresa. Diversas políticas, como observado na Figura 1, fazem menção aos ativos, sejam equipamentos físicos que foram identificados através do item “Ativos de Informação, sejam informações, que foram identificados na Figura 2 através do item “Ativos de Tecnologia da Informação”.

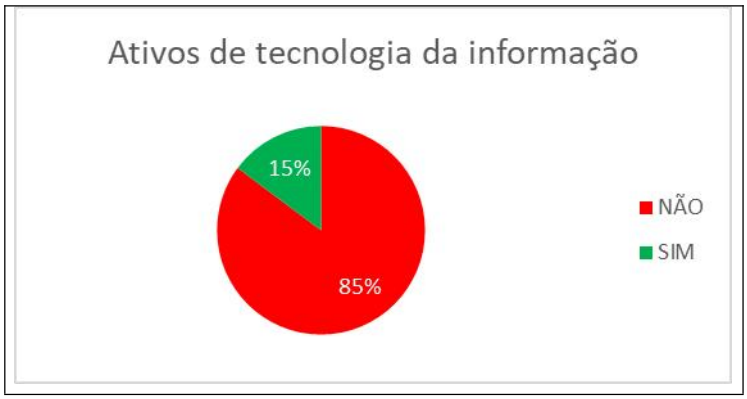


Figura 2 – Gráficos da Análise Parcial dos Dados Obtidos (do autor)

Nas políticas também é possível encontrar restrições em relação ao “Data Center” Algumas políticas detalham elementos referentes aos desenvolvimentos e aquisição de sistemas (“Desenvolvimento e Aquisição de Sistemas”). O percentual das empresas que fazem menção a esses itens está representado na Figura 3. Essa figura

também apresenta o percentual das empresas que estabelece uma restrição em relação ao acesso às instalações, identificadas através do item “Controle de Acesso Físico”.

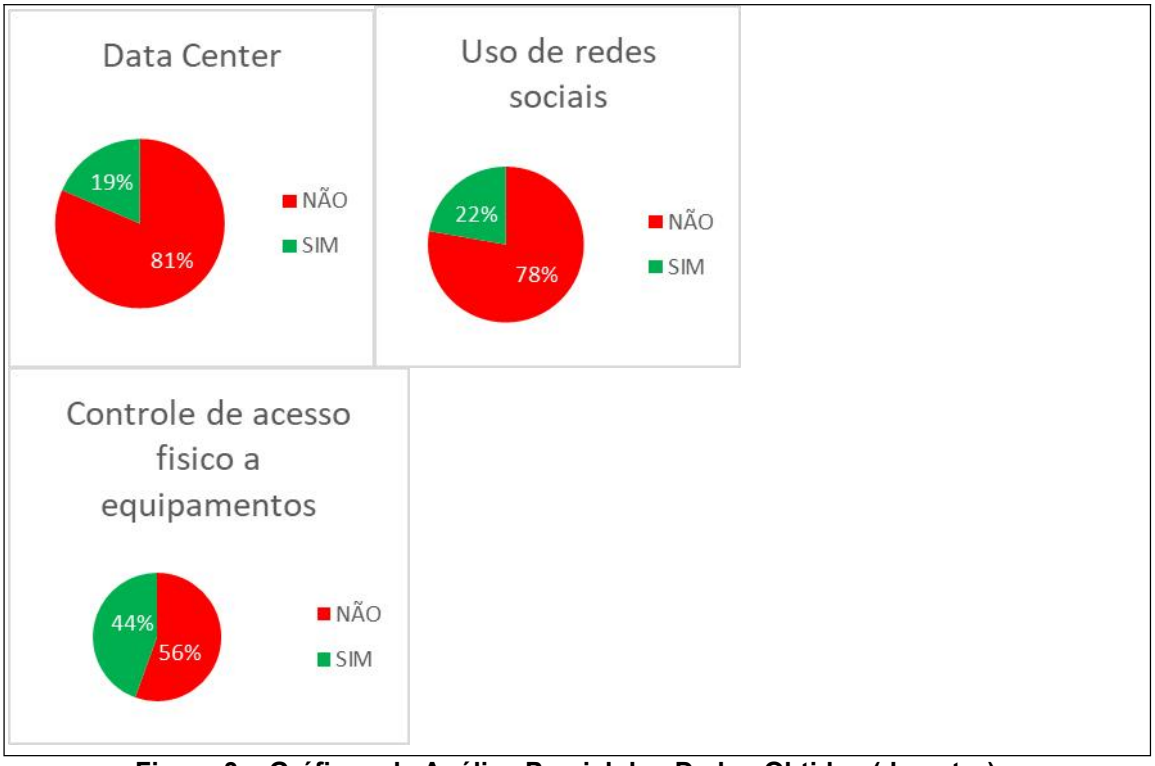


Figura 3 – Gráficos da Análise Parcial dos Dados Obtidos (do autor)

Itens específicos de segurança de informação foram encontrados nas políticas analisadas, incluindo a “Gestão de Continuidade”, que trata das medidas para preservar o funcionamento ou, ao menos, minimizar os efeitos adversos de ataques sobre os ativos. Como é possível observar na Figura 4, treze empresas mencionam planos de gestão de continuidade. Cabe ressaltar que são justamente os equipamentos e sistemas antigos os que normalmente são mais vulneráveis às ameaças externas e falhas.

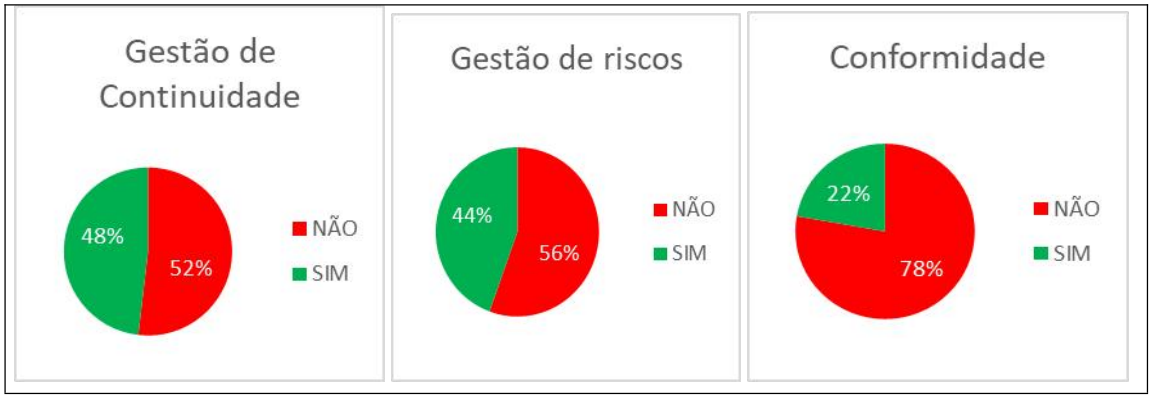


Figura 4 – Gráficos da Análise Parcial dos Dados Obtidos (do autor)

A “Gestão de Riscos”, que trata da análise de potenciais problemas também é apresentada na Figura 4. Nesse item, cerca de 56% das empresas analisadas não possuem na sua documentação uma parte dedicada a “Gestão de Risco”, o que pode gerar uma série de problemas para a organização como, por exemplo, o aumento de custos dos equipamentos, dificuldades para implementar mudanças nos sistemas em caso de alguma mudança na legislação, dificuldades de implantação de novas tecnologias, aumentos nos custos entre outros. Por fim, a Figura 4 apresenta o percentual de empresas onde a verificação de atendimento às normas, através do item “Conformidade” é implementada. Esse item envolve as ações da empresa que necessitam estar de acordo com as políticas implementadas.

Foram encontrados também itens relacionados a tarefa de verificação das proposições com o que foi, de fato, implementado, através de itens como a “Auditoria”, cujo percentual de definições nas políticas de segurança é apresentado na Figura 5.

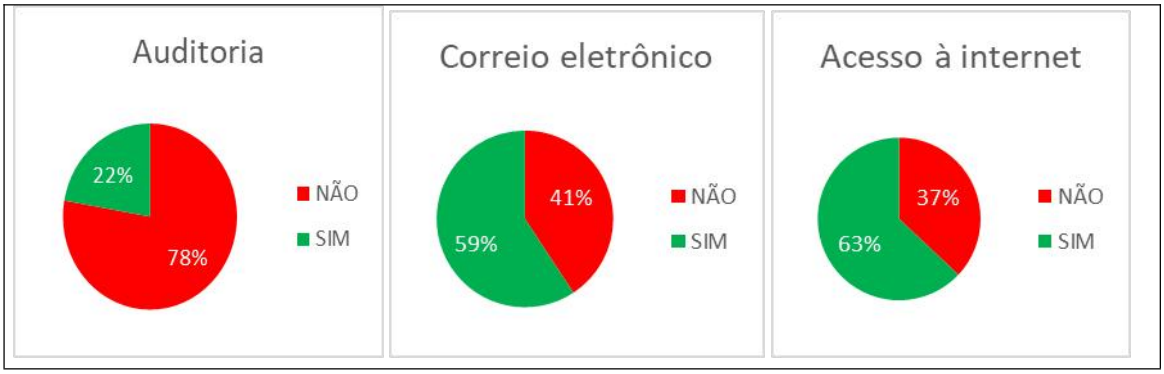
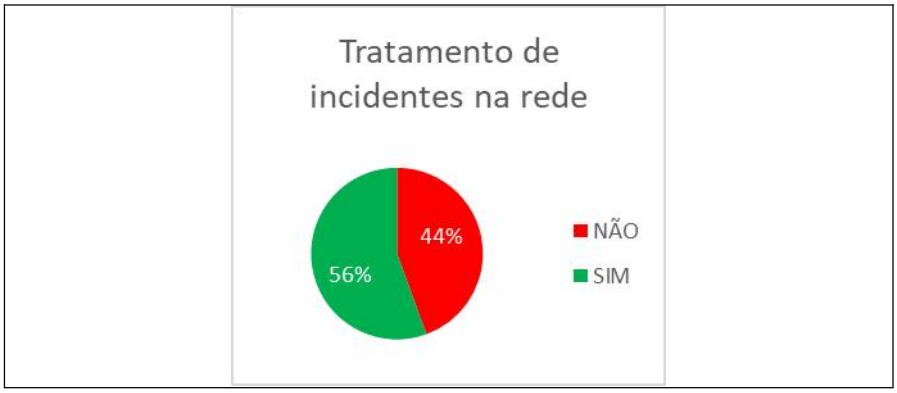


Figura 5 – Gráficos da Análise Parcial dos Dados Obtidos (do autor)

Na Figura 5, o percentual de itens relacionados à serviços mais específicos também são especificados. Esses itens, incluem, por exemplo, o “Correio Eletrônico”, “Acesso à Internet”, “Mensagens Instantâneas”, “Conteúdo Multimídia”, como rádio, TV, streaming de vídeo, “Uso de Redes Sociais” e “Uso de Dispositivos Móveis”. Sendo esses últimos apresentados na Figura 6.



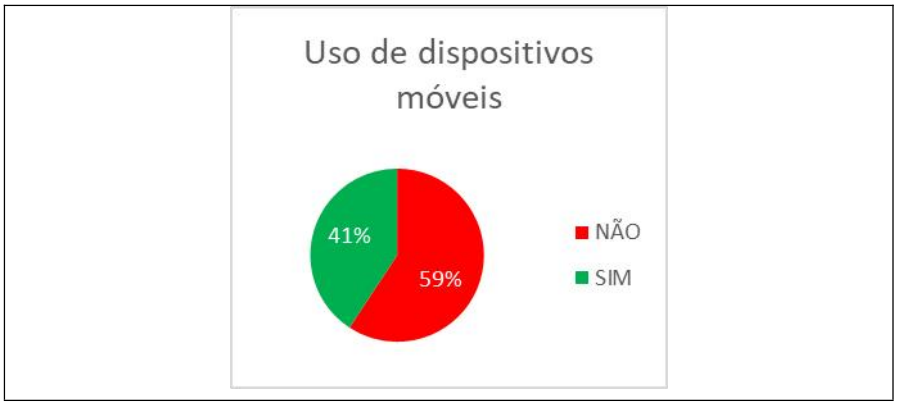


Figura 6 – Gráficos da Análise Parcial dos Dados Obtidos (do autor)

A partir da análise dos vários documentos de políticas de segurança não foi possível identificar uma hegemonia no conteúdo das Políticas de Segurança da Informação, independente do nicho da empresa e do tamanho dela. Como exemplo, as políticas do INMETRO e do IBGE contemplam diversos itens relevantes, mas, não possuem definições a respeito do sistema de backup. Aliás, definições sobre esse item não se encontram presentes em onze das empresas analisadas. Conforme apresentado na Figura 7.

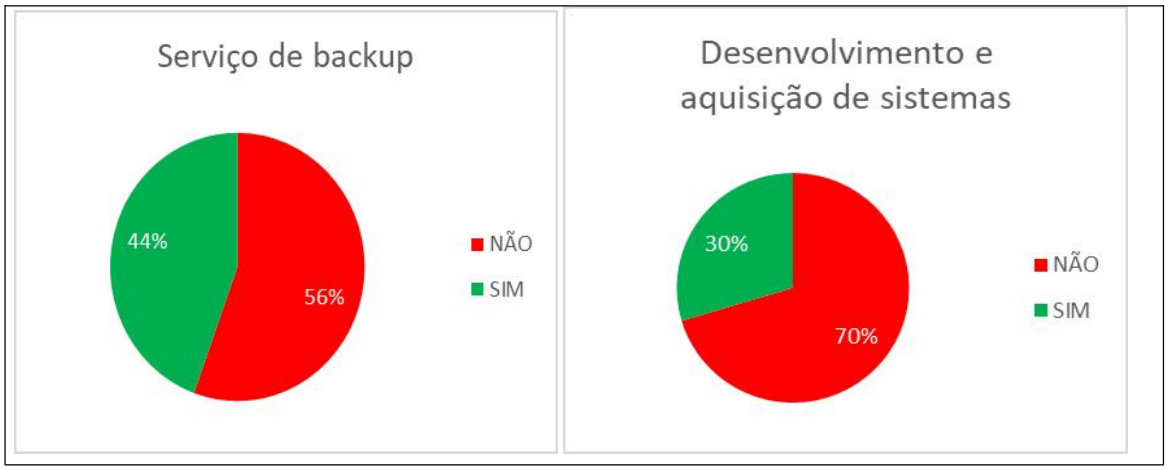


Figura 7 – Gráficos da Análise Parcial dos Dados Obtidos (do autor)

Apenas sete das empresas analisadas, que corresponde a um percentual de 25% da amostra considerada, mencionam na política um plano de desenvolvimento e aquisição de sistemas, como apresentado também na Figura 7.

As políticas de segurança da informação precisam ser constantemente revisadas e analisadas junto a novas ameaças presentes diariamente na informática e, através da análise, é possível observar que muitos planos estão defasados em relação aos seus conteúdos. É possível que tenha ocorrido a especificação e implantação do plano e, posteriormente, não houve uma atualização do mesmo em relação às novas tecnologias e ameaças.

3. Normas ISO 27001/27002

A norma da ISO 27001 (ABNT, 2015) estabelece diretrizes e princípios gerais para se iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Essa norma possui uma introdução sobre o processo de avaliação e tratamento de riscos e está dividida em catorze seções específicas, que são: políticas de segurança de informação; organização da segurança da informação; segurança em recursos humanos; gestão de ativos; controle de acesso; criptografia; segurança física e do ambiente; segurança nas operações; segurança nas comunicações; aquisição, desenvolvimento e manutenção de sistemas de informação; relacionamento na cadeia de suprimento; gestão de incidentes de segurança da informação; gestão da continuidade do negócio e gestão da conformidade. Essas seções, por sua vez, são detalhadas na norma da ISO 27002 (ABNT, 2018), que estabelece um guia prático para o desenvolvimento e implementação de procedimentos e controles de segurança da informação.

Na norma ISO 27002 cada seção define um ou mais objetivos de controle que nada mais são do que boas práticas para que a organização adote uma postura preventiva e proativa diante dos requisitos de segurança da informação. Particularmente, o controle inicial trata das políticas de segurança da informação e é formado por dois controles, conforme a Figura 8.

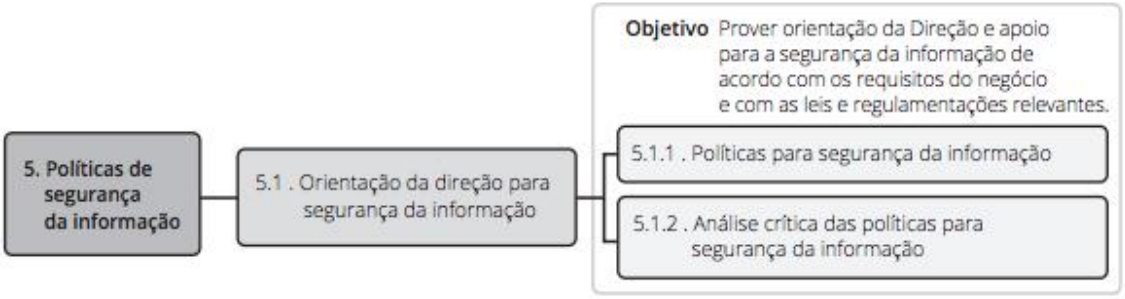


Figura 8 – Seção Políticas de Segurança da Informação (ABNT, 2018)

Na Figura 8, a seção é formada por dois controles. O primeiro, intitulado como "Políticas para segurança da informação", define que as especificações sobre a gerência e os objetivos da segurança da informação devem ser especificadas no nível mais alto da organização e que essa política deve contemplar a estratégia do negócio, a regulamentação, legislações e contratos e o ambiente de ameaça à segurança da informação, tanto atual quanto futuro. Esse controle ainda define que a política de segurança da informação deve conter declarações sobre os objetivos e os princípios para orientar os colaboradores. Define também que na política devem ser atribuídas as responsabilidades, gerais e específicas, com papéis definidos. Por fim, ela especifica que a política deve conter processos para o tratamento de possíveis desvios nas determinações, bem como para as exceções.

Assim, é possível observar que a norma, particularmente em relação à política de segurança, não define tópicos específicos e sim recomendações sobre a sua construção. Particularmente, ainda em relação ao controle inicial apresentado na Figura 7, ele estabelece que são recomendáveis a especificação de itens específicos, voltados à grupos da organização que incluam, entre outras ações, o controle de acesso, a classificação e o tratamento da informação, o treinamento dos usuários finais, o backup, a transferência das informações, entre outros.

O segundo controle apresentado na Figura 8, intitulado “Análise crítica das políticas para segurança da informação”, define que as políticas de segurança da informação sejam analisadas criticamente a intervalos planejados ou quando mudanças significativas ocorrerem. Esse controle, em particular, destaca a importância de um modelo automatizado para auxiliar na construção e, possivelmente na manutenção da política de segurança da informação das empresas, facilitando as modificações necessárias.

As demais seções e seus controles da norma ISO 27002 devem ser empregadas na definição das Políticas de Segurança das organizações. No entanto, como já mencionado, essas seções e seus controles são diretrizes que devem ser analisadas e implementadas de acordo com a realidade específica de cada organização. Assim, a proposta deste trabalho é que esses controles estejam associados aos itens já levantados na seção anterior e que possam ser apresentados ao elaborador da política de segurança por ocasião da sua construção, como será apresentado na próxima seção.

4. Guia para a Construção da Política de Segurança

A partir da análise das políticas de segurança mencionadas na Seção 2 foi possível estabelecer uma estrutura comum presente em grande parte desses documentos que, na proposta deste trabalho é dividida em duas partes. A primeira, definida como escopo, contém as informações gerais da política, incluindo sua definição, o nome da empresa, a data de emissão e revisões realizadas no documento, bem como associações entre as especificações do documento e as previsões legais. Informações sobre os responsáveis pela aprovação, implantação e treinamento da política também constam dessa parte, que termina com o modelo definido para a sua distribuição. Na segunda, definida como objetivo, estão os elementos técnicos, que foram levantados a partir da análise dos itens encontrados em diversas políticas de segurança analisadas na segunda seção deste trabalho, complementados com as definições encontradas nas normas ISO 27001 e 27002.

A Figura 9 apresenta a tela inicial do formulário que permite a construção da política baseada nos itens levantados ao longo deste trabalho. Através do e-mail, o usuário tem acesso a uma segunda tela, onde permanecem salvos os itens relacionados ao escopo da política.

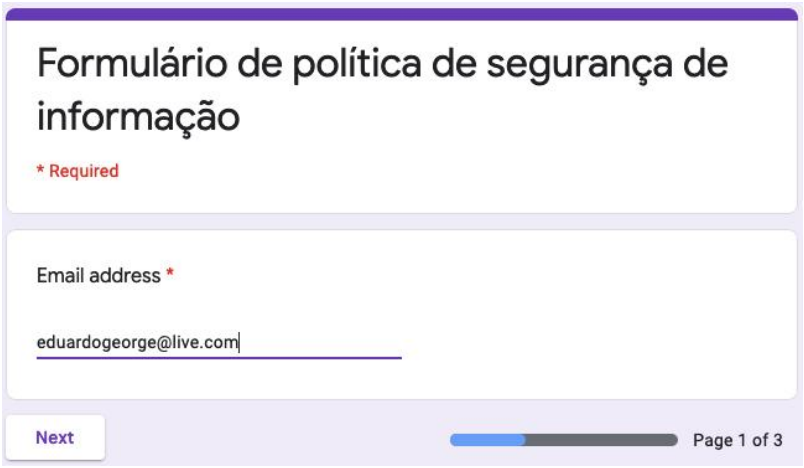


Figura 9 – Formulário de Políticas de Segurança da Informação (Fonte do autor)

Sobre o escopo, as opções iniciais, apresentadas parcialmente na Figura 10, incluem os dados da empresa, com informações sobre o nome destinado à política, o nome da empresa, a sua visão de negócios e as datas de emissão e da última revisão da política de segurança. Alguns desses campos foram omitidos da figura para simplificar a visualização.

Ainda no contexto do escopo da política, a Figura 11 apresenta informações complementares sobre a construção do documento que incluem o autor, o país e a documentação legal associada, bem como o período considerado e documentações associadas, incluindo documentos que poderiam estar anexados. Novamente, alguns campos foram omitidos para simplificar a representação da figura.

Figura 10 – Dados iniciais do Escopo da Empresa (Fonte do autor)

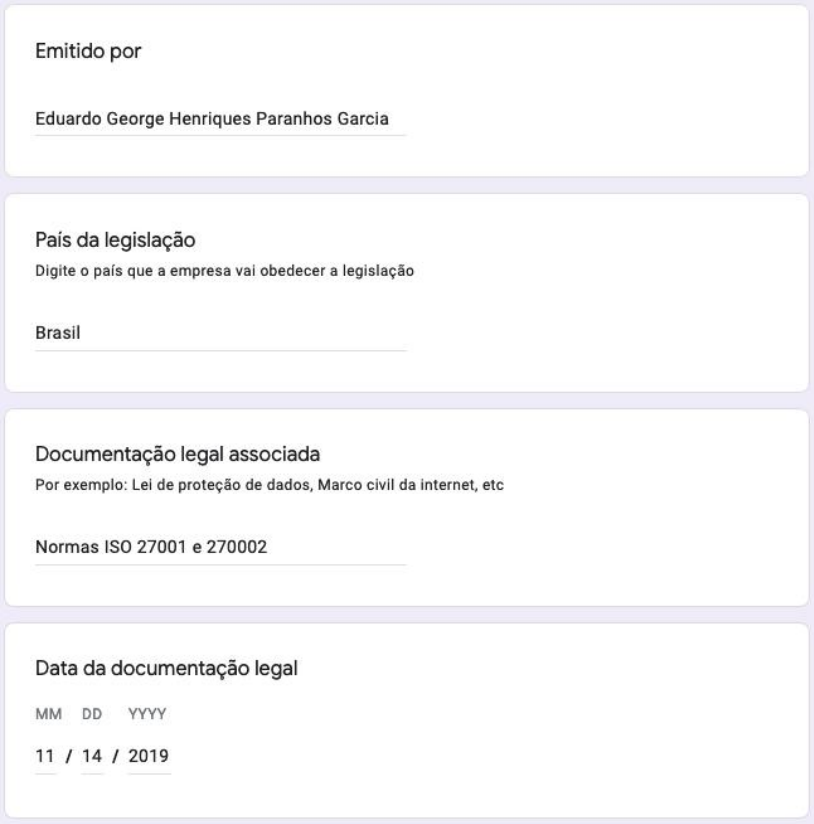


Figura 11 – Dados do escopo referentes à elaboração do documento (Fonte do autor)

Finalmente, os dados referentes ao escopo da política de segurança são encerrados com as informações referentes a sua aprovação que incluem o nome do responsável com a respectiva data de aprovação, o nome do responsável pela implantação com a respectiva data e o nome do responsável pelo treinamento, também com a data. Finalizando com a descrição do método empregado na distribuição dessa política, conforme apresentado na Figura 12, que apresenta esses campos de forma parcial.

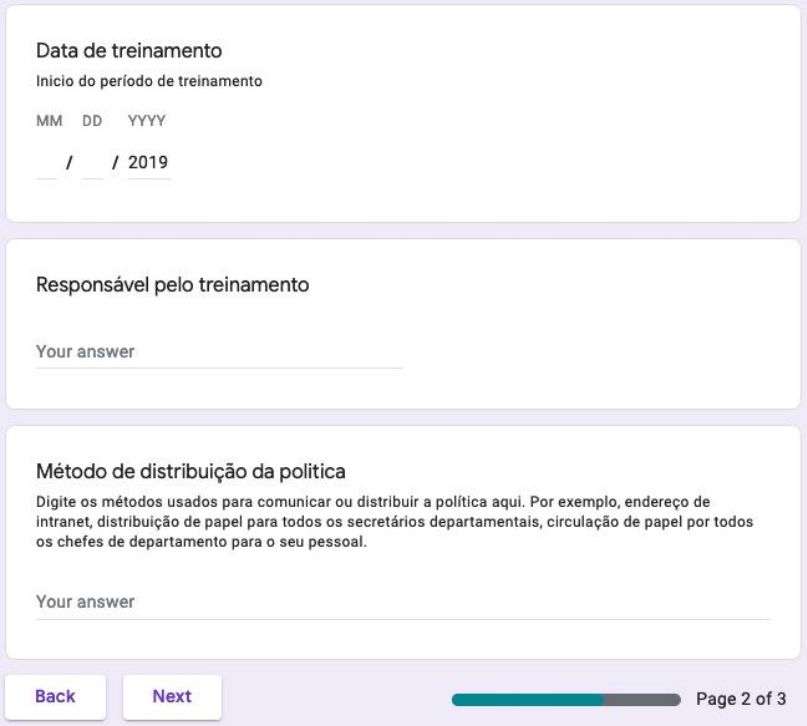


Figura 12 – Dados da aprovação, implantação, treinamento e distribuição (Fonte do autor)

Após a especificação das informações iniciais, referentes ao escopo, o usuário é guiado para a parte referente aos objetivos da política de segurança, cujos itens foram levantados, como já mencionado, a partir da análise de dezenas de políticas de segurança de organizações dos mais diversos segmentos. Assim, após definição inicial, apresentada na Figura 13, que corresponde ao âmbito da política, isto é, a quais elementos computacionais da organização a política se aplica, o usuário deve informar aspectos da política referente ao tratamento da informação, seguido pelos aspectos referentes ao controle de acesso.

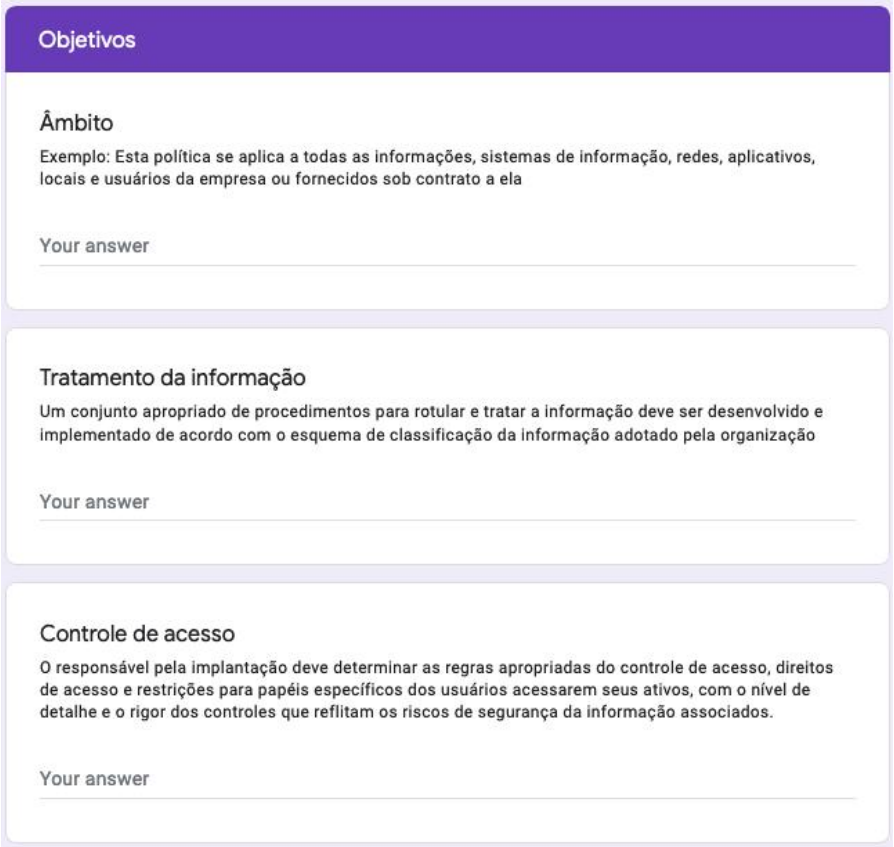


Figura 13 – Início dos aspectos objetivos da política de segurança (Fonte do autor)

Como ilustrado na Figura 13, para cada item do formulário uma explicação relacionada é apresentada, essa explicação é baseada nas políticas definidas na norma 27001 e complementada pela norma 27002. Assim, para cada item escolhido entre os itens usuais encontrados em uma política de segurança foi elaborada uma explicação que tem por objetivo ajudar os responsáveis pelo seu preenchimento nessa tarefa. Cabe destacar também que o preenchimento dos itens é opcional. Os itens não preenchidos simplesmente não farão parte do relatório final.

Os demais itens que compõem a parte objetiva do guia são formados pela especificação do uso do correio eletrônico, sobre o serviço de backup, sobre a gerência de data center, sobre os processos de auditoria, sobre o acesso à Internet, sobre o planejamento referente à gestão de riscos e gestão da continuidade, sobre o tratamento de incidentes na rede, sobre os ativos de informação e de tecnologia, sobre o controle de acesso aos equipamentos, sobre os aspectos de conformidade, sobre o desenvolvimento e aquisição de sistemas, sobre os sistemas de mensagens, sobre o uso das redes sociais e dos dispositivos móveis. A Figura 14 ilustra as mensagens referentes a esses últimos três itens.

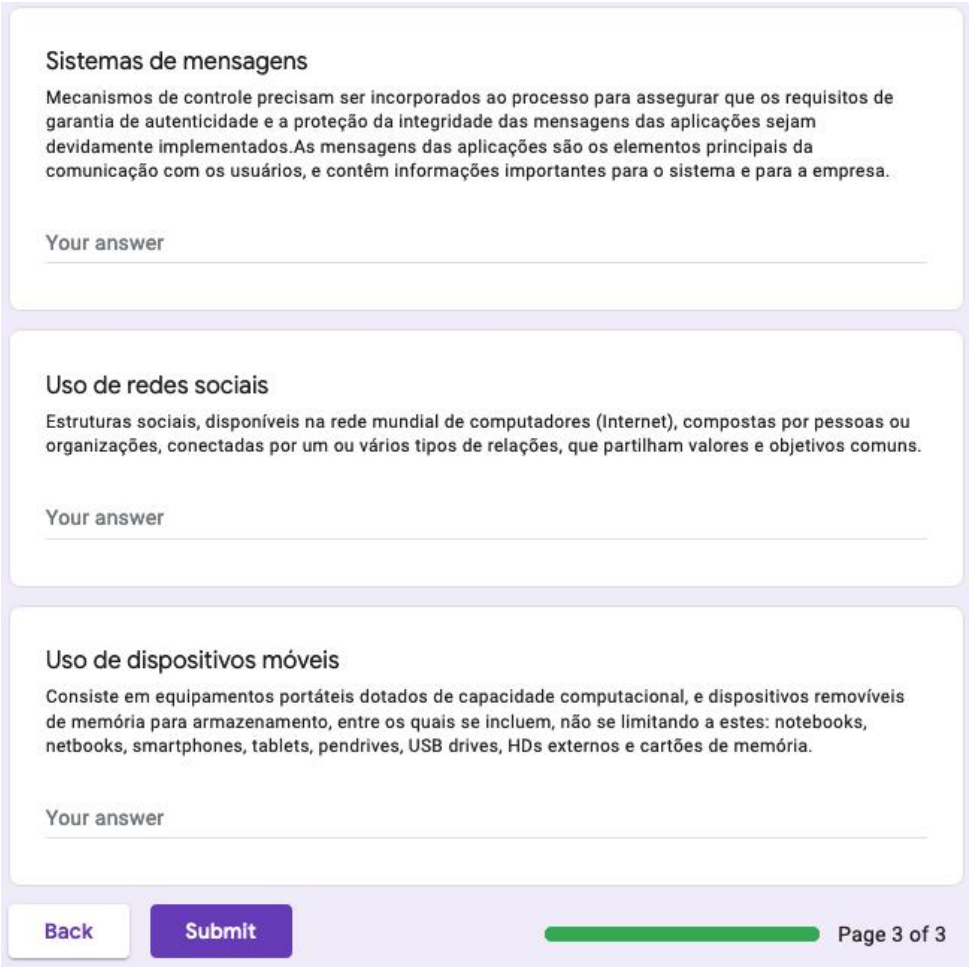


Figura 14 – Final dos aspectos objetivos da política de segurança (Fonte do autor)

5. Conclusão

A partir da análise dos percentuais levantados relativos aos itens de segurança especificados nas políticas das empresas foi possível concluir que existe a necessidade das empresas, independentemente do tipo de serviço e tamanho delas, de possuírem um guia para o Tratamento da Informação. Esse guia serviria de ponto de partida para estabelecer parâmetros importantes. Através das análises feitas, foi possível perceber que existe a necessidade de haver uma hegemonia nas políticas por parte das empresas, bem como uma constante atualização dos seus planos. Serviços importantes como sistema de backup, não são mencionados em 56% das empresas levantadas e, em relação ao desenvolvimento e aquisição de sistemas, 70% das empresas pesquisadas não possuem política que contemple esse quesito. No mundo digital, cada vez mais existe a necessidade de haver mecanismos para proteger a informação, as ameaças são diárias, bem como, também preservar, respeitar e assegurar a segurança da informação. As normas e conceitos, os modelos teóricos e conceituais, auxiliam no processo de gestão da informação, na gestão da segurança e na preservação da informação.

Assim, este trabalho buscou contribuir para a divulgação da importância da proteção digital e, facilitar a elaboração de documentos e medidas que são importantes para a preservação da segurança das instituições.

Uma boa de política de segurança deve compreender diretrizes, normativos, processos e padrões que orientem claramente as diversas equipes técnicas e de negócios para a implementação de tecnologia de forma segura, reduzindo os riscos e impactos de eventuais ataques, que certamente a empresa irá sofrer. Infelizmente, pode ser difícil representar esses conceitos teóricos em itens específicos. Ao analisar diferentes políticas de empresas das mais variadas áreas, bem como a normatização pertinente, este trabalho buscou contribuir para o entendimento e aperfeiçoamento de técnicas e práticas de segurança das informações.

6. Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. NBR ISO/IEC 27001:2015 - **Tecnologia da Informação - técnicas de segurança- código de práticas para gestão da informação**. 2015.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. NBR ISO/IEC 27002:2018 - **Tecnologia da Informação - técnicas de segurança- código de práticas para gestão da informação**. 2018.

BAYUK, J.L.; HEALEY, J.; ROHMEYER, P.; **Cyber Security Policy Guidebook**. 1ªed., John Willey & Sons, ISBN: 9781118027806. 2012.

FONTES, E. **Praticando a Segurança da Informação**. 1ªed., 288 páginas. Brasport Editora. ISBN 9788574526706. .2008.

FONTES, E. **Políticas e Normas para a Segurança da Informação**. 1ªed., 288 páginas. Brasport Editora. ISBN 9788574525150. 2012

FREITAS, F; ARAUJO, M. **Políticas de Segurança da Informação: Guia prático para elaboração e implementação**. 2ed. Ciência Moderna LTDA, 2008

JÚNIOR, A. G. **Metodologias de Gerenciamento de Riscos em Sistemas de Tecnologia da Informação e Comunicação - abordagem prática para conscientização e implantação nas organizações**. Trabalho de Conclusão de Curso de Especialista em Tecnologias, Gerência e Segurança de Redes de Computadores, Universidade Federal do Rio Grande do Sul, Porto Alegre. 2008.