A subutilização da Política de Segurança da Informação e a exposição dos dados da empresa

The under-utilization of the Information Security Policy and the exposure of corporate data

La subutilización de la Política de Seguridad de la Información y la exposición de los datos corporativos

Rafael Vitor dos Santos Baptista[1]
Cristiano Antônio Rocha Silveira Diniz[2]

Resumo: O presente artigo tem como objetivo apresentar uma análise dos princípios e fundamentos da segurança da informação, bem como expor a importância da utilização da Política de Segurança da Informação eos efeitos de sua subutilização. Trata-se de uma pesquisa do tipo exploratória para a qual se utilizou de pesquisa bibliográfica e documental. Esta teve como base obras de autores especializados no tema e a normalização da Associação Brasileira de Normas Técnicas (ABNT NBR ISO/IEC 27002:2005).
Palavras-chave: Informação. Segurança da Informação. Política de Segurança da Informação.

Abstract: *The purpose of this article is to present an analysis of the fundamentals and principles of information security, as well as to explain the importance of using the Information Security Policy and the effects of its underutilization. This is an exploratory research for which was used for bibliographic and documentary research. This was based on works by expert authors on the subject and the normalization of the Brazilian Association of Technical Standards (ABNT NBR ISO/IEC 27002:2005).*
Keywords:*Information. Information security. Information Security Policy*.

Resumen: *El objetivo de este artículo es presentar un análisis de los fundamentos y principios de la seguridad de la información, así como explicar la importancia de utilizar la Política de Seguridad de la Información y los efectos de su subutilización. Se trata de una investigación exploratoria para la cual se utilizó la investigación bibliográfica y documental. Esto se basó en trabajos de autores expertos sobre el tema y la normalización de la Asociación Brasileña de Normas Técnicas (ABNT NBR ISO / IEC 27002: 2005).*
Palabras clave:*Información. Seguridad de información. Política de Seguridad de la Información.*

1 INTRODUÇÃO

As organizações são compostas de infraestrutura, pessoas e tecnologias, elementos permeados pela informação.

A necessidade em se proteger as informações, que antecede a vinda dos meios tecnológicos digitais, tem levado à criação de unidades organizacionais

[1]Graduando do curso Bacharelado em Sistemas de Informação pela Faculdade Infórium de Tecnologia. rafaelbaptistaa@gmail.com
[2]Pós-graduado em Gestão de Segurança da Informação pela FUMEC. Professor da Faculdade Infórium de Tecnologia. cristianodiniz@gmail.com.

específicas, que tratam de fatores essenciais da segurança da informação e que, cada vez mais, vem se tornando peças essenciais nas operações corporativas. É válido ressaltar que a informação é um elemento crítico não só para a sobrevivência, mas também para sua habilidade de prosperar.

Neste contexto, a segurança da informação, é considerada como o ajuste de processos e tecnologias, medidas organizacionais e comportamentais designadas a assegurar a confidencialidade, integridade, e disponibilidade da informação e seu compartilhamento com base no papel e perfil de cada usuário.

Compreende-se como Política de Segurança da Informação (PSI), códigos de conduta, aos quais usuários de sistemas computacionais devem se adequar integralmente.

No entanto, observa-se que a subutilização dos usuários, no que diz respeito à Política de Segurança da Informação, torna, consequentemente, mais eminente o risco da exposição dos dados das empresas.

Ocorre que os usuários dos sistemas computacionais frequentemente se deparam com dificuldades próprias da Política de Segurança da Informação, pois esta, demanda, conhecimentos específicos quanto às suas normas, métodos e procedimentos.

Assim, o objetivo geral deste artigo é analisar os princípios e fundamentos da informação, a importância da gestão da segurança da informação alinhada com as áreas de negócio e consequentemente com os objetivos da organização, suportada por um código de conduta claro e bem elaborado.Os objetivos específicos são: explanar sobre os conceitos da informação, gestão da informação, os princípios da segurança da informaçãoe a importância da Política da Segurança da Informação, embasando-seemobras escritas por autores renomados e também pelanormalização da ABNT NBR ISO/IEC 27002:2005.

Nesse sentido, formulou-se a questão norteadora deste estudo: a subutilização da Política de Segurança da Informação compromete a continuidade

do negócio, tendo em vista a exposição dos dados, sendo ele, o ativo de maior valia para as empresas?

Justifica-se a relevância deste tema tendo-se em vista a valia da informação para as empresas e a importância da aplicação de políticas e normalizações em prol da continuidadeeprosperidadedo negócio.

Trata-se de uma pesquisa do tipo exploratória com fundamentação teórica emautores como: Lento (2011), Sêmola (2014); Cabral e Caprino (2015) e fonte documental da Associação Brasileira de Normas Técnicas (ABNT NBR ISO/IEC 27002:2005).

Para a compreensão do tema proposto dividiu-se este artigo em cinco seções: a seção 1, a qual estamosé referente a introdução, indicativa do estudo; a seção 2 tem como objetivo apresentar osFundamentosda Informação; a seção 3 traz o conceito da Gestão da Informação; a seção 4 apresenta informações sobre Segurança da Informação e sua importância; a seção 5apresenta Políticas da Segurança da Informação; a seção 6 apresenta asconclusões do artigo.

2 ABORDAGEM TEÓRICA SOBRE FUNDAMENTOSDA INFORMAÇÃO

A globalização tornou os mercados mundiais cada vez mais dinâmicos ecompetitivos. O risco do negócio está mais claro e evidente para uma organização,e a necessidade de cumprir prazos e entregar produtos com qualidade é umarealidade nesse novo mundo. A todo momento surgem descobertas, experimentos, conceitos, métodos e modelos nascidos pela movimentação de questionadores estudiosos, pesquisadores e executivos que não se conformam com a passividade da vida e buscam a inovação e quebra de paradigmas, revelando uma nova tendência promissora (SÊMOLA, 2014, p.1).

Para Sêmola (2014, p. 1), em todas essas etapas a informação sempre esteve presente e cumpre importante papel para a gestão dos negócios. É inegável que todas as empresas, independente do seu *core business* e porte, em todas essas

fases de existência, sempre usufruíram da informação, objetivando melhor produtividade, redução de custos, ganho de m*arket share*, aumento de agilidade, competitividade e apoio mais eficiente aos processos de tomada de decisão.

A figura 1 ~~identifica...~~ilustra o relacionamento dos processos, tecnologias e pessoasdo ponto de vista estratégico:

[a1] Comentário: Inserir um texto sobre a figura antes da figura. O leitor precisa entender sobre a figura antes de vê-la.

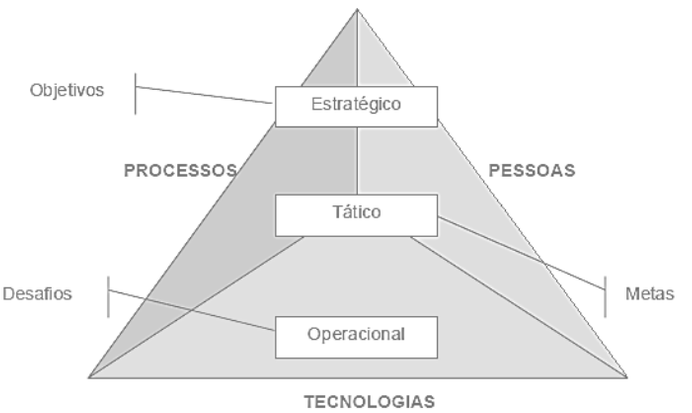

Figura 1 – o relacionamento dos processos, tecnologias e pessoas do ponto de vista estratégico
Fonte: Laureano (2005, p. 4)

A informação é utilizada como matéria-prima para a construção do planejamento voltado à construção da competitividade nas organizações; se essa postura não for adotada pela organização, se arriscará a ficar em uma posição desfavorável e até mesmo ultrapassada perante seus concorrentes mais capacitados no que se refere à busca e ao processamento da informação (JAMIL et al., 2010, p.4).

De acordo com a norma ABNT NBR ISO/IEC 27002:2005 (2005, p. x), o valor da informação vai além das palavras escritas, números e imagens: conhecimento, conceitos, ideias e marcas são exemplos de formas intangíveis da informação. Em um mundo interconectado, a informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações, são informações que, como outros ativos importantes, têm valor para o negócio da organização e, consequentemente, requer proteção contra vários riscos.

A informação pode estar presente em inúmeros elementos de todo o processo empresarial, chamados de ativos, os quais devem ser gerenciados de maneira estratégica e devem ser alvo de proteção da segurança da informação.

3 A GESTÃO DA INFORMAÇÃO

Apesar de a informação existir de várias formas, isto é, impressa, escrita empapel, armazenada eletronicamente, transmitida via correio tradicional oue-mail, tratada em conversações entre outras, ela deve ser protegidade forma apropriada em conformidade com as necessidades da organização.

Lento (2011, p.100) traz quereforçar a questão da proteção da informação é fundamental,principalmente pela crescente evolução tecnológica e a dependência dasempresas da TI, tornando-a uma questão estratégica para qualquer organização.É uma realidade no mundo virtual a adoção de soluções de segurança, com aaplicação de controles, sejam eles físicos ou lógicos, mas compatíveis com osprocessos e os riscos do negócio da organização.

3.~~2~~1 Classificação da informação

Nem toda informação é vital ou essencial para merecer cuidados especiais. Porém, temos informações vitais a ponto de ser extremamente relevante definir seu nível de confidencialidade (sigilo), integridade, ou mesmo, seu nível de criticidade de acesso (disponibilidade). Com base nestas informações, as organizações podem classificá~~a~~-las e disponibilizá~~a~~-las de maneira adequada, inclusive aquelas cruciais e essenciais que, o custo de sua integridade, por qualquer que seja, será menor que o custo que não dispô-la adequadamente.

Lento (2011, p. 102) cita a classificação utilizada pelo governo federal do Brasil, no Decreto 5.301, de dezembro de 2004, seção I,Da classificação segundo o grau de sigilo, Art. 5º, as informações são classificadasem ultrassecretas, secretas, confidenciais e reservadas, em razão do seu teor ou conteúdo:

> Ultrassecretas: trata-se de dados ou informações referentes à soberania e à integridade territorial nacionais, a planos e operações militares, às relações internacionais do País, a projetos de pesquisa e desenvolvimento científico e tecnológico de interesse da defesa nacional e a programas econômicos, cujo conhecimento não autorizado possa acarretar dano excepcionalmente grave à segurança da sociedade e do Estado.
>
> Secretas: trata-se de dados ou informações referentes a sistemas, instalações, programas, projetos, planos ou operações de interesse da defesa nacional, a assuntos diplomáticos e de inteligência e a planos ou detalhes, programas ou instalações estratégicas, cujo conhecimento não autorizado possa acarretar dano grave à segurança da sociedade e do Estado.
>
> Confidenciais: trata-se de dados ou informações que, no interesse do Poder Executivo e das partes, devam ser de conhecimento restrito e cuja revelação não autorizada possa frustrar seus objetivos ou acarretar dano à segurança da sociedade e do Estado.
>
> Reservados: trata-se de dados ou informações cuja revelação não autorizada possa comprometer planos, operações ou objetivos neles previstos ou referidos.

Sêmola (2014, p. 106) ressalta ainda que, em especial, a norma de classificação da informação é fator crítico de sucesso, pois assume a responsabilidade por escrever os critérios necessários a fim de sinalizar a importância e o valor das informações, premissa importante para a elaboração de praticamente todas as demais normais. Não há regra preconcebida para estabelecer essa classificação, mas é preciso entender o perfil do negócio e as características das informações que alimentam os processos e circulam no ambiente corporativo para que os critérios sejam personalizados. A figura 2 ~~abaixo~~ ilustra a relação entre classificação e tratamento definido na política para o ciclo de vida da informação:

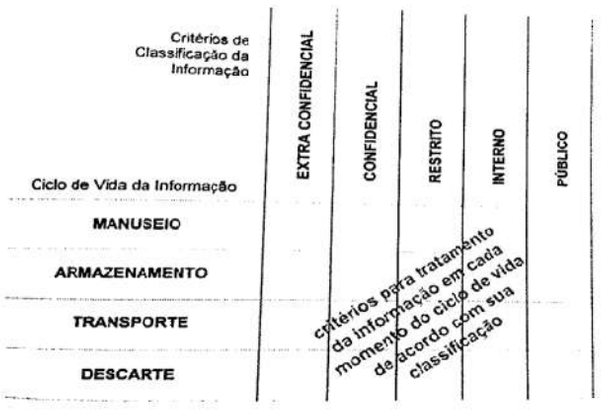

Figura 2 – Ilustração da relação entre classificação e tratamento definido na política para o ciclo de vida da informação.

Fonte: Sêmola (2014, p. 107)

A informação é um recurso estratégico para as empresas e sua classificação é uma das etapas mais importante de todo o processo, pois, se extraviadas, por quaisquer meios, poderão comprometer a estrutura como todo, incluindo suas operações e funcionamento, trazendo grandes prejuízos.

3.2Ciclo de vida da informação

Tendo conhecimento de quão valiosa é a informação para os negócios, temos que separar de maneira metódica e organizada todos os aspectos ligados à segurança, as propriedades que devem ser preservadas e protegidas para que a informação esteja efetivamente sob controle e, principalmente, enfatizar os momentos que fazem parte de seu ciclo de vida.

Toda informação é influenciada por três propriedades principais que foram destacadas no tópico anterior, sendo elas: confidencialidade, integridade e disponibilidade, além dos aspectos de autenticidade e legalidade, que complementam essa influência.

Sêmola (2014, p. 9) explana que o clico de vida, por sua vez, é composto e identificado pelos momentos vividos pela informação que a colocam em risco. Ele destaca ainda que estes momentos são vivenciados justamente quando os ativos

físicos, tecnológicos e humanos fazem uso da informação, sustentando processos que, por sua vez, mantêm a operação da empresa:

> Manuseio: momento em que a informação é criada e manipulada, ao folhear um maço de papéis, ao digitar informações recém-geradas em uma aplicação de Internet ou, ainda, ao utilizar a senha de acesso para autenticação, por exemplo.
> Armazenamento: momento em que a informação é armazenada, seja em um banco de dados compartilhado, seja em uma anotação de papel posteriormente postada em um arquivo de ferro, ou, ainda, em uma mídia externa depositado em um armário da empresa, por exemplo.
> Transporte: momento em que a informação é transportada, seja ao caminhar informações por e-mail, seja ao postar em um sistema da Internet ou, ainda, ao falar ao telefone uma informação confidencial, por exemplo.
> Descarte: momento em que a informação é descartada, seja ao depositar na lixeira da empresa um material impresso, seja ao eliminar um arquivo eletrônico do seu computador ou, ainda, ao descartar uma mídia externa usada que apresentou falha de leitura.

A figura ~~23, a seguir,~~ilustra os momentos do ciclo de vida da informação, considerando os conceitos básicos da segurança e os aspectos complementares:

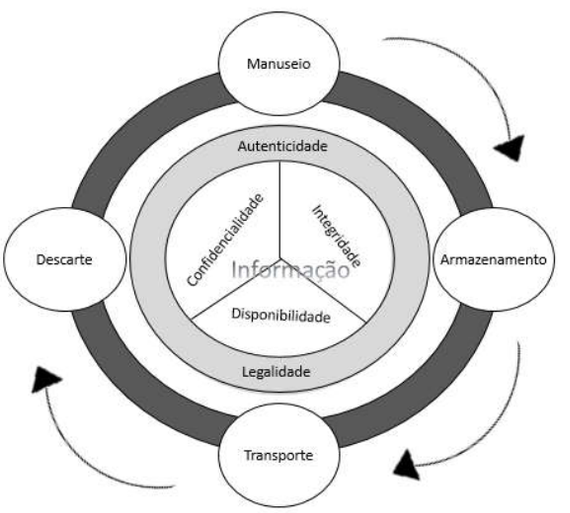

Figura 3 – Quatro momentos do ciclo de vida da informação, considerando os conceitos básicos da segurança e os aspectos complementares

Fonte: Sêmola (2014, p. 11)

Todo este ciclo merece atenção, pois, expondo as informações, teremos ameaças de segurança que colocam em risco suas propriedades. É importante salientar que o momento do descarte deve estar alinhado à política de segurança, pois o descarte incorreto pode por toda a segurança do negócio a perder.

4 SEGURANÇA DA INFORMAÇÃO

As organizações, seus sistemas de informação e de redes de computadores são expostos a diversos tipos de ameaças à segurança da informação, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundação. Danos causados por código malicioso, *hackers* e ataques de *denial of service* estão se tornando cada vez mais comuns, mais ambiciosos e incrivelmente mais sofisticados (ABNT NBR ISO/IEC 27002:2005, 2005, p. 16).

Sêmola (2014, p. 41) define a segurança da informação como a prática de gestão de riscos de incidentes que impliquem no comprometimento dos três principais conceitos da segurança: confidencialidade, integridade e disponibilidade da informação. Dessa forma, estaríamos falando da definição de regras que incidiram sobre todos os momentos do ciclo de vida da informação: manuseio, armazenamento, transporte e descarte, viabilizando a identificação e o controle de ameaças e vulnerabilidades.

A esse respeito e de maneira simples, Lento (2011, p. 15) cita a segurança da informação como a garantia deque as informações (em qualquer formato – mídias eletrônicas, papel e até mesmoem conversações pessoais ou por telefone) estejam protegidas contra o acessode pessoas não autorizadas; estejam sempre disponíveisquando necessárias; e, que sejam confiáveis.

Nesse sentido, Cabral e Caprino (2015, p. 4208) define estes conceitos como:

> Disponibilidade: a informação da qual o negócio é altamente dependente deve estar disponível sempre que necessário.

> Confidencialidade: prover o acesso a informação somente aos usuários em que de fato tem autorização para tal.
> Integridade: garantir que apenas alterações autorizadas sejam feitas a dados e softwares, consequentemente garante que a informação esteja sempre correta, confiável e precisa.

De acordo com aABNT NBR ISO/IEC 27002:2005 (2005, p. 17)é essencial que uma organização identifique e estabeleça os seus requisitos de segurança da informação por meio de três principais fontes:

a) Uma fonte é obtida a partir da análise/avaliação de riscos para a organização, levando-se em conta os objetivos e as estratégias globais de negócio da organização. Por meio da análise/avaliação de riscos, são identificadas as ameaças aos ativos e as vulnerabilidades destes, e realizada uma estimativa da probabilidade de ocorrência das ameaças e do impacto potencial ao negócio.
b) Uma outra fonte é a legislação vigente, os estatutos, a regulamentação e as cláusulas contratuais que a organização, seus parceiros comerciais, contratados e provedores de serviço tem que atender, além do seu ambiente sociocultural.
c) A terceira fonte é um conjunto particular de princípios, objetivos e os requisitos do negócio para o processamento da informação que uma organização tem que desenvolver para apoiar suas operações.

A vigilância da segurança da informação deve ser exercida por todos os usuários do sistema sob a coordenação de profissional especializado na área, que irá estabelecer práticas segundo a estrutura de administração das organizações (GADLER e MOTERLE, 2011, p. 17).

4.1Aspectos da segurança da informação

O objetivo o qual se pretende atingir depende de alguns elementos que são considerados essenciais na prática de segurança da informação. Sêmola (2014, p. 44) cita alguns deles:

> Autenticação: processo de identificação e reconhecimento formal da identidade dos elementos que entram em comunicação ou fazem parte

> de uma transação eletrônica que permite o acesso à informação e seus ativos por meio de controles de identificação desses elementos.
> Conformidade: processo de garantia do cumprimento de obrigações empresariais com *stakeholders* (investidores, empregados, credores etc.) e com aspectos legais e regulatórios relacionados à administração das empresas, dentro de princípios ético e de conduta estabelecidos com a alta direção das mesmas.

Além dos aspectos citados acima, Laureano (2005, p. 12) destaca que as combinações de outros aspectos devem ser consideradas para que a informação seja considerada segura, sendo eles:

> Autorização: concessão de permissão para o acesso às informações e funcionalidades das aplicações as participantes de um processo de troca de informações (usuário ou máquina), após a correta identificação e autenticação dos mesmos.
> Auditoria: processo de coleta de evidências de uso dos recursos existentes, a fim de identificar as entidades envolvidas em um processo de troca de informações, ou seja, origem, destino e meios de tráfego de uma informação.
> Autenticidade: garante que a informação ou o usuário que a acessa é mesmo autêntico; atesta com exatidão, a origem do dado ou informação.
> Severidade: gravidade do dano que determinado ativo pode sofrer devido à exploração de uma vulnerabilidade por qualquer ameaça aplicável.
> Relevância do ativo: grau de importância de um ativo para a operacionalização de um processo de negócio.
> Relevância do processo do negócio: grau de importância de um processo de negócio para o alcance dos objetivos e sobrevivência de uma organização.
> Criticidade: gravidade referente ao impacto ao negócio causado pela ausência de um ativo, pela perda ou redução de suas funcionalidades em um processo de negócio ou pelo seu uso indevido e não autorizado.

4.2Ameaças, ataques e vulnerabilidades

Antes considerados problemas de TI, os ricos de segurança e sigilo de dados ganharam maior destaque como uma nova ameaça as empresas em um mundo

cada vez mais digitalizado. A questão se agrava com o uso extensivo da nuvem, os dados regulatórios e o custo financeiro da gestão de riscos. A contínua diversificação global está clara e intimamente unida aos desafios de segurança digital (CABRAL e CAPRINO, 2015, p. 4155).

4.2.1 Ameaças

De acordo com Sêmola (2014, p. 45) as ameaças são agentes ou condições que causam incidentes que comprometem as informações e seus ativos por meio da exploração de vulnerabilidades, provocando perdas de confidencialidade, integridade e disponibilidade, e, consequentemente, causando impacto aos negócios de uma organização.

Sêmola (2014, p. 46) ainda classifica as ameaças quanto a sua intencionalidade, podendo dividi-las nos seguintes grupos:

> Naturais: ameaças decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades eletromagnéticas, maremotos, aquecimento, poluição, etc.
> Involuntárias: ameaças inconscientes, quase sempre causadas pelo desconhecimento. Podem ser causadas por acidentes, erros, falta de energia, etc.
> Voluntárias: ameaças propositais causadas por agentes humanos como *hackers*, invasores, espiões, ladrões, criadores e disseminadores de vírus de computador, incendiários.

4.2.12 Ataques

Ataques podem ser definidos como um assalto ao sistema de segurança que deriva de uma ameaça inteligente, isto é, um ato inteligente que seja uma tentativa deliberada (especial no sentido de um método ou técnica) para invadir serviços de segurança e violar as políticas do sistema (SHIREY, 2000, apud LAUREANO, 2005, p.16).

Um ataque pode ser ativo, tendo por resultado a alteração dos dados; passivo, tendo por resultado a liberação dos dados; ou destrutivo visando à negação do acesso aos dados ou serviços (WADLOW, 2000, apud LAUREANO, 2005, p.16).

Dado o exposto, Laureano (2005, p.16) afirma ainda que para implementar mecanismos de segurança faz-se necessário classificar as formas possíveis de ataques em sistemas:

> Interceptação: considera-se interceptação o acesso a informações por entidades não autorizadas; violação da privacidade e confidencialidade das informações.
> Interrupção: pode ser definida como a interrupção do fluxo normal das mensagens ao destino.
> Modificação: consiste na modificação de mensagens por entidades não autorizadas, violação da integridade da mensagem.
> Personificação: considera-se personificação a entidade que acessa as informações ou transmite mensagem se passando por uma entidade autêntica, violação da autenticidade.

O ato do ataque em si não significa que a ação terá sucesso absoluto, o nível de sucesso depende da vulnerabilidade do sistema ou da atividade e da eficácia das medidas de segurança existentes.

4.2.~~1~~3Vulnerabilidades

São fragilidades presentes ou associadas a ativos que manipulam e/ou processam informações que, ao serem exploradas por ameaças, permitem a ocorrência de um incidente de segurança, afetando negativamente um ou mais princípios da segurança da informação: confidencialidade, integridade e disponibilidade (SÊMOLA, 2014, p.46).

Laureano (2005, p. 17) afirma ainda que todos os ambientes são vulneráveis, partindo do princípio de que não existem ambientes totalmente seguros. Identificar estas vulnerabilidades que podem contribuir para ocorrências de incidentes de

segurança é um aspecto importante na identificação de medidas adequadas de segurança.

No entanto, Sêmola (2014, p. 46) diz que vulnerabilidades por si sós não provocam incidentes, pois são elementos passivos, necessitando de um agente causador ou condição favorável, que são as ameaças.Para exemplificar, seguem alguns tipos de vulnerabilidades:

I. Físicas: instalações prediais que não atendem as boas práticas ou as normas e regulamentações vigentes.
II. Naturais: ambientes com equipamentos eletrônicos próximos a locais suscetíveis a desastres naturais, como incêndios, enchentes, aumento de umidade, entre outros.
III. Hardware: computadores são suscetíveis a poeira, umidade, sujeira e acesso indevido a recursos inadequadamente protegidos, podendo ainda sofrer com componentes deficientes ou mal configurados.
IV. Software: Erros na codificação, instalação ou configuração de sistemas e aplicativos podem acarretar acessos indevidos, vazamento de informações ou até mesmo indisponibilidade do recurso quando necessário.
V. Comunicação: a comunicação telefônica é vulnerável a escutas (acesso indevido) ou a problemas na infraestrutura física ou lógica que a impeçam de ser estabelecida.
VI. Humanas: falta de treinamento ou de conscientização das pessoas, falta de avaliação psicológica adequada para verificação de antecedentes (*background check*) que identifique objetivos escusos ou problemas anteriores, ou mesmo má-fé ou descontentamento de um colaborador.

5 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Segurança da Informação é obtida a partir da implementaçãode uma série de controles, que podem ser políticas, práticas,procedimentos, estruturas organizacionais e funções de software.Esses controles precisam ser estabelecidos para garantir que osobjetivos de segurança específicos da organização sejam atendidos(ABNT NBR ISO/IEC 27002:2005, 2005, p. 8).

A política de segurança da informação é um documento que estabelece oenfoque da organização para gerenciar sua segurança. O documento deve seraprovado pela direção desta organização, publicado e comunicado para todos oscolaboradores e, também, aos parceiros comerciais, conforme a necessidade (GADLER e MOTERLE, 2011, p. 27).

Com o propósito de fornecer orientação e apoio às ações de gestão de segurança da informação, a política tem um papel fundamental e, guardadas as devidas proporções, tem importância similar à Constituição federal para um país. Dessa forma, assume uma grande abrangência e, por causa disso, é subdividida em três blocos: diretrizes, normas, procedimentos e instruções, sendo destinados, respectivamente, às camadas estratégica, tática e operacional (SÊMOLA, 2014, p. 105).

A política deve ser personalizada e escrita sob medida pela e para empresa, pois deve estabelecer padrões, responsabilidades e critérios para o manuseio, armazenamento, transporte e descarte das informações conforme o nível de segurança estabelecido internamente.

No que tange as diretrizes, Sêmola (2014, p. 105) enfatiza queelas por si só têm papel estratégico e precisam expressar a importância que a empresa dá à informação, além de comunicar aos funcionários seus valores e seu comprometimento em incrementar a segurança à sua cultura organizacional.

Para isto, é evidente a necessidade de envolvimento do alto escalão da empresa para que a política seja comunicada e compartilhada de maneira clara e objetiva, e que esteja nela transcritas as preocupações dos executivos quanto as linhas de ação que orientarão as atividades táticas e operacionais da organização.

Com caráter tático, as normas são o segundo nível da política, detalhando situações, ambientes e processos específicos, e fornecendo orientação para o uso adequado das informações (SÊMOLA, 2014, p. 105).

Os procedimentos e instruções deverão estar presentes na política em maior quantidade por seu perfil operacional, em que é necessário descrever meticulosamente cada ação e atividade associada a cada situação distinta de uso das informações (SÊMOLA, 2014, p. 107).

5.1Elaboração dos documentos da política

Para a elaboração do documento da política, a ABNT NBR ISO/IEC 27002:2005 (2005, p. 8) indica que o mesmo contenha declarações relativas a:

a) definição da segurança da informação;
b) uma declaração do comprometimento da direção, apoiando as metas eprincípios da segurança da informação, alinhada com os objetivose estratégias do negócio;
c) uma estrutura para estabelecer os objetivos de controle e os controles, incluindo a estrutura de análise/avaliação e gerenciamento de riscos;
d) breve explanação das políticas, princípios, normas e requisitos deconformidade de segurança da informação específicos para organização, incluindo:
    - conformidade com a legislação e com requisitos regulamentares econtratuais;
    - requisitos de conscientização, treinamento e educação em segurança da informação;
    - gestão da continuidade do negócio;
    - consequências das violações na política de segurança da informação;
e) definição das responsabilidades gerais e específicas na gestão dainformação, incluindo o registro dos incidentes de segurança dainformação;
f) referências à documentação que possam apoiar a política, por exemplo, políticas e procedimentos de segurança mais detalhados de sistemas de informação específicos ou regras de segurança que os usuários devem seguir.

É importante salientar ainda que a política da segurança da informação deve estar extremamente integrada com as diretrizes e políticas institucionais definidas pela organização, pois sem este relacionamento toda a definição e implementação das normas e politicas serão fracassadas.

5.2Implantação da política

Gadler e Moterle (2011, apud ABNT NBR ISO/IEC 27002:2005, p. 29) assinala alguns fatores críticos que devem ser observados para o sucesso da implantação da política de segurança:

a) reflexão sobre os objetivos e atividades do negócio;
b) abordagem e estrutura para a implementação, manutenção,monitoramento e melhoria da segurança da informação coerentementecom a cultura organizacional;
c) comprometimento e apoio visível de todos os níveis gerenciais;
d) levantamento de informação com base nos requisitos de segurança dainformação, da análise/avaliação de riscos e da gestão de risco;
e) divulgação e distribuição de diretrizes e normas da segurança dainformação para todos os gerentes, funcionários e outras partesenvolvidas para se alcançar a conscientização;
f) provisão de recursos financeiros para as atividades de gestão desegurança da informação;
g) definição de etapas para conscientização, treinamento e educação detodos os envolvidos;
h) estabelecimento de um eficiente processo de gestão de incidentes desegurança da informação;
i) implementação de um sistema de medição, o qual seja usado para avaliaro desempenho da gestão da segurança da informação e obtenção desugestões para a melhoria.

A implantação da política de segurança deverá ocorrer por meio de algumasiniciativas e apoio das diversas áreas da organização. Assim, o material a serutilizado para apresentação dessa política, quer seja promocional, de divulgaçãoou de consulta, deve ser preparado pelo setor de comunicação (GADLER e MOTERLE, 2011, p. 29).

É importante a realização de seminários com os executivos (diretores e gerentes) e ~~*key users*~~ usuários chavesdas organizações para uma melhor disseminação do conteúdo, pois estes poderão utilizar o conceito de *top down* para ~~que~~ exigir que as diretrizes transcritas na política sejam utilizadas por todos os níveis da organização.

A ABNT NBR ISO/IEC 27002:2005 (2005, p. 112), reforça ainda que os gestores devem garantir que todos os procedimentos de segurança da informação dentro da sua área de responsabilidade estejam sendo executados corretamente para atender à conformidade com as normas e políticas de segurança da informação.

5.3Treinamento e sensibilização em segurança

Em todo o processo de segurança da informação, os recursos humanos são os elos mais frágeis da corrente, pois são responsáveis por um ou mais fases dos processos que não são totalmente seguros. Por não podermos eliminarmos todas as vulnerabilidades por dependência dos humanos, uma pessoa pode colocar em risco toda a segurança do ambiente compartilhando uma senha supostamente pessoal e intransferível, mesmo com normas de criação, manuseio, armazenamento, transporte e descarte de senhas, recursos de auditoria e de acesso implementados.

Por este motivo, Sêmola (2014, p. 128) afirma que esses riscos precisam ser tratados de forma gradativa, objetivando formar uma cultura de segurança que se integre as atividades dos funcionários e passe a ser vista como um instrumento de autoproteção. As ações devem ter a estratégia de compartilhar a responsabilidade com cada indivíduo, transformando-o em coautor do nível de segurança alcançado.

Para atingir estes níveis de maturidade, é importante a realização de seminários abertos voltados a compartilhar a percepção dos riscos associados as atividades do negócio e deixando evidente os riscos a toda a reputação do negócio caso alguma ameaça se concretize naquele ambiente. Além disso, campanhas de divulgação e cartas do presidente devem ser utilizadas para que todos tenham conhecimento das políticas e manuais de segurança da informação e, por meio deste, oficialize a vontade e comprometimento da empresa em proteger o seu bem mais valioso que é a informação e seus ativos.

Os funcionários que não se sentirem seguros e necessitem de maior domínio dos conceitos, métodos e técnicas de segurança, cursos de capacitação e

certificação podem ser ofertados a fim de garantir a total integração das ações e, principalmente, alcançar os objetivos definidos.

5.~~3~~4Testes e auditoria

Enquanto a segurança tem a função de garantir a integridade dos dados,a auditoria vem garantir que estes dados estejam realmente íntegrospropiciando um perfeito processamento, obtendo os resultados esperados (LAUREANO, 2005, p. 99).

Todos os recursos tecnológicos utilizadospela empresa, sejam mais ou menos importantes, devem ser auditados, poiso processamento de dados é um conjunto de recursos necessários paradisponibilizar as informações, e, se apenas um destes recursos fica fora deoperação, a informação pode deixar de ser disponibilizada.

A garantia dos recursos tecnológicos também deve ser auditada, pois, semestes recursos prometidos, fatalmente alguma interferência na segurança dasinformações ocorrerá. As responsabilidades podem ser atribuídas a recursoshumanos, competência de auditoria, parecer da alta gerência, do mesmo modoque a responsabilidade sobre o futuro da aplicação das auditorias (LENTO, 2011, p. 96).

A auditoria e os testes devem ser flexíveis, não podem ser realizados somente para identificar defeitos e problemas, devem ser realizadas para garantir a continuidade dos negócios por meio de aplicação de melhorias e constantes atualizações das normas e diretivas de toda a organização.

Assim, podemos constatar que mesmo que a política de segurança da informação esteja escrita, implementada, divulgada e controlada, ela por si só não assegura que os usuários estão aplicando todas as normas e conceitos ali descritos. É imprescindível a realização de testes e auditoria em todo o ambiente tecnológico da organização para verificar se tudo o que foi definido está sendo cumprido e se

houve alguma tentativa de intervenção interna ou externa, direta ou indireta, neste ambiente.

5.54Gestão da continuidade do negócio

Pelas empresas estarem cada vez mais informatizadas, devemos garantir a continuidade de processos e informações vitais à sobrevivência da empresa, no menor espaço de tempo possível, com o objetivo de minimizar os impactos de um desastre (SÊMOLA, 2014, p. 98).

O processo de gestão da continuidade do negócio deve ser implementado para minimizar um impacto sobre a organização e recuperar perdas de ativos da informação (que pode ser resultante de, por exemplo, desastres naturais, acidentes, falhas de equipamentos e ações intencionais) a um nível aceitável através da combinação de ações de prevenção e recuperação. Convém que este processo identifique os processos críticos e integre a gestão da segurança da informação com as exigências da gestão da continuidade do negócio com outros requisitos de continuidade relativo a tais aspectos como operações, funcionários, materiais, transporte e instalações (ABNT NBR ISO/IEC 27002:2005, p. 103).

Um plano de contingenciamento pode assumir diversas formas, em função do objeto a ser contingenciado e da abrangência de sua atuação. Uma empresa não possui um plano único, mas diversos planos integrados e focados em diferentes perímetros, sejam físicos, tecnológicos ou humanos direcionados a múltiplas ameaças potenciais (SÊMOLA, 2014, p. 99).

A ABNT NBR ISO/IEC 27002:2005 (2005, p. 103) traz como elementos chave da gestão da continuidade dos negócios:

a) entendimento dos riscos a que a organização está exposta, no que diz respeito à sua probabilidade e impacto no tempo, incluindo a identificação e priorização dos processos críticos do negócio;
b) identificação de todos os ativos envolvidos em processos críticos do negócio;

c) entendimento do impacto que incidentes de segurança da informação provavelmente terão sobre os negócios e estabelecimento dos objetivos do negócio dos recursos de processamento da informação;
d) consideração de contratação de seguro compatível que possa ser parte integrante do processo de continuidade do negócio, bem como a parte de gestão de risco operacional;
e) identificação e consideração da implementação de controles preventivos e de mitigação;
f) identificação de recursos financeiros, organizacionais, técnicos e ambientais suficientes para identificar os requisitos de segurança da informação;
g) garantia de segurança de pessoal e proteção de recursos de processamentos das informações e bens organizacionais;
h) detalhamento e documentação de planos de continuidade de negócio que contemplem os requisitos de segurança da informação alinhados com a estratégia de continuidade do negócio estabelecida;
i) testes e atualizações regulares dos planos e processos implantados;
j) garantia de que a gestão da continuidade do negócio esteja incorporada aos processos e estrutura da organização.

Além da gestão de continuidade dos negócios, devemos considerar também no planejamento os seguintes itens:

a) identificação e concordância de todas as responsabilidades e procedimentos da continuidade do negócio;
b) identificação da perda aceitável de informações e serviços;
c) implementação dos procedimentos que permitam a recuperação e restauração das operações do~~e~~ negócio e da disponibilidade da informação nos prazos necessários;
d) procedimentos operacionais que permitam a conclusão de restauração e recuperação que estejam pendentes;
e) documentação de processos e procedimentos acordados;
f) educação adequada de pessoas nos procedimentos e processos definidos, incluindo o gerenciamento de crise;
g) teste e atualização de planos.

Neste contexto, é importante levantar o grau de relevância entre os processos ou atividades que fazem parte do escopo da contingência em função da continuidade do negócio.

6 CONCLUSÃO

Para a compreensão do tema de estudo, aA subutilização da Política de Segurança da Informação e a exposição dos dados da empresa; buscou-se inicialmente abase teórica e conceitual sobre esta questão.

Dado o exposto, a fundamentação teórica e conceitual nos permitiu verificar que a política e os procedimentos de segurança da informação são fundamentais e devem ser implementados para minimizar os riscos a que a organização está exposta e, também, para a prosperidade do negócio.

As práticas de segurança da informação no que concerne ao desenvolvimento eimplantação constituem uma realidade do mercado e são cada vez mais aplicadasao negócio da organização.

A normatização ABNT NBR ISO/IEC 27002:2005 traz as boas práticasque servem de orientação para a implementação das políticas de segurança, tornando-se imprescindível sua utilização para que a organização atinja o nível de maturidade pleiteado mundialmente.

Por todos esses aspectos, a política da segurança, em si, é apenas ummeio de registrar as normas e diretrizes estabelecidas pela e para a organização,porque os processos serão implementados a partir de uma mudança de cultura,da preparação do ambiente e do comprometimento de seus colaboradores. Poroutro lado, seu sucesso depende do apoio da administração da empresa e oalinhamento com as ações estratégicas que necessitam de informações paratomada de decisão.

Conclui-se que a pergunta de pesquisa do estudo foirespondida e os objetivos alcançados.

REFERÊNCIAS

ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação: ABNT NBR ISO/IEC 27002:2005.** 2a. ed. Rio deJaneiro, 2005.

CABRAL, Carlos; CAPRINO, Willian. **Trilhas em Segurança da Informação**: caminhose ideias para a proteção de dados. Rio de Janeiro: Brasport, 2015. Livro no formato *e-book*(posição 2 a 6139), adquirido em 16 de maio de 2017 na Amazon e disponível para leitura em <https://ler.amazon.com.br/>.

GADLER, Lindamir do Carmo Secchi; MOTERLE, Roseli Rocha. **Políticas e Procedimentos de Segurança da Informação**. Ed. Digital. Palhoça: UnisulVirtual, 2011.

JAMIL, G. L.; SOUZA, E. E.; VASCONCELOS, M. C. R. L**.. Como as empresas de base tecnológica protegem suas informações e conhecimentos?.** Revista Gestão & Tecnologia, v. 10, n. 1, art. 20, p. 1-11, 2010.

LAUREANO, Marcos Aurelio Pchek. **Gestão de segurança da informação.** Disponívelem: <http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf>. Acesso em 01de maio de 2017.

LENTO, Luiz Otávio Botelho. **Governança e Gestão da Segurança de Informação**. Ed. Digital. Palhoça: UnisulVirtual, 2011.

SÊMOLA, Marcos. **Gestão da segurança da informação**: uma visão executiva. 2ed. Rio de Janeiro: Campus, 2014.

~~ABNT – ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação: ABNT NBR ISO/IEC 27002:2005.** 2a. ed. Rio deJaneiro, 2005.~~CABRAL, Carlos; CAPRINO, Willian. **Trilhas em Segurança da**

Informação: caminhose ideias para a proteção de dados. Rio de Janeiro: Brasport, 2015. Livro no formato e *book*(posição 2 a 6139), adquirido em 16 de maio de 2017 na Amazon e disponível para leitura em <https://ler.amazon.com.br/>.

SÊMOLA, Marcos. **Gestão da segurança da informação**: uma visão executiva. 2ed. Rio de Janeiro: Campus, 2014.

CABRAL, Carlos; CAPRINO, Willian. **Trilhas em Segurança da Informação**: caminhose ideias para a proteção de dados. Rio de Janeiro: Brasport, 2015. Livro no formato e *book*(posição 2 a 6139), adquirido em 16 de maio de 2017 na Amazon e disponível para leitura em <https://ler.amazon.com.br/>.

LENTO, Luiz Otávio Botelho. **Governança e Gestão da Segurança de Informação**. Ed. Digital. Palhoça: UnisulVirtual, 2011.

GADLER, Lindamir do Carmo Secchi; MOTERLE, Roseli Rocha. **Políticas e Procedimentos de Segurança da Informação**. Ed. Digital. Palhoça: UnisulVirtual, 2011.

JAMIL, G. L.; SOUZA, E. E.; VASCONCELOS, M. C. R. L**.. Como as empresas de base tecnológica protegem suas informações e conhecimentos?.** Revista Gestão & Tecnologia, v. 10, n. 1, art. 20, p. 1-11, 2010.

LAUREANO, Marcos Aurelio Pchek. **Gestão de segurança da informação**. Disponívelem: <http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf>. Acesso em 01de maio de 2017.