PEDRO TENÓRIO MASCARENHAS NETO
WAGNER JUNQUEIRA ARAÚJO

SEGURANÇA DA INFORMAÇÃO

Uma visão sistêmica para implantação em organizações

Editora UFPB

PEDRO TENÓRIO MASCARENHAS NETO
WAGNER JUNQUEIRA ARAÚJO

SEGURANÇA DA INFORMAÇÃO

Uma visão sistêmica para implantação em organizações

Editora UFPB
João Pessoa
2019

UNIVERSIDADE FEDERAL DA PARAÍBA

Reitora MARGARETH DE FÁTIMA FORMIGA MELO DINIZ
Vice-Reitora BERNARDINA MARIA JUVENAL FREIRE DE OLIVEIRA

EDITORA DA UFPB

Diretora IZABEL FRANÇA DE LIMA
Supervisão de Administração GEISA FABIANE FERREIRA CAVALCANTE
Supervisão de Editoração ALMIR CORREIA DE VASCONCELLOS JUNIOR
Supervisão de Produção JOSÉ AUGUSTO DOS SANTOS FILHO

M395s Mascarenhas Neto, Pedro Tenório.
Segurança da informação: uma visão sistêmica para implantação em organizações / Pedro Tenório Mascarenhas Neto, Wagner Junqueira Araújo. - João Pessoa: Editora da UFPB, 2019.
160 p. : il.
Recurso digital (14,4MB)
formato: ePDF
Requisito do Sistema: Adobe Acrobat Reader

ISBN 978-85-237-1473-4

1. Segurança da informação. 2. Informação. 3. Segurança.
I. Mascarenhas Neto, Pedro Tenório. II. Araújo, Wagner Junqueira. III. Título.

UFPB/BC CDU 004.56

SUMÁRIO

Prefácio

Ter sido convidado para elaborar o prefácio dessa obra, trouxe toda uma história de vida que envolve o autor e sua trajetória profissional, chegando a se confundir com a história de uma instituição de ensino que teve ele como aluno, funcionário e, hoje, Diretor, numa sequência profissional de segurança, equilíbrio e dedicação, forma que representa muito bem essa obra.

Quando o autor fala em transformações do mundo, relatada na presente obra, e o quanto as mudanças que ocorrem com as novas tecnologias constituem um magnífico e dinâmico desenvolvimento e inovação baseados na informação das organizações, diz:

> " …O que já se tinha como conhecido e controlável dentro das organizações, hoje passam por mutações intensas de ordens diversas, tais como, econômicas, sociais, culturais, políticas, ideológicas e tecnológicas que impulsionam a metamorfose destes ambientes.
> A informação assume um papel fundamental na busca pela competitividade e sobrevivência das organizações, e sua gestão tornou-se a engrenagem estratégica que auxiliam os administradores, gestores e executivos no processo decisório. Os avanços tecnológicos têm transformado a forma que as organizações geram, processam e disseminam a informação, o aumento demasiado de informações, o poder de processamento e a agilidade de disseminá-las impõe grandes desafios às organizações, que buscam assegurar o sigilo, integridade e disponibilidade de suas informações."

Fica claro que a Informação é um elemento básico e peremptório do qual dependem os mais variados processos de decisão, sendo a

segurança da informação crucial dentro das organizações, para que se tenha Informação de qualidade e fidedigna, no momento certo e a custos controlados.

A obra rica em detalhes, dentro de um processo de pesquisa sério, demonstra o quanto o mundo corporativo está vulnerável em relação a segurança da informação e reafirma a necessidade de investimentos em prevenção contra ataques virtuais e proteção de dados corporativos. A obra demonstra a necessidade de controlar e gerenciar a infinidade de recursos, como indaga o autor: "... sem limitar, engessar e gerar conflitos? Como assegurar um ambiente informacional seguro frente à evolução tecnológica e da sociedade?"

Podemos ter a clareza nesse livro é com a preocupação em apresentar para as organizações a importância do sistema de segurança da informação dentro de um questionamento sistêmico de implantação. Fica evidente em vários estudos a necessidade de cada organização implantar um sistema de segurança como forma de garantir as suas informações num mundo atual, onde as redes virtuais são a grande transformação.

O autor teve a lucidez de apresentar momentos históricos da humanidade que evidencia, já em anos anteriores, onde não vivenciávamos um acelerado desenvolvimento da informação e a segurança da informação já era caracterizada.

Um dos motivos da leitura da obra é que nos leva ao nosso tempo, impulsionado pela evolução tecnológica, onde a informação, conectividade e interatividade estão dentro da grande preocupação das organizações, principalmente, interferindo na competividade e qualidade de gestão dada a nova realidade digital.

O desenvolvimento da obra apresentada foi elaborada numa sequência de cinco etapas, sendo a primeira responsável por aglutinar as atividades necessárias para o entendimento da organização, sendo

denominada de Contextualizando a Organização; na segunda etapa - Abrangência da PSI, define-se os limites e fronteiras da Política de Segurança da Informação; a Implementação da PSI constitui a terceira etapa, onde é realizado o inventário e classificação dos ativos, a análise de riscos e a construção da PSI; já na quarta etapa são descritas as atividades que darão visibilidade a PSI, bem como os treinamentos necessários, e por fim, a quinta etapa constitui os aspectos necessários para a manutenção das políticas na organização.

A leitura da obra é facilitada pela discrição das seções de forma ordenada possibilitando ao leitor interessado na implantação do sistema de segurança na sua organização, um melhor entendimento trazendo respostas ao questionamento: **como implementar e implantar a segurança da informação em uma organização?.**

Contudo é praticamente impossível ficar totalmente protegido, porém a obra se reporta a um planejamento adequado e medidas devidamente bem executadas, tornando possível se prevenir de problemas para organização nesse mundo globalizado e virtual.

No fundo, como a presente obra demonstra, os profissionais carecem de competências, conhecimento e qualificação para enfrentar a informação digital no nivel de evolução que estamos contemporâneamente vivenciando, porque um sistema de segurança de informação bem implantado e acompanhado é o que faz a diferença nas organizações.

A presente obra esta bem caracterizada quando o autor tem a sensibilidade e competência ao afirmar:

> Este estudo abriu a possibilidade da organização ampliar a segurança da informação para outras áreas de negócio, uma vez que, é possível replicar a metodologia utilizada e a Política de Segurança da Informação ser um documento interativo e abrangente.

Por fim, recebi com alegria o honroso convite do colega de trabalho e amigo leal para prefaciar sua obra de conclusão do mestrado que esta sendo transformado em livro dada a importância técnica do trabalho. Assim tive, antes do público leitor especializado, maravilhar-me com essa obra.

Mario Cesar Jucá

Contextualização

Nas organizações, percebe-se, uma mudança de paradigmas, em que os antigos "colaboradores" que recebiam as informações de forma passiva, dão lugar a "usuários" elementos ativos, que interagem com os processos e procedimentos organizacionais e com os sistemas de informação, estes por sua vez, vêm se tornando mutáveis e atrelados aos avanços tecnológicos.

Desta forma as organizações precisam assumir um comportamento dinâmico em relação à segurança de suas informações. Comportamentos letárgicos não são aceitáveis para os dias de hoje, pois vivemos um momento de transposição comportamental, em que a interação contínua, sem fronteiras e baseada nas relações de conectividade impõe diferentes desafios para as organizações do Século XXI e, principalmente, para a área de segurança da informação, que assume o papel crucial de proteger os ambientes informacionais das diferentes e numerosas formas de ataques existentes. O que já era considerado como conhecido e controlável, dentro das organizações, passa por mudanças intensas de ordens diversas - econômicas, sociais, culturais, políticas, ideológicas e tecnológicas - que impulsionam a metamorfose desses ambientes.

Nesse contexto, a informação assume um papel fundamental na busca pela competitividade e pela sobrevivência das organizações, e sua gestão tornou-se a engrenagem estratégica que auxilia os administradores, os gestores e os executivos no processo decisório.

Entendemos que a gestão da segurança da informação é uma atividade básica para proteger a informação de ameaças a sua integridade, disponibilidade e confidencialidade e responsável por assegurar e controlar o ambiente informacional na organização.

Segundo Nakamura e Geus (2002, p.9), "a informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e, consequentemente, necessita ser adequadamente protegida". Pode existir em diversos meios, ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio por meios eletrônicos e apresentada em filmes ou dita em conversas (ABNT NBR ISO/IEC 27002, 2013).

Vivenciamos uma avalanche de recursos tecnológicos - redes de relacionamentos, aplicativos móveis, redes de colaboração, ferramentas de mensagem instantânea e outros - que estão sendo inseridas no ambiente organizacional justificadas por inúmeros benefícios, dentre eles, agilidade, produtividade e poder de soluções no ambiente de trabalho. Em contrapartida, em alguns casos percebe-se uma certa negligência com os diferentes tipos de ameaças e vulnerabilidades introduzidas por tais ferramentas.

Em um momento em que, para muitos, não importa a exposição que tais ferramentas podem ocasionar, aplicativos e softwares são instalados sem nenhum conhecimento prévio dos seus riscos e vulnerabilidades que podem provocar.

A convergência tecnológica já não possibilita a proibição de alguns recursos tecnológicos dentro do ambiente organizacional, e os mesmos dispositivos e os recursos que beneficiam as organizações acabam tornando-as vulneráveis.

Nesse sentido, as organizações enfrentam este dilema: como controlar, proibir e gerenciar essa infinidade de recursos dentro da organização sem limitar, engessar e gerar conflitos? Como garantir um ambiente informacional seguro, considerando a evolução tecnológica e da sociedade?

Lyra (2008) enfatiza que a segurança da informação é obtida com a implementação de um conjunto de controles adequados que inclui políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Esses controles, além de implementados, precisam

ser estabelecidos, monitorados, analisados criticamente e melhorados onde for necessário, para garantir que os objetivos do negócio e da segurança da organização sejam atendidos.

Inúmeras organizações, institutos e órgãos mensuram o impacto da segurança da informação nas organizações avaliando sua maturidade no quesito 'segurança'. Constantemente são publicados relatórios oriundos de pesquisas, com o intuito de mapear o cenário de incidentes e seus impactos no mundo corporativo.

Nesse contexto, destacam-se as pesquisas realizadas pela PWC[1], que é constituída de um *network*[2] global de empresas, presentes em 157 países, em sua 18ª edição A *Global State of Information Security*[3], lançada em 2015 e a 19ª publicada em 2018, apresentam o crescimento exponencial nos incidentes de informação em âmbito mundial e indicam um aumento de 274% de números de ataques cibernético no Brasil, o que o coloca em uma situação de extrema preocupação.

Os resultados da pesquisa da *PWC* demonstraram, ainda, que as empresas brasileiras de pequeno porte relataram um aumento dramático nos incidentes, originado, provavelmente, por seus funcionários (41%); 39% apontaram que o roubo de dados inerentes aos seus funcionários trouxe perdas financeiras, e o investimento em segurança da informação realizado pelas pequenas empresas cresceu quando comparado com o crescimento das grandes empresas, o que demonstra uma forte preocupação e ascensão da segurança da informação dentro das organizações.

A *Information System Audit and Control Association* [4](ISACA), em sua publicação 'O estado de segurança cibernética: implicações para 2016', realizada

1 Empresa de consultoria empresarial originada pela fusão da Price Waterhouse com a Coopers.
2 Rede de colaboração de empresas;
3 Um estado global da Segurança da Informação;
4 Associação de Auditoria e Controle de Sistemas de Informação.

com profissionais certificados na área de segurança da informação, apresenta os tipos de ataques mais frequentes nas organizações, que são combatidos rotineiramente por esses profissionais: a saber: roubo online de identidade, *hacking*, códigos maliciosos, roubo de propriedade intelectual, danos intencionais aos sistemas de informática, perdas físicas, *phishing*[5] e negação de serviços.

Em âmbito nacional, destaca-se a Pesquisa Nacional de Segurança da Informação, realizada em 2014 pela DARYUS[6], um grupo de empresas brasileiras que atuam nas áreas de consultoria, educação e tecnologia para apoiar a gestão empresarial, a estratégica e a de riscos. Essa pesquisa revelou que 52,46% das organizações brasileiras participantes têm um sistema de segurança da informação implantado de forma parcial e iniciado exclusivamente pelo setor de Tecnologia da Informação (TI), o qual é responsável por gerir essas ações em 65% dessas organizações. No que diz respeito aos incidentes de segurança, o vazamento de informações foi o que se apresentou com o maior percentual (16,5%), o mau uso, com 16,5%, e a perda de informações, 12,4%, entre outros.

Esse cenário revela uma realidade comum nas organizações mundiais e nas nacionais, porém as organizações internacionais demonstram superioridade no nível de maturidade em suas práticas de segurança da informação, enquanto a maioria das organizações brasileiras ainda tentam, de alguma forma, implementar a segurança da informação em seu ambiente.

Diante do exposto, esta obra objetiva apoiar as organizações que desejem implantar a segurança de suas informações, por meio de uma abordagem sistêmica capaz de conduzir a implementação e a implantação de políticas de segurança com um processo flexível e adaptável as necessidades de cada organização.

---

5 Técnica de fraude online, empregada para roubar senhas e informações pessoais.

6 Grupo de empresas brasileiras de consultoria nas áreas de gestão, educação, segurança e eventos.

Organização espaço-temporal

Compreender as particularidades, as complexidades ou, a essência da segurança da informação não é um exercício fácil, principalmente por causa dos aspectos que envolvem a contemporaneidade.

Atualmente, mais do que em outras épocas, a informação assume o palco principal e figura como um ativo dotado de extremo valor para as organizações. Desde os tempos mais longínquos até a atualidade, a informação ganhou importância, significações e representações diversas que demandaram ações para dotá-las de algum grau de segurança. Para entender o ideário proposto acerca da segurança da informação, é essencial explicitar alguns diferentes conceitos e pontos de vista, porquanto esses aspectos são responsáveis pelas diversas visões e definições do tema. Antes de apresentar a conceituação em si, é necessário remontar a alguns fatos históricos que trazem em sua representatividade a importância e o valor que a informação adquiriu ao longo do tempo.

Dentro de um contexto histórico, evidenciou-se, nas mais diversas civilizações, a preocupação eminente de salvaguardar as informações. Por exemplo, na antiga China, a linguagem escrita era reservada a membros pertencentes à classe superior que exerciam o direito de aprender a ler e a escrever. Essa mesma civilização utilizava duas formas distintas de registrar suas informações, conforme seu grau de importância: a escrita demótica, utilizada para os assuntos do cotidiano, e a hieroglífica, mais complexa e formada por desenhos e símbolos, era usada para informações consideradas restritas a um grupo de pessoas.

Nos tempos da Roma antiga, marcada por intensas disputas de território, a interceptação de uma mensagem podia significar a queda de todo o Império. As famosas cifras de César, uma das primeiras incursões

no campo da criptografia, eram um simples sistema de substituição de algarismo que protegia as mensagens enviadas pelo Imperador Júlio César aos seus generais nos campos de batalha.

Embora tenhamos em nossa história inúmeros fatos que representam o valor que uma informação detém e a preocupação em assegurá-la, talvez, o mais importante e representativo fato histórico marcante seja a construção da máquina Enigma, utilizada pelos exércitos alemães durante a segunda guerra mundial para codificar e decodificar informações repassadas para suas tropas.

A Enigma é fruto da necessidade dos alemães de que o sigilo de suas informações fosse garantido. Sua operacionalidade era regida por normas impostas aos seus utilizadores, que obrigavam que a chave de sua configuração fosse mudada diariamente para dificultar a decodificação de suas informações. Durante a segunda guerra, registraram-se diversas tentativas de decifrar os códigos da Enigma, entre elas, a operação denominada *Ultra*[7], formada por poloneses e britânicos. O matemático britânico Alan Turing conseguiu decifrar o código da Enigma, que possibilitou a interceptação das informações alemãs e auxiliou a vitória dos aliados na guerra.

Na contemporaneidade, vivenciamos um novo paradigma informacional, impulsionado pela evolução tecnológica, e em que os conceitos de informação, conectividade e interatividade impõem grandes desafios às organizações. As informações tornaram-se acessíveis a todos e em qualquer momento, o conceito de fronteira foi transposto por uma nova realidade digital, e a tecnologia da informação perpetuou-se no cerne da evolução humana, imputando o surgimento de novos comportamentos em relação às informações.

Para o autor Araújo (2009), no mundo conectado em rede, onde a informação flui, as organizações, sejam empresas privadas ou do setor

7 Operação organizada pelos britânicos durante a 2ª guerra mundial, com objetivo de interceptar e decifrar os códigos gerados pela máquina Enigma.

governamental, necessitam de processos e controles de segurança para garantir e preservar suas informações de uma gama de novas ameaças. A norma ABNT NBR ISO/IEC 27002: 2013 reforça a afirmação do autor supracitado, ao declarar que "a informação é um ativo essencial para o negócio de uma organização e necessita ser adequadamente protegida".

Nas organizações do Século XXI, a informação assume sua importância devido ao deslocamento do paradigma de sociedade industrial para a sociedade da informação. A era industrial tinha como princípio fundamental associar os recursos terra, trabalho e capital como forma de criar riquezas. Nessa nova era, a informação é o mais importante recurso de agregação de valor para essas organizações, razão por que é imprescindível que identifiquemos a percepção do seu valor nos ambientes organizacionais.

Em seu espaço temporal, a informação assumiu universalmente um lugar de destaque na evolução da sociedade. Atualmente é consenso afirmar que a informação é o principal ativo de uma organização na busca pela competitividade e sua sobrevivência, e que sua gestão é a engrenagem estratégica que auxilia os administradores, os gestores e os executivos no processo decisório.

Os avanços tecnológicos têm transformado a forma como as organizações geram, processam e disseminam a informação. A convergência tecnológica impõe a ruptura de inúmeros paradigmas à segurança da informação, com desafios que visam assegurar o sigilo, a integridade e a disponibilidade de suas informações.

Vivenciamos uma guerra cibernética, com proporções difíceis de mensurar, nunca vista antes, em que a informação se tornou objeto de desejo das pessoas, e organizações e países buscam incessantemente produzir efeitos maléficos ou benéficos a seus propósitos. Nesse contexto, a falta da segurança da informação nas organizações as coloca como alvos vulneráveis às mais diversas ameaças.

A informação no contexto das organizações

A evolução das tecnologias de informação e comunicação, as mudanças das organizações e seus métodos de trabalho, o aumento exponencial da informação e do conhecimento, o acesso facilitado à informação, o surgimento de novos modelos de negócios, a comunicação síncrona e a competitividade imposta pela globalização são alguns fatores que têm provocado as alterações de paradigmas nas organizações contemporâneas. Nesse cenário, a informação assume um papel fundamental na nova realidade mundial de uma sociedade globalizada, e a aceitação dessa ideia a coloca como recurso chave de competitividade, de diferencial de mercado, de lucratividade e de poder nessa nova sociedade do Século XXI.

Ao longo do tempo, o termo informação recebeu inúmeros significados e interpretações das mais variadas áreas e subáreas do campo científico. Tais campos, influenciados por diversas correntes e perspectivas teóricas, desenvolveram conceitos particulares de informação, alguns convergentes e outros divergentes, porém fundamentados na objetividade de sua aplicação ao seu campo científico. Não tivemos a pretensão de explicitar os fundamentos teóricos e epistemológicos que suportam os diversos entendimentos acerca da informação, mas, em linhas gerais, apontar os pilares essenciais que dão suporte a essa nova perspectiva informacional no contexto das organizações.

A palavra informação deriva do latim, *informare,* que significa dar forma ou aparência, criar, representar uma ideia ou noção de algo que é colocado em forma, em ordem. Comumente encontramos o emprego da palavra informação como o ato ou efeito de informar, comunicar-se, algo transmitido e dotado de propósitos.

Cardoso (1996, p. 71) afirma que

> o termo, cujo uso remonta à Antiguidade, [...] sofreu, ao longo da história, tantas modificações em sua acepção, que na atualidade seu sentido está carregado de ambiguidade: confundido frequentemente com comunicação, outras tantas com dado, em menor intensidade com instrução, mas recentemente com conhecimento.

Adotamos a definição de informação que converge para os propósitos de investigar os conceitos de informação dentro de um limite e em um espaço bem delimitado, ou seja, o contexto das organizações. Nesse contexto, consideramos *dados*[8] como um elemento indissociável da informação. Drucker (2000, p. 13) define a informação como um "dado investido de propósito". Para Stair e Reynolds (2002, p.10), "informação é um conjunto de fatos organizados de modo a terem valor adicional, além do valor dos fatos propriamente ditos".

Segundo McGee e Prusak (1994, p. 24), a informação é representada por "dados coletados, organizados, ordenados, aos quais são atribuídos significados e contexto". Davenport (1994, p. 04) acrescenta que informação é uma "mensagem, geralmente na forma de um documento ou uma comunicação audível ou visível" e que, em um processo natural, os dados são transformados em informações.

Nesse sentido, podemos entender os dados como um elemento que representa eventos ocorridos em uma organização, antes de serem organizados em uma forma entendível, ou seja, os dados são elementos brutos desprovidos de significados. Depois de serem submetidos a um processo de organização, manipulação, análise e avaliação, os dados passam

8 Uma sequência de símbolos quantificados ou quantificáveis, dotados de representações diversas.

a ter valor para a organização, em um contexto especifico, e assumem a forma de informação.

O Tribunal de Contas da União reconhece a importância da informação quando, em seu Manual de Boas Práticas em Segurança da Informação, declara:

> Porque a informação é um ativo muito importante para qualquer instituição, podendo ser considerada, atualmente, o recurso patrimonial mais critico. Informações adulteradas, não disponíveis, sob o conhecimento de pessoas de má-fé ou concorrentes podem comprometer significativamente não apenas a imagem da instituição perante terceiros, como também o andamento dos próprios processos institucionais. É possível inviabilizar a continuidade de uma instituição se não for dada a devida atenção à segurança de suas informações. (TRIBUNAL DE CONTAS DA UNIÃO, 2012, p.10)

À medida que as informações se proliferam no seio das organizações, geram-se problemas de difíceis resoluções práticas, pois sua importância assume um caráter subjetivo e dinâmico em função do papel que pode desempenhar nas atividades da organização, o que exige esforços para distingui-las e classificá-las diante dos diversos critérios que podem ser adotados. Entendemos que, fundamentalmente, a classificação das informações em uma organização deve ser conduzida sob dois aspectos distintos e cruciais: o primeiro refere-se a sua importância para o negócio, e o segundo, à sua proteção durante seu ciclo de vida.

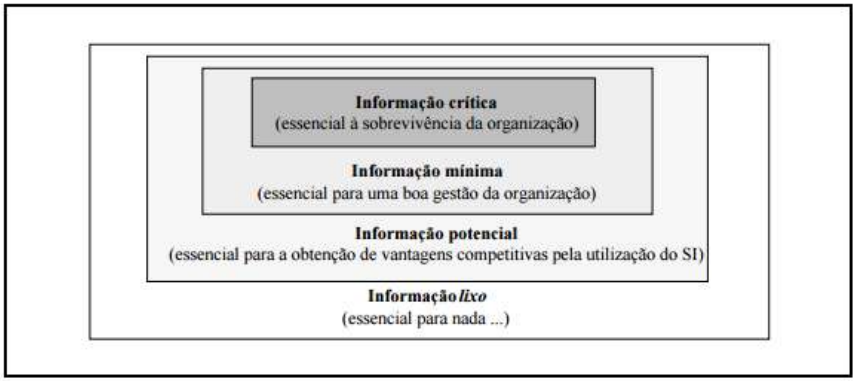
Amaral (1994) apresenta quatro classes de informação de acordo com sua importância para a organização, a saber:

- A informação crítica – essencial à sobrevivência da organização;
- A informação mínima – essencial para uma boa gestão da organização;

- A informação potencial – essencial para a obtenção de vantagens competitivas utilizando-se os sistemas de informação;
- A informação lixo – desprovida de qualquer valor.

Amaral (1994, p. 28) refere, ainda, que "deverá haver uma evolução do esforço por parte da organização na procura e manutenção da informação crítica, da informação mínima e da informação potencial. Já sobre a informação lixo, o esforço é, obviamente, para se evitar qualquer desperdício de recurso com ela". Essas classes de informações indicadas pelos autores podem ser visualizadas na figura 1.

Figura 1: Classes de informação nas organizações



Fonte: Amaral (1994, p.28)

Para Beal (2012), além de algumas classificações empregadas, cada organização precisa adotar um esquema de classificação da informação sob o ponto de vista de seus requisitos de segurança: sigilo, autenticidade, integridade e disponibilidade.

Nesse contexto, a estrutura organizacional assume um papel fundamental no bom manuseio de suas informações. Basicamente,

as estruturas organizacionais dividem-se em dois tipos: formal e informal. Segundo Oliveira (2001, p.82), a estrutura formal "é aquela deliberadamente planejada e formalmente representada, em alguns de seus aspectos, pelo organograma", e a estrutura informal relaciona-se "à rede de relações sociais e pessoais", ou seja, ocorre de forma espontânea, através da interação entre os indivíduos.

Em geral, as organizações diferenciam-se em três níveis organizacionais, qualquer que seja a natureza ou tamanho da organização. Para Chiavenato (2003, p.525-526), esses níveis organizacionais são denominados de:

institucional ou estratégico: corresponde ao nível mais elevado da organização e é composto de diretores, proprietários, acionistas e executivos. É o nível em que as decisões são tomadas e são definidos os objetivos da organização e as estratégias para alcançá-las;

intermediário: também chamado de nível mediador ou gerencial, é o nível colocado entre o institucional e o operacional e que cuida da articulação interna entre ambos. Esse nível é responsável por transformar as estratégias formuladas para atingir os objetivos de negócio em programas de ação;

operacional: denominado de nível técnico, localiza-se nas áreas inferiores da organização e se liga diretamente às atividades rotineiras da organização. É o nível em que as tarefas e as operações são realizadas.

É importante perceber que os níveis organizacionais supracitados apresentam-se de forma interligada, por meio de um processo de apoio mútuo, em que se estabelecem os fluxos de informações. Nesse sento, o nível operacional tem a função de sustentar os demais, visto que é nele que se origina grande parte das informações que irão subsidiar o nível estratégico.

Em sua essência, a informação traz um atributo de valor dentro do contexto em que é inserida, devido a sua característica abstrata e intangível, e quantificar seu valor é uma tarefa não trivial. Assim, surgem

inúmeros parâmetros capazes de verificar seu valor na organização, tais como: qualidade, comportamento, juízo de valor e outros.

Para Cronin (1990), uma das maneiras de quantificá-las é por meio dos seguintes juízos de valor:

- Valor de uso: baseia-se na utilização final da informação;
- Valor de troca: é aquele que os usuários estão preparados para pagar e varia de acordo com as leis de oferta e demanda. Também pode ser denominado de valor de mercado;
- Valor de propriedade: que reflete o custo substitutivo de um bem;
- Valor de restrição: que surge no caso de informação secreta ou de interesse comercial, quando o uso fica restrito a algumas pessoas.

Moresi (2000) enfatiza que é difícil quantificar monetariamente o valor das informações e que o valor de troca é o que mais se aproxima de uma equivalência monetária, porque, por meio dela, poderá ser obtido algum tipo de vantagem competitiva. O autor acrescenta que uma informação que tem seu valor de troca carrega um valor de restrição, uma vez que, normalmente, representa insumos cruciais de competitividade.

Beal (2012) observa que a informação de boa qualidade (relevante, precisa, clara, consistente, oportuna) tem um valor sobremaneira significativo para as organizações e pode ser aplicada em diferentes contextos. Já para Lesca e Almeida (1994), o valor da informação apresenta-se em quatro contextos:

- Fator de apoio à decisão: a informação possibilita que se reduzam as incertezas na tomada de decisão e possibilita que escolhas sejam feitas com menos risco e no momento adequado.
- Fator de produção: a informação é um elemento importante para criar e introduzir no mercado produtos (bens e serviços) de maior valor adicionado.

- Fator de sinergia: o desempenho de uma organização está condicionado à qualidade das ligações e das relações entre as unidades organizacionais, as quais, por sua vez, dependem da qualidade do fluxo informacional existente para proporcionar o intercâmbio de ideias e informações.
- Fator determinante de comportamento: a informação exerce influência sobre o comportamento dos indivíduos e dos grupos, dentro e fora das organizações: internamente, visa influenciar o comportamento dos indivíduos para que suas ações sejam condizentes com os objetivos corporativos; externamente, visa influenciar o comportamento dos envolvidos (clientes atuais ou potenciais, fornecedores, governo, parceiros etc.), de modo que se torne favorável ao alcance dos objetivos organizacionais.

Moody e Walsh (1999), ao analisar a informação como um ativo organizacional, relacionam as seguintes leis, que definem o comportamento da informação como um bem econômico:

- 1ª Lei: A informação é (infinitamente) compartilhável - A informação pode ser compartilhada infinitamente, sem que seja consumida nesse processo. Quando a informação de uso interno é compartilhada pelos funcionários, transforma-se em um valioso elemento de integração de processos e compreensão da organização. Já as informações destinadas ao ambiente externo têm seu valor aumentado quando um maior número de usuário é atingido.
- 2ª Lei: O valor da informação aumenta com o uso - Quanto mais a informação é utilizada, maior é o valor associado a ela.
- 3ª Lei: A informação é perecível - A informação perde parte de seu valor potencial à medida que o tempo passa.

- 4ª Lei: O valor da informação aumenta com a precisão – Quanto mais precisa for a informação, mais útil ela será, portanto, mais valiosa.
- 5ª Lei: O valor da informação aumenta quando há combinação de informações – Quanto mais integrada estiver a informação, maior será seu valor potencial dentro das organizações, porquanto possibilita uma visão sistêmica dos processos, em substituição à visão estanque de funções, departamentos e produtos.
- 6ª Lei: Mais informação não é necessariamente melhor – Para que as informações úteis tenham seu valor agregado, precisam ser filtradas com critérios de relevância, quantidade e qualidade de sua apresentação. As informações que não resultam em decisões ou processos produtivos melhores não apresentam valor associado, e assim como a insuficiência, a sobrecarga prejudica o desempenho.
- 7ª Lei: A informação se multiplica – A informação apresenta-se de forma "autogenerativa", e seu valor pode ser potencializado pelas oportunidades de reciclagem e de uso em novas situações.

Van e Hoog (1996) simplificam essa discussão e mencionam dois domínios a serem percebidos sobre a informação: no primeiro, se ela atender às necessidades de uma pessoa ou grupo; e no segundo, se satisfizer aos processos decisórios da organização. Nessa perspectiva, adota-se o ideário de Van e Hoog (1996), que entendem que a informação será valiosa para a organização quando satisfizer aos anseios dos desejos humanos e/ou aos bens e aos serviços da organização. Por conseguinte, a percepção de seu valor perpassa o efeito que ela exerce sobre a organização como um todo.

Princípios elementares da segurança da informação

Dentro da literatura e até mesmo no cotidiano emprega-se o termo segurança em múltiplos sentidos e frequentemente associa-se seu significado a ações de restrição, cerceamento, defesa entre outros, sendo muitas vezes compreendida como sinônimos de repressão, impedimento, proibição e punição.

Para Matos (2001, p.1), a palavra é de origem latina, significa "sem preocupações", e sua etimologia sugere o sentido de "ocupar-se de si mesmo" (se+cura). Ainda para o autor, "em uma definição mais comum, segurança é "um mal a evitar", por isso é a ausência de risco, a previsibilidade, a certeza quanto ao futuro". Nos ambientes organizacionais, a preocupação com os aspectos de segurança difere em grau e amplitude de importância e é frequente o equívoco de perceber a segurança por meio de abordagens isoladas dentro do contexto organizacional, geralmente fundamentas em aspectos tecnológicos, técnicos e sociais.

Summers (1997, p.21) percebe a segurança da informação como um componente intrínseco ao uso dos computadores e a considera como uma meta a ser atingida para proteger os sistemas computacionais contra ameaças à confidencialidade, à integridade e à disponibilidade. Para Oliveira (2001), a segurança da informação é "o processo de proteção de informações e ativos digitais armazenados em computadores e redes de processamento de dados".

A definição dos autores supracitados sustenta-se no viés de soluções tecnológicas voltadas apenas para a área de TI. Eles subestimaram elementos importantes de produtividade, como pessoas, ativos e processos.

Evidencia-se que, ao assumir essa abordagem, a organização ficará limitada a ações reativas, pontuais, sem embasamento de processos e dependentes de esforços individuais.

Segundo Peltier (2001, p.8), "a segurança da informação compreende o uso de controles de acesso físicos e lógicos, com o intuito de proteger os dados contra modificações acidentais ou não autorizadas, destruição, quebra de sigilo, perda ou dano aos ativos informacionais". Nessa definição, percebe-se que há uma delimitação da segurança em relação ao uso exclusivo de controles para atuar nos espaços físicos e lógicos da organização, abstendo-se dos fatores de interferência que os recursos humanos exercem sobre a segurança.

Em uma perspectiva mais recente, o fator humano passou a ser preponderante para o alcance dos objetivos da segurança da informação. Marciano (2006, p.114) propôs uma definição social em que

> a segurança da informação é um fenômeno social no qual os usuários dos recursos informacionais têm razoável conhecimento sobre o uso desses recursos, incluindo os ônus decorrentes, bem como sobre os papéis que devem desempenhar no exercício desse uso.

Mitnick e Simon (2003) afirmam que o homem é a maior causa de incidentes de segurança da informação. Alexandria (2009) concorda com os autores, ao alertar que é um erro comum não considerar os aspectos sociais e humanos evolvidos na construção da segurança da informação. Embora os autores supracitados apresentem definições ligeiramente divergentes, elas representam o entendimento a respeito da segurança da informação sob o domínio de suas áreas de estudo. É importante destacar as contribuições advindas dessas percepções para o entendimento global da segurança da informação.

A complexidade e o dinamismo das organizações, aliados ao aumento exacerbado de informações, impõem uma visão global sobre a segurança que a coloca como um problema de negócio e demandam esforços mais abrangentes, com foco em gerenciamento de riscos ligados a objetivos mais amplos, como a continuidade dos negócios, a redução de custos com incidentes de segurança e o aumento da competitividade. Essa visão passa a atender às organizações através de ações proativas, adaptativas, orientadas para processos, por um gerenciamento sistêmico e contínuo da segurança da informação.

A norma ISO/IEC 17799:2005, em sua seção introdutória, define segurança da informação como "a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio". Para Sêmola (2014, p.41), "a segurança da informação é uma área de conhecimento voltada à proteção da informação e dos ativos associados contra indisponibilidade, alterações indevidas e acessos não autorizados". O autor considera a segurança da informação de forma mais ampla, por meio de práticas de gestão de riscos e incidentes que impliquem o comprometimento da confidencialidade, da integridade e da disponibilidade das informações.

Para o desenvolvimento desta pesquisa, foram consideradas as definições da ISO/IEC 17799: 2005 e de Sêmola, porque convergem para a amplitude do contexto em estudo. Nesse sentido, fundamentalmente a segurança da informação tem a finalidade de proteger a informação referente à sua confidencialidade, integridade e disponibilidade.

Conforme Sêmola (2014, p.43),

- Confidencialidade – Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando limitar seu acesso e uso às pessoas a quem é destinada.

- Integridade – Toda informação deve ser mantida na mesma condição em que foi disponibilizada por seu proprietário, visando protegê-la contra alterações indevidas, intencionais ou acidentais.
- Disponibilidade – Toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível para seus usuários, no momento em que eles necessitam delas para qualquer finalidade.

Segundo o Tribunal de Contas da União, a confidencialidade

> consiste na garantia de que somente pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por meio de redes de comunicação. Manter a confidencialidade pressupõe assegurar que as pessoas não tomem conhecimento de informações, de forma acidental ou proposital, sem que possuam autorização para tal procedimento. (TRIBUNAL DE CONTAS DA UNIÃO, 2012, p.9)

A confidencialidade garante que só os destinatários da informação tenham acesso a ela. Isso significa que manter a confidencialidade das informações é ter a segurança de que o que foi dito ou escrito será transmitido ou cedido apenas a quem de direito. Ressalta-se que a violação desse requisito poderá trazer impactos imensuráveis para a organização. Podemos exemplificar como a quebra de confidencialidade o vazamento de informações ocorrido no ano de 2010, no Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira (INEP), onde José Joaquim, então presidente do INEP, divulgou, em nota pública, a confirmação do vazamento dos dados de cerca de 12 milhões de estudantes que fizeram as provas do Exame Nacional do Ensino Médio (ENEM) nos anos de 2007, 2008 e 2009, o que acarretou no acesso não autorizado a informações confidenciais dos participantes que poderiam ser utilizadas por estelionatários.

> A integridade consiste na fidedignidade de informações. Sinaliza a conformidade de dados armazenados com relação às inserções, alterações e processamentos autorizados. Sinaliza, ainda, a conformidade dos dados transmitidos pelo emissor com os recebidos pelo destinatário. A manutenção da integridade pressupõe a garantia de não violação dos dados. (TRIBUNAL DE CONTAS DA UNIÃO, 2012, p.9)

Garantir que a informação não seja alterada é o objetivo do segundo pilar – Integridade – que busca fidedignidade das informações. É importante destacar que essa garantia perpassa a violação intencional e estende-se a causas acidentais. Por isso se deve garantir a proteção das informações sob os aspectos intencionais e acidentais, como, por exemplo: hipoteticamente, os investimentos de uma organização foram pautados no relatório de desempenho de vendas de seus produtos. Depois dessa decisão, descobriu-se que o relatório foi alterado intencionalmente por um funcionário insatisfeito, o que pode ocasionar perdas financeiras e estratégias equivocadas da organização.

Para o Tribunal de Contas da União, a disponibilidade é a

> garantia de que as informações estejam acessíveis às pessoas e aos processos autorizados, a qualquer momento requerido, durante o período acordado entre os gestores da informação e a área de informática. Manter a disponibilidade de informações pressupõe garantir a prestação contínua do serviço, sem interrupções no fornecimento de informações para quem é de direito. (TRIBUNAL DE CONTAS DA UNIÃO, 2012, p.10)

A disponibilidade garante que a informação esteja disponível para todos os seus usuários, no momento em que houver necessidade. Por exemplo: uma organização atualiza sua tabela de preços de venda de produtos devido a um erro de sincronização das bases de dados dos

sistemas de venda de suas várias filias. Depois de um longo período de tempo, percebe-se que alguns milhares de produtos foram vendidos a um preço inferior.

Embora esses exemplos demonstrem aplicabilidade em diferentes contextos, é evidente que a violação de qualquer um dos pilares impacta de forma negativa a organização. Ressaltamos que não há, na literatura, o entendimento de que um pilar se sobreponha a outro no quesito de importância, pois todos os três formam a tríade a ser seguida na busca por segurança.

Apesar do consenso de que esses elementos formam a tríade que a segurança da informação deverá seguir na busca por segurança, alguns autores adicionam a autenticidade e o não repúdio como aspectos essenciais para a consecução dos objetivos que se pretendem alcançar. Para Beal (2012, p.52), além dos pilares supracitados, a autora considera os requisitos abaixo:

- Autenticidade – Garantia de que a informação seja proveniente da fonte à qual ela é atribuída.
- Irretratabilidade da comunicação (não repúdio) – Proteção contra a alegação por parte de um dos participantes de uma comunicação de que não ocorreu.

Coelho et al (2014) consideram, ainda, como essenciais os atributos:

- Conformidade – Estar em conformidade é estar de acordo seguindo e fazendo com que se cumpram leis e regulamentos internos e externos.
- Controle de acesso – Trata de limitar e controlar o acesso lógico/físico aos ativos de uma organização por meio dos processos de identificação, autenticação e autorização, com o objetivo de proteger os recursos contra acessos não autorizados.

A compreensão da segurança da informação, além dos conceitos primários já explanados, perpassa o entendimento de conceitos secundários que a circundam em todo o seu processo de proteção à informação, como ativo, vulnerabilidade, ameaças, ataques e risco.

Ativo

De forma geral, podemos entender um ativo como qualquer elemento de valor para uma organização, seja humano, tecnológico ou software, como, por exemplo, banco de dados, softwares, equipamentos (computadores e notebooks), servidores, elementos de rede (roteadores, switches, entre outros), pessoas, processos e serviços. O autor Sêmola (2012, p.43-44) o define como "todo elemento que compõe os processos que manipulam e processam a informação, a contar da própria informação, o meio em que ela é armazenada e os equipamentos em que é manuseada, transportada e descartada".

A norma ABNT NBR ISO/IEC 27005: 2011 sugere a distinção entre ativos primários e ativos de suporte e infraestrutura, apresentados no Quadro 1. Os primários são as informações, os processos e as atividades de negócio. Já os de suporte compreendem os meios em que os primários se apoiam e podem ser agrupados em: hardware, software, rede, recursos humanos, instalações físicas e estrutura da organização.

Quadro 1: Classificação de ativos

ATIVOS PRIMÁRIOS	
Classes	**Descrição**
Processos e atividades de negócio	São executados visando ao desempenho das funções da organização. Processos são os elementos que mais agregam valor à organização.
Informações	São usadas para apoiar a execução desses processos, além das de caráter pessoal, estratégicas ou com alto custo de aquisição.
ATIVOS DE SUPORTE	
Classes	**Descrição**
Hardware	Constituído de todos os elementos físicos que suportam a execução automática de processos.
Software	Constituído de programas computacionais
Rede de computadores	Constituída de todos os dispositivos de redes e telecomunicações que interconectam os dispositivos e os elementos dos sistemas de informação, como redes telefônicas, de computadores de longa distância, metropolitanas, locais e *ad hoc*[9], roteadores, *bridges*[10], hubs [11]e outras interfaces de comunicação.
Recursos humanos	Constituídos de grupos enquadrados entre tomadores de decisão, usuários, pessoal de manutenção e operação e desenvolvedores de software.
Instalações físicas	Constituídas de todos os lugares que agregam os demais ativos sob o escopo e os meios para operacionalizá-los, como: espaços exteriores, perímetros defensivos, zonas dentro do perímetro, serviços essenciais para operação de equipamentos, serviço de comunicação, utilidades para suprimento de energia elétrica, condicionamento do ar etc.
Estrutura organizacional	Constituída de autoridades, subunidades da organização, projetos, subcontratados e fornecedores.

Fonte: Elaborado pelos autores com base na ISO NBR 27005:2011 - 2018

9 Tipo de rede em que não há um nó ou terminal especial - geralmente designado como ponto de acesso - para o qual todas as comunicações convergem e que as encaminha para os respectivos destinos.

10 Equipamento de rede que possibilita a interconexão entre duas redes distintas.

11 É um equipamento que tem a função de interligar vários computadores em uma rede.

É de extrema importância que a organização conheça seus ativos tangíveis e intangíveis, classifique-os e lhes atribua responsabilidades pelos ativos. Isso poderá diminuir as chances de que a segurança desses ativos seja comprometida. Para isso, é necessário que seja realizado um inventário dos ativos e, para cada ativo identificado, seja definido seu proprietário, que ficará encarregado de manter os controles de segurança.

O inventário dos ativos é realizado por meio do seu levantamento e de seu enquadramento, em sua respectiva classe. Essa atividade é considerada como difícil de ser executada, devido às interdependências entre as partes que constituem a execução dos processos e os sistemas de informação de uma organização. Segundo Alberts e Dorofee (2002), o levantamento é feito com a realização de workshops de elicitação de conhecimento, empregando-se técnicas como entrevistas e *brainstorm,* em que os participantes selecionados das áreas de negócios da organização focam seus trabalhos e identificam os ativos relacionados ao desempenho de suas atividades.

Vulnerabilidade

Vulnerabilidade é a fragilidade de um ativo ou grupo de ativos, que pode ser explorada por uma ou mais ameaças. Segundo Sêmola (2012, p.47),

> 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.

As vulnerabilidades são falhas que, por si sós, não provocam incidentes, pois são elementos passivos que dependem de um agente causador ou favorável que a explorem tornando-as ameaças para a segurança da organização. As organizações devem conhecer e controlar as

ameaças a seus ativos informacionais, pois, quando as vulnerabilidades são exploradas por elas, podem gerar impactos de proporções imensuráveis. Sob o ponto de vista de Sêmola (2012), são exemplos de vulnerabilidade:

- Físicas – Falta de extintores, detectores de fumaças e de outros recursos para combater incêndios em ambientes com ativos ou informações estratégicas, acesso facilitado a ambientes de processamento de dados, deficiência de controles de acesso em locais de armazenamento de informações confidenciais ou sensíveis etc.
- Naturais – Ambientes com equipamentos eletrônicos perto de locais suscetíveis a desastres naturais, como incêndio, enchentes, terremotos, tempestades, e outros, como falta de energia, acúmulo de poeira, aumento de umidade etc.
- Hadware – Os computadores são suscetíveis à poeira, à umidade, à sujeira e ao acesso indevido a recursos inadequadamente protegidos e podem sofrer com componentes deficientes ou mal configurados, como falhas ou flutuações no suprimento energético ou aumento excessivo de temperatura ambiente.
- Software – Erros na codificação, na instalação ou na configuração de sistemas e aplicativos podem acarretar acessos indevidos, vazamento de informações, perda de dados e de trilhas de auditoria ou indisponibilidade do recurso quando necessário.
- Mídias – Discos, fitas, relatórios e impressos podem ser perdidos ou danificados, e falhas de energia podem causar panes em equipamentos e danificar trilhas lógicas de dados. Discos rígidos, usualmente, têm vida útil, e a radiação eletromagnética pode afetar diversos tipos de mídias magnéticas.
- Comunicação – A comunicação telefônica é vulnerável a escutas (acesso indevido) ou a problemas na infraestrutura física ou lógica que a impeçam de ser estabelecida.

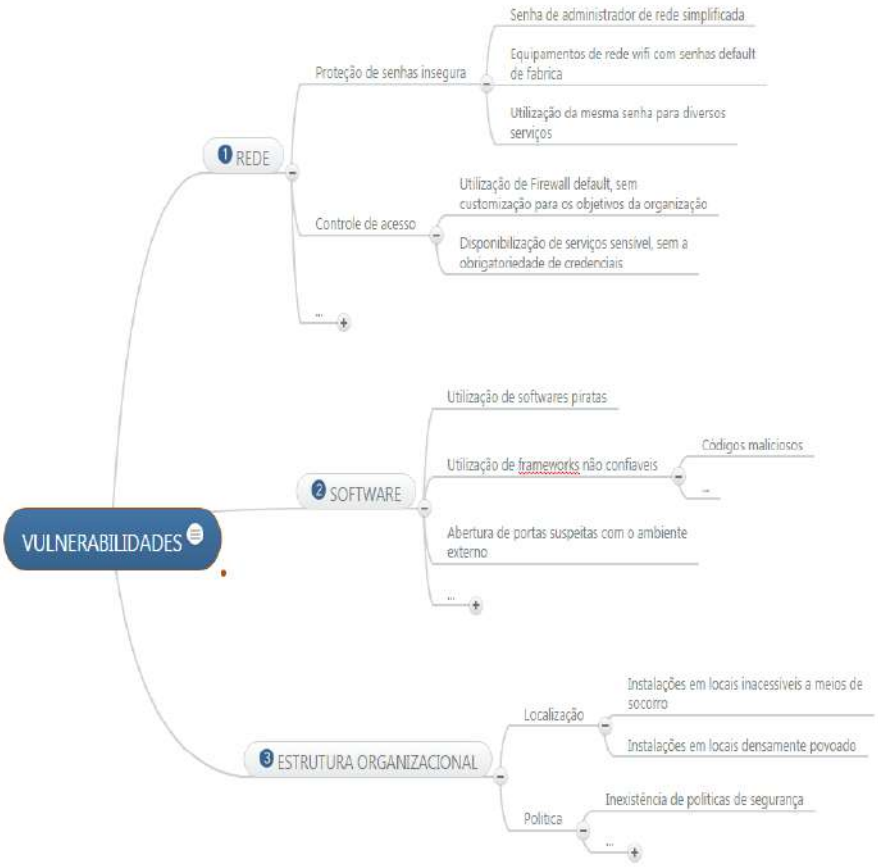
- Humanas – Falta de treinamento ou de conscientização das pessoas e de avaliação psicológica adequada ou de verificação de antecedentes que identifiquem objetivos escusos, problemas anteriores, má-fé ou descontentamento de um funcionário, entre outros, podem levar ao compartilhamento indevido de informações confidenciais, à não execução de rotinas de segurança ou a erros e omissões que ponham em risco as informações.

A norma ISO/NBR 27005:2011 classifica as vulnerabilidades quanto ao tipo de ativo secundário ao qual ela se aplica, a saber: vulnerabilidades de hardware, de softwares, de rede, de pessoal, de instalações e da estrutura organizacional.

O catálogo de vulnerabilidades da norma ISO/NBR 27005: 2011 tem uma natureza genérica e pouca aplicabilidade sobre vulnerabilidades específicas de ativos tecnológicos, como computadores e softwares. Para o caso em que se pretendem analisar as vulnerabilidades de ativos tecnológicos e os sistemas específicos, essa norma recomenda o uso de métodos, técnicas e ferramentas oriundas da gestão de risco.

A identificação das vulnerabilidades possibilita o cálculo aproximado da probabilidade de concretizar as ameaças inerentes à organização e podem ser representadas em uma árvore tipológica, conforme exposto na Figura 2, cujas folhas serão as vulnerabilidades que devem ser analisadas e mensuradas pela organização. Para Silva; Carvalho e Torres (2003), a identificação e a representação das vulnerabilidades devem ser classificadas como um processo confidencial, porque, como essas vulnerabilidades são exploradas, podem constituir ameaças e causar danos desastrosos à organização.

Figura 2: Exemplo de árvore de vulnerabilidades



Fonte: Elaborado pelos autores - 2018

Nesse sentido, a vulnerabilidade é uma característica que determinado recurso assume quando está suscetível a um ataque, ou seja, é uma condição encontrada em um ativo que o dota de fragilidades que podem ser exploradas com ameaças que podem resultar em danos de ordens diversas.

Ameaças

Uma ameaça é qualquer evento que explore as vulnerabilidades e lhes atribui a causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização. Para Dias (2000, p. 55), "é um evento ou atitude indesejável (roubo, incêndio, vírus etc.) que potencialmente remove, desabilita, danifica ou destrói um recurso". Segundo Sêmola (2012, p.45), "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 impactos aos negócios de uma organização".

Quanto à intencionalidade, o autor supracitado classifica as ameaças em três grupos:

- Naturais – que são as decorrentes de fenômenos da natureza, como incêndios naturais, enchentes, terremotos, tempestades eletromagnéticas, maremotos, aquecimento, poluição etc.
- Involuntárias – são as ameaças inconscientes, quase sempre causadas pelo desconhecimento, como acidentes, erros, falta de energia, entre outros.
- Voluntárias – são as ameaças propositais, causadas por agentes humanos, como hackers, invasores, espiões, ladrões, criadores e disseminadores de vírus de computador e incendiários.

A norma ISO/NBR 27005: 20011 classifica as ameaças de acordo com sua origem - de natureza humana deliberada, acidental e ambiental e com o tipo, como demonstrado no Quadro 2.

Quadro 2: Tipos de ameaça

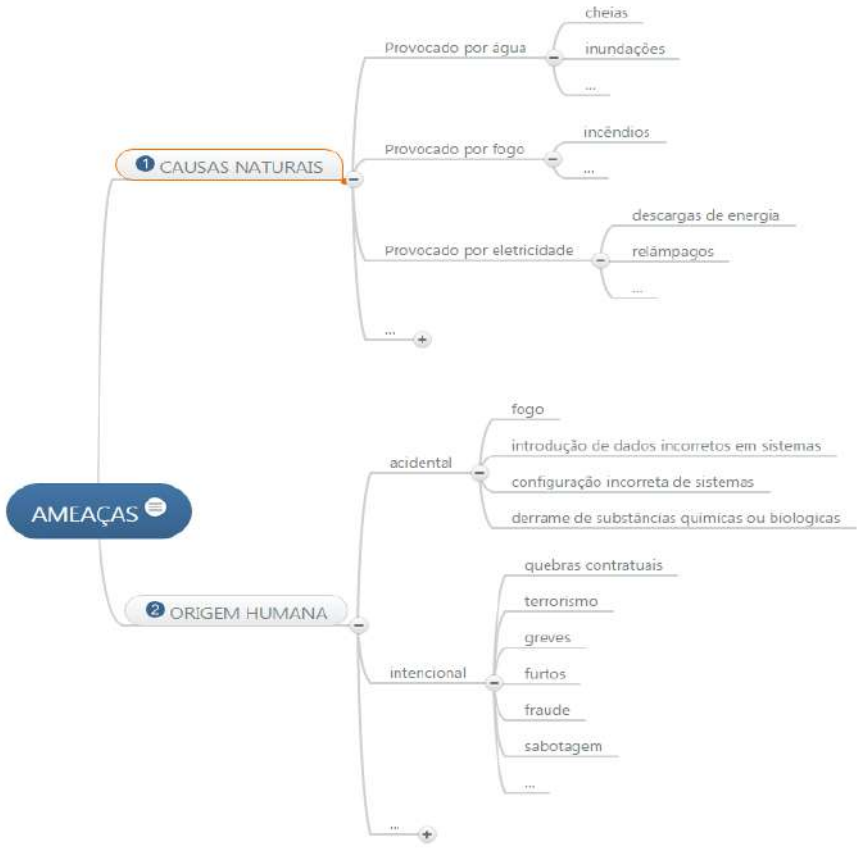
Ameaças	Descrição
Dano físico	Incidente com equipamento, instalação, mídia ou substância que foram comprometidos.
Eventos naturais	Incidentes com fontes de água, do solo, do subsolo ou do ar.
Paralisação de serviços essenciais	Incidentes em serviço de energia elétrica, água encanada, esgoto, condicionamento de ar etc.
Distúrbio causado por radiação	Incidentes causados por radiação térmica ou eletromagnética.
Comprometimento da informação	Interceptação, destruição, furto, cópia indevida, adulteração de hardware ou software.
Falhas técnicas	Falha, defeito, saturação ou violação das condições de uso de equipamento de informática.
Ações não autorizadas	Uso, cópia ou processamento ilegal de dados.
Comprometimento de funções	Uso errado, abuso de direitos, falsificação de direitos, repúdio de ações, indisponibilidade de pessoas.

Fonte: Elaborado pelos autores, com base na ISO NBR 27005: 2011 - 2018

As ameaças à segurança podem ser identificadas tanto por meio da produção de cenários quanto pela criação de listas de tipificação. A listagem de ameaças por tipificação é considerada a mais usual, porque facilita a obtenção de informação estatística sobre sua frequência de ocorrência no passado.

Para Silva; Carvalho; Torres (2003, p.36): "A forma clássica de tipificação dos riscos consiste na definição de categorias e subcategorias de classificação, criando-se uma "árvore", em que os ramos correspondem aos tipos de ameaças e as folhas às ameaças em si". Nessa forma de classificação, os autores supracitados apresentam na Figura 3 algumas das categorias principais mais comuns nos ambientes organizacionais.

Figura 3: Exemplo de árvore de ameaças



Fonte: Elaborado pelos autores - 2018

As ameaças surgem das mais diversas formas, podendo ser acidental ou intencional, sendo a intencional oriunda de um simples monitoramento não autorizado dos sistemas de informações até ataques mais sofisticados realizados por *crakers*[12]. Dentre as principais ameaças podemos citar a destruição de informações ou recursos, modificação ou

12 Termo usado para designar quem quebra um sistema de segurança.

deturpação da informação, roubo, remoção ou perda de informação, revelação de informações confidenciais ou não.

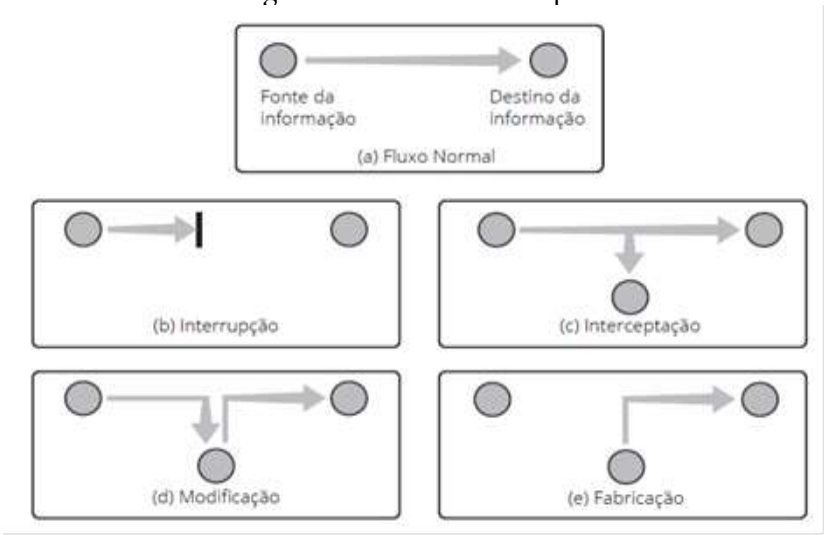
Ataques

Os ataques relacionados à segurança da informação podem ser destinados a qualquer uma de suas dimensões e são uma ameaça que, quando bem-sucedida, causa uma ação danosa à organização. Por sua vez, um ataque corresponde a qualquer ação que comprometa a segurança da organização. Coelho et al (2014, p. 5) asseveram que "o ataque é um ato deliberado de tentar se desviar dos controles de segurança, com o objetivo de explorar as vulnerabilidades". Existem dois tipos de ataque:

- passivos – baseados em escutas e monitoramento de transmissões, com o intuito de obter informações que estão sendo transmitidas. A escuta de uma conversa telefônica é um exemplo dessa categoria. Ataques dessa categoria são difíceis de detectar porque não envolvem alterações de dados, todavia podem ser prevenidos com a utilização de criptografia.
- ativos – envolvem modificação de dados, criação de objetos falsificados ou negação de serviço e têm propriedades opostas às dos ataques passivos. São difíceis de ser prevenidos, por causa da necessidade de proteger completamente todas as facilidades de comunicação e processamento, durante o tempo todo. Assim, é possível detectá-los e aplicar uma medida para recuperar prejuízos causados.

Ainda para os autores, há quatro modelos de ataque às informações, representados pela observação do fluxo normal da informação de uma origem para um destino, conforme a Figura 4:

Figura 4: Modelos de ataque



Fonte: Coelho et al (2014).

- Interrupção – quando um ativo é destruído ou fica indisponível (ou inutilizável), o que caracteriza um ataque contra a disponibilidade. Por exemplo, a destruição de um disco rígido.
- Interceptação – quando um ativo é acessado por uma parte não autorizada (pessoa, programa ou computador), tem-se um ataque contra a confidencialidade. Por exemplo, cópia não autorizada de arquivos ou programas.
- Modificação – quando um ativo é acessado por uma parte não autorizada (pessoa, programa ou computador) e é alterado, tem-se um ataque contra a integridade. Por exemplo, mudar os valores em um arquivo de dados.
- Fabricação – quando uma parte não autorizada (pessoa, programa ou computador) insere objetos falsificados em um ativo, temos um ataque contra a autenticidade. Por exemplo, a adição de registros em um arquivo.

Tipos de ataque

Inúmeras técnicas, ferramentas e métodos de ataque surgem, diariamente, no cenário mundial. Atacar deixou de ser um privilégio das pessoas com plenos conhecimentos tecnológicos, porquanto o acesso irrestrito, facilitado e de diversas formas propaga diversas possibilidades de qualquer usuário atacar os recursos informacionais de uma organização.

Nesse contexto, estabelece-se uma guerra em que, de um lado, atuam os profissionais de segurança da informação, que têm o objetivo de neutralizar os possíveis ataques que a organização possa sofrer, e, de outro, os atacantes que tentam, a todo custo, empreender ações contra a segurança informacional. Os ataques à segurança da informação podem ser denominados de acordo com a técnica empregada para sua realização e o objetivo a ser alcançado. Para se entender bem mais esses ataques, apresentam-se alguns que são feitos comumente à segurança.

- Engenharia social - seu objetivo é de enganar e ludibriar pessoas, a fim de obter informações que possam comprometer a segurança da organização. Suas ações são direcionadas a persuadir, muitas vezes abusando da ingenuidade ou da confiança do usuário para obter acesso não autorizado a recursos ou informações sigilosas.
- Negação de serviço (DoS e DDoS) – os ataques de negação de serviços DoS (*Denial of Service*) objetivam interromper um serviço ou um computador conectado à internet, com a geração de sobrecarga no processamento do computador alvo ou no tráfego de dados da rede à qual o alvo está conectado. O ataque DDoS (*Destributed Denial od Service*) segue o mesmo conceito, porém difere por ser um ataque distribuído, ou seja, um conjunto de computadores é utilizado para tirar de operação um ou mais serviços.

- Phishing (Phishing Scam, Scam) – objetiva capturar informações sensíveis, por meio de uma fraude eletrônica. Utiliza-se de pretextos falsos, com o intuito de receber informações sensíveis dos usuários, e ocorre com mais frequência por meio do envio de e-mails e páginas web falsas.
- Pharming – é uma variante do Phishing que explora as vulnerabilidades dos browsers, dos sistemas operacionais e dos servidores DNS (*Domain Name System*), com o objetivo de redirecionar os usuários a páginas web falsas para obter suas informações sensíveis.
- IP Spoofing – tem o objetivo de assumir a identidade de outro computador, através do envio de pacotes contendo IPs falsos de origem de outra máquina.
- Malware – termo genérico que abrange todos os tipos de programa que executam ações maliciosas em um computador, seja com a intervenção do usuário ou não, tais como: vírus, cavalos de Tróia, adware, spyware, backoors, keyloggers, worms, bots e rootkits.
- Ataques de força bruta – utiliza criptoanálise para buscar exaustivamente a descoberta de senhas nos mais variados meios tecnológicos, web, servidores, ativos de rede etc.

Vivenciamos novas formas e métodos de ataques informacionais a todo instante, e a dimensão humana é o alvo mais frequente dentro das organizações. Estabeleceu-se uma guerra cibernética de proporções gigantescas, em que, de um lado, figuram os profissionais e as empresas de segurança da informação que tentam, a todo instante, mitigar os riscos aos ativos da organização e, do outro, invasores que buscam burlar esses mecanismos e em muitos casos, obtêm sucesso.

Gestão de riscos

Na literatura, encontramos diversas definições para o conceito de risco, de acordo com a área de estudo, o autor e sua aplicabilidade. Este trabalho assumiu a definição posta pela norma ABNT NBR ISO/IEC 27005:2011, que aponta as diretrizes e descreve um processo genérico para a Gestão de Riscos de Segurança da Informação de uma organização.

O processo descrito pela norma ABNT NBR ISO/IEC 27005:2011 adota, em sua essência, um método iterativo de gerir composto de quatro passos, utilizado para controlar e melhorar continuamente seu processo, denominado de PDCA (PLAN-DO-CHECK-ADJUST). Dentre as diversas metodologias existentes para a gestão de riscos, consideramos o método proposto pela norma, porquanto possibilita flexibilidade e pragmatismo para ser utilizado em uma vasta gama de circunstâncias.

Segundo a norma ABNT NBR ISO/IEC 27005:2011, riscos de segurança da informação "é a possibilidade de determinada ameaça explorar vulnerabilidades de um ativo ou conjunto de ativos, causando impactos negativos a organização". Nesse conceito, podemos perceber a existência de quatro elementos cruciais para entender e executar a gestão de riscos: ativos, ameaças, vulnerabilidades e impacto. Os três primeiros elementos já foram discutidos neste livro. Adiciona-se, ainda, o conceito de impacto, que se traduz nas consequências da concretização das ameaças à organização. De acordo com a norma ABNT NBR ISO/IEC 27005:2011, impacto é uma mudança adversa no nível obtido dos objetivos de negócios, que pode se manifestar em diversos âmbitos, tais como prejuízo financeiro, de reputação, de produto etc.

Vários termos e definições são adotados no processo de gestão de risco. Araújo (2009, p.51) relaciona alguns termos ligados à gestão de risco, apresentados no Quadro 3.

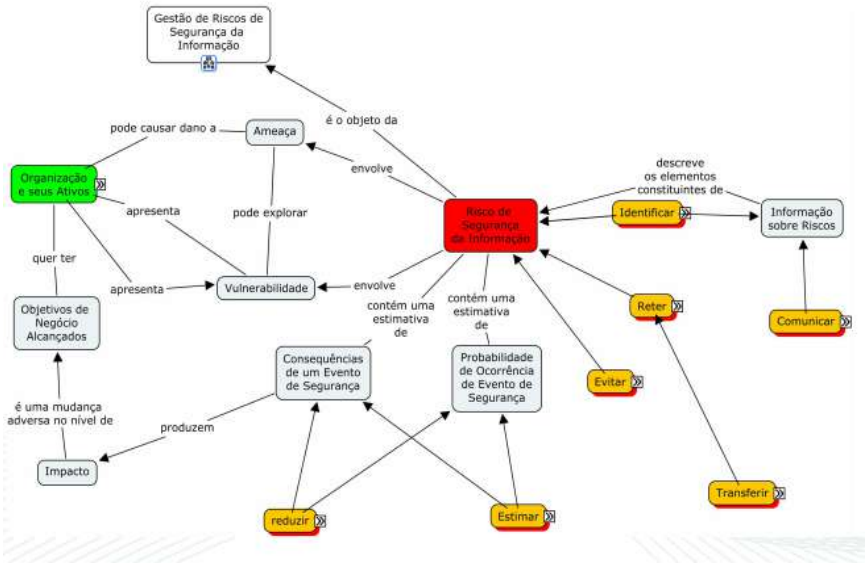
Quadro 3: Alguns termos relacionados à gestão de risco

Termo	Descrição
Ameaça	É a presença de todo evento potencial que causa um impacto indesejável na organização. Pode ser provocada ou natural, ter um efeito pequeno ou grande na segurança ou na viabilidade de uma companhia.
Ativo	É um recurso, processo, produto ou infraestrutura, que uma organização determinou que deve ser protegido. A perda desse recurso poderia afetar a confidencialidade, a integridade ou a disponibilidade. Pode ser tangível ou intangível e afetar a continuidade do negócio de uma organização. O valor de um ativo é composto de todos os elementos que são relacionados a esse recurso: criação, desenvolvimento, sustentação, reposição, credibilidade, custos considerados e valor de aquisição.
Brecha	É quando um mecanismo da segurança pode ser contornado por uma ameaça. Quando uma brecha é combinada com um ataque, pode resultar em uma invasão.
Exposição	Suscetibilidade à perda de um ativo devido a uma ameaça. É possível que uma vulnerabilidade seja explorada por um agente ou por um evento da ameaça. A exposição não significa que um evento de perda esteja ocorrendo realmente. Isso significa que, se houver uma vulnerabilidade e uma ameaça que possam ser exploradas, poderá haver uma exposição.
Invasão	É quando um agente da ameaça tem acesso à infraestrutura de uma organização com a subversão dos controles de segurança e pode causar danos diretamente aos ativos.
Proteção	É um controle ou contramedidas empregadas para reduzir o risco associado a uma ameaça específica ou o grupo de ameaças.
Risco	É a possibilidade de que uma ameaça específica explore uma vulnerabilidade específica e cause dano a um ativo.
Vulnerabilidade	É a falta ou a fraqueza de uma proteção. Uma ameaça mínima tem o potencial de se transformar em grande ameaça ou em ameaça mais frequente, por causa de uma vulnerabilidade.

Fonte: Araújo (2009, p.51)

Fernandes (2009) assevera que podemos entender bem mais o processo de gestão de risco através de um mapa que apresenta um arcabouço conceitual geral sobre o qual se apoia a norma ABNT NBR ISO/IEC 27005:2011, observando o relacionamento de seus elementos.

Figura 5: Mapa de conceitos sobre o risco de segurança da informação



Fonte: Fernandes (2009, p.17)

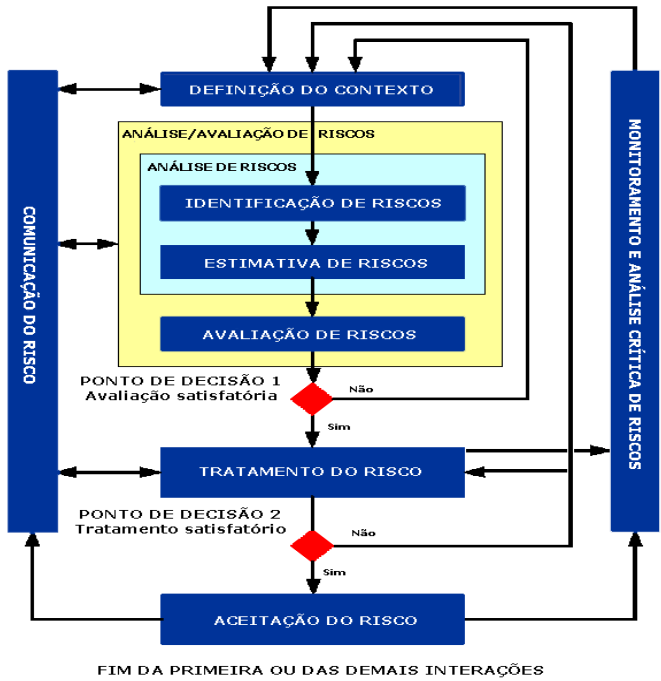
A Figura 5 mostra os elementos que circundam o conceito ora descrito sobre o risco de segurança da informação. Percebeu-se que a determinação de um risco de segurança da informação envolve a coleta de dados sobre vários elementos, como: ativo, ameaças, vulnerabilidades, probabilidades, consequências e impactos. O processo de gestão de riscos é uma etapa crucial e fundamental para a segurança da informação, porquanto é nela que os conceitos e os elementos descritos neste trabalho se relacionam através de um processo contínuo e interativo. Suas etapas e fases serão apresentadas na seção seguinte.

Processo de gestão de riscos

Basicamente, podemos entender a gestão de risco como uma tentativa de minimizar as fontes de riscos de segurança da informação, por meio da análise e da avaliação dos elementos que constituem a segurança da informação. A norma ABNT NBR ISO/IEC 27005:2011 adota um processo genérico de gestão de riscos fundamentado no ciclo PDCA, composto de seis fases: definição do contexto, processo de avaliação de riscos, tratamento do risco, aceitação do risco, comunicação e consulta do risco e monitoramento e análise crítica de riscos.

A fase de avaliação de risco subdivide-se em três etapas: a de identificação de riscos, a de análise de riscos e a de avaliação de riscos, demonstradas na Figura 6:

Figura 6: Processo de gestão de risco da ISO/IEC 27005:2011



Fonte: NBR ISO/IEC 27005 (2008, p. 5)

Na figura 6, podemos perceber o processo de gestão de risco com a definição do contexto, em que são definidos os critérios e o escopo que fundamentam a implementação da análise de risco. Em seguida, executam-se as etapas da fase de avaliação de riscos, em que os riscos são identificados, estimados e avaliados de acordo com os critérios estabelecidos na fase anterior. No final da fase de avaliação de risco, surge o primeiro ponto de decisão, e se verifica se a avaliação foi satisfatória ou não. Caso não seja, o processo deverá ser repetido até que os resultados sejam satisfatórios.

Depois de avaliar os riscos, devemos fazer seu tratamento. Nessa fase, os riscos podem ser reduzidos, retidos, evitados ou transferidos. E se houver riscos em que o tratamento não seja aceitável pela organização, devemos reavaliar a forma de tratar e, a depender do risco, deve ser executado o processo novamente para esses riscos.

A fase de aceitação do risco compreende a formalização do aceite dos riscos pela organização e é de extrema importância que todos os riscos sejam avaliados e documentados. A fase de comunicação é composta de um conjunto de atividades que devem ser executadas continuamente entre os *stakeholders*[13] da organização. Já a fase de monitoramento e de revisão do risco compreende ações contínuas, por meio das quais se pretendem identificar quaisquer mudanças no contexto da organização, atualizar o panorama de riscos e melhorar o processo de sua gestão.

No processo descrito, suas fases e atividades são organizadas em forma de processos, que contêm entradas, ações, guias para implementação e saídas bem caracterizadas. No Quadro 4, apresentamos as entradas e as saídas das fases desse processo.

13 Uma pessoa ou um grupo que está diretamente envolvido em um projeto.

Quadro 4: Entradas e saídas do processo de gerenciamento de risco da ISO/IEC 27005: 2011

Fase	Entrada	Saída
Definição do contexto	- Todas as informações relevantes sobre a organização	(i) Especificação dos critérios básicos para a gestão de risco; (ii) especificação do escopo e limites cujos riscos serão geridos; (iii) Uma organização preparada para operar a gestão de risco.
Avaliação de riscos	- Critérios básicos - Escopo e limites - Organização para gerência de risco	(i) Lista de riscos avaliados e priorizados, conforme os critérios estabelecidos.
Tratamento do risco	- Lista dos riscos priorizados conforme os critérios de avaliação em relação aos cenários de incidente que levaram a tais riscos.	(i) Plano de tratamento do risco (ii) Lista de riscos residuais.
Aceitação do risco	- Plano de tratamento de riscos - Avaliação de riscos residuais	(i) Lista de riscos aceitos

Fonte: Elaborado pelos autores, baseado na ISO NBR 27005:2011 - 2018

A fase de avaliação de risco é a mais sensível nesse processo. Nela são executadas atividades que subsidiam a identificação, a análise e a avaliação dos riscos. Para isso, é necessário executar diversas atividades que possibilitem uma gestão eficaz dos riscos. O Quadro 5 apresenta essas atividades.

Quadro 5: Atividades oriundas da fase de avaliação de riscos

Identificação de riscos		
Atividades	**Entrada**	**Saída**
Identificação de ativos	- Declaração do escopo e limites da gestão de risco - Inventário dos ativos	(i) Lista de ativos cujos riscos devem ser gerenciados, relacionados a uma lista de processo de negócios relacionados aos ativos e à relevância desses relacionamentos.
Identificação de ameaças	Ameaças oriundas da revisão dos registros de incidentes, dos eventos de segurança dos responsáveis pelos ativos dos usuários e de outras fontes	(i) Lista de ameaças com a identificação do tipo de fonte da ameaça.
Identificação de controles	- Documentação dos controles e dos planos de implementação de tratamento de riscos, se houver	(i) Lista de todos os controles existentes e planejados, com seu status de implementação e uso.
Identificação de vulnerabilidades	- Lista de ameaças conhecidas - Lista de ativos - Lista de controles existentes e planejados	(i) Lista de todas as vulnerabilidades existentes
Identificação de consequências	- Lista de ativos - Lista de processo de negócio - Lista de ameaças e de vulnerabilidades correlacionadas a ativos e suas relevâncias	(i) Lista de cenários de incidentes, com suas consequências relacionadas aos ativos e aos processos de negócio
Análise de riscos		
Atividades	**Entrada**	**Saída**
Estimativa das consequências	- Lista de cenários de incidentes identificados como relevantes, incluindo a identificação de ameaças, vulnerabilidades, ativos afetados e consequências.	(i) Lista de avaliações de impacto (consequências) apreciadas, decorrentes de um cenário de incidente, expressas com respeito a ativos e a critérios de impacto
Estimativa da probabilidade de incidente	- Lista de cenários de incidentes identificados como relevantes, incluindo identificação de ameaças, vulnerabilidades, ativos afetados e consequências - Lista de todos os controles existentes e planejados, seu status e implementação de uso	(i) Lista das probabilidades de cenários de incidentes
Estimativa do nível de risco	- Lista de cenários de incidentes, associados às probabilidades (qualitativas e quantitativas).	(i) Lista de riscos com níveis de valoração atribuídos.
Avaliação de riscos		
Atividades	**Entrada**	**Saída**
Avaliação de risco	- Lista de riscos com valorações de níveis - Critérios de avaliação de riscos (declarados na definição do contexto) - Critérios de aceitação do risco (declarados na definição do contexto)	(i) Lista de riscos priorizados, conforme critérios de avaliação, em relação aos cenários de incidentes que levam a esses riscos.

Fonte: Elaborado pelos autores, baseado na ISO NBR 27005: 2011, 2018.

A norma apresenta dois métodos a serem seguidos na etapa de análise de riscos: o quantitativo e o qualitativo. Para Peltier (2005, p. 77), ao se avaliarem os riscos, devem-se considerar as vantagens e as desvantagens da utilização dos métodos quantitativos e qualitativos. Dantas (2011, p. 55-61) contribui para o entendimento desses métodos ao ressaltar que a análise de risco pode ser

> [...] tanto quantitativa – baseada em estatísticas, numa análise histórica dos registros de incidentes de segurança, utilizada quando a probabilidade de um evento pode ser medida em valores numéricos, e a sua consequência pode ser calculada em perdas financeiras [...] – quanto qualitativa – baseada em qualquer método que utiliza valores nominais para descrever o risco, sendo utilizada quando não há disponibilidade e confiança no registro dos dados, quando não há necessidade de precisão do método quantitativo, dentre outros fatores.

Escolher um método para analisar riscos não é uma tarefa simples, pois diferentes métodos estão disponíveis na literatura especializada. Cabe ao gestor que está conduzindo o processo conhecer e avaliar os métodos já elaborados e determinar qual o que tem potencial para atender às necessidades de sua organização. Eventualmente, é possível que diferentes métodos sejam aplicados em uma mesma organização, mas se deve atentar para o fato de que tanto os procedimentos de aplicação de análise de riscos quanto a avaliação de seus resultados devem ser conduzidos por pessoal capacitado.

Métodos de análise e avaliação de riscos

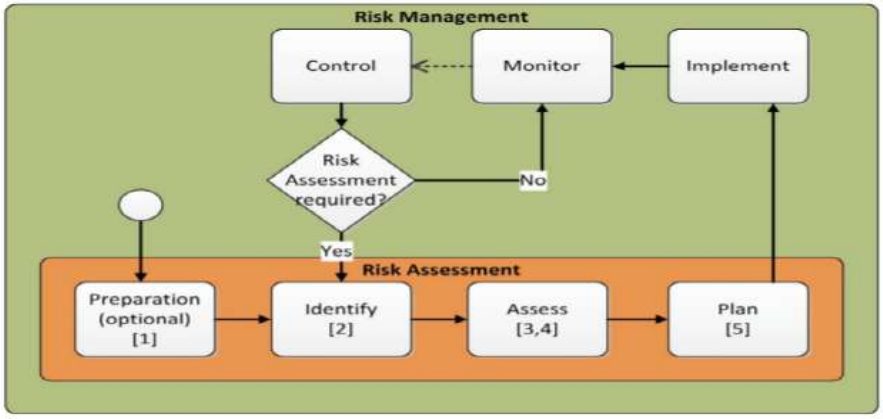
A Gestão de Riscos em Segurança da Informação pode ser parte do processo de Gestão de Risco Global da Organização ou pode ser implementada em separado, constituindo-se como um amplo processo formado por um conjunto de atividades coordenadas que englobam a cultura, os processos e a estrutura organizacional, com o objetivo de

potencializar as oportunidades, ao mesmo tempo em que gerencia os efeitos adversos.

> Geralmente a Gestão de Riscos em Segurança da Informação inclui em suas atividades a implementação de políticas apropriadas e controles relacionados, promovendo a sensibilização, bem como o monitoramento e avaliação da política e da eficácia de controles, constituindo-se um processo cíclico". (PIETERS *et al*, 2013, p.11, tradução nossa).

O autor enuncia, ainda, que o processo de gerenciamento de risco em segurança da informação é formado de sete etapas: a de 'preparação', que é opcional e sugerida quando esse processo é conduzido por agentes sem prévio conhecimento sólido da organização; a de 'identificação dos riscos', que é feita por meio da análise de ameaças e de vulnerabilidades; a de 'análise e avaliação dos riscos identificados'; a de 'planejamento das ações de combate aos riscos'; a de 'implementação das ações na organização'; a de 'monitoramento das ações e dos riscos; e a de 'controle de riscos'.

Figura 7: Visão geral de um processo de Gestão de Risco em Segurança da Informação.



Fonte: Pieters et al (2013, p.12)

Das atividades que compõem o processo de gerenciamento de riscos, demonstrado na figura 7, destacam-se a etapa de monitoramento e a de avaliação dos riscos. A primeira é contínua, realizada em paralelo com todas as outras etapas e iniciada depois do processo de controle dos riscos. Já a segunda é considerada um passo crítico no processo, por envolver a avaliação de cada risco, o risco total e a definição de suas prioridades. Porém não é contínuo e é uma atividade distinta, que só se inicia quando é necessário ou em intervalos regulares.

Para Pieters *et al* (2013, p.12, tradução nossa), as avaliações de risco geralmente servem "para identificar e analisar possíveis vulnerabilidades e ameaças a determinado sistema de informação, bem como o valor relativo dos ativos e possíveis danos resultantes de seu compromisso".

A avaliação de risco é uma tarefa multidisciplinar, geralmente composta pelas seguintes etapas:

- Preparação – Estabelecimento do contexto por meio da identificação e da definição tecnológica e social e do contexto de negócio em que o sistema de informação está inserido. Pode ter outras atividades relevantes, como definir o escopo da avaliação, os requisitos de segurança, os objetivos das partes interessadas, os critérios de risco, dentre outras.
- Identificação do risco – É considerada como o cerne de qualquer avaliação de risco e está intimamente relacionada aos dados disponíveis para identificar possíveis vetores de ataques e vulnerabilidades.
- Análise do risco – Estabelece a compreensão das probabilidades, os impactos e outros parâmetros associados aos riscos identificados, a fim de facilitar a compreensão das vulnerabilidades.
- Avaliação do risco – Nessa etapa, os riscos são classificados e prio-

rizados, a fim de subsidiar as decisões sobre os controles que serão implementados para os riscos.

- Planejamento – É a etapa em que se selecionam os controles diante dos resultados obtidos das etapas anteriores, estratégias de mitigação, controle ou políticas de segurança.

Segundo Dantas (2011), a análise qualitativa é utilizada, geralmente, quando não existe a disponibilidade de dados ou quando eles são precários, e sua análise é realizada com base em valores referenciais. Já a quantitativa é utilizada quando os dados são confiáveis, estão disponíveis e sua análise é baseada em valores absolutos.

A avaliação de riscos pode ser realizada de diferentes maneiras, a depender da metodologia escolhida, sempre levando em consideração dois aspectos: na análise e na avaliação do risco, um tem relação com o método escolhido para estimar a probabilidade e aferir a consequência de um risco, e o outro diz respeito aos critérios de escolha para parametrizar a criticidade do risco.

Nesse sentido, a norma ABNT NBR ISO/IEC 27005:2011 aborda, de forma sistemática, a gestão de riscos de segurança da informação e estabelece as diretrizes para a execução das ações a serem implementadas. Entretanto a norma não inclui um método específico para a gestão de riscos. Cabe à organização definir sua abordagem em conformidade com suas particularidades e características. A norma estabelece um processo contínuo global para a gestão dos riscos e define as etapas do processo de avaliação de riscos, como identificação dos riscos, análise dos riscos e avaliação dos riscos.

- Identificação de riscos – Determina eventos que possam causar uma perda potencial, deixando claro como, onde e por que a perda pode acontecer. Essa etapa é composta de sube-

tapas, que visam coletar dados de entrada para a análise de risco, tais como identificação dos ativos, ameaças, controles existentes, vulnerabilidades, consequências e processos de negócio.

- Análise de riscos – Pode ser empreendida com diferentes graus de detalhamento, a depender da criticidade dos ativos, da extensão das vulnerabilidades conhecidas e dos incidentes anteriores que envolvem a organização. A metodologia aplicada na análise pode ser qualitativa ou quantitativa ou uma combinação de ambas, de acordo com as circunstâncias. Nessa etapa, são avaliadas as consequências e as probabilidades de os incidentes ocorrerem e são determinados os níveis de riscos.
- Avaliação de riscos – Fase em que se definem medidas para reduzir, reter, evitar ou transferir o risco e subsidiar o processo de decisão e o plano de tratamento dos riscos.

Apesar de a norma apresentar uma abordagem abrangente e sistemática, ela não fornece tampouco recomenda um método específico com detalhes técnicos para se analisarem os riscos. Esclarece as abordagens de análise qualitativas e quantitativas, porém não demonstra sua implementação. Para se compreender bem mais o processo de análise de risco, nas próximas subseções, apresentamos as metodologias de avaliação de riscos CORAS, CRAMM, COBIT 5 FOR RISK, FRAAP, NC04/IN01/DSIC/GSIPR e a GRSIC, por apresentarem uma alta taxa de aceitação nas organizações e ser baseadas nas boas práticas, normas e padrões nacionais e internacionais de gerenciamento

CORAS – The Coras Method

A metodologia CORAS ou "The Coras Method" é o resultado de um projeto financiado pela União Europeia, que objetivou criar um método prático baseado em um modelo de suporte informatizado de avaliação de riscos voltada para a identificação precisa e inequívoca de riscos de segurança em sistemas críticos. Utiliza uma abordagem baseada em modelos para fazer suas atividades e tem uma linguagem própria, fundamentada na *Unified Modeling Language* (UML), que possibilita a captura e a modelagem das informações importantes durante os vários estágios da análise.

Essa metodologia oferece uma ferramenta computacional projetada para documentar, manter e gerar relatórios de análise por meio da modelagem de risco, através de quatro tipos de diagramas - ativo, ameaça, risco e tratamento - para dar suporte a várias etapas do processo. O método diferencia os ativos em duas categorias - ativos diretos e indiretos - e classifica as ameaças a esses ativos em: ameaça humana acidental, ameaça humana deliberada e ameaça não humana.

A análise de riscos feita por meio do CORAS compreende oito passos consecutivos, como demonstrado no Quadro 7, a saber: 1- preparação para a análise; 2- apresentação ao cliente da meta; 3- refinamento da descrição dos alvos, por meio de diagramas de ativos; 4- aprovação de descrição da meta; 5- identificação dos riscos utilizando diagramas de ameaças; 6- estimativa de risco por meio de diagramas de ameaças; 7- avaliação de risco por meio de diagramas de risco; 8- tratamento de riscos utilizando diagramas de tratamento. Vejamos, no Quadro 6, essas etapas de forma bem detalhada:

Quadro 6: Etapas da metodologia CORAS

Etapas	Descrição
Preparação	O processo inicia-se com a etapa de preparação, que consiste em identificar os objetivos gerais da análise e o alvo a ser analisado por meio de uma reunião com o cliente.
Apresentação	Nessa etapa, faz-se uma reunião com o cliente, com o intuito de validar o entendimento comum dos objetivos gerais que foram discutidos na primeira reunião e no estudo da documentação disponibilizada pelo cliente.
Refinamento	Nessa etapa, definem-se os alvos de avaliação e os ativos mais valiosos e discute-se sobre os cenários de ameaças, vulnerabilidades e riscos. Os objetivos são refinados, e a descrição detalhada dos alvos é documentada usando-se a linguagem do CORAS.
Aprovação	Definem-se os critérios da análise de risco que será utilizada nas etapas seguintes e se verifica se o cliente aprova a descrição detalhada do alvo e seu contexto, incluindo hipóteses e precondições.
Identificação dos riscos	Essa etapa é constituída de um *brainstorming* multidisciplinar destinado às pessoas com experiência no objeto analisado, com o intuito de identificar o máximo de incidentes indesejáveis possíveis, bem como ameaças, vulnerabilidades e cenários de ameaças.
Estimativa dos riscos	É organizada através da técnica de *brainstorming* e concentra-se na estimativa dos valores das consequências e das probabilidades de cada um dos incidentes indesejáveis identificados.
Avaliação dos riscos	Nessa etapa, os critérios de avaliação de riscos previamente estabelecidos são usados para considerar cada risco, bem como seu tratamento aceitável ou exigido.
Tratamento dos riscos	A última etapa desse método destina-se a identificar o tratamento, bem como da análise custo/benefício dos tratamentos.

Fonte: Elaborado pelos autores, com base em Pieters et al (2013, p.28)

O método CORAS baseia-se nas normas ISO 27002, 27005, e o padrão AS/NZS 4360 apresenta uma forte preocupação em entender as partes sobre os alvos, o contexto e os objetivos da avaliação realizada nas quatro primeiras etapas do método. As etapas restantes destinam-se à análise e à avaliação dos riscos por intermédio da modelagem de diagramas. Alguns fatores o distinguem de outros métodos. Um ponto considerado potencialmente forte é a disponibilização de uma ferramenta computacional que proporciona um processo interativo e colaborativo entre as partes interessadas, e um ponto potencialmente negativo é que o método exige conhecimentos especializados de várias origens, que são inviáveis para muitos iniciantes e profissionais com pouca experiência.

CRAMM – CCTA Risk Analysis and Management Method

O método CRAMM – *CCTA* Risk Analysis and Management Method - foi originalmente desenvolvido pela *Central Computer and Telecommunications Agency (CCTA)* ou Agência Central de Computadores e Telecomunicações do governo britânico. Vem sendo aperfeiçoado pela empresa britânica *Insight Consulting*, uma divisão da *Siemens Enterprise Communications Ltd*. Essa metodologia é utilizada por muitas organizações por oferecer suporte à implementação da ISO/IEC 27001 amplamente aceita pelas organizações.

Segundo Barber e Davey (1992), essa metodologia apresenta-se de forma flexível e possibilita que seus usuários executem as tarefas em vários níveis de complexidade. Seu processo utiliza uma abordagem para o desenvolvimento de gerenciamento de riscos que identifica as ameaças aos ativos e as vulnerabilidades para gerir o risco e propor contramedidas. Seu processo é executado com o suporte de ferramentas computacionais livres, que conta com uma base de dados com mais de 3000 registros de

controles de segurança organizadas em 70 grupos lógicos que são sugeridas de forma automática depois da identificação dos ativos, das ameaças e das vulnerabilidades da organização.

Seu processo consiste de três etapas principais descritas no Quadro 7. Os dois primeiros são responsáveis pela identificação e pela análise dos riscos aos sistemas, e a terceira etapa faz uma série de recomendações sobre a forma como esses riscos devem ser gerenciados.

Quadro 7: Etapas da metodologia CRAMM

Etapas	Descrição
Estabelecimento dos objetivos de segurança	1- Definir o escopo do estudo; 2- Identificar e avaliar os ativos físicos que compõem o sistema; 3- Determinar o valor do dado mantido pelos usuários entrevistados sobre os impactos potenciais dos negócios que poderiam resultar da indisponibilidade, da destruição, da revelação ou da modificação.
Análise dos riscos para o sistema proposto e os requisitos de segurança	1- Identificar e analisar o tipo e o nível das ameaças que podem afetar o sistema; 2- Analisar a extensão das vulnerabilidades do sistema para as ameaças identificadas; 3- Combinar análises de ameaças e vulnerabilidades com os valores dos ativos para calcular os valores dos riscos.
Identificação e seleção das contramedidas	1- Seleção das contramedidas sugeridas pela ferramenta CRAMM express.

Fonte: Elaborado pelos autores, baseado em Pieters et al (2013, p.30) - 2018

Na metodologia CRAMM, a complexidade da avaliação pode ser ajustada às necessidades da organização e, geralmente, é utilizada por grandes organizações que demandam uma análise de riscos mais complexa. Seu processo é automatizado, em grande parte, pela ferramenta computacional que apoia a execução de suas tarefas. Sua utilização demanda conhecimento especializado sobre o tema, e a avaliação completa pode ser demorada ou excessivamente complexa. Essa metodologia só pode ser utilizada em conjunto com a ferramenta CRAMM express.

COBIT 5 for risk

O método Cobit 5 for Risk foi elaborado pela associação ISACA, com o objetivo de abordar o risco de segurança da informação na tecnologia. Esse método liga cenários associados aos riscos de segurança da informação à resposta apropriada. Para a Isaca (2013a, p.12-28), as atividades de identificação, avaliação, mitigação, monitoramento e relatório de riscos devem fazer parte do ciclo de vida da informação. Por meio das perspectivas de função e gerenciamento de risco, o Cobit 5 for Risk pretende oferecer um gerenciamento de risco efetivo baseado em sete habilitadores: Processo; Estrutura organizacional; Cultura, ética e comportamento; Princípios, políticas e frameworks; Informação; Serviço, infraestrutura e aplicação; e Pessoas, habilidades e competências. As etapas do método Cobit 5 for Risk encontram-se no quadro 8.

Quadro 8 - Gerenciamento de risco do Cobit 5 for Risk

ETAPA	DESCRIÇÃO
Coletar dados	Coletar os dados de cibersegurança de forma apropriada.
Analisar risco	Analisar e avaliar os riscos para cada cenário.
Manter um perfil de risco	Criar um perfil de risco para cada cenário.
Articular risco	Articular risco para cada cenário com uma visão para o apetite de risco existente.
Definir um portfólio de ação de gerenciamento de risco	Definir um portfólio de ação para o gerenciamento dos riscos.
Responder ao risco	Decidir a resposta ao risco por meio da aceitação, do compartilhamento, da mitigação ou da prevenção.

Fonte: Adaptado para o quadro de ISACA (2013b, p. 69, tradução nossa)

Observa-se que o método de gestão de riscos Cobit 5 for risk consiste de seis etapas a serem implementadas em uma organização e baseia-se em cenários de risco que devem ser relevantes e ligados ao risco real do negócio.

Facilitated risk analysis process

O Facilitated Risk Analysis Process (FRAAP) é uma metodologia de análise e avaliação de riscos que objetiva identificar o ativo, verificar o risco, determinar a probabilidade e identificar a ação ou medida corretiva de um sistema, aplicação ou processo de negócio por vez. Esse método

é executado por especialistas da própria organização, por meio de uma reunião mediada cujo objetivo é de identificar os riscos, as medidas e as ações de controle que podem minimizá-los, identificar os *stakholders*[14] e atribuir os ativos sobre suas responsabilidades e estabelecer datas para executar as ações oriundas de seu plano de ação. Em termos de tempo, o FRAAP é executado em um curto espaço de tempo, o que o torna viável econômica e temporalmente para a organização.

Segundo Peltier (2010), o FRAAP é um processo de análise e avaliação de riscos qualitativos que tem sido utilizado mundialmente durante os últimos quinze anos. É uma metodologia eficiente e disciplinada para garantir que os riscos sejam identificados, examinados e documentados. As conclusões dos participantes do FRAAP sobre a existência de ameaças, o nível de risco e controles necessários são documentadas por meio de seus instrumentos de coleta que serviram para elaborar o plano de ação a ser executado pela organização.

Esse método é implementado em três etapas, apresentadas no Quadro 9: a reunião Pré-FRAAP, que, normalmente, é realizada em uma hora, tem a participação do proprietário ou de seu representante legal, dos gerentes de TI, do gerente de projetos, dos líderes de setores e do facilitador. Nessa reunião, produzem-se sete artefatos para conduzir as etapas posteriores. A Sessão FRAAP leva aproximadamente quatro horas, deve incluir de sete a quinze participantes e produz três artefatos para o processo e a Pós-FRAAP que é responsável pela análise, pela divulgação dos resultados e pela elaboração do relatório final. Essa etapa pode demorar até cinco dias para ser concluída e produz três artefatos.

14 Stakeholders – é uma pessoa ou um grupo, que legitima as ações de uma organização e desempenha um papel direto ou indireto em sua gestão e em seus resultados.

Quadro 9: Etapas da metodologia FRAAP

Etapas	Descrição
Pré-FRAAP	1- Pré-triagem 2- Declaração do escopo 3- Diagrama visual 4- Formação da equipe do FRAAP 5- Definição da reunião FRAAP 6- Definições essenciais 7- Minissessão de *brainstorming*
Sessão FRAAP	1- Identificação dos riscos 2- Priorização dos riscos 3- Sugestão de controles de compensação 4- Sugestão do controle base
Pós-FRAAP	1- Construção da tabela de referência cruzada 2- Construção do plano de ação 3- Produção do relatório final.

Fonte: Elaborado pelos autores com base em Peltier (2010, p.3)

Antes de iniciar as etapas do FRAAP, sugere-se a criação de um programa de conscientização, que deverá mapear o conhecimento dos funcionários que farão parte do FRAAP sobre os aspectos da segurança da informação. Esse programa é único e condizente com as particularidades das unidades de negócio. O programa de conscientização contempla a verificação do nível atual de compreensão de avaliação de risco, necessidades de aprendizado dos gerentes e funcionários, mensura o nível de receptividade ao programa e define estratégias de adesão ao programa.

> O FRAAP é conduzido pelo facilitador que irá orientar a equipe nas identificações de ameaças, definição do nível dos riscos através da probabilidade e impacto e a seleção de controles […]. Devido à natureza subjetiva da avaliação de risco qualitativa, o facilitador detém a responsabilidade de liderar a equipe em diferentes áreas de preocupação para garantir que o maior número de ameaças seja identificado e que o processo de análise e avaliação de riscos seja direcionado aos impactos aos negócios da organização. (PELTIER, 2010, p. 7-8)

A etapa Pré-FRAAP é considerada a mais importante desse método, porque objetiva determinar os requisitos e os atributos que permearam toda a análise, e é realizada por meio de uma reunião com a participação do proprietário da organização ou de seu representante legal, gerente de projeto e o facilitador. Segundo Peltier (2010), essa reunião deverá gerar como resultado os seguintes artefatos:

- Pré-triagem – Atividade inicial, que visa determinar o que será necessário para fazer a análise e avaliar os riscos. O projeto classifica-se em crítico ou não crítico. Se não for crítico, somente os controles bases deverão ser implementados. Nessa atividade, também são levantadas todas as normas, os regulamentos e as leis a que os negócios estejam submetidos.
- Declaração do escopo – Nesse artefato, é descrito o objeto de análise do FRAAP e suas fronteiras e são determinados, preliminarmente, os atributos de informação que serão analisados. Não se limita, necessariamente, aos atributos confidencialidade, integridade e disponibilidade.
- Diagrama visual – É construído o modelo visual do fluxo do processo FRAAP, para que todos possam conhecer as etapas e as atividades a serem realizadas.
- Formação da equipe do FRAAP – A equipe deverá ser formada de funcionários experientes, que estejam envolvidos com o objeto

analisado e conheçam as regras de negócio da organização. Sugere-se que a equipe seja o mais multidisciplinar possível.

- Definição da reunião FRAAP – Essa reunião é agendada pelo proprietário que será responsável por convidar os envolvidos no FRAAP e todos os recursos necessários para a reunião.
- Definições essenciais – Nesse artefato são definidos os conceitos de ativo, ameaça, probabilidade, impacto, vulnerabilidade e risco, que servirão de base para todo o processo.
- Minissessão de *brainstorming* – Tendo alcançado o acordo sobre os itens anteriores, os membros do FRAAP identificaram, no mínimo, quatro ameaças para cada atributo de informação estabelecido que causem impacto nos negócios da organização.

Segundo Peltier (2010), a Sessão FRAAP é o momento em que os membros do FRAAP analisam e avaliam os riscos e identificam os controles para sua mitigação. Para isso, o facilitador deve ter habilidade para conduzir o *brainstorming* e primar pela eficácia dos resultados esperados. Esse momento gera como resultados os seguintes artefatos:

- Identificação dos riscos – Essa atividade inicia-se com a identificação das ameaças para os atributos de informação, podendo ser utilizado uma lista de exemplos para auxiliar a equipe.
- Priorização dos riscos – É determinado a probabilidade de ocorrência dos riscos e seu impacto sobre o ativo e negócio.
- Sugestão de controles de compensação – Para os riscos classificados como crítico, são construídos controles e planos que garantam a continuidade do negócio.
- Sugestão do controle base – É selecionado para todo e qualquer risco identificado.

Na última etapa do método, denominada de Pós-FRAAP, o facilitador apresenta ao proprietário a tabela de referência cruzada, com o intuito de validar os riscos que a organização irá assumir e de construir o plano de ação que deverá conter os responsáveis pela implementação dos controles e a data em que será implementado. Por fim, elabora-se o relatório final de forma objetiva, que deve ser apresentado aos membros do FRAAP. Essa etapa gera como saída os seguintes artefatos:

- Tabela de referência cruzada – É um documento de trabalho baseado na tabela de risco e de controles, para identificar os controles que correspondem aos riscos encontrados.
- Plano de ação – Documento que determina o tipo apropriado de mitigação dos riscos, de acordo com o ativo analisado, e por quem e quando será implementado.
- Relatório final – Relatório gerencial que apresenta o processo executado.

Para que esse método seja executado com sucesso, devem-se observar fatores primordiais, entre eles, que o facilitador esteja habilitado a conduzir o processo; os membros do FRAAP estejam comprometidos; que a análise e a avaliação de risco sejam aplicadas a um ativo, sistema ou processo por vez, e que os controles sejam selecionados com foco nos negócios.

Norma complementar 04/IN01/DSIC/GSIPR

Visando à gestão de risco na administração pública federal, o governo brasileiro emitiu, em 15 de fevereiro de 2013, com o apoio do Departamento de Segurança da Informação e Comunicação, por intermédio do Gabinete de Segurança Institucional, a Norma Complementar nº. 04

da Instrução Normativa nº 01 - NC04/IN01/DSIC/GSIPR, que objetiva estabelecer diretrizes para a Gestão de Riscos de Segurança da Informação e Comunicações nos órgãos ou entidades da Administração Pública Federal. Esse método visa identificar as necessidades da organização em relação aos requisitos de segurança da informação e da comunicação. Essas necessidades devem estar alinhadas ao planejamento estratégico da organização e limitar-se a proteger os ativos de informação. A análise de riscos é definida nessa norma como o "uso sistemático de informações para identificar fontes e estimar riscos".

Segundo a NC04/IN01/DSIC/GSIPR (BRASIL, 2013, p. 2), a gestão de riscos deve ser contínua e estar alinhada ao ciclo PDCA (Plan-Do-Check-Act). As etapas do método de gestão de riscos da Norma Complementar 04 da Instrução Normativa 01 estão contempladas no Quadro 10.

Quadro 10 - Gerenciamento de risco da NC04/IN01/DSIC/GSIPR

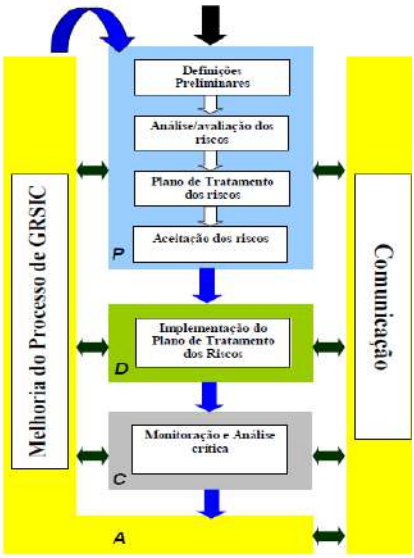
ETAPA	DESCRIÇÃO
Definições preliminares	Nessa etapa, analisa-se a organização, visando estruturar o processo de acordo com as características do órgão ou entidade; define-se o escopo e adota-se uma metodologia de gestão de riscos.
Análise a avaliação de risco	Etapa em que se identificam os riscos, considerando as ameaças e as vulnerabilidades associadas aos ativos de informação e ações já adotadas; estimam-se os riscos levantados, tendo em vista as probabilidades e a consequência do risco associado à perda de disponibilidade, integridade, confidencialidade e autenticidade nos ativos considerados; avalia-se se os riscos são aceitáveis ou requerem tratamento; priorizam-se os riscos que requeiram tratamento de acordo com critérios estabelecidos pelos órgãos.
Plano de tratamento dos riscos	Determina se os riscos deverão ser evitados, reduzidos, transferidos ou retidos e observa a eficácia das ações de segurança da informação existentes, as restrições organizacionais, técnicas e estruturais, os requisitos legais e a análise de custo/benefício. Também se deve formular um plano para o tratamento dos riscos e relacionar, no mínimo, as ações de segurança da informação, os responsáveis, as prioridades e os prazos de execução necessários à sua implantação.
Aceitação do risco	Verificam-se os resultados do processo executado, de acordo com o plano de tratamento, aceitando-os ou submetendo-os a uma nova avaliação.
Implementação do plano de tratamento dos riscos	Executam-se as ações de segurança incluídas no plano de tratamento de riscos aprovados.
Monitoramento e análise crítica	Essa é a fase em que se detectam possíveis falhas nos resultados, monitoram-se os riscos e as ações e se analisam criticamente a eficácia do método de Gestão de Riscos e as mudanças nos critérios de avaliação/aceitação, no ambiente, nos ativos, nas ações e nos fatores de risco (ameaça, vulnerabilidade, probabilidade e impacto).
Melhoria do processo de GRSIC	Propõem-se melhorias, identificadas nas fases de monitoramento e de análise crítica, e executam-se ações corretivas ou preventivas aprovadas.
Comunicação do risco	Mantêm-se as instâncias superiores informadas a respeito de todas as fases de gestão de risco, compartilhando informações entre o tomador de decisão e as partes interessadas.

Observa-se que a metodologia da NC04/IN01/DSIC/GSIPR foi construída de modo a manter as instâncias superiores da administração pública federal informadas sobre a gestão de riscos executadas pelos órgãos hierarquicamente inferiores, com a possibilidade de haver um controle macro pelo governo federal.

Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC

O Departamento de Segurança da Informação e Comunicações, do Governo Federal do Brasil, estabelece o processo de GRSIC (Gestão de Riscos de Segurança da Informação e Comunicações) nos órgãos ou entidades da Administração Pública Federal, direta e indireta, de acordo com as seguintes etapas, conforme ilustrado na figura 8:

Figura 8 – Processo de GRSIC



Fonte: BRASIL, 2009.

Primeiramente, o processo GRSIC baseia-se no ciclo PDCA (Plan-Do-Check-Act / Planejar-Fazer-Verificar-Agir), uma sequência de passos utilizada para controlar qualquer processo definido. O uso dos ciclos pode ser assim relatado: 1 – planejar envolve definir como será feito (quem, o que, quando, onde, como) e as metas e os métodos para atingir o objetivo; 2 – fazer significa tomar a iniciativa, educar, treinar, implementar e executar o planejado conforme as metas e os métodos definidos; 3 – checar consiste em verificar os resultados que estão sendo obtidos e de forma contínua, para garantir a execução dos trabalhos programados; 4 – agir determina fazer as correções necessárias através de ações corretivas ou melhorias.

Nesse contexto, e de acordo com a norma 04/IN01/DSIC/GSIPR, de 14/08/2009, as etapas do GRSIC são estas:

Definições preliminares - nessa fase, analisa-se a organização, a fim de estruturar o processo de GRSIC, considerando as características do órgão e as restrições a que estão sujeitas. Nesse caso, define-se o escopo, que pode abranger o órgão como um todo, um segmento, um processo, um sistema, um recurso ou um ativo da informação. É importante que o GRSIC atenda aos objetivos gerais e ao escopo definido e contemple, no mínimo, os critérios de avaliação e de aceitação do risco.

Análise/avaliação dos riscos - nesse momento, identificam-se os ativos e seus respectivos responsáveis dentro do escopo estabelecido; apuram-se os riscos levando em consideração as ameaças, as vulnerabilidades e as ações já existentes de segurança da informação; estimam-se os riscos levantados, de acordo com os valores ou os níveis de probabilidade e a consequência do risco associado à perda de disponibilidade, integridade, confidencialidade e autenticidade nos ativos considerados; avaliam-se os riscos, determinando se são aceitáveis ou se requerem tratamento, e relacionam-se os que precisam de tratamento, priorizando-os de acordo com os critérios determinados pelo órgão.

Plano de tratamento dos riscos – a partir daqui, as formas de tratar os riscos serão determinadas, tendo em vista as opções de reduzir, evitar, transferir ou reter o risco e atentando para a eficácia das ações de segurança já existentes, as restrições organizacionais, técnicas e estruturais, os requisitos legais e a análise de custo/benefício.

Aceitação do risco – nessa quarta etapa, os resultados dos processos anteriores serão verificados de acordo com o plano de tratamento, aceitando o risco ou submetendo-o à nova avaliação.

Implementação do plano de tratamento dos riscos – compreende a execução das ações de segurança da informação e do plano de tratamento dos riscos aprovado.

Monitoração e análise crítica – nessa etapa, detectam-se as possíveis falhas nos resultados, monitoram-se os riscos e as ações de segurança da informação e checa-se a eficácia do processo de GRSIC.

Melhoria do processo de GRSIC – essa é a fase em que se propõe à autoridade decisória do órgão a necessidade de implementar as melhorias identificadas na etapa anterior, que, depois de aprovadas, serão executadas, para assegurar que as melhoras atinjam os objetivos desejados.

Comunicação do risco – nessa fase, devem-se manter as instâncias superiores informadas sobre todas as fases da gestão do risco e compartilhar as informações entre a autoridade decisória e as demais partes envolvidas e interessadas (BRASIL, 2009, p. 4, 5).

A norma 04/IN01/DSIC/GSIPR, do Departamento de Segurança da Informação e Comunicações, específica para os órgãos e entidades do governo federal, pode ser complementada por argumentos de outros autores relacionados à segurança em sistemas de informação, objeto deste estudo. Para Laureno (2005, p. 74), a análise de risco pode ser

> quantitativa – baseada em estatísticas, numa análise histórica dos registros de incidentes de segurança – e qualitativa – baseada em know-how, geralmente realizada por especialistas, que têm profundos conhecimentos sobre o assunto.

De acordo com Sêmola (2009, p. 52), o aspecto quantitativo para analisar riscos é "orientado a mensurar os impactos financeiros provocados por uma situação de quebra de segurança a partir da valoração dos próprios ativos". Araújo (2009, p. 52) salienta que essa mensuração inclui o valor do recurso, a frequência de ameaça, a eficácia da proteção, os custos da proteção, a incerteza e a probabilidade, que serão medidos, divididos e atribuídos ao processo.

Quanto à análise qualitativa, Peltier (2005, p. 79) argumenta que, nesse processo, priorizam-se os diferentes elementos de riscos por meio de uma revisão sistemática das ameaças, para que a equipe estabeleça probabilidades de ocorrência e de perdas em contrapartida com as atitudes que serão concebidas para reduzir esses riscos a um nível aceitável. São muitas as técnicas que poderão ser aplicadas em uma análise qualitativa de risco, entre elas, brainstorming; técnica de Delpho; storyboarding; grupo focal; surveys; questionários; checklists; reuniões e entrevistas (ARAÚJO, 2009, p. 52).

No quadro 11, a seguir, apresentam-se as semelhanças e as diferenças entre os dois tipos de análise.

Quadro 11 – Análise de risco quantitativa e qualitativa

Propriedade	Quantitativa	Qualitativa
Análise de custo/benefício	Sim	Não
Cálculos complexos	Sim	Não
Custos financeiros	Sim	Não
É objetiva	Sim	Não
Envolve suposições.	Baixa	Alta
Envolve tempo/trabalho.	Alta	Baixa
Fácil comunicação	Alta	Baixa
Oferece resultados úteis e significativos.	Sim	Sim
Pode ser automatizada.	Sim	Não
Requer grande volume de informações.	Alta	Baixa
Resulta em valores específicos.	Sim	Não
Usa opiniões.	Não	Sim

Fonte: Araújo (2009, p. 53)

O modelo de análise qualitativo é mais ágil, pois não requer cálculos complexos para ser feito. Por isso, as organizações tendem a aceitá-lo com mais facilidade. Porém, independentemente do método adotado, uma análise de risco requer atividades por meio das quais se pode fazer o levantamento dos ativos, definir a lista de ameaças e identificar as vulnerabilidades desses ativos (LAUREANO, 2005, p. 75).

Normas ABNT ISO/IEC e padrões de segurança da informação

Com o intuito de orientar as organizações sobre as melhores práticas de segurança da informação, diversos órgãos buscam consolidar os aspectos de segurança com normas e boas práticas que devem ser seguidos para o alcance efetivo da segurança em seu ambiente.

"As normas e os padrões têm por objetivo definir regras, princípios e critérios, registrar as melhores práticas e prover uniformidade e qualidade a processos, produtos ou serviços, tendo em vista sua eficiência e eficácia" (BEAL, 2005, p. 36). Sêmola (2012) refere que uma norma tem o propósito de definir regras, padrões e instrumentos de controle que deem uniformidade a um processo, produto ou serviço.

Com o objetivo de implementar e normalizar a atuação das organizações no que diz respeito à segurança da informação, em 1995, a comunidade britânica, liderada pela Inglaterra, através da *British Standard Institute* (BSI), criou a norma BS 7799, composta de duas partes: a primeira, denominada de BS 7799: 1995, que apresentava um conjunto de melhores práticas para gerenciar a segurança da informação; e a segunda, publicada em 1999, com a nomenclatura de BS 7799: 1999, um modelo empregado para estabelecer o sistema de gestão de segurança da informação, sujeito à certificação de conformidade.

Sêmola (2012, p. 69) afirma que, "quando os reflexos da falta de segurança no mundo começaram a ser veiculados e a ganhar visibilidade, diversos países da comunidade britânica, como Austrália, África do Sul e Nova Zelândia, passaram a adotar a norma BS 7799".

Considerado o mais completo padrão da época a BS 7799 foi adotada pela *International Organization for Standartization* (ISO) e o *International Engineering Consortium* (IEC) que em conjunto publicaram como norma internacional a ISO/IEC 17799:2000. Em 2001 a Associação Brasileira de Normas Técnicas (ABNT), traduziu e publicou a versão brasileira da ISO/IEC 17799:2000 que ficou com a denominação de NBR/ISO 17799 – Código de Práticas para a Gestão da Segurança da Informação.

A ISO é uma organização internacional fundada em 1947 que trata de normalização. Sua sede é em Genebra, na Suíça, é formada por um Conselho e Comitês com membros oriundos da maioria dos países, e seu objetivo é de criar normas e padrões mundialmente aceitos sobre como realizar as mais diversas atividades comerciais, industriais, científicas e tecnológicas. Já o IEC é uma organização sem fins lucrativos, fundada em 1944 e sustentada por universidades e sociedades de engenharia. Basicamente, funciona por meio de parcerias entre universidades e indústrias e promove o desenvolvimento de pesquisas inovadoras e programas de serviço.

Ao longo do tempo, a ABNT consolidou o tema 'segurança da informação' através de uma série de normas conhecidas como família ISO/IEC 27000, apresentadas no Quadro 10, que abrange orientações para os mais diversos propósitos da gestão da segurança da informação. Atualmente essa família é composta de 44 normas, que orientam os mais diversos segmentos de mercado e atua da governança à implementação da segurança da informação, além de critérios de auditabilidade dessas organizações. Nesta pesquisa, destacaram-se as normas que fundamentam as boas práticas de implementação de uma Política de Segurança da Informação e os aspectos que a cercam.

Quadro 12: Normas da NBR/ISO fundamentais para a implementação da segurança da informação

NORMA	EM VIGOR	TÍTULO	OBJETIVO
27000	2016	Tecnologia da Informação - Técnicas de Segurança - Sistemas de gestão da Segurança da Informação - Descrições e vocabulários	Proporcionar uma visão geral de sistemas de gestão de segurança da informação, de termos e de definições comumente usados na família ISMS de normas. Essa Norma é aplicável a todos os tipos e tamanhos de organização (por exemplo, empresas comerciais, agências governamentais e organizações não lucrativas).
27001	2013	Tecnologia da informação - Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos	Especificar os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação no contexto da organização. Essa Norma também inclui requisitos para avaliar e tratar riscos de segurança da informação voltados para as necessidades da organização.
27002	2013	Tecnologia da informação - Técnicas de segurança - Código de prática para controles de segurança da informação	Estabelecer diretrizes para as práticas de gestão de segurança da informação e normas de segurança da informação para as organizações, incluindo a seleção, a implementação e o gerenciamento de controles, considerando os ambientes de risco da segurança da informação da organização.

NORMA	EM VIGOR	TÍTULO	OBJETIVO
27003	2011	Tecnologia da informação - Técnicas de segurança - Diretrizes para a implantação de um sistema de gestão da segurança da informação	Tratar dos aspectos críticos necessários para a implantação de um projeto bem-sucedido de um Sistema de Gestão da Segurança da Informação (SGSI), de acordo com a ABNT NBR ISO IEC 27001:2005. A norma descreve o processo de especificação e o projeto do SGSI desde a concepção até a elaboração dos planos de implantação. Ela descreve o processo de obter a aprovação da direção para implementar o SGSI, define um projeto para implementar um SGSI (referenciado nessa Norma como o projeto SGSI), e estabelece as diretrizes sobre como planejar o projeto do SGSI, o que resulta em um plano final para a implantação do projeto do SGSI.
27004	2010	Tecnologia da informação - Técnicas de segurança - Gestão da segurança da informação - Medição	Estabelecer as diretrizes para o desenvolvimento e o uso de métricas e medições, a fim de avaliar a eficácia de um Sistema de Gestão de Segurança da Informação (SGSI) implementado e dos controles ou grupos de controles, conforme especificado na ABNT NBR ISO/IEC 27001.
27005	2011	Tecnologia da informação - Técnicas de segurança - Gestão de riscos de segurança da informação	Essa Norma dá as diretrizes para o processo de gestão de riscos de segurança da informação.

Fonte: Baseado na Associação Brasileira de Normas Técnicas - 2018

Em setembro de 2013, entraram em vigor as normas NBR/ISO 27001 e 27002, revisadas e atualizadas, visando, principalmente, atualizar e reorganizar seus conteúdos, priorizando uma abordagem mais flexível e simplificada, a fim de garantir uma gestão de riscos mais efetiva.

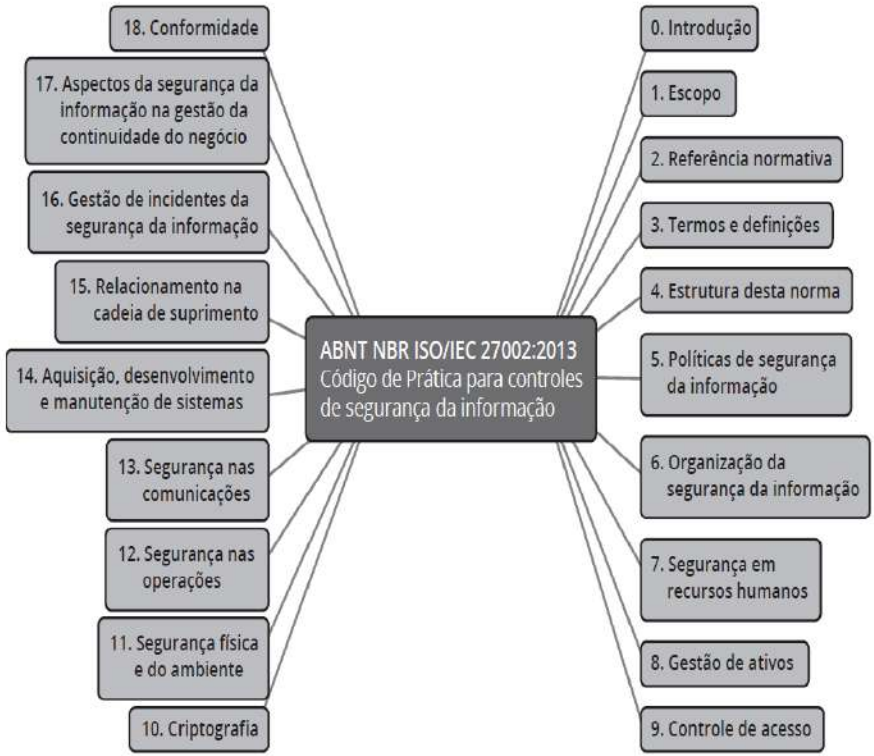
A norma NBR/ISO 27002, diferentemente da NBR/ISO 27001, que é auditável e não menos importante, sugere, através de um modelo menos formal, a preocupação com aspectos importantes e a utilização de controles que orientem as empresas a reduzirem seus riscos operacionais, que causariam impactos nos negócios. Essa norma é um importante instrumento sinalizador da direção que se deve seguir para implantar a segurança nas organizações.

É importante ressaltar que, conforme o próprio texto transcrito da norma, nem todos os controles estabelecidos precisam ser implementados pelas organizações, às quais caberá utilizar os controles condizentes com suas necessidades organizacionais, uma vez que há um aumento exponencial das complexidades e do dinamismo desses ambientes.

A norma NBR/ISO 27002:2013 contém 19 capítulos, numerados de 0 a 18. Os quatro primeiros são considerados introdutórios, e os demais representam as seções (ou domínios), organizadas em 35 objetivos de controles, que se expandem em um total de 114 controles sugeridos para implementar a segurança da informação nas organizações.

No sentido horário, a Figura 9 demonstra a sequência estrutural da norma e destaca as catorzes seções de controles de segurança da informação.

Figura 9: Estrutura da norma 27002:2013



Fonte: Coelho et al (2014, p. 20)

Convém atentar para o fato de que cada organização tem suas nuances e peculiaridades relacionadas ao seu ramo de negócio, à cultura organizacional, à estrutura etc. As normas só indicam orientações, mais cada organização deve, ao seu tempo, estruturar as recomendações das normas em suas políticas internas. Essa citação não é diferente no caso da gestão da segurança da informação em que cada organização deve desenvolver a própria política de segurança da informação adequada às suas necessidades.

Política de segurança da informação

Para que as organizações protejam suas informações adequadamente, elas precisam adotar procedimentos e ações de segurança condizentes com suas necessidades, com o objetivo de possibilitar que as organizações funcionem adequadamente, ao depender de suas informações e de seus recursos informacionais. Nesse sentido, emergem as Políticas de Segurança da Informação (PSI) como o ponto de partida para garantir a segurança da informação nas organizações.

Embora a área em estudo tenha adotado o termo Política de Segurança da Informação para designar os documentos que contêm as diretrizes, as normas e os procedimentos a serem seguidos para a consecução dos objetivos de assegurar as informações, tornou-se frequente a tentativa de simplificá-lo. Diferentes autores, em suas obras, referenciam-no, ora como Política, ora como Política de Segurança, ou até mesmo mencionam os três termos, sempre no mesmo sentido.

Neste livro, utilizamos o termo política como um sinônimo de Política de Segurança da Informação, que é a diretriz e a orientação básica para o assunto abordado. Maximiniano (2010, p.86), que define a política como sinônimo de diretriz.

> Uma política ou diretriz é uma orientação genérica que define em linhas gerais o curso de ação a ser seguido quando determinado tipo de problema se apresenta. A política orienta o processo de tomada de decisões através da definição de critérios que devem ser seguidos.

Para Sêmola (2012, p.105), "com o propósito de fornecer orientação e apoio ás ações de gestão de segurança, a política tem um papel

fundamental e, guardadas as devidas proporções, tem importância similar à Constituição Federal para um país".

Peltier (2004) considera a política como o mais alto nível de declaração do que a organização acredita e quer que exista em todas as suas áreas. A política é uma diretiva do corpo diretivo para criar um programa de segurança da informação, estabelecer seus objetivos e definir responsabilidades. "Política de segurança é um conjunto de regras e padrões sobre o que deve ser feito para assegurar que as informações recebam a proteção conveniente que possibilite garantir a sua confidencialidade, integridade e disponibilidade" (BARMAN, 2002, p.4).

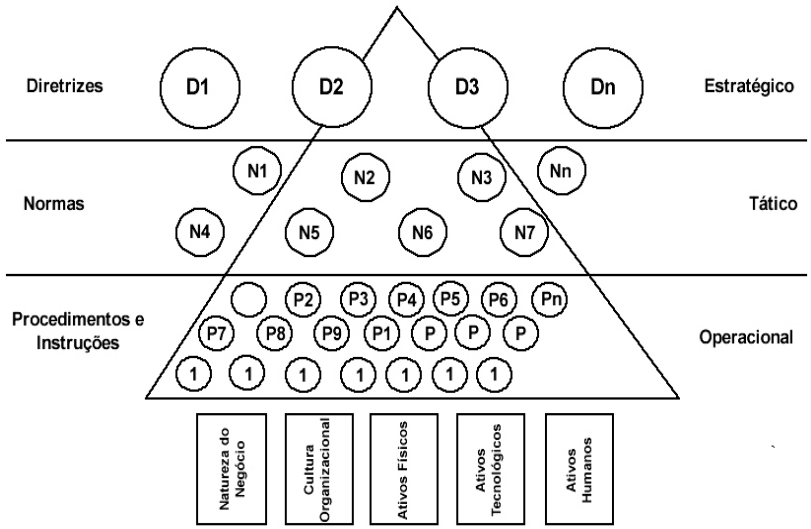
Para o Tribunal de Contas da União, a política de segurança de informações é um conjunto de princípios que norteiam a gestão de segurança de informações e que deve ser observado pelo corpo técnico e gerencial e pelos usuários internos e externos. As diretrizes estabelecidas nessa política determinam as linhas mestras que devem ser seguidas pela instituição para que sejam assegurados seus recursos computacionais e suas informações (TRIBUNAL DE CONTAS DA UNIÃO, 2012, p.10).

A norma ABNT NBR/ISO 27002:2013 declara, em seu texto, que a segurança da informação é alcançada com a implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware. Esses controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário, para assegurar que os objetivos de negócio e de segurança da organização sejam atendidos.

Assim, foi observado que a Política de Segurança da Informação assume um caráter abrangente e atende a todos os níveis organizacionais, institucionais, estratégicos, intermediários ou táticos e operacionais. Suas diretrizes são definidas pelo nível estratégico, suas normas e processos, destinados ao tático, e seus procedimentos, ao operacional.

Sêmola (2012) assevera que a política de segurança assume um caráter abrangente na organização. Com base na ordem de grandeza, podemos estimar 10 a 20 diretrizes em empresas de qualquer porte, mas teremos de multiplicar esse número por 100, ou mais, para estimar o volume de normas aplicáveis. O autor esclarece que esse volume tende a ser proporcional ao porte da empresa, à heterogeneidade de seus ativos físicos, tecnológicos e humanos e ao grau de detalhamento necessário para levar a empresa a operar com um nível de risco adequado.

Figura 9: Conceito dos componentes da política e seus pilares de personalização e sustentação



Fonte: Sêmola (2012, p. 106)

O capítulo 5 da norma ABNT NBR/ISO 27002:2013 trata dos aspectos da Política de Segurança da Informação e recomenda que o documento a ser desenvolvido apresente algumas definições como,

por exemplo, de que forma a organização quer tratar esse assunto, que sejam atribuídas as devidas responsabilidades, contemple um conjunto de controles a serem utilizados e garanta a divulgação para todas as pessoas da organização, para que o processo de segurança seja eficiente e eficaz ao longo do tempo. Ou seja, apresenta o que deve conter e sinaliza os controles que devem ser implementados.

A norma ABNT NBR/ISO 27002:2013 descreve, em seus capítulos, os controles que devem ser considerados nos documentos quando da elaboração da Política de Segurança da Informação. Ressalte-se que os controles são feitos de acordo com as necessidades da organização. Para se entender bem mais esse trabalho, o Apêndice B mostra apenas os controles considerados "obrigatórios" a serem verificados quando da elaboração desse documento.

Porém, a ABNT NBR/ISO 27002:2013 e as demais normativas da série NBR/ISO 27000 trazem as orientações sobre como deve ser elaborada a Política de Segurança da Informação ou como deve ser estruturado esse documento. Esse fato leva muitas organizações a empreenderem esforços de forma equivocada, ao tentar implantar a segurança da informação sem um processo sistêmico, unicamente baseado na implantação de controles de segurança.

> O fato de já existirem normas nacionais e internacionais que rezem sobre o código de conduta para o gerenciamento da segurança da informação não soluciona por completo o desafio que as empresas enfrentam. Isso acontece porque a norma tem o nítido papel de apenas apontar os aspectos que merecem atenção, indicando O QUE fazer para o adequado gerenciamento sem, no entanto, indicar com precisão metodológica COMO se deve realizar as atividades. (SÊMOLA, 2012, p.72)

Embora as normas apresentem uma orientação clara sobre boas condutas, a complexidade das organizações e os desafios impostos para a segurança da informação exigem uma metodologia de implantação

alinhada aos negócios e às estratégias da organização, primando pela especificidade de cada organização. Segundo Sêmola (2012), devido aos desafios da segurança da informação, não há uma única metodologia recomendada para sua implantação.

> Muitas organizações começam a desenvolver seus documentos de política de segurança da informação sem definir ou adotar alguma estrutura e planejamento. O que acontece na prática é um conjunto de documentos confusos, de difícil leitura, com assuntos repetidos ou com falta de assuntos de segurança da informação (FONTES, 2015, p.37).

Considerando a complexidade e a abrangência de uma Política de Segurança da Informação, é imprescindível que seja realizado um planejamento baseado em uma arquitetura que defina como os diversos tipos de documentos se relacionarão entre si, sua hierarquia e como os assuntos relacionados à segurança da informação estarão segmentados.

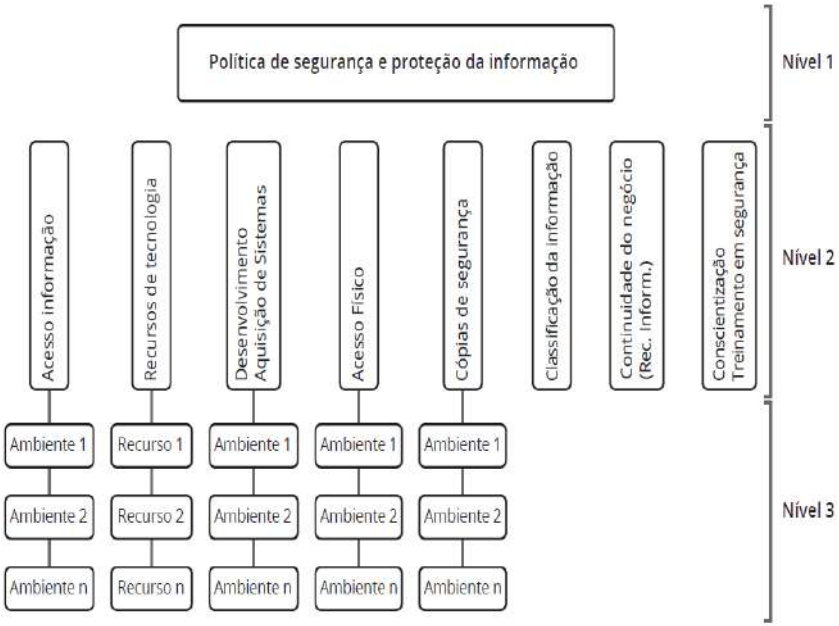
Para Fontes (2015, p. 37), "a arquitetura é a estrutura que permite que a Organização entenda e planeje (antes de ter os regulamentos), como será o seu conjunto de documentos que terão nos seus textos as regras de segurança da informação que deverão ser seguidas por todos". A arquitetura de segurança da informação, além de possibilitar uma visão global de como a segurança será estruturada dentro dos níveis organizacionais, atende a diversos aspectos fundamentais da segurança da informação. Ela deve ser capaz de estabelecer a implementação de controles de segurança de forma estruturada, abranger todos os envolvidos, estar em conformidade com seus aspectos legais, ser flexível e, principalmente, estar alinhada aos requisitos de negócio da organização.

Segundo Fontes (2015), cada organização deve construir sua arquitetura de segurança. O que existe em comum entre as empresas são os tipos de elementos que devem ser considerados nessa arquitetura, tais como:

- Estrutura básica – É necessário que a arquitetura se sustente em uma base teórica.
- Diversas plataformas – Os controles devem compreender todas possíveis plataformas.
- Gestão de usuário – É preciso garantir controles adequados à gestão dos usuários, desde sua admissão até o pós-desligamento.
- Gestão de acesso à informação – Deverá contemplar as regras para liberar e, posteriormente, cancelar o acesso às informações.
- Conformidade – Deverá atender aos requisitos legais do negócio e contemplar os casos específicos setoriais, quando houver.
- Continuidade de negócio – É preciso considerar o tempo de restabelecimento do negócio, em caso de contingência ou de desastres.
- Produtos de segurança – Deve utilizar programas e de produtos que atendam à necessidade de segurança da organização.
- Comprometimento com negócio – É necessário garantir que ações de segurança existam para sustentar a realização do negócio.
- Pessoas – Responsabilizar os usuários, garantir o cumprimento das regras e efetuar continuamente os treinamentos e a capacitação diante da Política de Segurança da Informação.

Convém enfatizar que esses aspectos constituem uma base comum a todas as organizações, independentemente de seu porte, porém, como já exposto neste trabalho, a necessidade da organização e de seu negócio é que conduzirá a uma arquitetura eficaz e eficiente quando da implementação da segurança da informação.

Figura 10: Estrutura da arquitetura da Política de Segurança da Informação



Fonte: Fontes (2015, p.39)

Processo para implementar e implantar uma política de segurança da informação

Sêmola (2012) entende que um dos principais desafios, quando se vai implantar a segurança da informação, é a falta de um planejamento sistêmico das ações a serem colocadas em prática. Corroborando o autor, Fontes (2015) afirma que é de fundamental importância estabelecer um processo de organização de segurança da informação que norteie as ações necessárias para implantar a segurança da informação.

Para Dantas (2011), o ponto de partida para implantar a segurança da informação é a construção da Política de Segurança da Informação.

> Para nós, a política é a materialização da intenção do que desejamos fazer, e essa intenção é transformada em princípios, valores, compromissos, requisitos, objetivos e orientações sobre o que deve ser feito para alcançar um padrão desejável de proteção para as informações. (DANTAS, 2011).

Segundo Davenport (1994, p.7), processo é "uma ordenação específica das atividades de trabalho no tempo e no espaço, com um começo, um fim e *inputs*[15] e *outputs*[16] claramente identificados: uma estrutura para a ação". Podemos considerar que um processo é um conjunto de atividades a serem realizadas numa sequência lógica, com o objetivo de produzir um bem ou serviço que agregue valor à organização.

15 Termo utilizado com significado de entrada
16 Termo utilizado com significado de saída

Apesar de haver um consenso sobre a necessidade de um planejamento prévio das ações a serem executadas no processo de implantação da segurança da informação, os autores não citam as atividades que deverão compor esse processo, e as normas não estabelecem como fazer, apenas o que deve ser feito. Por isso, é necessário criar um processo de acordo com o código de boa conduta do TCU, de acordo com as normas ABNT NBR/ISO 27001:2013, 27002: 2013 e 27005:2011, bem como os ideários dos autores que guiaram este estudo.

Convém ressaltar que o processo aqui construído não é inflexível ou único, mas adaptável para ser seguido pelas organizações que se encontram em estágio inicial de maturidade em segurança da informação, com o intuito de elucidar os vazios existentes para implantar a segurança nas organizações, com uma visão sistêmica. Esse processo pode ser consultado em sua completude no Apêndice A desta obra.

Para elaborar o processo proposto, adotamos o agrupamento das atividades em cinco etapas: a primeira, denominada de 'Contextualizando a Organização', concentrou as atividades necessárias para se entender a organização; na segunda – 'Abrangência da PSI' - definiram-se os limites e as fronteiras da Política de Segurança da Informação; na terceira - a de 'Implementação da PSI' – foram realizados o inventário, a classificação dos ativos informacionais, a análise de riscos e a construção da PSI; na quarta etapa, foram descritas as atividades que dariam visibilidade à PSI, bem como os treinamentos necessários; e na quinta etapa, apresentaram-se os aspectos necessários para manter as políticas na organização. A Figura 11 traz a representação em camadas dessas etapas.

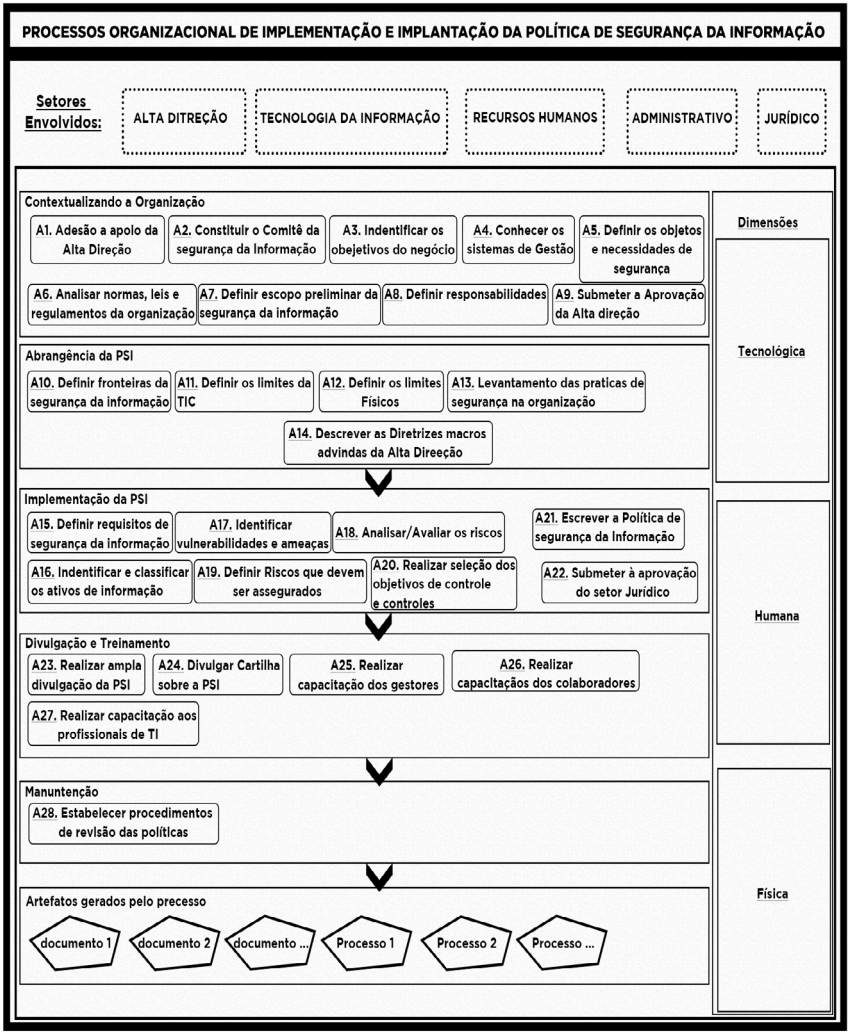
Figura 11: Conjunto de etapas que formaram o Processo Organizacional de Implementação e implantação da PSI

Fonte: Elaborado pelos autores - 2018

As etapas apresentadas na Figura 11 são decompostas em 28 atividades que deverão ser executadas para a implementação e a implantação da Política de Segurança da Informação. Suas inter-relações e os fluxos de atividades estão descritos no Apêndice A deste trabalho.

Esse processo foi construído considerando-se os aspectos das três dimensões da segurança da informação, e suas atividades foram ordenadas de forma sequencial e cíclicas, com o intuito de garantir a validade e a conformidade das ações a serem desempenhadas. A Figura 12 apresenta uma visão global do planejamento e da estruturação das atividades que compõem esse processo.

Figura 12: Visão global do planejamento do Processo Organizacional de implementação e implantação da PSI



Fonte: Elaborado pelos autores - 2018

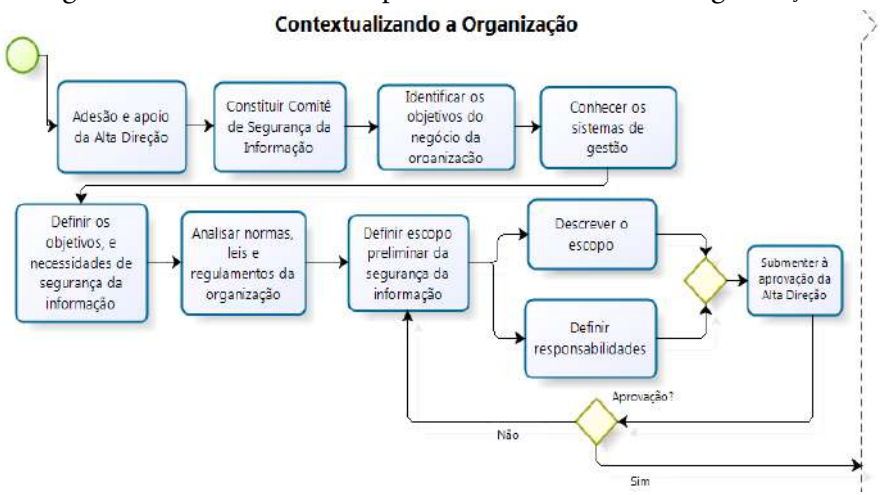
Nesse processo, as atividades precedentes geram outputs para suas subsequentes, e algumas atividades são responsáveis pela geração de

inúmeros documentos necessários para a consecução da segurança das informações. Para se entender bem mais o processo proposto, suas etapas e atividades serão descritas nas seções seguintes.

Contextualização da Organização

Essa etapa tem o objetivo de entender todo o contexto da organização, ou seja, interpretar e analisar toda a organização para determinar as questões internas e externas que possam afetar a capacidade da organização de garantir a segurança da informação. É nessa etapa em que se alcança a profundidade e se pode saber como a organização irá conduzir a segurança de suas informações. Suas atividades estão estruturadas em conformidade com os objetivos desejados e serão descritas no decorrer deste tópico. Para identificar as atividades, elas foram representadas por meio do código 'A' e sua respectiva ordem de execução (A1, A2, A3, A28). As relações entre as atividades e seu fluxo são representadas na Figura 13.

Figura 13: Atividades da etapa 'Contextualizando a Organização'



Fonte: Elaborado pelos autores - 2018

Essa etapa tem o objetivo de interpretar e analisar toda a organização para determinar as questões internas e externas que possam afetar a capacidade da segurança da informação na organização. É nessa etapa em que se alcança a profundidade e se sabe como a organização irá conduzir a segurança de suas informações. Suas atividades estão estruturadas em conformidade com os objetivos desejados e serão descritas neste tópico. Para facilitar a identificação, as atividades foram representadas com o código 'A' e sua respectiva ordem de execução (A1, A2, A3, A28).

A1. Adesão e apoio da Alta Direção

O processo inicia-se com a adesão da Alta Direção da organização, que deverá ser formalizada por meio de um documento formal, denominado de Carta de aceite e compromisso para a segurança da informação. Essa carta assume um papel fundamental para o sucesso da implantação das práticas de segurança da informação, porque poderá garantir que os assuntos relacionados à segurança tenham uma abordagem top-down[17] e sejam seguidos por todos os níveis da organização.

A adesão por parte da Alta Direção visa garantir o cumprimento das normas e dos procedimentos. Desde o nível operacional até o estratégico, há um consenso na literatura de que a sobrevivência de uma Política de Segurança da Informação passa pelo apoio dos que a dirigem, e suas normas são cumpridas com mais facilidade quando exigidas pela mais alta hierarquia da organização.

17 Abordagem de "cima para baixo" iniciada pela mais alta instância com poderes de se fazerem cumprir suas determinações.

A2. Constituição do Comitê de Segurança da Informação

Depois que a Alta Direção conscientiza sobre a importância das ações de segurança, deverá ser constituído o Comitê de Segurança da Informação, formado por uma equipe multidisciplinar, que conduzirá as ações e os assuntos relacionados à segurança.

Devido à abrangência de uma Política de Segurança da Informação e à complexidade de suas dimensões, sugere-se que o Comitê seja constituído de funcionários que já tenham um conhecimento sólido sobre a cultura organizacional, seus desafios e as estratégias que a organização assume para alcançar seus objetivos.

O Comitê de Segurança será o responsável por avaliar, monitorar, melhorar e conduzir os processos e controles da segurança. Dessa forma, a inclusão de gestores de áreas distintas da organização converge para o alcance de uma visão global dos desafios e das práticas que a organização deve assumir. Nesse sentido, sugere-se mais não se limita à inclusão de representantes de setores, tais como: Alta Direção, Recursos Humanos, Tecnologia da Informação, Administrativo e Jurídico.

A3. Identificação dos objetivos de negócio

A segurança da informação deve estar alinhada aos objetivos de negócio da organização e primar pela consecução de seus objetivos. Portanto, é necessário identificar todas as suas nuances. Para isso, sugere-se que sejam verificados os documentos estratégicos da instituição e que se faça um *brainstorming*[18] com a Alta Direção, porque os objetivos de negócio presentes nos planos estratégicos podem não estar de acordo com as práticas atuais. Essa atividade se encerrou com um documento que

18 Técnica grupal cuja finalidade é de resolver problemas específicos.

continha uma lista de objetivos de negócio da organização, que deverá ser validada pela Alta Direção.

A4. Conhecer os sistemas de gestão

A implantação de ações de segurança demanda o conhecimento dos modelos de sistemas de gestão que a organização utiliza e das formas de gerir. Suas práticas conduzirão à formulação das estratégias que serão assumidas para que todos os colaboradores cumpram cumprir as práticas de segurança. Nessa atividade, são identificadas características cruciais do modelo de gestão organizacional, que, a depender das formas existentes, poderá exigir múltiplas estratégias a fim de consolidar as práticas na organização.

A5. Definir os objetivos e as necessidades de segurança das informações

A definição dos objetivos e as necessidades de segurança culminarão no desenvolvimento da arquitetura de segurança da informação, que deverá contemplar as dimensões de segurança que a Política de Segurança da Informação irá reger dentro da organização, bem como todos os elementos a serem controlados.

A construção dessa arquitetura deverá seguir as orientações apresentadas na seção 1.5.1 deste trabalho. Cabe destacar que as atividades que a precedem consubstanciarão a construção dessa arquitetura.

A6. Análise das normas, das leis e dos regulamentos

Uma vez definidos as dimensões e os elementos a serem controlados, deve-se analisar a existência de normas, leis e regulamentos institucionais, com o intuito de identificar os aspectos legais que devem ser atendidos. Embora essa

atividade seja mais evidente em instituições públicas onde seu funcionamento é regido por leis, decretos, regulamentos e normas, ela também é necessária para a esfera privada, porquanto se busca a conformidade com o negócio da organização, e não, somente, com sua natureza.

A7e A8. Definição do escopo preliminar

A definição do escopo preliminar subdivide-se em duas atividades: a descrição do escopo e a atribuição das responsabilidades com a segurança da informação. Essa atividade apresenta-se de forma cíclica e deve ser submetida à aprovação da Alta Direção. O escopo compreende a transcrição do trabalho que precisa ser realizado para implantar a segurança da informação na organização, e suas características e funções devem ser especificadas, com o objetivo de proporcionar uma visão global à Alta Direção do processo de implantação.

Nesse documento, é fundamental que sejam especificadas as atribuições e as responsabilidades de todos os envolvidos no processo, a fim de assegurar a colaboração fidedigna sobre os aspectos necessários para implementar a segurança na organização.

A9. Submeter à aprovação da Alta Direção

Essa atividade tem o objetivo de obter aprovação da Alta Direção para se prosseguir com as atividades restantes do processo.

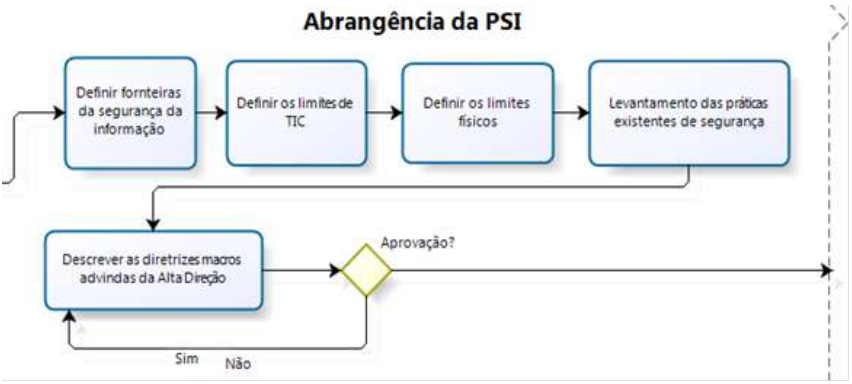
Abrangência

A segunda etapa do processo refere-se aos limites e fronteiras que a Política de Segurança da Informação irá abranger, todas as atividades

dessa etapa deverão ser documentadas a fim de manter o histórico do que será assegurado na organização. As atividades que compõe essa etapa são descritas abaixo:

As relações entre as atividades e seu fluxo são representadas na Figura 14.

Figura 14: Atividades da etapa Abrangência



Fonte: Elaborado pelos autores, 2018.

A10. Definir fronteiras da segurança da informação

Essa atividade tem como objetivo descrever os limites organizacionais da segurança da informação e apresenta como resultados as funções e a estrutura da organização, as trocas de informações, através dos limites, e os responsáveis pelos ativos de informação da organização. A delimitação das fronteiras da segurança na organização possibilitará a concentração de esforços em ações direcionadas a identificação dos processos e dos ativos que serão contemplados pela segurança.

A11. Definir os limites da Tecnologia da Informação e Comunicação

O uso de tecnologias da informação e comunicação está cada vez mais presente nas organizações. Por essa razão, é necessário estabelecer quais desses recursos serão contemplados com ações de segurança.

Os recursos destinados ao processamento de dados e à disseminação de informações, seja no âmbito interno ou no externo, deverão ser contemplados nesse documento. Sugere-se que sejam descritos os sistemas de informação e de redes de telecomunicações, detalhando o que estará no âmbito da segurança e o que não será assegurado.

A12. Definição dos limites físicos

Descrever a organização e suas características geográficas é uma forma de identificar potenciais riscos naturais que possam interferir na segurança das informações. Um exemplo disso é o de uma organização que esteja geograficamente localizada em uma área onde há quedas ininterruptas no fornecimento de energia, e isso coloque em risco as informações armazenadas em seus servidores que podem corromper seus discos rígidos.

A13. Levantamento das práticas existentes

Comumente as organizações praticam alguma ação para assegurar suas informações, sejam formais ou informais. Elas devem realizar o levantamento de todas as práticas utilizadas pela organização, com o intuito de conhecer possíveis vícios que possam comprometê-la.

A14. Descrição das diretrizes macros

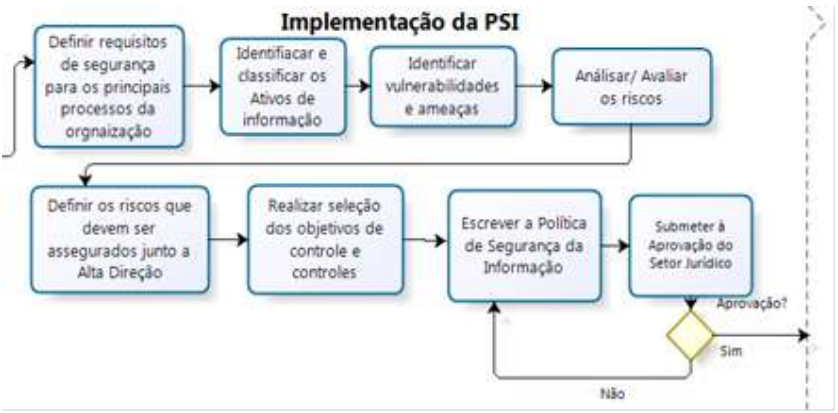
Depois de definir os limites de abrangência da segurança da informação, inicia-se a construção das diretrizes gerais que nortearam a

construção das normas e dos procedimentos adotados pelos colaboradores da organização. Além das informações que precedem essa atividade, devem-se formular as diretrizes alinhadas às estratégias, aos negócios e aos objetivos da organização que deverão ser submetidas à aprovação da Alta Direção. Essa atividade assume uma característica cíclica até obter a aprovação do corpo diretivo da organização.

Implementação

As atividades que compõem essa etapa são consideradas críticas para o sucesso da implantação da segurança da informação na organização e contemplam uma sequência de ações que possibilitarão identificar as vulnerabilidades e as ameaças às informações organizacionais, mapear os ativos informacionais e mensurar os riscos existentes. As atividades a serem seguidas são descritas abaixo, e as relações entre as atividades e seu fluxo são representadas na Figura 15.

Figura 15: Atividades da etapa de implementação



Fonte: Elaborado pelos autores - 2018

A15. Definir requisitos de segurança para os principais processos da organização

Todas e quaisquer condições necessárias para proteger as informações devem ser listadas nessa atividade. Sugerimos que os principais processos, funções, locais, sistemas de informação e rede de computadores da organização sejam analisados sob a ótica das necessidades de garantir a disponibilidade, a confidencialidade e a integridade das informações.

A16. Identificar e classificar os ativos de informações

Logo que são identificados os principais processos da organização e concluído o escopo de abrangência, devem-se identificar os ativos de informações e classifica-los. Essa atividade tem o objetivo de identificar todos os ativos que agreguem valor para a organização para, posteriormente, protegê-los e assegurar a continuidade dos negócios.

Nessa atividade, devem ser considerados todos os ativos envolvidos no escopo dos processos, em especial, dos que são diretamente relacionados aos objetivos de negócio. Portanto, sugere-se que seja realizado um levantamento cuidadoso desses ativos.

A17. Identificar vulnerabilidades e ameaças

Depois de identificar os ativos que devem ser protegidos na organização, devem-se levantar as probabilidades de cada ativo estar vulnerável a qualquer tipo de ameaças, seja interna ou externa, e atentar para o comprometimento potencial dos riscos à integridade, à confidencialidade e à disponibilidade das informações.

A18. Analisar/Avaliar os riscos

Essa atividade contempla um conjunto de ações que identificam e avaliam, de forma sistemática e metodológica, os riscos de segurança a que os recursos críticos do negócio estão sujeitos. A execução dessa atividade demanda uma abordagem de gerenciamento de risco voltada para a análise das ameaças, das vulnerabilidades e dos impactos, como forma de classificá-los dentro do seu grau de importância para os negócios da organização.

A19. Definir riscos que devem ser assegurados

Para analisar e avaliar os riscos, deve-se, junto com a alta Direção, definir uma classificação de prioridades para os riscos, dando visibilidade aos seus critérios de tratamento.

A 20. Selecionar os objetivos de controle de segurança

Essa atividade demandará a seleção dos controles presentes na norma ABNT NBR ISO/27002:2013 para mitigar os riscos aos ativos da organização.

A 21. Escrever a Política de Segurança da Informação

Atividade responsável pela escrita da Política de Segurança da Informação.

A 22. Submeter à aprovação do Setor Jurídico

Depois de escrita, a Política de Segurança da Informação deve ser submetida ao setor jurídico da organização para validar os aspectos legais

contidos nas normas, nos procedimentos e, principalmente, nas ações punitivas pelo descumprimento das normas.

Divulgação e treinamento

Deverão ser feitas uma ampla divulgação da Política de Segurança da Informação dentro da organização e treinamentos com todos os seus funcionários. As atividades que compõem essa etapa estão representadas na Figura 16 e devem ser conduzidas de forma exaustiva e periódica, para garantir que todos conheçam as normas e os procedimentos a serem praticados na organização.

Figura 16: Atividades da etapa de 'Divulgação e treinamento'

Fonte: Elaborado pelos autores - 2018

A 23. Divulgar amplamente a PSI na organização

A PSI deverá ser divulgada amplamente na organização, para que todos os funcionários a conheçam. Para isso, sugerimos que seja feito um planejamento de ações contínuas, utilizando diversos recursos, tais

como: tela de computador, folheto, informativo, reuniões, cartilha sobre a segurança da informação etc.

A 24. Divulgar cartilha sobre a PSI da organização

É de extrema importância que as normas e os procedimentos a serem seguidos sejam compreendidos por todos os colaboradores da organização. Para isso, sugere-se que seja elaborada uma cartilha de segurança da informação escrita em um linguajar informal, em que as mensagens possam ser compreendidas por todos da organização.

A 25, A 26 e A 27 - Capacitação dos gestores, dos colaboradores e dos profissionais de TI

Todos os colaboradores da organização devem receber uma capacitação sobre a segurança da informação, para que tenham condições de seguir os procedimentos estabelecidos. O nível de aprofundamento das capacitações deve ser direcionado ao público que está sendo capacitado, respeitando os objetivos da estratégia assumida para se implantar a segurança da informação.

Manutenção

Por fim, mas não menos importante, é preciso documentar e estabelecer procedimentos que garantam a efetividade e o cumprimento das ações de segurança na organização e a atualização contínua e periódica dos controles utilizados para assegurar os ativos de informação.

Figura 17: Atividades da etapa de manutenção

Fonte: Elaborado pelos autores - 2018

A 28. Estabelecer procedimentos de revisão das políticas

As políticas deverão ser revisadas periodicamente ou quando houver necessidade. Essa revisão será feita através de fatores que devem estar documentados, como: ocorrência de um incidente de informação, inserção de ativos informacionais, mudança de objetivos do negócio etc.

Implementação e implantação de uma política de segurança da informação

Na implementação e na implantação de uma Política de Segurança da Informação, devem-se levar em consideração as três e distintas dimensões organizacionais: a tecnológica, a física e a humana, bem como as particularidades da organização objeto dessa ação. Todavia, para atingir esse objetivo, é imprescindível que o processo a ser criado contemple um conjunto de atividades condizentes com a realidade e as particularidades da organização e uma análise e avaliação de riscos, com o intuito de revelar as ameaças, as vulnerabilidades e os riscos a que a organização possa estar suscetível.

Para validar o processo apresentado, adotou-se como objeto de estudo uma fundação privada sem fins lucrativos, que atua, entre outros serviços, como organizadora de concursos públicos, localizada na cidade de Maceió, no estado de Alagoas, com o fim de nortear as organizações para que implantem sua segurança. Este capítulo apresenta sistematicamente o percurso seguido para conseguir fazê-lo, os resultados da aplicação do processo e o método utilizado.

Elaborar uma política de segurança da informação requer várias atividades, e a de analisar e de avaliar riscos é considerada a mais complexa e importante. Basicamente, é responsável por coletar e analisar os dados, objetivando identificar as ameaças, as vulnerabilidades e os riscos e selecionar seu controle. O método FRAAP foi adotado porque possibilita que o processo seja executado pelos próprios especialistas da organização e conduzido em poucos dias, com um custo benefício baixo, o que proporciona um nível maior de aceitação já que não é

estabelecido por meio de uma consultoria externa com procedimentos genéricos.

Procedeu-se a uma análise e a uma avaliação de risco no processo referente à elaboração e à execução de concursos públicos, com a aplicação do método FRAAP, que objetiva analisar um ativo ou processo utilizando a técnica de *brainstorming* para a coleta de dados e instrumentos de análise e avaliação com uma abordagem qualitativa.

A Política de Segurança da Informação inclui políticas restritivas, normas e diretrizes que descrevem a forma como a organização conduzirá a segurança da informação a partir dos procedimentos a serem adotados, levando em consideração as dimensões tecnológica, física e humana, para garantir a integridade, a confidencialidade e a disponibilidade das informações da organização.

Coleta e análise dos dados

Como já referido, durante o processo de construção de uma Política de Segurança da Informação, os dados são coletados e analisados na execução do processo de análise e de avaliação de risco. Assim, para executar essa atividade, adotou-se o método FRAAP como metodologia. A coleta e a análise dos dados obedeceram rigorosamente aos preceitos da metodologia FRAAP e foram feitos em três etapas ora descritas no capítulo 5 - a pré-FRAAP, a sessão FRAAP e a pós-FRAAP.

Antes de iniciar a implementação do FRAAP, foi criado e executado um programa de sensibilização com todos os funcionários envolvidos diretamente no processo de elaboração e execução de concursos públicos, com o objetivo de proporcionar a todos os participantes o conhecimento sobre o processo objeto do FRAAP, de estabelecer o envolvimento dos participantes, de avaliar o conhecimento relativo à avaliação de risco, de

determinar a necessidade de aprendizado dos colaboradores sobre avaliação de risco, de verificar o nível de aceitação dos aspectos de segurança da informação e de identificar os possíveis aliados no processo.

A participação no programa de sensibilização foi por intermédio de uma convocatória realizada pela direção executiva da organização e enviada por e-mail, que tornava obrigatória a participação dos 21 colaboradores envolvidos no processo de elaboração e execução de concursos públicos, com exceção das justificativas previamente informadas.

Dos 21 colaboradores convocados para participar do programa de sensibilização, compareceram 17. Duas ausências foram justificadas porque os convocados estavam alocados em outra atividade crucial para a organização; uma, porque o colaborador estava aniversariando, portanto estava automaticamente dispensado de suas atividades trabalhistas; e uma, por causa da incompatibilidade de horário entre a execução do programa e suas atividades na organização.

Os participantes do programa de sensibilização foram divididos em dois grupos: o primeiro composto pelos colaboradores que exerciam função de gestores ou detinham responsabilidades com as atividades críticas do processo, e o segundo, pelos funcionários de suporte operacional, conforme pode ser verificado no Quadro 11.

Quadro 11: Participantes do programa de sensibilização

Participantes do programa de sensibilização			
Participante	**Grupo**	**Cargo / Responsabilidade no processo**	**Tempo em anos na Organização**
Participante 1	Gestores	Diretora executiva e a principal responsável pelo processo	16
Participante 2		Diretora de ensino/ seleção de docentes para elaborar questões de provas.	5
Participante 3		Gestora de Pós-Graduação e chefe do Setor Jurídico/ suporte jurídico	3
Participante 4		Analista de Sistema/formatação e impressão de provas	3
Participante 5		Gestora de infraestrutura de TI/ infraestrutura tecnológica	7
Participante 6		Gestora de RH/ contratação de pessoas para aplicarem provas	9
Participante 7		Gestora financeira/ responsável pela aplicação de provas, pelos materiais e pelos pagamentos.	9
Participante 8	Operacional	Técnico em informática II/ suporte operacional	2
Participante 9		Técnico em informática I/suporte operacional	2
Participante 10		Secretária acadêmica/suporte operacional	5
Participante 11		Assistente administrativo/suporte operacional	2,5
Participante 12		Assistente administrativo/suporte operacional	1
Participante 13		Assistente administrativo/suporte operacional	1
Participante 14		Coordenadora de apoio/impressão de provas	11
Participante 15		Advogada/suporte jurídico	2
Participante 16		Assistente administrativo/suporte operacional	1,5
Participante 17		Assistente administrativo/suporte operacional	1

Fonte: Elaborado pelos autores. Pesquisa direta - 2018

As colunas do Quadro 11, em que demonstramos o tempo, em anos, de cada colaborador na organização e o cargo ou função exercida no processo serviram e como critérios para definir os participantes da Sessão FRAAP, pois entendemos que essas duas variáveis eram determinantes para melhorar a qualidade das identificações das ameaças, as vulnerabilidades e os riscos, porque, quanto maior o tempo do colaborador na organização e a responsabilidade do cargo ocupado, maior seu conhecimento sobre o processo analisado e os negócios da organização.

Estrategicamente, o programa de sensibilização foi realizado em um único dia e aplicado em dois momentos distintos, conforme as atribuições e as responsabilidades dos colaboradores no processo. O primeiro momento foi focado no grupo operacional, e o segundo, no grupo de gestores do processo.

No primeiro momento, apresentamos e explicamos conceitos fundamentais de segurança da informação e avaliação de risco por meio de apresentação realizada em Datashow. Depois de encerrada a apresentação e da retirada de dúvidas existentes sobre os conteúdos, solicitamos a todos os participantes que, a partir da observação de suas rotinas, registrassem as ameaças, as vulnerabilidades e os riscos para os negócios da organização, como forma de consolidar as informações repassadas e familiarizá-las com o tema 'segurança da informação'.

O segundo momento começou depois que o grupo operacional foi dispensado da reunião e contou com a participação do grupo de gestores, que estabeleceu uma discussão de pontos mais profundos acerca do tema e da realidade organizacional. Nesse momento, discutiu-se sobre as necessidades de se praticar a segurança da informação na organização, inicialmente no processo de elaboração e execução de concursos públicos.

Depois que os envolvidos no processo em análise tomaram conhecimento das ações que seriam colocadas em prática na organização,

com o objetivo de implantar a segurança da informação, iniciou-se a aplicação do método FRAAP.

Etapa Pré-FRAAP

Nessa etapa, foram determinados os requisitos e os atributos que permearam toda a análise e a avaliação de risco, em uma reunião com a participação do diretor geral da organização, a diretora executiva e o facilitador do método, no dia 03 de outubro de 2016, que durou 1 hora e 16 minutos. A execução das atividades inerentes a essa etapa gerou como resultados os artefatos necessários para a realização da análise e da avaliação de risco. A seguir, descrevemos essas atividades.

Pré-triagem

Como todo o corpo diretivo da organização se posicionou a favor do projeto e definiu o processo como o mais crítico de seu negócio, levando em consideração a natureza do serviço que o processo representa, procedeu-se a uma análise da viabilidade da execução do FRAAP no processo sobre dois prismas fundamentais: a sensibilidade das informações do processo e a criticidade do processo para os negócios da organização.

Ao analisar a sensibilidade das informações, verificou-se que todas as que eram referentes aos concursos públicos devem ser confidenciais, íntegras e estar disponíveis em data e hora estabelecidas em edital. Em relação ao processo, qualquer incidente de informação que haja poderá impactar diretamente na imagem e no negócio da organização. Assim, ratificou-se a necessidade de executar o projeto e de classificar o processo como crítico para a organização.

No âmbito das análises de regulamentação, encontraram-se leis que impactam diretamente na atividade de construção do edital, porém não há uma que seja aplicada diretamente às organizadoras de concursos. Todo órgão ou entidade da administração pública pode atuar como fiscalizador do concurso público, no entanto o Ministério Público da União atua de forma mais incisiva na fiscalização das organizadoras de concursos, porém não normatiza nem orienta sobre o processo a ser seguido, apenas exige os princípios da ética, da inviolabilidade das informações e do cumprimento das Leis às quais o certame está submetido.

Declaração do escopo

O escopo do projeto consistiu em identificar ameaças, vulnerabilidade, riscos, impactos e controles inerentes ao processo de elaboração e execução de concursos públicos, considerando as dimensões tecnológicas, física e humana, para assegurar a confidencialidade, a integridade e a disponibilidade das informações por meio da construção de uma Política de Segurança da Informação.

As fronteiras da análise e da avaliação de risco limitaram-se ao processo de elaboração e execução de concursos públicos e foram aplicadas aos ativos informacionais que estivessem diretamente ligados aos subprocessos de licitação, edital, inscrições, elaboração das questões de prova, confecção de prova, logística, contratação de pessoal, aplicação de prova, correção e divulgação de resultados.

Definiu-se que, quanto à origem e à intencionalidade, as ameaças seriam classificadas em:

- 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.

Diagrama visual

Essa atividade mostrou que a organização só dispunha do processo de elaboração e execução de concursos públicos descritos de forma textual, o que acarretou a necessidade de modelá-lo em uma linguagem visual que facilitasse identificar as atividades realizadas durante a execução do processo. Por solicitação da direção executiva da organização, o processo modelado não será exposto nesta dissertação, para garantir sua competitividade de mercado e assegurar a privacidade de suas atividades e os fluxos de informações.

As etapas oriundas do FRAAP foram diagramadas para serem expostas durante a execução da Sessão FRAAP, para que todos tomassem ciência das atividades a ser desempenhadas.

Formação da Equipe FRAAP

De acordo com as diretrizes do método FRAAP, que sugere uma equipe composta de sete a 15 pessoas e respeita os critérios de mais tempo em anos na organização e a importância do cargo exercido no processo, foram definidos os participantes da Sessão FRAAP, conforme o Quadro 12.

Quadro 12: Participantes da Sessão FRAAP

Participantes do FRAAP			
Participante	**Grupo**	**Cargo / Responsabilidade no processo**	**Tempo em anos na Organização**
Participante 1	Gestores	Diretor geral - Proprietário	17
Participante 2		Diretora executiva, principal responsável pelo processo	16
Participante 3		Diretora de Ensino/Seleção de docentes para elaborar questões de provas	5
Participante 4		Gestora de Pós-Graduação e chefe do Setor Jurídico/ Suporte Jurídico	3
Participante 5		Gestora de infraestrutura de TI/ infraestrutura tecnológica	7
Participante 6	Operacional	Analista de Sistema/ Formatação e impressão de provas	3
Participante 7		Técnico em informática II/ Suporte operacional	2
Participante 8		Coordenadora de apoio/ impressão de provas	11

Fonte: Elaborado pelos autores - Pesquisa direta - 2018

É importante destacar que o Diretor geral e proprietário foi incluído na equipe de participantes do FRAAP, por solicitação própria, o que demonstrou a importância e o interesse da organização em implantar a segurança da informação.

Definição da reunião do FRAAP

Foi acordado que a reunião referente à aplicação da Sessão FRAAP ocorreria na Unidade Barro Duro, no dia 10 de outubro, e começaria às 8:30h. Os recursos utilizados para sua realização foram

a sala de reunião, datashow, canetas, folhas A4, caixa de som e *coffe break*. Todos os recursos necessários para a Sessão FRAAP, foram providenciados pelo proprietário da organização, que também convidou os participantes.

Definições essenciais

Os termos fundamentais que orientaram a construção da Política de Segurança da Informação e a atividade de análise e avaliação de risco foram definidos nessa atividade. Inicialmente, estabelecemos os termos de caráter geral, apresentados no Quadro 13.

Quadro 13: Termos gerais utilizados na PSI

Termos gerais	
Termo	**Definição**
Ativo	É um recurso com valor. Pode ser uma pessoa, um processo ou uma informação.
Ameaça	É qualquer coisa (ato humano intencional ou não, ou causada pela natureza) que tem potencial para causar danos.
Probabilidade	É a chance de que um evento aconteça ou de um valor de perda específica ser atingido se o evento ocorrer.
Impacto	Uma medida da magnitude da perda ou dano no valor de um ativo da informação.
Vulnerabilidade	É uma fragilidade que pode ser usada para colocar em perigo a um ativo de informação ou lhe causar danos.
Risco	É a combinação de ameaça com probabilidade e impacto, expresso em níveis de valor acordados.

Fonte: Elaborado pelos autores. Pesquisa direta - 2018

Depois foram apresentados os conceitos de probabilidade e impacto assumidos durante a avaliação de risco. Durante a avaliação de risco, os conceitos de probabilidade e de impacto receberam uma escala de mensuração e foram cruzados em uma matriz de avaliação de risco que determinou seu nível para a organização.

Minissessão de brainstorming

Depois de apresentar os itens anteriores, procedemos a uma minissessão de *brainstorming*, com o intuito de avaliar os objetivos de negócios futuros e de orientar os participantes sobre as ameaças aos negócios da organização. Foi solicitado que cada participante mencionasse quatro ameaças para cada atributo de informação estabelecido, que causassem impacto nos negócios da organização.

Ainda nessa atividade foram definidas as diretrizes macros que comporão a Política de Segurança da Informação e acordado que a política seria construída de forma iterativa possibilitando no futuro a adição de novos ativos e processos da organização.

Etapa Sessão FRAAP

Essa etapa foi executada em quatro horas e dez minutos, no dia 13 de outubro de 2016. Iniciou às 14:00 horas e terminou às 18:10, na sala de reunião da Diretoria geral da organização. Nessa oportunidade, os dados foram coletados por meio da técnica de *brainstorming* e analisados com técnicas e instrumentos oriundos da gestão de risco. Somente os membros da equipe FRAAP participaram dessa etapa e foram responsáveis pela aplicação do processo de análise e avaliação de risco.

Durante a fase de análise dos riscos, foram identificados os ativos, as vulnerabilidades, as ameaças e os riscos relacionados ao processo em análise. Já a fase de avaliação dos riscos incidiu na comparação de cada risco analisado e no critério de avaliação previamente estabelecido pela organização. Depois de avaliar a criticidade dos riscos, verificamos os controles já existentes na organização e construímos novos controles para os riscos residuais.

A reunião de *brainstorming* foi organizada de forma que os participantes sentassem à mesa de reunião em forma de "U". Depois que receberam as explicações iniciais, apresentamos o processo objeto de análise de forma visual e explicamos o fluxo que as informações percorriam durante sua execução. Depois de retirar algumas dúvidas dos participantes sobre o processo de identificação das ameaças, de probabilidades e de controles, iniciamos a rodada de identificação, que consistiu em apresentar o atributo a ser considerado na identificação das ameaças. Os participantes tinham cinco minutos para pensar e anotar as possíveis ameaças correspondentes ao atributo exposto.

Depois do término do tempo estipulado para identificar as ameaças, era solicitado que o participante que se localizava na ponta do "U" lesse em foz alta uma única ameaça que era registrada na tabela de identificação de ameaças, e assim sucessivamente, até o último participante. Cada participante expôs uma única ameaça por vez, o que tornou o processo de identificação cíclico até que não existissem mais ameaças ou só restassem participantes expondo ameaças fora do escopo do projeto.

Foram identificadas 53 ameaças - 28 relacionadas à confidencialidade, 12, à disponibilidade, e 13, à integridade. Em seguida, foram identificados os agentes das ameaças e sua origem. As ameaças são descritas no Quadro 14, cujos caracteres N, I, V, na coluna de origem, representam (N) origem natural, (I) origem involuntária e (V) origem voluntária.

Quadro 14: Identificação das ameaças, de seus agentes e suas origens

CONFIABILIDADE		
AMEAÇA	**AGENTE DE AMEAÇAS**	**ORIGEM**
Acesso não autorizado às áreas restritas.	Pessoal interno; Pessoal externo; *Hacker;*	V
Utilização de equipamentos eletrônicos pessoais na área de confecção de provas.	Pessoal interno;	I, V
Informações de provas podem ficar armazenadas nas impressoras e levadas para manutenção.	Pessoal interno;	I
Elaboradores de questões de prova podem divulgar suas questões a pessoas não autorizadas.	Pessoal interno;	V
Sigilo das provas pode ser violado por funcionários internos.	Pessoal interno;	V
Informações sigilosas podem ser deixadas à vista em uma mesa.	Pessoal interno;	I
Furto interno de informações	Pessoal interno; Pessoal externo; *Hacker;*	V
Falta de uma política de informação	Organização	I
Senhas de e-mail inseguras podem ser descobertas.	Pessoal interno; Pessoal externo; *Hacker;*	I, V
Bases de dados podem ser hackeadas.	*Hacker;* Espionagem industrial;	V
Softwares maliciosos podem roubar informações.	*Hacker;*	V
Conversas informais podem revelar informações sigilosas.	Pessoal interno;	I, V
Acesso remoto não autorizado às estações de trabalho durante os finais de semana.	Pessoal interno; *Hacker;*	V
Descarte inadequado de informações	Pessoal interno;	I, V

Acesso às redes wifi por pessoas não autorizadas	Pessoal interno; *Hacker;*	V
Programas não confiáveis podem capturar informações.	Pessoal interno; *Hacker;*	V
Bases de dados podem ser violadas por funcionários internos.	Pessoal interno;	V
Informações armazenadas em pendrives podem ser perdidas ou interceptadas.	Pessoal interno; Pessoal externo; *Hacker;*	I, V
Funcionários podem ser aliciados a entregar informações.	Pessoal externo;	V
Pastas compartilhadas inadequadamente podem dar acesso a informações não autorizadas.	Pessoal interno;	I, V
Dar informações por telefone a pessoas que não podem ser identificadas.	Pessoal interno;	I
Informações sigilosas podem ser armazenadas em celulares e notebooks pessoais.	Pessoal interno;	V
Utilização da infraestrutura de rede compartilhada com toda a organização pode gerar ataques de captura de dados.	*Hacker;*	V
Divulgação acidental de informações sigilosas.	Pessoal interno;	I
Manipulação intencional do resultado do certame	Pessoal interno;	V
Fiscais de provas podem beneficiar candidatos ou fazer com que vazem informações durante a execução das provas.	Pessoal interno;	I, V
As provas podem ser violadas no local onde estão sendo aplicadas antes de começar.	Pessoal interno;	V
O sigilo dos nomes dos elaboradores de questões pode ser violado e divulgado.	Pessoal interno; Hacker;	V

DISPONIBILIDADE		
AMEAÇA	**AGENTE DE AMEAÇAS**	**ORIGEM**
Falta de energia pode tornar os sistemas inoperantes.	Fornecedor;	I
Falta ou instabilidade do serviço de internet	Fornecedor;	I
Falha de infraestrutura de tecnologia da informação e comunicação	Pessoal interno;	I
Ausência do responsável por extrair informações da base de dados.	Pessoal interno;	I
Arquivos armazenados em diretórios pessoais podem não estar disponíveis para outros funcionários quando necessário.	Pessoal interno;	I, V
Indisponibilidade dos servidores	Pessoal interno;	I
Ataques de negação de serviços	Hacker;	V
Falha de hardware ou software	Fornecedor;	I
Roubo de equipamentos	Pessoal interno; Pessoal externo;	V
Não localização do elaborador de questão para responder aos recursos.	Pessoal interno;	I, V
Falta de informações sobre as bases legais a que o cliente está submetido.	Pessoal externo;	I, V
Erros técnicos na operacionalização dos dados dos candidatos, locais de provas e cartão do candidato	Pessoal interno;	I
Desastres naturais podem destruir ou corromper os servidores e as estações de trabalho.	Natureza	I
INTEGRIDADE		
AMEAÇA	**AGENTE DE AMEAÇAS**	**ORIGEM**
Adulteração intencional de dados	Pessoal interno; *Hacker;*	V
Entrada de dados errôneos no sistema de gestão de concurso	Pessoal interno;	I
Erros técnicos no manuseio dos dados	Pessoal interno;	I
Estação de trabalho logada quando da ausência dos funcionários.	Pessoal interno;	I, V

Senhas frágeis podem ser descobertas por terceiros e usadas para modificar dados.	Pessoal externo; *Hacker;*	V
Hackers podem interceptar e alterar os dados.	*Hacker;*	V
Os malotes de provas podem ser violados durante o transporte.	Pessoal interno;	I, V
Os cartões-repostas dos candidatos podem sofrer adulteração ou ser extraviados.	Pessoal interno;	I, V
Os CDs das provas podem ser corrompidos, extraviados ou destruídos, intencionalmente ou não.	Pessoal interno;	I, V
As provas podem ser roubadas durante o transporte.	Pessoal externo;	V
O resultado do certame pode ser manipulado.	Pessoal interno;	V
Os cartões-respostas dos candidatos podem ser molhados, danificados ou rasurados na área dos clocks.	Pessoal externo;	I
Pessoas contratadas para executar as provas podem passar informações errôneas para os candidatos.	Pessoal interno;	I
A empresa pode sofrer ataques de sabotagem no local de armazenamento das provas.	Pessoal externo;	V

Fonte: Elaborado pelos autores - Pesquisa direta, 2017.

Essa etapa foi executada em quatro horas e dez minutos, no dia 13 de outubro de 2016. Começou às 14:00 h e terminou às 18:10 h, na sala de reunião da diretoria geral da organização. Nessa oportunidade, os dados foram coletados através da técnica de *brainstorming* e analisados por meio de técnicas e de instrumentos oriundos da gestão de risco. Somente os membros da equipe FRAAP participaram dessa etapa e foram responsáveis pela aplicação do processo de análise e de avaliação de risco.

Durante o processo de identificação das ameaças, constatou-se que, à medida que as rodadas de exposição das ameaças evoluíam, as ameaças apresentavam-se cada vez mais semelhantes com as já identificadas

e fora do escopo do projeto. Assim, optou-se por descartá-las em comum acordo com os participantes. O Quadro 14 só aglutina as ameaças válidas durante o processo.

Os riscos foram estimados por meio de uma abordagem qualitativa, em virtude do método utilizado e das características da análise dos riscos. Efetuou-se a identificação do nível de exposição do risco com a probabilidade de haver ameaças sobre os impactos e as consequências geradas na organização. Para isso, foi necessário atribuir uma escala de mensuração para as probabilidades, conforme mostra o Quadro 15, e aos impactos, como demonstra o Quadro 16.

Quadro 15: Escalas utilizadas para Probabilidade

Probabilidade		
Nível	**Escala**	**Definição**
A	Alta	Muito provável que a ameaça ocorra
B	Média	Possível que a ameaça ocorra
C	Baixa	Altamente improvável que a ameaça ocorra

Fonte: Elaborado pelos autores, com base nos dados da pesquisa

Quadro 16: Escalas utilizadas para impacto

Impacto		
Nível	**Escala**	**Definição**
3	Alta	Missão inteira ou negócio impactado
2	Média	Perda limitada à única unidade de negócio ou objetivo.
1	Baixa	Negócio como de costume.

Fonte: Elaborado pelos autores - Pesquisa direta - 2017

Com as probabilidades e o impacto com escalas próprias de medição, utilizamos uma matriz de risco para mensurar o nível de cada risco de forma qualitativa. O nível do risco foi determinado pela multiplicação da probabilidade de ocorrência e seu impacto, conforme o Quadro 17.

Quadro 17: Matriz utilizada para mensurar os riscos

PROBABILIDADE	IMPACTO		
	1	2	3
A	Moderado	Alto	Alto
B	Baixo	Moderado	Alto
C	Baixo	Baixo	Moderado

Fonte: Elaborado pelos autores. Pesquisa direta - 2017

A matriz de risco objetivou calcular a estimativa dos riscos e demonstrou a relação entre as probabilidades de ocorrerem riscos e seus impactos, possibilitando um mapeamento gráfico que facilitou a determinação dos níveis dos riscos e norteou a identificação dos controles que fizeram parte da Política de Segurança da Informação. A estimativa dos riscos pode ser visualizada no Quadro 18.

Quadro 18: Matriz de riscos

Ameaça	Probabilidade	Impacto	Nível do risco
Acesso não autorizado às áreas restritas.	B	2	Moderado
Utilização de equipamentos eletrônicos pessoais na área de confecção de provas.	A	2	Alto
As informações de provas podem ficar armazenadas nas impressoras e levadas para manutenção.	B	3	Alto
Os elaboradores de questões de prova podem divulgar suas questões para pessoas não autorizadas.	B	3	Alto
O sigilo das provas pode ser violado por funcionários internos.	B	3	Alto
Informações sigilosas podem ser deixadas à vista em uma mesa.	A	2	Alto
Furto interno de informações.	B	2	Moderado
Falta de uma política de informação.	A	3	Alto
Senhas de e-mail inseguras podem ser descobertas.	B	1	Baixo
Bases de dados podem ser hackeadas por agentes externos.	B	3	Alto
Softwares maliciosos podem roubar informações.	B	2	Moderado
Conversas informais podem revelar informações sigilosas.	B	2	Moderado
Acesso remoto não autorizado às estações de trabalho durante os finais de semana.	C	3	Moderado
Descarte inadequado de informações.	B	3	Alto
Acesso às redes wifi por pessoas não autorizadas.	B	1	Baixo
Programas não confiáveis podem capturar informações.	B	3	Alto
Bases de dados podem ser violadas por funcionários internos.	C	3	Moderado

Informações armazenadas em pendrives podem ser perdidas ou interceptadas.	B	1	Baixo
Funcionários podem ser aliciados a entregar informações.	C	3	Moderado
Pastas compartilhadas inadequadamente podem dar acesso a informações não autorizadas.	B	2	Moderado
Dar informações por telefone a pessoas que não é possível ser identificadas.	B	1	Baixo
Informações sigilosas podem ser armazenadas em celulares e notebooks pessoais.	A	3	Alto
Utilização da infraestrutura de rede compartilhada com toda a organização pode gerar ataques de captura de dados.	B	3	Alto
Divulgação acidental de informações sigilosas.	B	3	Alto
Manipulação intencional do resultado do certame	B	3	Alto
Fiscais de provas podem beneficiar candidatos ou fazer vazarem informações durante a execução das provas.	C	3	Moderado
As provas podem ser violadas antes de começar a ser aplicadas.	B	3	Alto
O sigilo dos nomes dos elaboradores de questões pode ser violado e divulgado.	B	2	Moderado
Falta de energia pode tornar os sistemas inoperantes.	B	3	Alto
Falta ou instabilidade do serviço de internet	B	3	Alto
Falha de infraestrutura de tecnologia da informação e comunicação	B	2	Moderado
Ausência do responsável por extrair informações da base de dados	B	1	Baixo

Arquivos armazenados em diretórios pessoais podem não estar disponíveis para outros funcionários quando necessário.	C	1	Baixo
Indisponibilidade dos servidores	B	2	Moderado
Ataques de negação de serviços	C	3	Moderado
Falha de hardware ou software.	B	2	Moderado
Roubo de equipamentos.	B	2	Moderado
Não localização do elaborador de questão para responder aos recursos.	B	3	Alto
Falta de informações sobre as bases legais a que o cliente é submetido.	B	2	Moderado
Erros técnicos na operacionalização dos dados dos candidatos, locais de provas e cartão do candidato.	B	3	Alto
Adulteração intencional de dados.	C	3	Alto
Entrada de dados errados no sistema de gestão de concurso	B	2	Moderado
Erros técnicos no manuseio dos dados	B	2	Moderado
Estação de trabalho logada quando faltam funcionários.	A	2	Alto
Senhas frágeis podem ser descobertas por terceiros e ser usadas para modificar dados.	B	3	Alto
Hackers podem interceptar e alterar os dados.	B	3	Alto
Os malotes de provas podem ser violados durante o transporte.	B	3	Alto
Os cartões-respostas dos candidatos podem sofrer adulteração ou ser extraviados.	B	3	Alto
Os CDs das provas podem ser corrompidos, extraviados ou destruídos, intencionalmente ou não.	B	3	Alto

As provas podem ser roubadas durante o transporte.	B	3	Alto
Os cartões-respostas dos candidatos podem ser molhados, danificados ou rasurados na área dos clocks.	B	1	Baixo
Pessoas contratadas para a execução das provas podem passar informações errôneas aos candidatos.	B	2	Moderado
A empresa pode sofrer ataques de sabotagem no local onde as provas ficam armazenadas.	C	3	Moderado

Fonte: Elaborado pelos autores - Pesquisa direta - 2017

A matriz de risco objetivou fazer a estimativa dos riscos e demonstrou a relação entre as probabilidades de haver os riscos e seus impactos, o que possibilitou um mapeamento gráfico e facilitou a determinação dos níveis dos riscos e norteou a identificação dos controles que fizeram parte da Política de Segurança da Informação. A estimativa dos riscos pode ser visualizada no Quadro 18.

A estimativa dos níveis de riscos resultou em 26 considerados alto; 20, moderados; e sete, baixos. Dos 53 riscos analisados, 19 tinham controles na organização. No entanto, oito controles já existentes apresentaram-se insatisfatórios para o risco a que foram relacionados. Então, foram construídos novos controles para os 42 riscos residuais.

Os controles de segurança foram construídos de acordo com a norma NBR/ISO 27002:2013 e subsidiaram a criação da Política de Segurança da Informação, que será apresentada na seção 5.2 deste capítulo. Cabe destacar que a quantidade de controles para assegurar um risco varia

de acordo com suas necessidades. Assim, foram 118 controles de segurança que aderiram às seções da norma, como mostra o Quadro 19.

Quadro 19: Conformidade dos controles produzidos com a norma NBR/ISO 27002:2013

Conformidade dos controles com a norma NBR/ISO 27002:2013		
Sessão	**Descrição**	**Quantidade de controles construídos**
5	Políticas de segurança da informação	2
6	Organização da segurança da informação	2
7	Segurança em recursos humanos	19
8	Gestão de ativos	13
9	Controle de acesso	10
10	Criptografia	-
11	Segurança física e do ambiente	24
12	Segurança nas operações	28
13	Segurança nas comunicações	5
14	Aquisição, desenvolvimento e manutenção de sistemas	1
15	Relacionamento na cadeia de suprimento	7
16	Gestão de incidentes de segurança da informação	2
17	Aspectos de segurança da informação na gestão da continuidade do negócio	4
18	Conformidade	1
TOTAL		118

Fonte: Elaborado pelos autores - 2018

De acordo com o Quadro 19, não foram criados controles relacionados à criptografia, porquanto o custo benefício de sua implementação tornou-se alto para a organização, que decidiu assumir os riscos inerentes a esses aspectos. A avaliação dos riscos, que consistiu em decidir qual o risco que a organização assumiria e quais teriam os controles implementados, foi executada junto com o Diretor geral e proprietário da organização.

Etapa Pós-FRAAP

O método adotado nesta pesquisa sugeriu como etapa final que fossem criados planos de ação para mitigar os riscos identificados e elaborado um relatório de aplicação do método. No entanto, devido aos objetivos desta pesquisa, os planos de ações foram substituídos pela criação das políticas de segurança que foram implantadas. Foram necessários quatro dias para executar essa etapa. Na seção seguinte, serão apresentados os controles.

Implementação da Política de Segurança da Informação

A Política de Segurança da Informação foi fundamentada nos riscos ora identificados e elaborada de forma a apresentar a utilização adequada dos recursos da organização, as responsabilidades dos intervenientes, o que deve ser protegido e os procedimentos a serem mantidos e desenvolvidos para salvaguardar as informações organizacionais.

A estrutura desse documento obedeceu aos pressupostos do corpo teórico que embasou este trabalho - a norma NBR/ISO 27002:2013 e as boas práticas sugeridas pelo Tribunal de Contas da União. O documento é dividido em oito seções, a saber:

- Aspectos gerais, que envolve os objetivos, a abrangência, as responsabilidades dos envolvidos e a terminologia utilizada;
- Diretrizes Gerais para a gestão da segurança da informação, gerenciamento de riscos, inventário de ativos e plano de continuidade do negócio;
- Políticas para Segurança de Pessoal;
- Políticas para Segurança Física;
- Politicas para Segurança Tecnológica;
- Procedimentos de Auditória;

- Gerenciamento de riscos;
- Plano de continuidade do negócio.

Devido à extensão do documento, que foi constituído de 35 páginas, contempla 23 objetivos de controle e 118 controles, optou-se por limitar a apresentação dos controles em, no máximo, cinco por cada objetivo de controle. No entanto, serão explicitadas as oito seções que compõem a política e toda e qualquer informação necessária para se entender bem mais esse documento.

Na seção que aborda as políticas para segurança de pessoal, há um conjunto de medidas e de procedimentos que norteiam as diretrizes gerais e específicas, que devem ser observadas por todos os colaboradores da organização e prestadores de serviço, a fim de proteger os ativos da organização e os procedimentos a serem adotados pelo Setor de Recursos Humanos, desde a admissão de um colaborador ou prestador de serviço ao seu desligamento.

A seção de políticas de segurança física apresenta os procedimentos que devem ser seguidos no controle de acesso, nas políticas de mesa limpa, no bloqueio do ecrã e no entorno dos locais onde as provas são elaboradas.

Por fim, a seção de políticas de segurança tecnológica aborda as diretrizes relacionadas à utilização dos sistemas computacionais, de máquinas servidoras, rede de computadores, internet cabeada e wireless, utilização de dispositivos eletrônicos pessoais, controle de senhas e combate a softwares maliciosos.

Aspectos gerais

Nesta seção, apresentam-se os aspectos fundamentais da Política de Segurança da Informação, as definições dos objetivos, a abrangência das políticas, as responsabilidades dos envolvidos e a terminologia utilizada.

Objetivo

O objetivo dessa política é de definir, em nível estratégico, as diretrizes do Programa de Segurança da Informação da organização objeto deste estudo.

Esse documento expressa o posicionamento da organização objeto deste estudo em relação à proteção de suas informações, objetivando prover orientação e apoio aos aspectos de segurança da informação que garantam a integridade, a confidencialidade e a disponibilidade das informações, em conformidade com os requisitos do negócio, as leis e as regulamentações vigentes. Propõe-se a ser uma referência para auditoria, apuração e avaliação de responsabilidades dos intervenientes relacionados à segurança da informação.

Abrangência

Essa política abrange os seguintes aspectos:

I. Segurança de pessoal;
II. Segurança física;
III. Segurança tecnológica.

Responsabilidade dos envolvidos

A segurança da informação é uma responsabilidade de todos os colaboradores da organização, que deverão exercer suas tarefas para garantir o pleno funcionamento dos controles e dos procedimentos estabelecidos, com o intuito de salvaguardar as informações organizacionais.

Responsabilidade do Diretor geral e do executivo

O Diretor geral e o Diretor executivo são responsáveis por assegurar, de forma integral, o estabelecimento da presente política, sua divulgação e comprovação do uso pelos colaboradores e prestadores de serviço. Dentre suas atividades, destacam-se:

I. Promover a segurança organizacional;
II. Aprovar a política de segurança;
III. Avaliar planos de segurança e seu alinhamento com o negócio;
IV. Apoiar as aplicações de sanções decorridas de descumprimento dessa política.
V. Constituir o comitê de segurança da informação.

Responsabilidade do Comitê de Segurança da Informação

O Comitê de Segurança da Informação deve definir e aprovar estratégias e os mecanismos de implantação e métricas de avaliação dessa política, a fim de proporcionar sua melhoria contínua. Dentre suas atividades, destacam-se:

I. Aprovar as normas de segurança, designar os papéis na gestão de segurança, bem como assegurar a implantação do Programa de Gestão de Segurança da Informação.
II. Aprovar a proposta da política de segurança antes de submetê-la à aprovação do corpo diretivo.
III. Aprovar iniciativas internas para aperfeiçoar a segurança da informação.
IV. Acompanhar os incidentes de segurança ocorridos ou as tentativas.
V. Promover a gestão de riscos.

VI. Propor as estratégias de segurança da informação.
VII. Elaborar e implantar políticas e normas de segurança da informação.
VIII. Revisar, acompanhar e reportar incidentes críticos de TI e/ou de segurança da informação.
IX. Manter e garantir o treinamento e a conscientização dos colaboradores quanto ao tema segurança da informação.
X. Promover e implantar teste de conformidade para verificar a adesão normativa e legal.

Responsabilidade da Gerência de Tecnologia da Informação

As principais responsabilidades da Gerência de Tecnologia da Informação são:

I. Definir e implantar controles e tecnologias, objetivando prover a segurança adequada para infraestrutura, redes e comunicação.
II. Definir e implantar controles e tecnologias, com o fim de prover segurança adequada para aplicações, incluindo o controle de acesso lógico, mas sem se limitar a ele.
III. Estabelecer a segurança física para o ambiente de Data Center.
IV. Revisar, monitorar e responder imediatamente aos incidentes de segurança da informação relacionados à TI.
V. Reportar os incidentes de tecnologia da informação e/ou incidentes de segurança da informação críticos, incluindo tentativas de ataques à infraestrutura e aos sistemas aplicativos para a Diretoria Geral, a Diretoria Executiva e o Comitê de Segurança da Informação.
VI. Acompanhar os incidentes de segurança ocorridos ou as tentativas.

VII. Identificar e gerenciar vulnerabilidades de infraestrutura e nos sistemas de informação.

VIII. Avaliar a segurança no ambiente de TI, através de análises de vulnerabilidade ou testes de intrusão independentes, realizados periodicamente, incluindo o estabelecimento de planos de ação corretivos.

IX. Auxiliar a implantação de definições estabelecidas pelo Comitê de Segurança da Informação.

Responsabilidade da Auditoria Interna

A Auditoria Interna será constituída pelo Diretor Geral e pelo Diretor Executivo. Cabe ao Comitê avaliar, de forma periódica, a adesão da organização à política e reportar os eventuais descumprimentos ao Diretor Geral, ao Diretor Executivo e ao Comitê de Segurança da Informação e assegurar que ações corretivas sejam definidas.

Responsabilidade de todos os colaboradores

As principais responsabilidades dos colaboradores são:

I. Cumprir essa política, seu conjunto de documentos derivados e relatar qualquer comportamento que seja contrário às políticas estabelecidas ao Comitê de Segurança da Informação.

II. Administrar, de forma adequada, a segurança das informações custodiadas e/ou pertencentes à organização.

Nesta seção, apresentamos os documentos que se relacionam com a política e as definições sobre os atributos confidencialidade, integridade e disponibilidade.

Políticas de segurança de pessoal

Nesta seção, elencamos um conjunto de medidas e procedimentos de segurança que devem ser cumpridos pelos colaboradores e prestadores de serviço, com o intuito de contribuir para manter a segurança da informação. Foram elaborados oito objetivos de controle, que permearão os riscos identificados, como demonstra o Quadro 20.

Quadro 20: Objetivos de controle para proteger a dimensão 'pessoas'

DIMENSÃO PESSOAS	
Descrição do controle	**Objetivos**
Processo de admissão	Assegurar que candidatos e prestadores de serviços entendam suas responsabilidades e estejam de acordo com os papéis para os quais foram selecionados.
Levatamento de dados pessoais	Levantar o perfil dos candidatos a funções críticas na organização.
Entrevista de admissão	Assegurar que os candidatos e os prestadores de serviços estejam conscientes e cumpram com suas responsabilidades pela segurança da informação.
Credencial de segurança	Assegurar que os colaboradres só obtenham as permissões devidas ao exercicio de sua função.
Treinamento em segurança da informação	Garantir a execução de treinamentos, a educação e a conscientização apropriadas para manter a segurança da informação.
Processo de desligamento, férias e licença	Proteger os interesses da organização como parte do processo de mudança, interrupção ou encerramento da contratação.
Processo de liberação de permissão	Estabelecer responsansabilidades para as concessões de permissão de acesso às informações confidenciais e críticas da organização.
Entrevista de desligamento	Garantir o sigilo das informações organizacionais.

Fonte: Elaborado pelos autores, com base nos dados da pesquisa - 2017

Objetivo

Os controles implementados nesta seção objetivam reduzir os riscos de erros humanos, como furto, roubo, apropriação indébita, fraude ou uso inapropriado dos ativos da organização objeto deste estudo. Visam prevenir e neutralizar as ações de pessoas que possam comprometer a segurança da organização, com a adoção de medidas de proteção compatíveis com sua realidade.

Todos os colaboradores devem estar cientes, de maneira formal, de suas responsabilidades com a segurança da informação e devem participar das atividades de conscientização e qualificação profissional em temas de segurança.

O processo de admissão

Para selecionar os candidatos que exercerão as funções críticas ou ligadas à tecnologia da informação, devem-se adotar critérios rígidos, com o propósito de selecionar pessoas reconhecidamente idôneas e sem antecedentes que possam comprometer a segurança da organização.

Alguns controles estabelecidos são demonstrados a seguir:

I. A organização não admite estagiários no exercício de atividades diretamente relacionadas com os processos críticos, gerenciamento de servidores e desenvolvimento de softwares;

II. Os colaboradores e os prestadores de serviços deverão assinar o termo de compromisso, a fim de cumprir a política de segurança.

III. Os colaboradores deverão ser informados formalmente quanto os seus deveres de manter sigilo, mesmo quando desligado, sobre todos os ativos de informações e de processos da organização.

IV. Os prestadores de serviços deverão assinar o termo de confiden-

cialidade antes de ter acesso a qualquer informação da organização.

V. Os prestadores de serviços deverão comprovar qualificação técnica que o credencie para a execução dos serviços.

Levantamento de dados pessoais

Toda contratação para cargos considerados críticos e para o setor de Tecnologia da Informação deverá ser precedida de um levantamento de dados do candidato, com o intuito de verificar antecedentes ou comportamentos suspeitos que possam ir de encontro às diretrizes de segurança.

Alguns controles estabelecidos são demonstrados a seguir:

I. O levantamento de dados pessoais será executado para todos os candidatos a ocuparem cargos críticos ou no setor de Tecnologia da Informação.

II. O levantamento deverá ser realizado em fontes públicas da internet. É obrigatória a análise dos perfis de redes sociais.

Credenciais de segurança

Todos os colaboradores deverão ser identificados e receber credenciais de acesso às informações que o restrinjam a visualizar e a utilizar informações a que tenham direito. A concessão de credenciais deverá ser realizada por intermédio de solicitação formal e ter tempo de validade.

Alguns controles estabelecidos são demonstrados a seguir:

I. Os colaboradores serão identificados por meio de uma credencial (perfil apropriado) que os habilite a ter acesso às informações sensíveis dos servidores da organização, de acordo com a clas-

sificação do grau de sigilo da informação e, consequentemente, com o grau de sigilo compatível com o cargo e/ou a função a ser desempenhada.

II. A credencial de segurança só é concedida pelo setor de Tecnologia da Informação e é fundamentada na necessidade de conhecimento técnico dos aspectos inerentes ao exercício funcional e na análise da sensibilidade do cargo e/ou função.

III. As credenciais de segurança terão validade máxima de um ano. Esse prazo poderá ser prorrogado por igual período, quantas vezes forem necessárias, por ato da Gerência de Tecnologia da Informação.

Treinamento em Segurança da Informação

Todos os colaboradores deverão ser treinados e conscientizados continuamente sobre as diretrizes, as normas e os procedimentos existentes na Política de Segurança da Informação. Isso deve ser feito, obrigatoriamente, quando da alteração ou adição de políticas.

Alguns controles estabelecidos são demonstrados a seguir:

I. Nos treinamentos de segurança, todas as diretrizes, as normas e os procedimentos relativos ao manuseio de informações sigilosas deverão ser apresentados, com o propósito de desenvolver e manter uma conscientização de segurança efetiva.

II. Os colaboradores deverão ser orientados sobre as técnicas de Engenharia Social e seu comportamento com as partes externas.

III. Todo colaborador deverá ser treinado, quando for admitido na organização, e passar por reciclagem, pelo menos, uma vez por ano.

IV. Os treinamentos só serão feitos uma vez, revisados, quando necessário, e disseminados em plataforma de ensino online, com o

intuito de garantir a isonomia de informação e utilização quando for preciso.

Processo de desligamento, férias e licença

As credenciais de segurança e o acesso a locais restritos só serão permitidos a colaboradores que estejam em efetivo exercício de suas funções.

Alguns controles estabelecidos são demonstrados a seguir:

I. Todo colaborador que for desligado terá suas credenciais e acesso aos equipamentos e físicos e lógicos revogados.
II. Todo colaborador que estiver de férias ou de licença terá suas credenciais e seus acessos físicos e lógicos suspensos.
III. O acesso desses colaboradores às instalações da organização será restrito às áreas de acesso público.
IV. Todo ativo da organização deverá ser devolvido ao setor responsável por ele

Nessa seção, também foram definidos os deveres dos colaboradores, chefes de setores e prestadores de serviços e atribuídas suas devidas responsabilidades quanto aos ativos da organização e ao cumprimento efetivo dos controles estabelecidos. A seguir, são descritas as responsabilidades gerais e dos chefes de setores.

Responsabilidades gerais

São consideradas responsabilidades gerais:

I. Todo setor que detém os ativos de processamento e de informação é responsável por eles, portanto, deve prover sua proteção.
II. Todos os ativos de informações têm definidos claramente os res-

ponsáveis por seu uso.

III. Toda e qualquer ação que incida no descumprimento das diretrizes de segurança deverão ser informadas imediatamente ao chefe do setor e ao Comitê de Segurança da Informação.

Responsabilidades dos cargos de chefia

As responsabilidades das chefias compreendem, dentre outras, as seguintes atividades:

I. Gerenciar o cumprimento da Política de Segurança da organização por parte de seus funcionários e prestadores de serviço.

II. Identificar os desvios praticados e adotar as medidas corretivas apropriadas.

III. Proteger, em âmbito físico e lógico, os ativos de informação e de processamento da organização relacionados à atuação de seu setor.

IV. Comunicar formalmente à área de Tecnologia da Informação quais os funcionários e prestadores de serviço, sob sua supervisão, que podem acessar as informações sigilosas da organização, seguindo as normas de classificação de informações e os perfis de cada cargo.

V. Comunicar imediatamente ao Comitê de Segurança da Informação o descumprimento por parte de seus supervisionados das normas da política de segurança.

Políticas para Segurança Física

Esta seção traz um conjunto de medidas e procedimentos de segurança, com o intuito de prevenir o acesso não autorizado aos ambientes da

organização, assegurar os ativos permanentes da organização e prevenir danos, perdas, roubo ou interrupção do negócio. Foram elaborados seis objetivos de controle, que permearão os riscos identificados, conforme o Quadro 21.

Quadro 21: Objetivos de controle para a Dimensão Física

DIMENSÃO FÍSICA	
Descrição do controle	**Objetivo**
Controle de acesso	Assegurar que áreas restritas sejam protegidas por controles de entrada para que só pessoas autorizadas tenham acesso.
Mesa e telas limpas	Salvaguardar o sigilo de informações que estejam em dispositivos removíveis, papel e computadores na ausência do colaborador.
Descarte do lixo	Assegurar o descarte adequado das informações.
Segurança dos ativos	Proteger os ativos contra danos e perdas e remoção sem prévia autorização.
Uso dos equipamentos	Assegurar o uso adequado dos equipamentos da organização e definir regras para o uso de equipamentos pessoais dentro da organização.
Uso da sala de confecção de provas	Proteger o sigilo das provas referente aos concursos públicos.

Fonte: Elaborado pelos autores com base nos dados da pesquisa - 2017

Objetivo

Os controles implementados nesta seção objetivam proteger equipamentos e informações contra utilizadores não autorizados a recursos institucionais, envolvendo aspectos de prevenção contra falhas de equipamentos, incêndios, acesso de pessoas a locais restritos, roubos, desastres naturais e outros aspectos fiscos.

Os controles de acesso incidem na proteção de todas as áreas, em especial, nas consideradas restritas e são só abrangem o acesso ao local como também protegem seu perímetro. A proteção deve ser proporcional aos riscos identificados.

Alguns controles estabelecidos são demonstrados a seguir:

I. As responsabilidades pela segurança física da organização são definidas e atribuídas à Gerência Administrativa e Patrimonial.

II. Os recursos e as instalações críticas ou sensíveis devem ser fisicamente protegidos de acesso não autorizado, dano ou interferência, com barreiras de segurança e controle de acesso.

III. Os ambientes onde ocorrem os processos críticos da organização devem ser monitorados, em tempo real, e as imagens registradas por meio de sistemas de CFTV.

IV. O inventário de todo o conjunto de ativos de processamento é registrado e atualizado semestralmente.

V. A entrada e a saída, nas áreas críticas, deverão ser acompanhadas por funcionários autorizados.

VI. A localização das instalações e os servidores da organização não são publicamente divulgados.

VII. O acesso aos componentes da infraestrutura e as atividades fundamentais para o funcionamento dos sistemas das entidades, como painéis de controle de energia, comunicação e cabeamento, são restritos ao pessoal dos setores de Tecnologia da Informação e Manutenção.

VIII. Os sistemas e os servidores deverão ser localizados em área protegida (ambientes de nível 4) e afastada de fontes potentes de magnetismo ou interferência de rádio-frequência.

IX. Não é permitido o acesso remoto a qualquer equipamento de processamento da organização.

X. As impressões devem ser controladas de modo a registrar o destinatário da impressão e o que foi impresso.

Mesa e tela limpas

Alguns controles estabelecidos são demonstrados a seguir:

I. As informações confidenciais ou críticas, seja em formato de papel ou digital, deverão ser guardadas em locais seguros quando não estiverem em uso.

II. As impressoras só devem ser utilizadas por pessoas autorizadas, e as informações confidenciais ou críticas deverão ser retiradas imediatamente.

III. As estações de trabalham deverão ser mantidas, desligadas ou protegidas com mecanismo de travamento de tela e senhas, quando não estiverem em uso.

Descarte do lixo

Alguns controles estabelecidos são demonstrados a seguir:

I. O lixo em papel gerado nos locais de acesso restrito deverá ser descartado de forma adequada.

II. Os lixos gerados na sala de confecção de provas de concursos públicos deverão permanecer na sala, armazenados em locais próprios e só devem ser descartados depois que as provas forem realizadas.

III. Os colaboradores deverão executar a limpeza da lixeira virtual de sua estação de trabalho constantemente.

Uso da sala de confecção de provas

Alguns controles estabelecidos são demonstrados a seguir:

I. É de responsabilidade do chefe de confecção de provas super-

visionar e monitorar o acesso a esse local, bem como a posse da chave de acesso.

II. Somente é permitida a entrada em pares de colaboradores devidamente autorizados.

III. O acesso deverá ser precedido da identificação na portaria e registrado no livro de controle assinado pelo vigilante em atividade.

IV. É proibido usar qualquer dispositivo eletrônico pessoal nesse ambiente. Eles devem ser guardados com o vigilante em atividade.

V. É proibido usar internet ou qualquer tipo de dispositivo de armazenamento removível que não seja disponibilizado pela da organização.

VI. Tanto o perímetro desse ambiente quanto seu interior são monitorados por câmeras de vigilância.

VII. É vedada a remoção de impressoras sem a autorização, por escrito, do chefe de confecção de provas.

VIII. É proibido consumir alimentos, bebidas ou cigarros.

Políticas para Segurança Tecnológica

Nesta seção, apresentam-se as normas e os procedimentos que envolvem os aspectos de prevenção contra a interceptação e a modificação de informações, a fim de proteger o sigilo no tráfego dos dados na rede, a alteração de software, as invasões em servidores e sistemas e a correta utilização de equipamentos de armazenamento. Foram elaborados nove objetivos de controle, expostos no Quadro 22.

Quadro 22: Objetivos de controle para a Dimensão Tecnológica

DIMENSÃO TECNOLÓGICA	
Descrição do controle	**Objetivo**
Sistemas	Estabelecer a proteção dos sistemas computacionais utilizados na organização.
Máquinas servidoras	Assegurar a proteção de acesso aos recursos e às informações armazenadas nos servidores.
Mensagens eletrônicas	Assegurar a utilização correta de transferência de informações por meio digital.
Internet	Estabelecer procedimentos e regras para o uso adequado da internet.
Utilização da rede e seus serviços	Proteger as informações de interceptações e de destruição e estabelece o uso adequado dos recursos de rede.
Controle de acesso lógico (baseado em senhas)	Estabelecer níveis de proteção de acesso aos recursos computacionais.
Computação pessoal	Assegurar a proteção das informações quanto ao armazenamento indevido em dispositivos pessoais.
Cópias de segurança	Proteger as informações sensiveis por meio de copias de segurança garantindo a continuidade do negócio.
Combate a vírus e a walmare	Assegurar procedimentos para o combate de invaões e roubo de informações.

Fonte: Elaborado pelos autores, com base nos dados da pesquisa - 2017

Objetivo

Os controles implementados, nesta seção, objetivam proteger e garantir o correto funcionamento das operações de manipulação e processamento das informações e estabelecer medidas que possibilitem o monitoramento e a identificação de tentativas de ataque às informações e aos recursos computacionais.

Diretrizes gerais

Algumas diretrizes gerais estabelecidas são demonstradas a seguir:

I. As informações devem ser protegidas de acordo com o seu valor, sua sensibilidade e criticidade. Para isso, a organização deve manter um sistema de classificação da informação.

II. Os dados, as informações e os sistemas de informação da organização devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, o sigilo e a disponibilidade desses bens.

III. As violações de segurança devem ser registradas. Esses registros são analisados periodicamente para os propósitos de caráter corretivo, legal e de auditoria.

    a. Cada tipo de registro será analisado mensalmente ou quando necessário. Os registros devem ser protegidos e armazenados de acordo com sua classificação e mantidos sob a custódia do Setor de Tecnologia da Informação.

    b. Os tipos de registros mantidos pela organização são:

        i. Registros de sistemas operacionais – *login, logout*, acesso a arquivos do sistema, dentre outros.

        ii. Registros de aplicativos – registros de transações realizadas por servidores Web e banco de dados.

        iii. Registros do sistema de detecção de invasão – tentativas de invasão da rede externa para a rede interna e vice-versa.

IV. Os sistemas e os recursos que suportam funções críticas para operacionalizar a organização devem assegurar a capacidade de re-

cuperação nos prazos e nas condições definidas em situações de contingência.

V. O inventário sistematizado de toda a estrutura que serve como base para manipular, armazenar e transmitir os ativos de processamento deve ser registrado e atualizado semestralmente.

Máquinas servidoras

Alguns controles estabelecidos são demonstrados a seguir:

I. O acesso lógico ao ambiente ou aos serviços disponíveis em servidores é controlado e protegido. As autorizações são revistas, confirmadas e registradas continuadamente. O responsável pela autorização ou confirmação da autorização é claramente definido e registrado. Todas as exceções devem ser aprovadas pelo gerente de Tecnologia da Informação.

II. Os acessos lógicos deverão ser registrados em logs, que são analisados mensalmente.

III. Serão adotados procedimentos sistematizados para monitorar a segurança do ambiente operacional, principalmente no que diz respeito à integridade dos arquivos de configuração do sistema operacional. Devem existir medidas preventivas, como procedimentos detectivos que possibilitem identificar qualquer anomalia.

IV. Os eventos são armazenados em relatórios de segurança (logs), de modo que sua análise possibilite a geração de trilhas de auditoria a partir desses registros. Todos os registros são mantidos pela área de Tecnologia da Informação, em local seguro e centralizado.

V. A proteção lógica adicional (criptografia) é adotada para evitar o acesso não autorizado às informações, segundo classificações de segurança definidas para as informações.

VI. São utilizados somente softwares autorizados pela Gerência de Tecnologia da Informação nos equipamentos da organização. Sua distribuição e instalação são controladas.

Controle de acesso lógico (baseado em senha)

Alguns controles estabelecidos são demonstrados a seguir:

I. Todos os usuários e as aplicações que necessitem ter acesso a recursos da organização são identificados e autenticados.

II. Não é permitido a nenhum usuário obter direitos de acesso de outro usuário.

III. As autorizações são definidas de acordo com a necessidade de desempenho das funções e considerando o princípio dos privilégios mínimos (ter acesso apenas aos recursos ou sistemas necessários para a execução de tarefas).

IV. As senhas são individuais, secretas, intransferíveis e protegidas com grau de segurança compatível com a informação associada.

V. O sistema de controle de acesso deve ter mecanismos que impeçam a geração de senhas fracas ou óbvias.

VI. As senhas deverão seguir os seguintes critérios:

   a. O conjunto de caracteres permitidos deve incluir letras (maiúsculas e minúsculas), números e caracteres especiais;

   b. Tamanho mínimo de oito caracteres;

   c. Prazo de validade de 120 dias;

   d. Restrições específicas para cada ambiente, aplicação ou plataforma poderão ser adotadas, se necessárias;

VII. Os usuários são bloqueados depois de 35 dias sem acesso e/ou três tentativas sucessivas de acesso malsucedidas.

VIII. O sistema de controle de acesso deve solicitar nova autenticação depois de uma hora de inatividade da sessão (time-out).

Computação pessoal

Alguns controles estabelecidos são demonstrados a seguir:

I. Informações sigilosas, corporativas ou cuja divulgação possa causar prejuízo à organização só são utilizadas em equipamentos da organização onde foram geradas ou nos que ela autorizou com controles adequados.

II. As informações armazenadas em meios eletrônicos deverão ser protegidas contra danos, furtos ou roubos e devem ser adotados procedimentos de backup, definidos em documentos específicos.

Auditoria

A Política de Segurança da Informação é um documento incremental que deverá ser verificado periodicamente, a fim de verificar o cumprimento das diretrizes, das normas e dos procedimentos estabelecidos. Nesse sentido, foram elaborados dois questionários, de acordo com a norma NBR/ISO 27002:2013, cujo objetivo foi o de mensurar os aspectos de segurança e o cumprimento das diretrizes desenvolvidas.

É de responsabilidade da Direção Geral e da Diretoria Executiva constituir a comissão interna, que deverá ser formada por colaboradores multidisciplinares que executem uma auditoria anualmente. Dentre as responsabilidades da comissão interna de auditoria, destaca-se o monitoramento das ações necessárias para enquadrar a organização nos aspectos de segurança.

Implantação

O processo de implantação começou depois que o Setor Jurídico da organização validou as políticas de segurança, e corpo diretivo o aceitou. Foram realizadas ações que objetivaram capacitar todos os colaboradores da organização a conhecerem as políticas de segurança a serem seguidas. Sua implantação foi formalizada por meio da Resolução nº 09/2016, de 20 de novembro de 2016, expedida pela Direção Geral, que instituiu a Política de Segurança da Informação na organização e responsabilizou todos os colaboradores por seu cumprimento.

No mesmo dia em que as políticas foram formalizadas na organização, houve uma reunião com todos os gerentes de setores, com o intuito de apresentar a resolução aos colaboradores do seu setor e de responsabilizá-los pela disseminação das novas práticas de segurança. Nessa oportunidade, foi apresentado o plano de capacitação dos colaboradores sobre as novas práticas e políticas a serem seguidas, que contemplou dois cursos: o primeiro destinado aos colaboradores diretamente envolvidos no processo analisado nesta pesquisa, e o segundo, para todos os colaboradores da organização.

Os cursos supramencionados foram construídos nos padrões do ensino a distância e ministrados por meio da plataforma de educação a distância da própria organização. Ambos os cursos têm uma carga horária de 40 horas, diferenciam-se, em forma e em profundidade, dos conteúdos abordados de acordo com seu público-alvo e podem ser utilizados a qualquer momento pela organização, seja para reciclagem ou para a contratação de novos colaboradores.

Convém enfatizar que, apesar de a política ter sido implantada formalmente, o processo de readequação de alguns procedimentos e de conscientização dos colaboradores aconteceu de forma gradativa e

interativa, e o comitê de segurança da informação tem a responsabilidade de executar e de acompanhar ações que possibilitem que os colaboradores conheçam amplamente as normas e as diretrizes a serem seguidas. Nesse sentido, foi solicitada ao setor de Marketing a confecção de cartilhas, folhetos e mídias digitais para disseminar as boas práticas a serem seguidas.

Breves considerações

Em um mundo globalizado, cujas fronteiras são transpostas pelas redes de comunicação, a informação, independentemente de seu formato, é o bem de maior valor de uma organização moderna e vital para qualquer organização que deseja se manter competitiva. Por essa razão, deve estar segura contra as inúmeras ameaças informacionais que possam incidir sobre seus negócios. Nesse sentido, esta obra procurou respostas para este questionamento: **como implementar e implantar a segurança da informação em uma organização?**

Para isso, foi construído um processo que orientou, de forma sistematizada, as ações necessárias para a execução de uma política de segurança em uma organização. É importante ressaltar que o processo supramencionado foi construído de acordo com as particularidades e as características da organização objeto deste estudo de caso e pode ser adaptado por outras organizações que desejem implantar e executar sua Política de Segurança da Informação.

Durante a execução do processo, percebemos que, dentre outros aspectos que possibilitaram atingir os objetivos deste trabalho, a efetiva participação da alta direção, o envolvimento do Setor Jurídico da organização e a constituição do Comitê de Segurança da Informação foram determinantes para que os colaboradores aceitassem participar do processo e se engajassem nele.

Dentre as atividades que compõem o processo, a análise e a avaliação de riscos foram consideradas como as mais críticas a serem executadas, porque compreenderam a identificação dos ativos, das vulnerabilidades, das ameaças e dos riscos relacionados ao processo analisado, conforme já

referido nesse estudo. Essas atividades são apoiadas por metodologias que proporcionam um conjunto de atividades coordenadas, com o intuito de potencializar os resultados a serem alcançados.

Para proceder à análise e à avaliação de riscos, adotou-se a metodologia FRAAP sugerida por Peltier (2010), direcionada ao processo de elaboração e execução de concursos públicos, que possibilitou identificar 53 ameaças. Depois de correlacionar as ameaças aos seus respectivos atributos de informação, obtivemos 28 relacionadas à confidencialidade; 12, à disponibilidade; e 13, à integridade. Em seguida, classificaram-se as ameaças de acordo com os parâmetros predefinidos de probabilidade e impacto, cujo resultado possibilitou a construção da matriz de risco, que determinou os níveis dos riscos sob uma abordagem qualitativa. Em seguida, foram criados os controles de segurança para cada risco identificado e selecionados os controles da norma NBR/ISO 27002:20013 relacionados a cada risco, objetivando minimizá-los.

Consideramos que a utilização do método FRAAP foi fundamental para o alcance dos resultados desta pesquisa, porquanto proporcionou um contínuo envolvimento da alta direção da organização durante todo o processo e possibilitou que os dados da pesquisa fossem coletados em um ambiente democrático, participativo e colaborativo, para que os riscos fossem elucidados pelos próprios colaboradores, o que gerou uma sensação coletiva de responsabilidade sobre eles.

Conforme já referido, independentemente do processo de análise e de avaliação de riscos, a abordagem a ser utilizada é um processo crítico e complexo. No entanto, a utilização da metodologia FRAAP possibilitou que a extração e a análise dos dados fossem feitas em um período de quatro dias, cinco horas e 26 minutos. Assim, foi possível direcionar mais esforços na construção e na seleção dos controles de segurança. Outro fator que merece ser destacado refere-se à abordagem qualitativa utilizada pelo

método, que gerou resultados satisfatórios e confirmou a criticidade do processo analisado para a organização.

Por meio do cruzamento da probabilidade de ocorrência de um risco e seu impacto na organização, foram identificados: 26 riscos considerados altos, 20, moderados, e sete, baixos. O agrupamento dos riscos na escala qualitativa adotada possibilitou uma melhor visualização e compreensão pela Alta Direção dos riscos aos quais a organização está sujeita, o que facilitou a tomada de decisão quanto a aceitar ou não os riscos. Foram criados 118 controles de segurança, que subsidiaram a construção da Política de Segurança da Informação. No entanto, a organização optou por não implementar controles de criptografia, por causa do alto custo de sua implementação, e passou a assumir esses riscos.

A Política de Segurança da Informação abrangeu as dimensões humana, física e tecnológica. Esse documento descreveu a forma adequada de utilizar os recursos, as responsabilidades dos intervenientes, o que deve ser protegido e concebeu procedimentos a serem adotados pela organização, a fim de assegurar a confidencialidade, a integridade e a disponibilidade de suas informações.

A construção dos treinamentos sob os moldes da educação a distância possibilitou uma redução de custo para a organização, bem como proporcionará seu reuso a qualquer momento, seja na contratação de um novo colaborador ou até mesmo para reciclar antigos colaboradores. Nesse sentido, acreditamos ter mitigado grandes dificuldades que a organização poderia encontrar em manter todos os colaboradores treinados para cumprir seu papel de manter a segurança da informação.

Embora as políticas tenham sido implantadas na organização, e os procedimentos determinados sejam cumpridos por todos os colaboradores, os riscos não deixaram de existir, e por menores que sejam, podem comprometer a segurança da organização. Assim, entendemos

que o comitê de segurança da informação assume um papel fundamental na segurança e deve, dentre outras atribuições, empreender esforços para supervisionar, monitorar e atualizar em espaços de tempo regulares ou quando necessário às políticas de segurança.

Para verificar futuramente a adesão da organização aos aspectos de segurança da informação, foram elaborados dois questionários fechados de múltipla escolha, fundamentados na norma NBR ISO 27002:2013, que irá mensurar possíveis deficiências e desacordos com as diretrizes, as normas e os procedimentos presentes na Política de Segurança da Informação da organização.

É importante ressaltar que este estudo não exaure o assunto. Futuras ações que visam à sua continuidade deverão ser implementadas, com o objetivo de acompanhar a maturidade da organização quanto à segurança da informação. Sugerimos que, depois de consolidar uma nova cultura organizacional voltada para a segurança da informação, seja revisto e refinado o processo de classificação das informações, porque não foi possível obter com clareza os requisitos desejáveis pela organização.

Por fim, é necessário implementar planos de ações para os riscos considerados altos, com o intuito de dar respostas rápidas e eficazes aos seus intervenientes, e um plano de continuidade dos negócios que possibilite o funcionamento da organização em um incidente de informação. Este estudo abriu a possibilidade de a organização ampliar a segurança da informação para outras áreas de negócio, porquanto é possível replicar a metodologia utilizada, e que a Política de Segurança da Informação seja um documento interativo e abrangente.

Referências bibliográficas

ALEXANDRIA, João C. S de. **Gestão de Segurança da Informação:** uma proposta para potencializar a efetividade da segurança da informação em ambiente de pesquisa científica. São Paulo, 2009. 193f. Tese (Doutorado em Tecnologia Nuclear) – Universidade de São Paulo, São Paulo, 2009.

ALBERTS, C. J.; DOROFEE, A. J. **Managing Information Security Risks:** the OCTAVE approach. Boston: Addison-Wesley, 2002.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 17799: Técnicas de segurança e código de práticas para a gestão de segurança da informação**. Rio de janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 27002: Tecnologia da Informação, técnicas de segurança e código de prática para controles de segurança da informação**. Rio de janeiro, 2013.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR 27005: Tecnologia da Informação – Técnicas de segurança – Gestão de riscos de segurança da informação.** Rio e janeiro, 2011.

AMARAL, L. A. M. **PRAXIS**: um referencial para o planejamento de sistemas de informação**.** Tese de Doutorado apresentada na Universidade do Minho, Portugal, 1994.

ARAÚJO, Wagner Junqueira de. **A segurança do conhecimento nas práticas da gestão de segurança da informação e da gestão do conhecimento**. Tese de Doutorado em Ciência da Informação – Universidade de Brasília, 2009.

BARBER, B. DAVEY, J. **The use of the CCTA risk analysis and management methodology CRAMM in health information systems**, in Proc MEDINFO 92, p. 1589–1593, 1992.

BARNARD. C. I. **As funções do executivo**. São Paulo: Atlas, 1971.

BARMAN, S. **Writing information security policies**. in: New Riders. 2002.

BEAL, A. **Gestão estratégica da informação:** como transformar a informação e a tecnologia da informação em fatores de crescimento e de alto desempenho nas organizações. São Paulo: Atlas, 2012.

_____, **Segurança da informação:** princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2005.

CARDOSO, A. M. P. **Pós-modernidade e informação:** conceitos complementares? perspectivas em Ciência da Informação. Belo Horizonte, v. 1, n. 1, p. 63-79, jan./jun. 1996.

COELHO, F.E.S; ARAUJO, L.G.S; BEZERRA, E.K. **Gestão da segurança da informação.** 2. ed. Rede nacional de ensino e pesquisa, 2014. 198 p.

CHIAVENATO, I. **Introdução à Teoria Geral da Administração:** uma visão abrangente da moderna administração das organizações. Rio de Janeiro: Elsevier, 2003.

DANTAS, L. M. **Segurança da informação:** uma abordagem focada em gestão de riscos. Olinda: Livro Rápido, 2011.

DARYUS. **Pesquisa nacional de segurança da informação**. Disponível em:< http://conteudo.daryus.com.br/pesquisa-nacional-de-seguranca-da-informacao-2014>. Acesso em: 11 de setembro de 2016.

DAVENPORT, T. H. **Reengenharia de processos**. Rio de Janeiro: Campus, 1994.

DIAS, C. **Segurança e auditoria da tecnologia da tecnologia da informação**. Rio de Janeiro: Axcel, 2000.

DRUCKER, P. F. **O advento da nova organização**. In: HAVARD Business Review. Rio de Janeiro: Campus, 2000. p. 09-26.

FERNANDES, J. H. C. **Introdução à gestão de riscos de segurança da informação.** Texto desenvolvido para suporte das atividades de Ensino do Programa de Pesquisas e Formação de Especialistas, Universidade de Brasília (UNB), Brasília, 2009.

FONTES, E. G. L. **Políticas de segurança da informação.** Rio de Janeiro: RNP/ESR, 2015.

GIL, A. C. **Como elaborar projetos de pesquisa**. 5. ed. São Paulo: Atlas, 2009.

ISACA. **Information systems audit and control association**. **O estado de segurança cibernética:** implicações para 2016. Disponível em: < http://www.isaca.org/cyber/Pages/state-of-cybersecurity-implications-for-2015.aspx?cid=pr_1107003&appeal=pr>. Acesso em: 20 de Setembro de 2016.

_____, COBIT 5 RISK IT: **framework manage IT risk**. ISACA, 2016

_____, COBIT 5: **Modelo corporativo para governança e gestão de TI da organização**. Rolling Meadows: ISACA, 2012.

_____, COBIT 5 for Risk. **Rolling Meadows**, IL: ISACA, 2013a.

_____. **Transforming cybersecurity using** Cobit 5. Rolling Meadows, IL: ISACA, 2013b.

LAUREANO, M. A. P. **Gestão de Segurança da Informação**, 2005. Disponível em:

<http://www.mlaureano.org/aulas_material/gst/apostila_versao_20.pdf> Acessado em 15 de setembro de 2011.

LESCA, Humberto. ALMEIDA, Fernando C. de. **Administração estratégica da informação**. Revista de Administração – RAUSP, São Paulo, v.29, nº3, p. 66-75, jul./set. 1994.

LYRA, Maurício R. **Segurança e auditoria em sistemas de informação**. Rio de Janeiro:

Ciência Moderna, 2008.

MATOS, L. S. **Dicionário de Filosofia Moral e Política**. Instituto de Filosofia da Linguagem. 2001. Disponível em: <http://ifilnova.pt/file/uploads/20b80ffab42e5adbe998e8d35b6450a0.pdf>. Acesso em: 13 mai. 2016.

MARCIANO, João Luiz Pereira. **Segurança da informação**: uma abordagem social. Tese de Doutorado em Ciência da Informação – Universidade de Brasília, 2006**.**

MAXIMINIANO, A. C. A. **Introdução à Administração**. São Paulo: Atlas, 2010.

MCGEE, J. PRUSAK, L. **Gerenciamento estratégico da informação:** aumente a competitividade e a eficiência de sua empresa utilizando a

informação como uma ferramenta estratégica. Rio de Janeiro: Campus, 1994.

MITNICK, Kevin, D.; SIMON, Willian L. Mitnick. **A arte de enganar:** ataques de hackers: controlando o fator humano na segurança da informação. São Paulo: Makron Books, 2003.

MOODY, Daniel; WALSH, Peter. **Measuring the value of information:** an asset evaluation approach. European Conference on Information Systems, 1999.

MORESI, E. A. D. **Delineando o valor do sistema de informação de uma organização**. Ciência da Informação, Brasília, v.29, n.1, jan./abr. 2000.

NAKAMURA, Emílio; GEUS, Paulo. **Segurança de redes em ambientes corporativos**. São Paulo: Berkeley Brasil, 2002.

OLIVEIRA, D. **Estrutura organizacional:** sistemas, organizações e métodos: uma abordagem gerencial. São Paulo: Atlas, 2001.

OLIVEIRA, Sidnei. **Geração Y:** o nascimento de uma nova geração de líderes. São Paulo: Integrante Editora, 2010.

OLIVEIRA, W. **Segurança da informação:** técnicas e soluções. São Paulo: Atlas, 2001.

PELTIER, T. R. **Information security policies, procedures, and standards:** Establishing an Essential Code of Conduct**.** USA: Aurebach Publications, 2001.

_____, **Information security risk analysis**. 2. ed. United States: CRC Press, Taylor & Francis Group, 2005.

_____, I**nformation Security Risk Analysis** – 3. ed. United States: CRC Press, Taylor & Francis Group, 2010.

PIETERS, W… (et al). **Current established risk assessment methodologies and tools.** UT publication and University of Twent (2013).

PWC. **A global state of information security. 18. ed.** Disponível em: < http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey/data-explorer.html>. Acesso em: 20 de setembro de 2016.

RICHARDSON, J. R. **Pesquisa social:** métodos e técnicas. 3. ed. São Paulo: Atlas, 2012.

SÊMOLA, Marcos. **Gestão da segurança da informação: uma visão executiva** – Rio de Janeiro: Campus, 2003.

_____, **Gestão da segurança da informação: uma visão executiva.** 2 ed. Rio de Janeiro: Elsevier, 2014.

SILVA, T. P.; CARVALHO, H.; TORRES, B. C., **Segurança dos sistemas de informação:** gestão estratégica da segurança empresarial. Portugal: Centro Atlântico, 2003.

STAIR, R.; REYNOLDS, G. **Princípios de sistemas de informação:** uma abordagem gerencial. Rio de Janeiro: LTC, 2002.

SUMMERS, R. C. **Secure computing:** threats and safeguards. New York: McGraw-Hill, 1997.

TRIBUNAL DE CONTAS DA UNIÃO. **Boas práticas em segurança da informação**. 4. ed. Brasília. 2012.

VAN WEGEN, Bert. DE HOOG, Robert. **Measuring the economic value of information system**. USA: Journal of Information Technology, v. 11, n.3, p. 247-260, Sept 1996.

APÊNDICE: processo de implementação e implantação de uma política de segurança da informação