ORIENTAÇÕES PARA A IMPLEMTAÇÃO DO SISTEMA DE GESTAO DA INFORMAÇÃO COM BASE NA ISSO 27001 E O CICLO PDCA

Eviana A L Cordeiro, Fatec São Caetano do Sul, evianacordeiro@yahoo.com.br
Gisele Cristina Martins, Fatec São Caetano do Sul, gisele242011@hotmail.com
Elias Ramos, Fatec São Caetano do Sul, elias.ramos777@gmail.com
Nicolas Souza Silva, Fatec São Caetano do Sul, nicolas--silva@outlook.com
Edna Mataruco Duarte, Fatec São Caetano do Sul, edna.duarte@fatec.sp.gov.br

Resumo

O mundo está cada dia mais conectado e unido pela rede mundial de computadores. As empresas que buscam acompanhar as inovações do mercado são mais modernas e com olhar mais voltado para as novas tecnologias. Assim sendo, o objetivo deste artigo é elaborar orientações simples e prática, para implementação do Sistema de Gestão de Segurança da Informação, tendo como base a norma ISO 27001 e o Ciclo PDCA. Essas orientações buscam contribuir com organizações de pequeno e médio porte de diferentes setores, de forma, que possam atingir níveis de proteção adequado para as informações que manejam. Essa pesquisa se caracteriza como bibliográfica, pois foram utilizados em sua construção artigos, capítulos de livros e principalmente a família de normas ISO 27000, que provê as diretrizes para a implementação da Gestão de Segurança da Informação. Ao final, foi possível apresentar uma visão da Gestão de Segurança da Informação associada as fases do Ciclo PDCA, que poderá servir como orientação para sua implementação.

Palavras-chave: Sistema de Gestão de Segurança da Informação, ISO 27001, Ciclo PDCA, Segurança da Informação.

Abstract

The world is increasingly connected and united by the worldwide web of computers. Companies that seek to keep up with market innovations are more modern and look more focused on new technologies. Therefore, the objective of this article is to elaborate simple and practical guidelines for the implementation of the Information Security Management System, based on the ISO 27001 standard and the PDCA Cycle. These guidelines seek to contribute to small and medium-sized organizations from different sectors, so that they can achieve adequate levels of protection for the information they handle. This research is characterized as bibliographical, as articles, book chapters and mainly the ISO 27000 family of standards were used in its construction, which provides guidelines for the implementation of Information Security Management. At the end, it was possible to present a vision of Information Security Management associated with the phases of the PDCA Cycle, which can serve as a guide for its implementation.

***Keywords**: Three to five, separated from each other by a comma, font size 11.*

1. Introdução

Muitas organizações, de ideias inovadoras e com crescente desempenho no mercado, por vezes, negligenciam o investimento em segurança de dados. Isso acontece porque essas

empresas não possuem o montante financeiro das grandes corporações e se sentem invisíveis e longe dos holofotes e atenções dos cibercriminosos. Com isto, minimizam a existência da possibilidade de ocorrência de um vazamento de dados ou roubo de informações, e se tornam alvos vulneráveis. Isto torna cada vez mais evidente a necessidade de todas as empresas, seja ela de grande ou pequeno porte, implantar um Sistema de Gestão de Segurança da Informação, pois em alguns casos, elas podem demorar meses para se recuperarem de um incidente de segurança da informação.

Desta forma, a *International Organizational for Standardization* – ISO, desenvolveu normas com o objetivo de fornecer diretrizes que asseguram a capacidade da organização em oferecer serviços que supram as expectativas de seus clientes e parceiros. Dentre estas normas está a ISO 27001. Essa norma descreve uma série de diretrizes para a implementação de um Sistema de Gestão de Segurança da Informação em uma empresa. Com a norma, é possível inserir diversas camadas de proteção contra incidentes que afetariam a disponibilidade, confidencialidade e/ou integridade das informações da organização, além de identificar de forma contínua as oportunidades de melhoria, aumento da confiança e satisfação dos clientes e parceiros. Ainda, é possível aplicar processos de avaliação de risco, permitindo a identificação de vulnerabilidades que afetariam os ativos da empresa e a elaboração de um plano de ações para prevenir tais problemas.

Levando-se em consideração esses aspectos, é possível inferir que empresas que possuem a certificação ISO 27001 transmitem aos seus clientes e fornecedores que possuem preocupação com os dados sob a sua tutela. Todavia, o processo para implantar estas regulamentações pode, inúmeras vezes, ser algo trabalhoso devido à complexidade para seguir todas as diretrizes impostas na norma. Isto posto, este artigo visa a elaboração de orientações que busca tornar o seu processo de implantação acessível e efetivo para pequenas e médias organizações.

O *Global Risk Report*, elaborado *pelo World Economic Forum*, expõe a necessidade de se implantar normas de segurança devido ao crescimento dos incidentes de segurança da informação. As normas mais conhecidas como a ISO e o *National Institute of Standards and Technology* - NIST, apoiam a implantação de boas práticas de proteção das informações. Contudo, tanto a ISO quanto o NIST não possuem um modelo de fácil compreensão para aplicação de suas diretrizes. Mesmo havendo muitas maneiras de facilitar a implantação desta norma e evitar possíveis incidentes, muitas empresas não possuem estes *frameworks* devido à complexidade de compreensão para aplicação de suas diretrizes, além de não possuírem uma área dedicada à segurança da informação.

Com o objetivo de adquirir níveis de proteção adequados para as informações de uma companhia, faz-se necessário um conjunto de controles e mecanismos de segurança da informação apropriados, visando assegurar que os requisitos do negócio sejam amplamente atendidos. Corroborando com essa visão, o *World Economic Forum* declarou em 2019, no documento *Global Risk Report*, que incidentes envolvendo fraudes e ciberataques estão posicionados em quarto e quinto lugar no *top* 10 em termos de probabilidade de ocorrência.

Assim, esse artigo que tem como objetivo elaborar orientações simples e prática, para implementação do Sistema de Gestão de Segurança da Informação, tendo como base a norma ISO 27001 e o Ciclo PDCA, caracteriza-se como uma pesquisa bibliográfica, na qual foi utilizada uma norma técnica da área de Segurança da Informação, pertencente à família de normas ISO 27000, que provêm as diretrizes corretas para a implantação do Sistema de Gestão de Segurança da Informação, também foram utilizados artigos, livros e outros documentos

para escrita do referencial teórico, e que contribuíram diretamente para sua elaboração.

2. Gestão de Segurança da Informação

Atualmente é possível observar o surgimento de novos modelos de negócios que, impulsionados pelas inovações tecnológicas, possuem dados que se transformaram em ativos fundamentais, capazes de gerar valor para o negócio, com isso, tornou-se essencial que haja uma boa Gestão de Segurança da Informação. Desta forma, a Gestão de Segurança da Informação é uma área importante e que deve estar de acordo com o objetivo geral da empresa além de desempenhar o seu papel, que é o de proteger um dos ativos mais importantes da organização: a informação.

Fontes (2017, p. 24), afirma que "a informação deve ser cuidada por meio de políticas e regras". O autor, ainda, cita que "cada organização, considerando o tipo de negócio e o porte, define uma estrutura adequada para a proteção da informação." Tal estrutura é definida por meio das políticas e regras enumeradas, e é de responsabilidade da área de segurança da informação. Sendo assim, a Gestão de Segurança da Informação pode ser compreendida como o ato de administrar os processos conduzidos pela área de Segurança da Informação que, estando alinhada aos objetivos da empresa, deve atingir o objetivo de proteger suas informações.

De acordo com Sêmola (2014) a Gestão de Segurança da Informação atua conduzindo os processos que visam preservar características primordiais para a proteção da informação, dentre elas: a confidencialidade, a integridade e a disponibilidade. Essas três características formam a sigla CID, mas é comum encontrar em outras literaturas alguns aspectos que também podem ser atribuídos à informação.

Outra característica que pode ser acrescentada à informação é a privacidade. A privacidade define a garantia de reserva da informação que é pessoal, que diz respeito à vida íntima de uma pessoa. A proteção de informações pessoais tem como um dos fundamentos a inviolabilidade da intimidade, da honra e da imagem, de acordo com o Art. 2ª da Lei nº 13.709, de 14 de agosto de 2018 (Brasil, 2018).

A informação pode possuir algumas das características citadas anteriormente. E para preservar as suas características, a norma ABNT NBR ISO/IEC 27001 (2013) sugere "estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação (SGSI)", em suma, incluir o SGSI em um Ciclo PDCA, tendo como base essa premissa que este artigo foi desenvolvido. Cabe ressaltar, que entendemos que um Sistema de Gestão da Informação é algo mais amplo e que requer alguns requisitos que acabam dificultando sua tratativa por organizações de pequeno e médio porte, por este motivo tratamos, neste artigo, de uma forma mais simples e trazendo os aspectos principais para sua elaboração, buscando prover algo mais acessível, e que seja mais próximo da realidade dessas organizações.

Assim, o Ciclo PDCA, segundo Andrade (2003, p 11), "[...] é projetado para ser usado como um modelo dinâmico. A conclusão de uma volta do ciclo irá fluir no começo do próximo ciclo, e assim sucessivamente". Andrade (2003, p. 11), também diz que, "seguindo no espírito de melhoria de qualidade contínua, o processo sempre pode ser reanalisado e um novo processo de mudança poderá ser iniciado". Atualmente, por oferecer uma sequência

lógica e motivar o aumento do conhecimento dos gestores, diversas novas metodologias utilizam alguns conceitos do PDCA, como o *SCRUM* e o *Design Thinking*. Aguiar (2002) descreve também o Ciclo PDCA em quatro etapas, sendo elas: *Plan-Do-Check-Act*, ou em português, Planejamento, Execução, Verificação e Ação.

2.1. A ISO 27001 e a Gestão de Segurança da Informação

Segundo a ISO 27001 (2013), "o Sistema de Gestão de Segurança da Informação preserva a confidencialidade, integridade e disponibilidade da informação por meio da aplicação de um processo de gestão de riscos", mas antes de uma empresa iniciar este processo, ela deve determinar as questões internas e externas que são relevantes para o seu propósito, e ainda deve determinar:

> a) as partes interessadas que são relevantes para o Sistema de Gestão da Segurança da Informação; e b) os requisitos dessas partes interessadas relevantes para a Segurança da Informação. (ISO 27001, 2013)

No âmbito do Sistema de Gestão de Segurança da Informação, as partes interessadas podem ser os funcionários, clientes, fornecedores, governo, investidores, sócios, entre outros. A compreensão destes aspectos possibilita determinar o perímetro do Sistema de Gestão de Segurança da Informação, pois a ISO 27001 (2013) menciona que "a organização deve determinar os limites e a aplicabilidade do sistema de gestão da segurança da informação para estabelecer o seu escopo". Para a definição do escopo, a norma sugere que a organização leve em consideração as questões internas e externas; os requisitos; as interfaces e dependências entre as atividades desempenhadas pela organização e aquelas que são desempenhadas por outra organização (ISO 27001, 2013).

Em suma, a ISO 27001 propõe que o Sistema de Gestão de Segurança da Informação seja pautado na análise do micro e do macroambiente; identificação de todas as partes envolvidas com o SGSI e quais os seus requisitos; levantamento das atividades que são realizadas pela organização e quais são realizadas por terceiros; e a definição do alcance do SGSI, ou seja, do seu escopo.

Contudo, para que o Sistema de Gestão de Segurança da Informação tenha êxito, a ISO 27001 (2013) sugere que "a organização deve estabelecer, implementar, manter e continuamente melhorar um sistema de gestão da segurança da informação". Isso só é possível com a contribuição de todos os envolvidos com o SGSI e com o comprometimento da Alta Direção que deve demonstrar sua liderança e comprometimento (ISO 27001, 2013).

Um outro aspecto relevante e que cabe à Alta Direção é a elaboração de uma política de Segurança da Informação que seja apropriada ao propósito da organização; inclua os objetivos de segurança da informação ou forneça a estrutura para estabelecer os objetivos de segurança da informação; inclua um comprometimento para satisfazer os requisitos aplicáveis, relacionados com segurança da informação; e inclua um comprometimento para a melhoria contínua do sistema de gestão da segurança da informação (ISO 27001, 2013). Os papéis e responsabilidades também precisam ser definidos, pois a ISO 27001 (2013) menciona que "a Alta Direção deve assegurar que as responsabilidades e autoridades dos papéis relevantes para a segurança da informação sejam atribuídos e comunicados".

Na fase de planejamento do Sistema de Gestão de Segurança da Informação, a

organização deve definir e aplicar um processo de avaliação de riscos de segurança da informação (ISO 27001, 2013) e é imprescindível que este processo também defina os critérios para aceitação do risco. O objetivo da análise de risco é encontrar caminhos para que os riscos sejam mitigados, contudo em quase todos os cenários haverá um risco residual, os critérios de aceitação de risco devem detalhar quando um determinado risco será aceito ou não pela organização. No processo de avaliação de riscos é importante que a organização identifique os riscos de segurança da informação aplicando o processo de avaliação do risco de segurança da informação para identificar os riscos associados com a perda de confidencialidade, integridade e disponibilidade da informação dentro do escopo do sistema de gestão da segurança da informação; e identifique os responsáveis dos riscos (ISO 27001, 2013).

Após a identificação dos riscos existentes, deve-se executar a fase de análise dos riscos. Para isso, é necessário que a organização avalie as consequências potenciais que podem resultar se os riscos identificados forem materializados; avalie a probabilidade realística da ocorrência dos riscos identificados e determine os níveis de risco (ISO 27001,2013). Esta análise deve ter um viés matemático, de forma que fique claro o nível de risco. A próxima etapa remete a avaliação dos riscos. Para isso é importante que a empresa compare os resultados da análise dos riscos com os critérios de riscos estabelecidos; e priorize os riscos analisados para o tratamento do risco (ISO 27001, 2013).

Na fase de tratamento dos riscos, a ISO 27001 (2013) sugere que a organização deve "selecionar, de forma apropriada, as opções de tratamento dos riscos de segurança da informação, levando em consideração os resultados da avaliação do risco", e ainda que é preciso "determinar todos os controles que são necessários para implementar as opções escolhidas do tratamento do risco da segurança da informação". Para a escolha dos controles, a norma possui um anexo com diversos controles de segurança da informação que poderão ser elencados, além dos seus objetivos que devem ser mencionados durante o processo de tratamento dos riscos.

Assim que os controles e seus objetivos são definidos, a organização precisa elaborar uma declaração de aplicabilidade que contenha os controles necessários e a justificativa para inclusões, sejam eles implementados ou não, bem como a justificativa para a exclusão dos controles (ISO 27001, 2013). A organização precisa também, segundo a norma, preparar um plano de tratamento dos riscos de segurança da informação (ISO 27001, 2013), este plano se refere à implantação dos controles na organização e precisa ter a aprovação dos responsáveis pelos riscos. A organização deve manter a informação documentada relativa ao processo de tratamento dos riscos de segurança da informação (ISO 27001, 2013).

Para a norma, é importante que os objetivos de segurança da informação sejam estabelecidos (ISO 27001, 2013), tendo estes objetivos um alinhamento com a política de segurança da informação. Estes objetivos devem estar também alinhados com o plano de tratamento de riscos e, para alcançá-los, a norma sugere que a organização determine: "1. o que será feito; 2. quais recursos serão necessários; 3. quem será responsável; 4. quando estará concluído; 5. como os resultados serão avaliados" (ISO 27001, 2013).

Todos os funcionários da organização precisam ser conscientizados da Política de Segurança da Informação, das suas contribuições para a eficácia do sistema de gestão da segurança da informação, incluindo os benefícios da melhoria do desempenho da segurança

da informação e das implicações da não conformidade (ISO 27001, 2013). Mas para que essa conscientização seja eficaz, é necessário haver um plano de comunicação do Sistema de Gestão de Segurança da Informação.

Toda informação do Sistema de Gestão de Segurança da Informação deve ser documentada, contendo os seguintes aspectos:

> Quando da criação e atualização da informação documentada, a organização deve assegurar de forma apropriada: a) identificação e descrição (por exemplo, título, data, autor ou um número de referência); b) formato (por exemplo, linguagem, versão do software, gráficos) e o seu meio (por exemplo, papel, eletrônico); e c) análise crítica e aprovação para pertinência e adequação. (ISO 27001, 2013)

No que tange a operação, a organização deve planejar, implementar e controlar os processos necessários para atender os requisitos de segurança da informação, e para implementar as ações determinadas (ISO 27001, 2013). É nesta fase que é executada a implementação do plano de tratamento dos riscos, todos os controles que foram elencados serão aplicados seguindo o cronograma criado para sua aplicação. Cada responsável deve se comprometer a executar o plano conforme estipulado durante o processo de gerenciamento dos riscos.

Após a implantação do plano de tratamento dos riscos, a organização deve, segundo a ISO 27001 (2013), “avaliar o desempenho da segurança da informação e a eficácia do Sistema de Gestão da Segurança da Informação”, além de conduzir processos periódicos de auditoria interna objetivando identificar a não conformidade. Esta não conformidade pode estar relacionada a diversos aspectos como os requisitos da organização, a política de segurança da informação, legislação vigente, normas, entre outros, por isso é uma etapa importante de ser realizada. A organização deve:

> a) planejar, estabelecer, implementar e manter um programa de auditoria, incluindo a frequência, métodos, responsabilidades, requisitos de planejamento e relatórios. Os programas de auditoria devem levar em conta a importância dos processos pertinentes e os resultados de auditorias anteriores; b) definir os critérios e o escopo da auditoria, para cada auditoria; c) selecionar auditores e conduzir auditorias que assegurem objetividade e imparcialidade do processo de auditoria; d) assegurar que os resultados das auditorias são relatados para a direção pertinente; e) reter a informação documentada como evidência dos programas da auditoria e dos resultados da auditoria (ISO 27001,2013).

A norma recomenda que a Alta Direção também faça uma análise crítica do Sistema de Gestão de Segurança da Informação em intervalos planejados (ISO 27001, 2013), pois diversos aspectos podem mudar com frequência, como por exemplo, as questões internas e externas. Tanto a análise crítica pela Alta Direção e as auditorias internas existem para apoiar a última etapa do ciclo PDCA e que irá garantir que o Sistema de Gestão de Segurança da Informação passe por processos de melhoria contínua, pois segundo a ISO 27001 (2013): “A organização deve continuamente melhorar a pertinência, adequação e eficácia do sistema de gestão da segurança da informação”. Este processo só pode ser realizado após a identificação de não conformidade pela auditoria interna ou por mudanças estratégicas da organização conduzidas pela Alta Direção.

Diante de tanta informação fornecida pela ISO 27001 (2013) com relação ao Sistema de Gestão de Segurança da Informação, fica difícil para organizações que não possuem uma equipe de Segurança da Informação ou profissional com conhecimento na área elaborá-lo, podendo passar, a essas, a impressão que é algo inalcançável e muito complexo de ser

realizado, por este motivo, neste trabalho, apresentamos orientações para sua implantação, próximo tópico. Ainda, com o passar do tempo, e com constantes notícias de perdas, exposições de dados que deveriam ser confidenciais e, até mesmo problemas de continuidade de negócio sendo veiculados em todas as mídias, fica mais fácil convencer a todos da necessidade de investir em Gestão de Riscos e em Segurança da Informação. Não é apenas positivo do ponto de vista técnico, pois asseguram à empresa certa tranquilidade, uma vez que poderá conhecer seus pontos fracos e realizar ações necessárias para assegurar a continuidade de seus negócios, mas também acaba por transmitir uma imagem de empresa consciente de seus objetivos, além de reconhecer a importância da confidencialidade, disponibilidade e integridade de seus ativos e processos. Assim, demonstra preocupação com as informações que ela manipula, tendo em vista que as organizações estão, a cada dia que passa, manipulando um volume cada vez mais robusto e delicado de informações.

3. Orientações para implementação do Sistema de Gestão de Segurança da Informação

Os tópicos anteriores tinham como objetivo contextualizar a importância de orientações para implantação do Sistema de Gestão de Segurança da Informação (SGSI), e trazer um maior entendimento a respeito das diretrizes presentes na ISO 27001 (2013). Conforme dito, a ISO 27001 traz um sistema que engloba todos os tipos de práticas, instrumentos e procedimentos necessários para gerenciar a segurança da informação baseada no ciclo PDCA. Desta forma, as etapas para tal implantação serão divididas utilizando como base nas fases de: Planejamento, Execução, Verificação e Ação.

A fase de Planejamento do Sistema de Gestão de Segurança da informação visa recolher e analisar todos os dados relevantes, além de definir os objetivos e metas necessárias para atingir os resultados esperados. As etapas são:

- Análise do micro e macroambiente: análise dos fatores relevantes que influenciarão o SGSI;
- Identificação das partes interessadas e das interfaces e dependências: levantamento dos setores relevantes ao SGSI e seus requisitos;
- Definir o escopo do SGSI: definição do alcance do SGSI;
- Aprovação pela Alta Direção: respaldo da Diretoria;
- Política do SGSI: elaboração de uma política de SI que seja adequada aos objetivos da empresa;
- Papéis e Responsabilidades: definição e atribuição das funções de cada um que tem envolvimento com o SGSI;
- Identificação dos riscos e seus responsáveis: levantamento dos riscos de SI e seus responsáveis;
- Análise dos riscos identificados: avaliação das consequências potenciais, probabilidade de ocorrência e dos níveis de risco;

- Avaliação dos riscos e suas prioridades: comparação dos resultados da análise dos riscos para determinar quais devem ser tratados primeiro;
- Tratamento dos riscos: seleção dos controles para mitigar os riscos;
- Definir os objetivos dos controles: definição do propósito de cada controle, pois será descrito também no tratamento dos riscos;
- Declaração de aplicabilidade: elaboração de um documento contendo todos os controles selecionados e suas justificativas para uso e/ou exclusão.

Após a execução de todas estas etapas da fase de planejamento, será alcançada a fase de Implantação do Sistema de Gestão de Segurança da Informação. Essa fase, é essencial para a efetivação do ciclo PDCA pois é aqui que serão executados os planos de ação. Esta fase contém 4 etapas:

- Elaborar o plano de tratamento dos riscos: definição das etapas para a implantação dos controles selecionados anteriormente;
- Definição do cronograma de implantação dos riscos: definição do que será feito, quando será feito e quando estará concluído;
- Implementar os controles: execução do plano de tratamento de riscos;
- Comunicação do SGSI: conscientizar a todos que se envolvem com o SGSI das políticas de SI.

Concluindo a implantação do SGSI, entramos na etapa de monitoração e avaliação. O objetivo desta fase é medir os resultados em relação às metas que foram definidas. Serão apresentadas 2 etapas nesta fase, sendo:

- Avaliação de desempenho do SGSI: avaliar o desempenho e eficácia do SGSI baseado nos objetivos e metas definidas na fase de planejamento;
- Auditoria do SGSI: condução de auditoria interna periódica com o objetivo de identificar a não conformidade.

Após a identificação dos resultados alcançados com a avaliação e auditoria do Sistema de Gestão de Segurança da Informação, ocorre a fase para manter e trazer melhorias, utilizando o levantamento realizado pela auditoria. Neste caso:

- Análise crítica pela alta direção de acordo com os resultados da Auditoria do Sistema de Gestão de Segurança da Informação: havendo conformidade identificada pelo processo de auditoria, tudo o que foi elaborado durante o processo de implantação deverá ser padronizado, para que o trabalho não se perca e seja necessário solucionar os mesmos problemas de forma recorrente. Caso contrário, a organização terá que realizar uma análise crítica a respeito dos detalhes das causas do não cumprimento de requisitos.

Assim, seguindo todas as etapas conforme a ISO 27001, as organizações poderão transmitir aos seus clientes e fornecedores que se preocupam com seus dados, visto que o

Sistema de Gestão de Segurança da Informação implementado com excelência irá aprimorar processos internos além de reduzir os riscos de vazamento de informações e ataques. Vale ressaltar que este artigo é um recorte de uma monografia desenvolvida no Curso Superior Tecnológico em Segurança da Informação da Fatec São Caetano do Sul, e o Apêndice A, apresenta um trecho do guia desenvolvido.

4. Considerações Finais

Com o aumento dos incidentes de segurança, é possível constatar, que algumas organizações, encontram dificuldade em realizar a implementação de um sistema que garanta a segurança de suas atividades. Os motivos que levam a esse obstáculo são variados. Entre eles, é possível destacar: a falta de conhecimento específico com relação: a Análise de Risco, Gestão de Segurança da Informação e Privacidade. Ainda, há crença de que empresas de pequeno porte, sem o montante financeiro das grandes corporações, se sentem invisíveis e longe dos holofotes e atenções dos cibercriminosos. Neste cenário, por vezes, os investimentos com Segurança da Informação são negligenciados, sem se darem conta de que este tipo de incidente pode ser irreversível para a maioria dessas organizações.

Diante do exposto, este artigo, teve como objetivo elaborar orientações simples e prática, para implementação do Sistema de Gestão de Segurança da Informação, tendo como base a norma ISO 27001 e o Ciclo PDCA. Neste sentido, foi apresentado um conjunto de controles e mecanismos de segurança da informação apropriados, com uma metodologia de aplicação simples e objetiva; e informações fundamentais para que as organizações possam concentrar seus esforços em suas atividades em conformidade com as leis, agregando valor de mercado ao seu negócio.

É sabido que em organizações de porte maior, processos como a criação de um Plano Diretor de Segurança comandado por um comitê e de um Plano de Continuidade de Negócio são altamente recomendados, porém, empresas de pequeno e médio porte, nem sempre terão recursos disponíveis para endereçar a criação destes planos. Assim, as orientações apresentadas, foram elaboradas seguindo os procedimentos indicados na norma ISO 27001, trazendo orientações para um Sistema de Gestão de Segurança da Informação, tendo como princípio as características próprias dessas organizações, com isso elas poderão ter um ponto inicial para tratar a Segurança da Informação.

Referências

ABNT - Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 27001:2013: Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos. 2013

AGUIAR, S. Integração das Ferramentas da Qualidade ao PDCA e ao Programa Seis Sigma. Belo Horizonte: Ed. de Desenvolvimento Gerencial, 2002.

ANDRADE, Fábio Felippe de. O método de melhorias PDCA – São Paulo: Escola politécnica da Universidade de São Paulo, 2003;

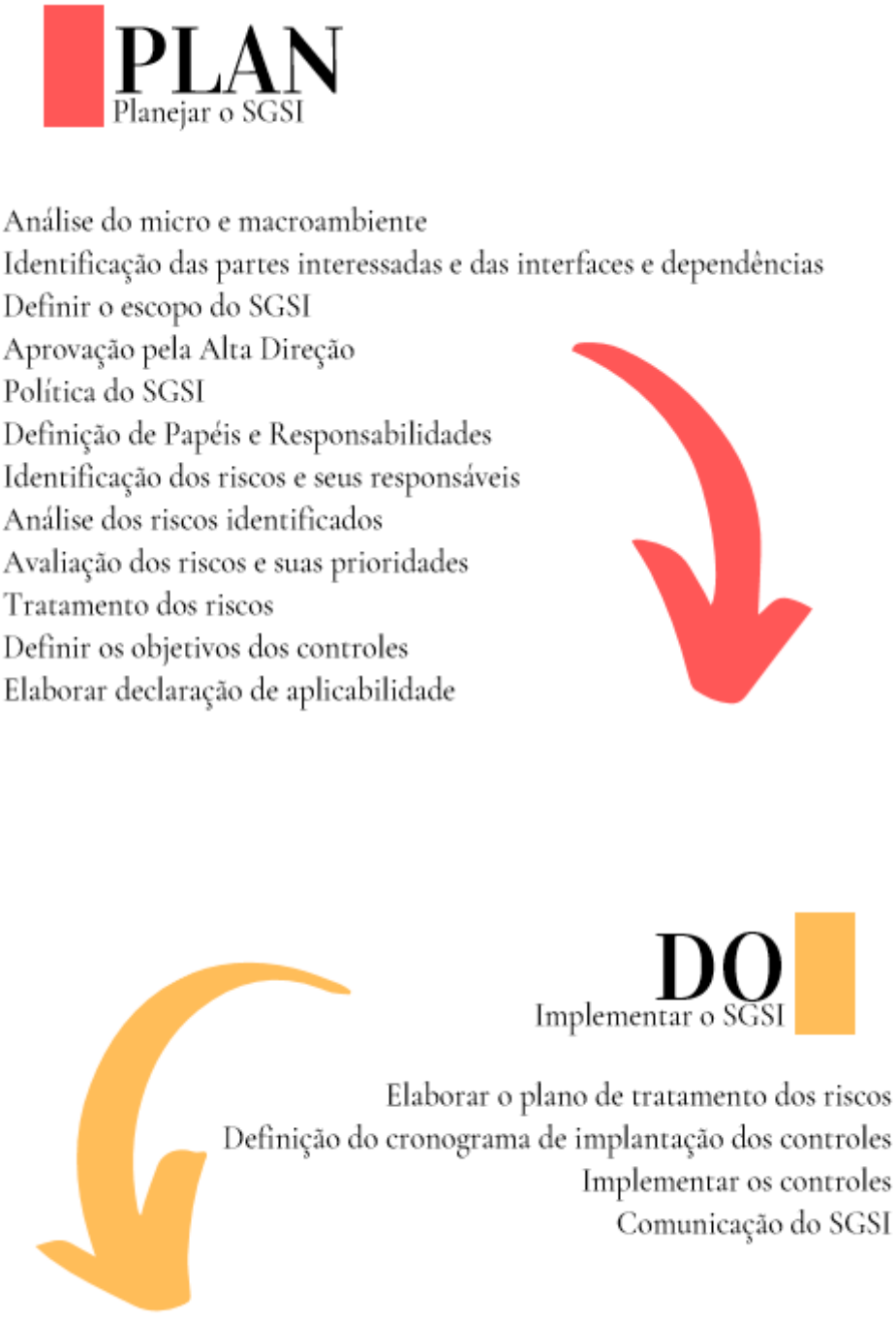
BRASIL. LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 13 de novembro de 2020

FONTES, Edison. Segurança da Informação: o usuário faz a diferença - São Paulo: Saraiva, 2007.

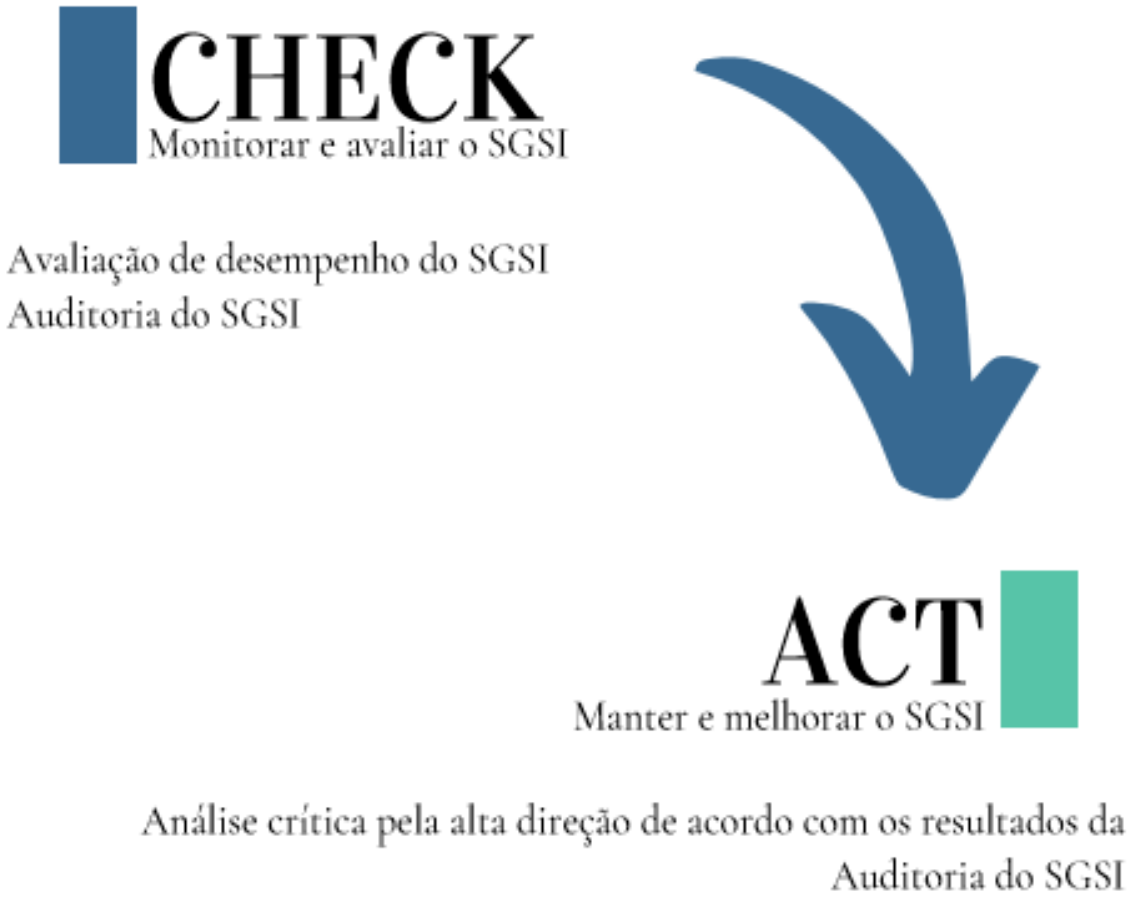
SÊMOLA, Marcos. Gestão da Segurança da Informação: uma visão executiva - Rio de Janeiro: Campus, 2014.

WORLD ECONOMIC FORUM. The Global Risks Report 2019 14th Edition. Disponível em: <https://www.weforum.org/reports/the-global-risks-report-2019> Acesso em: 07, set, 2020

APÊNDICE A – Guia com orientações para implantação da Gestão de Segurança da Informação



Fonte: Acervo da pesquisa (2021)



Fonte: Acervo da pesquisa (2021)

Agradecimentos

À FATEC São Caetano do Sul - Antonio Russo e seu corpo docente pelo apoio.