A SEGURANÇA DA INFORMAÇÃO COMO FOCO DO PLANEJAMENTO ESTRATÉGICO EM AGRONEGÓCIOS

Adrian Brito de Moraes Junior[1]
Prof. MSc. Flávio Aparecido Pontes[2]
Prof. Esp. Luiz Egidio Costa Cunha[3]

INTRODUÇÃO

Cooperativas são organizações que como qualquer outra precisam encontrar formas de se manter competitivas dentro do mercado em que elas se encontram. A Cooplantas, objeto de estudo deste trabalho, é mais uma dessas cooperativas que busca se manter ativa e competitiva dentro de um mercado cada vez mais disputado.

No entanto, atualmente a Cooplantas tem em seus processos operacionais e administrativos pouquíssima influência de tecnologias computacionais em suas operações, pois trata-se de uma pequena empresa do ramo agro familiar formada por um conjunto de mulheres assentadas, com pouco ou quase nenhum conhecimento em práticas computacionais, mas com grandes propósitos, onde buscam a todo tempo, mesmo com as dificuldades financeiras, se adaptarem as necessidades do mercado e suas novas tecnologias.

A Cooplantas, conta hoje com alguns computadores que são administrados e operados pela alta gestão da empresa, onde neles são realizadas tarefas operacionais e administrativas do dia a dia da organização, como atualização de planilhas de produtos, estoque, vendas, faturamento, compras e etc. Contudo, sabe-se que se tem nos planos futuros dessa organização a expansão e a progressão total da Tecnologia da Informação para todos os seus processos produtivos, operacionais e administrativos.

Com isso, dentro de um mercado competitivo e um mundo virtual altamente perigoso para a sobrevivência dos negócios, surge a preocupação em torno da proteção de informações valiosas para a organização. Então, o presente trabalho, sendo parte de um completo planejamento estratégico de TI, através da realização de pesquisas bibliográficas e visitas *in loco, se propõe* a desenvolver um planejamento de Segurança da Informação para esta empresa.

Laudon e Laudon (2011, p.227) enfatizam que embora a proteção dos sistemas de informação seja essencial para a realização de atividades das organizações, muitas empresas ainda resistem em gastar com a segurança de suas informações. Isso ocorre, muito pelo fato da Segurança da Informação não estar diretamente ligada aos lucros de vendas. Mas certamente essas organizações têm ativos de informações importantes para proteger, como por exemplo: informações sigilosas sobre segredos de negócio, planos de criação de novos produtos, estratégias de marketing, impostos, movimentação financeira, desempenho, etc.

[1] Estudante do curso de Especialização em Gestão da Tecnologia da Informação, IFSP – Boituva/SP - adrianbmjr@gmail.com

[2] Professor do curso de Especialização em Gestão da Tecnologia da Informação, IFSP – Boituva/SP - flaviopontes@ifsp.edu.br

[3] Professor do curso de Especialização em Gestão da Tecnologia da Informação, IFSP – Boituva/SP - egidiocunha@ifsp.edu.br

Logo, percebe-se que para as empresas, as informações possuem um valor imensurável e precisam ser protegidas, caso contrário à sua divulgação em massa poderia causar danos irremediáveis aos negócios das organizações.

Portanto, o presente trabalho justifica-se a partir da necessidade identificada em desenvolver o planejamento de Segurança da Informação para uma cooperativa localizada na cidade de Itapeva-SP, a Cooplantas. Pois conforme observação *in loco*, pôde-se perceber a inexistência de estratégias ou métodos para proteção das informações necessárias aos processos produtivos, operacionais e administrativos da organização, bem

Este trabalho tem por objetivo geral desenvolver através dos estudos levantados, o planejamento estratégico da Segurança da Informação da Cooplantas, uma cooperativa do ramo agro familiar no interior paulista. Desta forma, com o propósito de criar um plano para proteção e prevenção contra ameaças virtuais às informações do negócio desta cooperativa, buscando minimizar os problemas causados pela falta de procedimentos que visam a proteção de um dos ativos mais importantes para as organizações, a informação.

COOPERATIVISMO E SUAS CARACTERÍSTICAS

O cooperativismo é um modelo de associação econômica baseada em empresas (cooperativas) fundamentadas em sociedade, onde seus sócios recebem o nome de cooperados e passam a ser responsáveis pela saúde econômica e social da organização. Portanto, Mauad (2000, p. 211) cita que as cooperativas são associações formadas por pessoas físicas com interesses comuns, que reunidas irão gerar lucros através de um exercício profissional, onde o propósito é gerar aos cooperados uma melhora de condição econômica, de forma democrática e livre de adesão, mensalidades ou taxas.

Logo, o cooperativismo pode ser definido como um modelo solidário de associação econômica, criado para a produção de bens ou serviços, apoiado por conceitos democráticos e sociais, colaboração mútua, gestão democrática e participativa, objetivos econômicos e sociais comuns, sendo assim, pode-se afirmar que as cooperativas prestam serviços a seus cooperados através de fornecimento de materiais, produtos e serviços.

As cooperativas são constituídas por valores humanos, fundamentadas em solidariedade, responsabilidade, democracia e igualdade, unindo desenvolvimento econômico e social, produtividade e sustentabilidade, ganhos individuais e coletivos. Assim, o cooperativismo surge como um modelo econômico de negócio que busca transformar a vida das pessoas, oferecendo melhores oportunidades para todos e transformando a sociedade em um lugar mais justo e equilibrado (ORGANIZAÇÃO DAS COOPERATIVAS BRASILEIRAS, 2018).

No cooperativismo todos os cooperados possuem o mesmo grau de responsabilidade pelo negócio, ou seja, todos são responsáveis pelas dívidas e lucros da cooperativa, não sendo diferente quando surge a necessidade de tomar alguma decisão, criando assim uma gestão democrática pelos cooperados. Mas para que tudo funcione da melhor maneira, dentro das cooperativas são constituídos alguns órgãos que atuam em sua administração. Segundo Crúzio (2000, p.43), são eles:

Tabela 1 – Definições dos órgãos de uma cooperativa

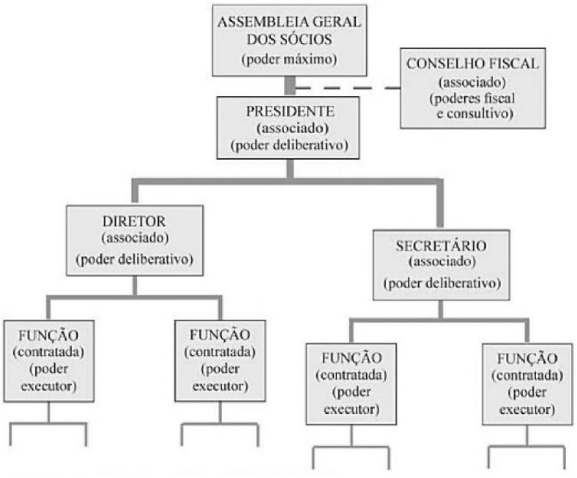
ÓRGÃO	DEFINIÇÃO
Assembleia Geral dos Sócios (AGS)	Órgão formado por todos os cooperados, o qual possui a responsabilidade de democraticamente tomar todas as decisões em relação a cooperativa, como por exemplos: a eleição da diretoria, a escolha dos conselheiros, a definição da política de divisão dos resultados e etc., portanto, todas as principais decisões de uma cooperativa são tomadas em conjunto nesta

	assembleia, através de uma votação, onde todos têm voz e poder de decisão. Assim, sendo democraticamente tomada aquela decisão que tiver mais votos.
Assembleia Geral Ordinária (AGO)	É um tipo de Assembleia Geral que acontece anualmente, geralmente durante os 3 primeiros meses após o término do exercício social de cada ano da cooperativa. É responsável por tratar assuntos como: eleger membros da direção no Conselho de Administração, conselheiros fiscais, decidir o que fazer com sobras líquidas, aprovar as contas gerais da cooperativa, definição de valor dos honorários dos Conselho de Administração e etc.
Assembleia Geral Extraordinária (AGE)	É um tipo de Assembleia Geral que acontece eventualmente ou sempre que houver a necessidade de discutir qualquer assunto urgente do interesse dos cooperados e da cooperativa, como por exemplo: tomar decisão referente a mudanças na missão e objetivos da cooperativa, destituição de membros da direção ou conselheiros fiscais, encerramento das operações da cooperativa e etc.
Conselho Fiscal (CF)	É o órgão responsável por fiscalizar o desempenho das decisões tomadas na Assembleia Geral (Ordinária e/ou Extraordinária), ou seja, é um órgão com poderes de fiscalização de todas as operações e atividades das cooperativas além dos atos da direção/administração. Formado por cooperados eleitos pela Assembleia Geral Ordinária.
Conselho de Administração (CA)	É o órgão responsável por realizar a administração da cooperativa, como por exemplo: intermediar compras e vendas dos produtos ou serviços, levantar necessidades e providenciar recursos e materiais, convocar reuniões da Assembleia Geral e apresentar os resultados operacionais e financeiros e/ou atividades gerais da cooperativa e etc. Formado por cooperados eleitos pela Assembleia Geral Ordinária.

Fonte: Adaptado de Crúzio (2000, p.43)

Perante as informações apresentadas acima, destaca-se a hierarquia de participação dos órgãos na estrutura organizacional de uma cooperativa. Porém, é importante frisar que cada cooperativa tem as suas particularidades nas estruturas organizacionais, por isso a nível demonstrativo, abaixo será apresentado um organograma com órgãos básicos para o funcionamento de uma cooperativa, como mostra a Figura 1:

Figura 1 – Estrutura básica organizacional de uma cooperativa.



Fonte: CRÚZIO, 2015

Na Figura 2 pode-se observar os números do cooperativismo brasileiro no ano de 2017, segundo estudo levantado pela Mundocoop (2017, p.64). Destaca-se então a significativa participação do cooperativismo na economia e o seu impacto na sociedade, gerando milhares de empregos, produtos, serviços e oportunidades, onde em território nacional conta-se com aproximadamente 6.655 cooperativas divididas em 13 ramos de atividade, somando mais de 13 milhões de cooperados beneficiados.

Figura 2 – Números do cooperativismo brasileiro

Fonte: MUNDOCOOP, 2017

TECNOLOGIA DA INFORMAÇÃO NA COMPETITIVIDADE DOS NEGÓCIOS

Com a alta competitividade do mercado, as empresas cada vez mais vêm buscando formas de se destacarem em relação aos seus concorrentes, tentando se aproximar ainda mais de seus clientes e fornecedores. À vista disso, o mundo globalizado dos negócios exige das organizações, adaptações rápidas e pontuais às diversas mudanças do mercado, onde as informações geradas pelas empresas têm um papel fundamental para essas adaptações. (MARTENS, 2001, p. 6)

Neste cenário, destacam-se os grandes volumes de informações gerados pelas empresas em seus processos de negócio. Então, para Freitas et al (1997, p. 24 apud MARTENS, 2001, p. 6) o valor da informação dentro das empresas está diretamente ligada e aumenta gradativamente com o desenvolvimento da sociedade e das organizações, sendo fundamental em todos os níveis da estrutura organizacional (operacional, tático e estratégico).

Então, é evidente que as informações de uma organização precisam ser organizadas, armazenadas e protegidas, até pelo fato de que algumas delas são vitais para o negócio e para a competitividade da empresa. Diante dessa necessidade, surge a Tecnologia da Informação (TI), que está relacionada com todas as áreas de uma empresa, abrangendo toda e qualquer atividade executada através de recursos computacionais para gerir e gerar informações relevantes para o negócio.

A partir da necessidade de realizar a gestão das informações, as organizações começam a investir em TI (hardware e softwares), buscando assim garantir um melhor desempenho em seus processos, agilizando atividades operacionais e estratégicas e melhorando a exatidão nas tomadas de decisão das gestões. (WALTON, 1993 apud MORAES et al, 2004, p. 30)

Moraes et al (2004, p. 37) cita também que as oportunidades oferecidas pela TI (quando bem aplicada), proporcionam reduções de custos e principalmente o aumento de lucros.

Portanto, a informação é um dos ativos mais importante para os processos de negócio dentro de uma empresa e um fator crucial para o seu desenvolvimento diante da alta competividade. Com isso surge a TI assumindo a responsabilidade de realizar a gestão de toda a informação gerada e utilizada pelas organizações através de recursos de informática.

a) O Uso da Informação nas Organizações

Na Tecnologia da Informação, informação é tudo aquilo que se resulta de um processamento de dados, podendo ser apresentada de diversas maneiras, sendo elas: escritas, impressas, desenhadas, armazenadas eletronicamente e entre outras. Assim, podendo ser trafegada através de correio, e-mail, sistemas, meios lógicos e etc.

Para as organizações, segundo a norma NBR ISO/IEC 27002 (2005), a informação é um ativo que como qualquer outro ativo importante, é primordial para os negócios de uma empresa. Apoiando este raciocínio, Dias (2003 apud LAUREANO e MORAES, 2005) salienta que a informação é o principal patrimônio de uma empresa e consequentemente por estar em risco constante, precisa ter a sua integridade protegida. Seguindo nesta linha, Drucker (1993 apud BRUM, 2011) afirma que dentro de uma empresa, a função da informação é servir de apoio para que as organizações e as pessoas que atuam dentro das empresas tomem decisões embasadas em conhecimentos gerados através dela (informação).

Então, é possível afirmar que a informação surge como um elemento importante e primordial para o sucesso de uma organização, servindo de base para qualquer processo administrativo e de gestão dentro de uma empresa, sendo utilizada não só no operacional, mas também na diferenciação e no plano estratégico de qualquer organização perante ao mercado e sua competitividade.

Laureano e Moraes (2005) enfatizam que, quando se fala de estratégias de negócio, o domínio da informação passa a ser fundamental para as organizações, pois é sabido que ao utilizar a informação correta, no exato momento de uma tomada de decisão, significa que essa decisão será tomada de forma precisa, ágil e eficiente. Portanto, pode-se dizer que a informação é um ativo que basicamente representa a inteligência competitiva de uma empresa, funcionando como um recurso fundamental para a evolução constante da organização em suas estratégias de negócio, e por isso deve ser administrada, diferenciada e guardada/protegida.

Para proteger uma informação, deve-se saber antes classifica-la, desse modo simplificando a escolha e a definição do método de proteção exigido por aquele determinado tipo de informação, assim garantindo que aquela informação possa receber um nível adequado de proteção. Portanto, Ferreira e Araújo (2008, p. 78) destacam que a classificação da informação "[...] é o processo de estabelecer o grau de importância das informações mediante a seu impacto no negócio, ou seja, quanto mais estratégica e decisiva para a manutenção ou sucesso da organização, maior será a sua importância". Mas para iniciar esse processo de classificação, torna-se necessário estabelecer antes

algumas definições baseadas no negócio da empresa, compreendendo processos e atividades operacionais realizadas, como por exemplo:

- Classificação: é a definição do grau de sigilo de acordo com o uso e atividade que a informação está inserida;
- Proprietário: é a definição do dono da informação, ou seja, é o responsável pelo ativo de informação de uma determinada área da organização;
- Custodiante: é a definição do responsável por assegurar que a informação está conforme definida pelo proprietário da informação;
- Criptografia: é a definição do tipo de codificação que será usada para proteger arquivos contra acessos e alterações indevidas;
- Perfil de acesso: é a definição do tipo de usuário que poderá ter acesso a informação e o que ele poderá fazer com ela (visualizar, alterar e/ou excluir). (FERREIRA; ARAUJO, 2008)

Após entender e estabelecer as definições acima, se faz necessário determinar a classificação das informações, apoiando-se através do valor que aquela informação possui para o negócio. Assim sendo, a ISO/IEC 27005 (2008 apud ANDRÉ, 2014, p. 24) define 4 tipos de classificação para informações, sendo elas:

- Informação Pública: Trata-se daquele tipo de informação que não exige sigilo e nem causa impactos negativos ao funcionamento da empresa, ou seja, a divulgação dessa informação não traria problema sendo cedidas ao público, pois não é o tipo de informação vital para o negócio;
- Informação Interna: É o tipo de informação que precisa ter a sua integridade mantida, pois é aquela informação de nível operacional, utilizada por todos os trabalhadores da empresa. No entanto, se vazadas, essas informações não trariam danos tão graves ao negócio;
- Informação Confidencial: É aquela informação que deve ser guardada e protegida dentro e fora da organização, pois a sua divulgação acarretaria em situações críticas, bem como perda de privacidade, rompimento do equilíbrio e do ambiente de trabalho, danos financeiros e competitivos e muitos outros. Portanto é muito válido que sejam feitos investimentos na proteção dessas informações;
- Informação Secreta: Refere-se àquela informação crítica/vital para o negócio e as atividades da organização, causando danos cruciais na competitividade e nas estratégias de negócio da empresa. Então, a integridade dessa informação deve ser severamente preservada, tendo o seu acesso restrito apenas às pessoas autorizadas e responsáveis por ela.

b) A TI nas Pequenas Empresas

Segundo Prates e Ospina (2004, p.10), quando se fala nas principais funções da administração (planejamento, organização, direção e controle) percebe-se que as informações geradas através dos sistemas de informação possuem um importante valor aos administradores de empresas. Reforçando este pensamento, Stoner (1999) apud Prates e Ospina (2004, p.10) diz que os administradores só podem acompanhar a evolução de seus planos e objetivos quando têm em mãos informações precisas e no momento exato. Então, pensando em atender a estas demandas, surge a TI com a responsabilidade de gerir essas informações, e que de acordo com Tapscott (1997) apud Martens (2001, p.7), pode propor não só mudanças aos processos administrativos, como também transformar a produção de produtos e serviços, auxiliando e criando métodos de comercialização e aprimorando a estrutura e as metas da empresa, desenvolvendo relacionamentos com a concorrência e com o mercado de forma geral.

A Figura 3 demonstra a evolução do uso dos sistemas da informação ao longo do tempo e comprova cada vez mais o valor que as informações geradas por esses sistemas possuem, impactando de forma geral os usuários e gestores das organizações, sendo utilizados ao longo do tempo como suporte operacional e administrativo, realizando processamento de dados e gerando informações e conhecimento.

Figura 3 – Evolução dos Sistemas de Informação

Evolução dos Sistemas de Informação

Período / Uso	Funções dos Sistemas de Informação
De 1950 a 1960 ('50-'60): Processamento de dados	Sistemas de processamento eletrônico de dados: processamento de transações, manutenção de registros e aplicações contábeis tradicionais.
De 1960 a 1970 ('60-'70): Relatórios administrativos	Sistemas de informação gerencial: relatórios administrativos de informações pré-estipuladas para apoiar a tomada de decisão.
De 1970 a 1980 ('70-'80): Apoio à decisão	Sistemas de Apoio à Decisão (SAD): apoio interativo e *ad hoc* ao processo de tomada de decisão gerencial.
De 1980 a 1990 ('80-'90): Apoio estratégico e ao usuário final	Sistemas de computação do usuário final: apoio direto à computação para produtividade do usuário final e colaboração de grupos de trabalho. Sistemas de suporte a executivos: informações críticas para a alta gerência. Sistemas especialistas: conselho especializado baseado em conhecimento para os usuários finais. Sistemas de informação estratégica. Produtos e serviços estratégicos para obtenção de vantagem competitiva.
A partir de 1990 ('90-): Empresa e conexão em rede global	Sistemas de informação interconectados: sistemas direcionados ao usuário final, à empresa e à computação, às comunicações e à colaboração interorganizacionais, incluindo operações e administração globais nas Internet, intranets, extranets e outras redes empresariais e mundiais.

Fonte: O'BRIEN, 2004 apud ROSSETTI; MORALES, 2007

Nas pequenas empresas, tudo vai depender de como a TI será aplicada ao negócio, sabendo que não há uma tecnologia boa ou má, mas sim aquela tecnologia que se adequa ao negócio e ao tamanho da organização. Assim, ao ser auxiliada por sistemas de informação no desenvolvimento organizacional, a pequena empresa poderá colher maiores e melhores resultados na eficiência da administração de seus processos, recursos e atividades, desta forma alcançando suas metas e objetivos pré-estabelecidos de modo eficaz (SOLOMON, 1986 apud PRATES; OSPINA, 2004, p.12).

De acordo com Beraldi e Escrivão Filgo (2000) apud Moraes et al (2004, p.35), a maioria das pequenas empresas contam com uma característica comum entre elas, a realização de controles e atividades através de papeladas e anotações, não possuindo nenhum tipo de informatização, ou sistema de informação em seus processos operacionais, administrativos ou estratégicos. Portanto, faltam às pequenas empresas tecnologias que possam oferecer um suporte na execução de seus processos, melhorando a qualidade dos resultados e das informações como apoio a gestão estratégica do negócio.

Contudo, segundo o estudo realizado por Thong (2001) apud Prates e Ospina (2004, p.15), as pequenas empresas que obtêm sucesso em TI, geralmente contam ou contaram com uma forte participação de especialistas de TI externos, sendo suportados por uma gerência geral, desta forma, auxiliando nas tomadas de decisões referente a investimentos de TI, no desenvolvimento do conhecimento dos usuários e do grau de envolvimento de cada um.

Isso ocorre porque, segundo Migliato (2003) apud Moraes et al (2004, p.35), geralmente os administradores de pequenas empresas costumam não valorizar as

informações relevantes para o negócio, as quais podem ser eventualmente obtidas no dia-a-dia da empresa, desta forma não fazendo o aproveitamento adequado (quando tem) do seu sistema de informação (geralmente simples). Então, como nas pequenas empresas os dirigentes não costumam buscar informações, entender suas origens e nem levantar questionamentos, é comum que realizem com dificuldades qualquer tipo de análise de ambiente, seja ele interno ou externo.

Isto posto, quando uma pequena empresa conta com uma administração leiga ou inexperiente na parte estratégica do negócio, um auxílio de um especialista de TI é bem-vindo, sendo benéfica a sua participação nas decisões referentes a investimentos em tecnologias e definições de estratégias.

Portanto, Firmino (1999) apud Moraes et al (2004, p.36) cita que as pequenas organizações necessitam de soluções que facilitem e automatizem os processos do dia-a-dia da empresa, desenvolvendo uma produtividade efetiva e propondo novas perspectivas estratégicas de negócio com o mínimo possível de investimentos em ativos tecnológicos.

Deste modo, é possível entender que a TI faz parte e está diretamente ligada ao negócio das pequenas empresas, embora algumas pequenas organizações ainda tratem a TI como um centro de custo, sendo utilizada apenas como apoio para os processos operacionais e administrativos. Contudo, segundo os autores acima, a informação gerada pela TI através do processamento de dados tem um valor estratégico para o negócio de uma pequena empresa, podendo ser usada e transformada em conhecimento, e assim passando então a gerar lucros, fixando a ideia de que os investimentos em TI cada vez mais incidem no faturamento das organizações.

c) Segurança da Informação

De acordo com a norma NBR ISO/IEC 17799 (2005), a Segurança da Informação é a proteção de ativos de informação contra diversos tipos de ameaças, visando garantir a continuidade do negócio, a minimização de riscos, a maximização do retorno sobre os investimentos e das oportunidades de negócio**.**

Dito isso, uma vez que a TI está inserida no negócio de uma empresa, torna-se indispensável a adoção de políticas de controle e proteção das informações, como destaca Laudon e Laudon (2015, p.256):

> "Em resumo, se você opera uma empresa hoje precisa ter a segurança e o controle como prioridades. O termo segurança abarca políticas, os procedimentos e as medidas técnicas usadas para impedir o acesso não autorizado, alteração, roubo ou danos físicos a sistemas de informação. Os controles, por sua vez, consistem em todos os métodos, as políticas e os procedimentos organizacionais que garantem a segurança dos ativos da organização, a precisão e a confiabilidade de seus registros contábeis e a aderência operacional aos padrões administrativos.".

Então é perceptível que existe uma preocupação das empresas com a segurança de seus dados e informações, pois conforme Mattos (2010, p.121), não existe computador absolutamente confiável, já que toda e qualquer tecnologia está sujeita a falhas humanas e a softwares mal-intencionados. Deste modo, a maioria das empresas almejam alcançar o mais alto nível de Segurança da Informação, mesmo sabendo que

não há sistema 100% seguro, tornando essa uma das preocupações mais importantes em um departamento de TI.

Assim sendo, parte-se do ponto de que a segurança absoluta da informação é inalcançável, contudo, hoje existem políticas, medidas e práticas que tornam essa tarefa um pouco mais simples, cabendo ao responsável pela Segurança da Informação garantir que todos os possíveis riscos sejam ao menos considerados em suas análises, a fim de encontrar com essas políticas e práticas a melhor solução/prevenção para todas as situações.

Com a pretensão de alcançar o mais alto nível de Segurança da Informação, Lyra (2008, p.4) salienta que aplicar a Segurança da Informação é "tomar ações para garantir a confidencialidade, integridade, disponibilidade e demais aspectos da segurança das informações dentro das necessidades do cliente".

Mas antes de decidir qual ação tomar para uma determinada situação, é necessário entender os aspectos que devem ser preservados para uma segurança efetiva. Então, segundo Lyra (2008, p.3), alguns aspectos são necessários para pôr de fato em prática o conceito de Segurança da Informação, sendo eles:

Tabela 2 – Definições de aspectos importantes em Segurança da Informação

Aspecto	Definição
Confidencialidade	É a característica de um sistema que permite e faz o controle de acesso a determinadas informações, concedendo a visualização e alteração dessas informações apenas por usuários autorizados.
Integridade	É a garantia de que a informação está correta, não sendo alterada ou corrompida por algum software mal-intencionado.
Disponibilidade	É o acesso da informação para todos os usuários que precisam dela para a realização de alguma tarefa ou objetivo empresarial.
Autenticação	É o processo que garante a identidade do usuário, provando que ele é realmente quem alega ser.
Não-Repúdio	É uma característica de um sistema que permite provar qual usuário executou uma determinada ação.
Legalidade	É a garantia de que o sistema esteja funcionando dentro da legislação adequada.
Privacidade	É característica do sistema que garante o sigilo ou anonimato das ações do usuário quando necessário.
Auditoria	É o processo que valida tudo o que é realizado pelo usuário, detectando tentativas de ataques ou fraudes.

Fonte: Adaptado de Lyra (2008, p.3)

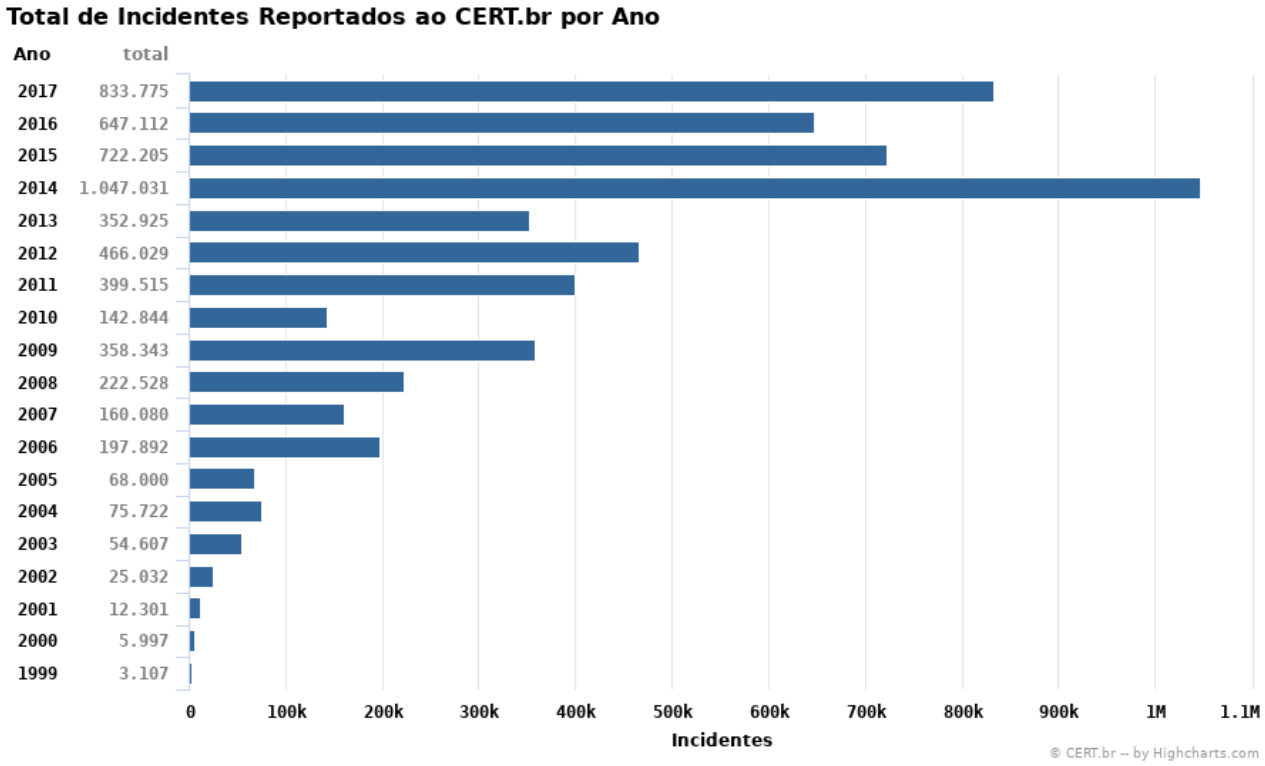
Logo, a identificação das vulnerabilidades de um sistema é um processo primordial para que os aspectos citados acima sejam garantidos. Mas apesar disso, é importante destacar que, dentro da Segurança da Informação, as vulnerabilidades são objetos passivos, ou seja, precisam da ação de um agente causador ou alguma situação que comprometa as informações do sistema, assim causando a não conformidade da confidencialidade, integridade, disponibilidade e dos outros aspectos de segurança das informações. (SÊMOLA, 2003, p.48)

Por outro lado, Laudon e Laudon (2011, p. 216) ressaltam a preocupação existente também em fatores que possam gerar falhas em hardwares de dispositivos que armazenam informações, como por exemplo: quedas de energia, enchentes, incêndios e outros desastres naturais que possam causar danos e destruição de hardwares. Fatores que podem aumentar quando a informação foge do controle da organização, como por

exemplo no caso de alguma parceria estabelecida com empresas duvidosas que prometem oferecer serviços de servidores e armazenamento de informação, mas não se preocupam em investir em uma boa estrutura, colocando em risco os dados valiosos de seus clientes/parceiros.

Como pode ser observado na Figura 4, o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) recebe notificações diárias e voluntárias de incidentes ocorridos em organizações brasileiras.

Figura 4 – Total de incidentes reportados ao CERT.br por ano. (CERT.br, 2018)



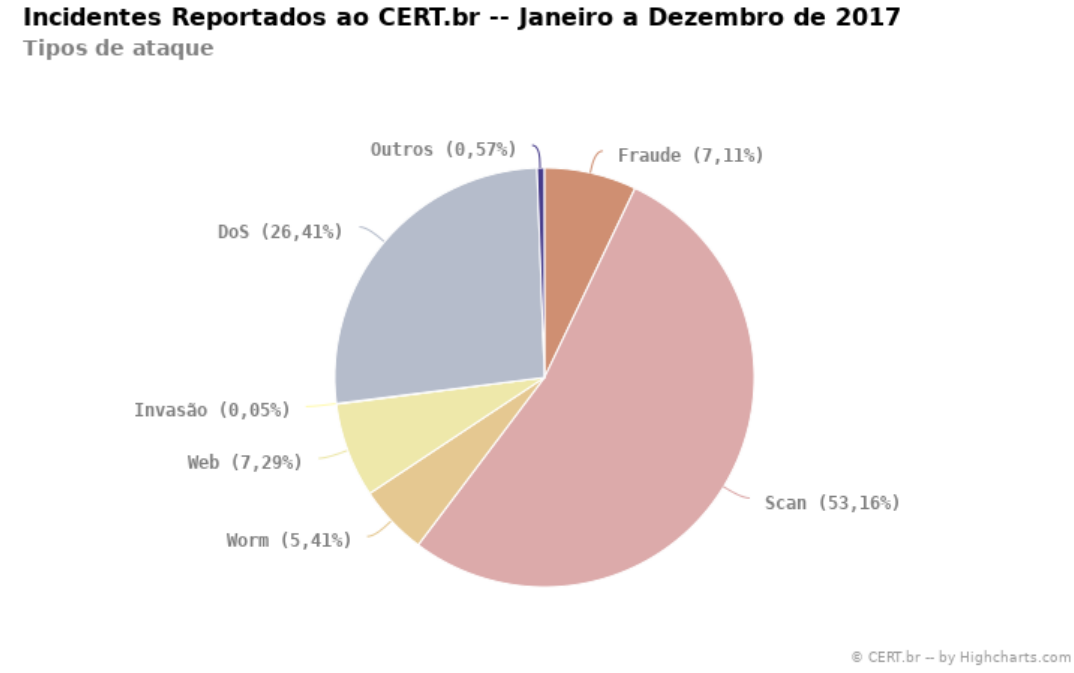
Analisando os dados acima, é possível observar que as ocorrências entre os anos de 1999 e 2005 se mantinham em pequena escala e com diferenças discretas em números de incidentes entre os anos. A partir de 2006, com a popularização da internet no Brasil, o número de usuários e registros de incidentes no CERT.br aumentou, e desde 2014 os números de ocorrências estão muito mais elevados do que os anos anteriores, chegando a bater (ou quase) 1 milhão de incidentes por ano em território brasileiro. Com isso, entende-se a necessidade enxergada pelas empresas em investirem cada vez mais na segurança de suas informações.

Diante disso, é pertinente apresentar os principais tipos de incidentes e ataques a redes de computadores e sistemas segundo o Cert.br (2018):

- *Worms:* São softwares mal-intencionados que se espalham em redes de computadores. Funcionam sozinhos e automaticamente, sem a necessidade de uma ação humana para executa-lo, por esse motivo os *Worms* se espalham rapidamente e acabam interrompendo o funcionamento normal de uma rede de computadores, corrompendo arquivos e programas. (LAUDON E LAUDON, 2011, p. 258)

- *DoS (Denial of Service):* São ataques em massa sendo executados simultaneamente contra um alvo definido, até que algum servidor, site ou serviço, seja derrubado.
- Invasão: Ataque bem-sucedido no acesso não autorizado de informações, computadores ou rede. (CERT.br, 2018)
- *Web:* Ataques que visam derrubar páginas específicas da Internet, bem como algum servidor. (CERT.br, 2018)
- Fraude: Ataques promovidos através de anúncios e mensagens de e-mail fraudadas e infectadas com vírus, ludibriando máquinas e usuários. (LAUDON E LAUDON, 2011, p. 266)
- *Scan:* São ataques que agem observando o comportamento de redes e computadores, buscando com isso definir quais computadores e serviços estão vulneráveis e disponíveis, para assim estabelecer possíveis alvos. (CERT.br, 2018)

Figura 5 – Tipo de incidentes reportados ao CERT.br - Janeiro a Dezembro de 2017



De acordo com a Figura 5, o incidente mais reportado ao CERT.br em 2017 foram os do tipo *Scan*, revelando que a grande maioria das ocorrências de ataques no Brasil no ano de 2017 se deu através de tentativas de encontrar brechas e oportunidades de invasão. Portanto, isso indica que cada vez mais os profissionais da área precisam se preocupar com a implantação e controle de políticas de Segurança da Informação dentro de suas organizações, com o intuito de dificultar ao máximo o acesso externo e indevido a redes internas, computadores e sistemas. No entanto, é pertinente destacar que o *Scan* pode e deve ser utilizado também como uma forma de se antecipar a falhas e vulnerabilidades, realizando varreduras em redes e em computadores para identifica-las e corrigi-las ou aplicar uma solução, podendo ser utilizado através de programas de proteção (antivírus) e firewalls.

I) Premissas Necessárias para Segurança da Informação

Conforme o pensamento de Laudon e Laudon (2011, p. 229), para alcançar uma Segurança da Informação efetiva em sistemas de informação é preciso identificar as principais e melhores ferramentas de segurança para cada caso, sabendo exatamente como e onde utiliza-las, facilitando na identificação dos riscos e controles que devam ser adotados em cada caso para a proteção de sistemas de informação. Os autores ressaltam também a importância da adoção de políticas de Segurança da Informação para alcançar um nível adequado de confiabilidade e proteção das informações do negócio.

Já para Marciano e Marques (2006, p.96), a necessidade do engajamento de todos os usuários nesse processo é fundamental para que a gestão da Segurança da Informação ocorra de forma assertiva, pois são eles que deverão seguir à risca todo o planejamento de Segurança da Informação, que deve envolver: atividades de planejamento, implementações e avaliações das atividades voltadas à segurança.

Com isso, as duas ideias citadas acima trazem conceitos que podem se unir para um alcance ainda maior de uma Segurança da Informação efetiva. Então, é possível afirmar que para a consecução de um nível adequado de Segurança da Informação, a identificação dos riscos e a escolha das ferramentas certas para controle de Segurança da Informação, unidas ao engajamento onde todos os usuários do sistema/rede estejam compromissados a colaborar com o planejamento de segurança, são indispensáveis para o seu sucesso.

II) Gestão de Segurança da Informação

Laudon e Laudon (2011, p. 229) afirmam que sistemas de informações, mesmo com o apoio das indispensáveis ferramentas de segurança, só serão confiáveis e seguros se usados de forma correta e no momento certo. Portanto, destacam a importância de conhecer os riscos que a empresa corre e quais controles são necessários para realizar a segurança de sistemas de informação, sendo preciso também a implementação das indispensáveis políticas de Segurança da Informação.

Para este trabalho, como trata-se de uma pequena organização onde o uso de tecnologias da informação são requisitados apenas para controles administrativos, será usado a metodologia de Laudon e Laudon (2014) que dividem a gestão da Segurança da Informação em: análise e revisão de riscos, implantações de controles de segurança através de tecnologias e ferramentas, políticas de segurança, planos recuperação de desastres e continuidade dos negócios e auditoria.

Portanto, Laudon e Laudon (2014, p. 271) afirmam que uma análise (ou avaliação) de riscos define o que pode realmente causar impactos negativos de acordo com a probabilidade de um evento ocorrer. Dessa forma, a análise de riscos determina algumas situações de risco que devem ser prioridades em um SGSI. No entanto, frente a um cenário tão disruptivo, riscos podem passar despercebidos devido à falta de conhecimento sobre os novos elementos introduzidos por esse cenário, portanto o SGSI deve a todo momento, através de controles e análise de risco, identificar os ativos a serem protegidos.

Segundo, Laudon e Laudon (2014, p. 270), os controles de Segurança da Informação podem ser compostos por duas categorias: controles gerais e controle de aplicação, ambos podendo ser automatizados ou manuais. Controles gerais engloba todas as aplicações computacionais de uma organização e consistem de uma combinação de hardware, software e procedimentos manuais, formando um ambiente de controle, como mostra a Tabela 3. Controles de aplicação são os controles atentos a entrada, processamento e saída de dados, que com o apoio de procedimentos manuais ou automatizados deverá garantir que apenas dados autorizados sejam processados pelas aplicações, demonstrados na Tabela 4.

Tabela 3 – Controles Gerais

Controles Gerais	
Controles de software	Monitoram o uso de sistemas de software e previnem o acesso não autorizado a programas de softwares, sistemas de softwares e programas de computador.
Controles de hardware	Garantem que o hardware do computador esteja fisicamente seguro e verificam o mau funcionamento do equipamento, criando cópias de segurança de dados e/ou operações contínuas de manutenção de serviços constantes quando necessário.
Controles de operações de computador	Supervisionam o trabalho do departamento de informática para garantir que os procedimentos programados sejam consistentes e corretamente aplicados ao armazenamento e processamento de dados. Incluem controles sobre as tarefas de processamento e dos procedimentos de recuperação do computador para processamentos que terminam de maneira anormal.
Controles de segurança de dados	Garantem que os valiosos arquivos de dados do sistema, gravados em disco ou fita, não estejam sujeitos a acesso não autorizado, a modificações ou a destruição enquanto estão em uso ou armazenados.
Controles de Implementação	Auditam o processo de desenvolvimento de sistemas em diversos pontos para garantir que ele seja devidamente controlado e gerenciado.
Controles Administrativos	Formalizam padrões, regras, procedimentos e controlam disciplinas de modo a garantir que os controles gerais e de aplicação da empresa sejam propriamente executados e cumpridos.

Fonte: Laudon e Laudon (2014, p. 271)

Tabela 4 – Controles de Aplicação

Controles de aplicação	
Controles de entrada	Verificam a precisão e a completude dos dados quando entram no sistema. Existem controles de entrada específicos para autorização de entrada, conversão de dados, edição de dados e tratamentos de erros.
Controles de processamento	Verificam se os dados estão completos e precisos durante a atualização.
Controles de saída	Garantem que os resultados do processamento computacional sejam precisos, completos e distribuídos de maneira apropriada.

Fonte: Laudon e Laudon (2014, p. 270)

A partir da identificação de todos os riscos e de todos os controles que devem ser adotados em uma empresa, deve-se desenvolver uma política de segurança que deverá ser executada por softwares e principalmente usuários, para proteger esses ativos. Assim, Laudon e Laudon (2014, p. 272) definem que:

> "Política de segurança é uma declaração que estabelece hierarquias aos riscos de informação e identifica metas de segurança aceitáveis, assim como os mecanismos para atingi-las.".

Desse modo, as políticas definem regras como a posição da organização em relação ao uso dos equipamentos de informática e das redes da empresa, definindo normas quanto à privacidade e responsabilidade do usuário em relação as informações da corporação, bem como as consequências do não cumprimento da norma estabelecida quanto a ações aceitáveis e inaceitáveis de usuários (LAUDON E LAUDON, 2014, p. 272).

APRESENTAÇÃO E ANÁLISE DE PESQUISA

Para a realização deste trabalho, foi escolhido como objeto de estudo uma cooperativa do interior paulista chamada Cooplantas, uma organização localizada na cidade de Itapeva-SP, constituída por um coletivo de mulheres assentadas e engajadas em realizar um trabalho social, identificando na produção de medicamentos através de plantas fitoterápicas, uma oportunidade social e econômica para o desenvolvimento financeiro de suas famílias.

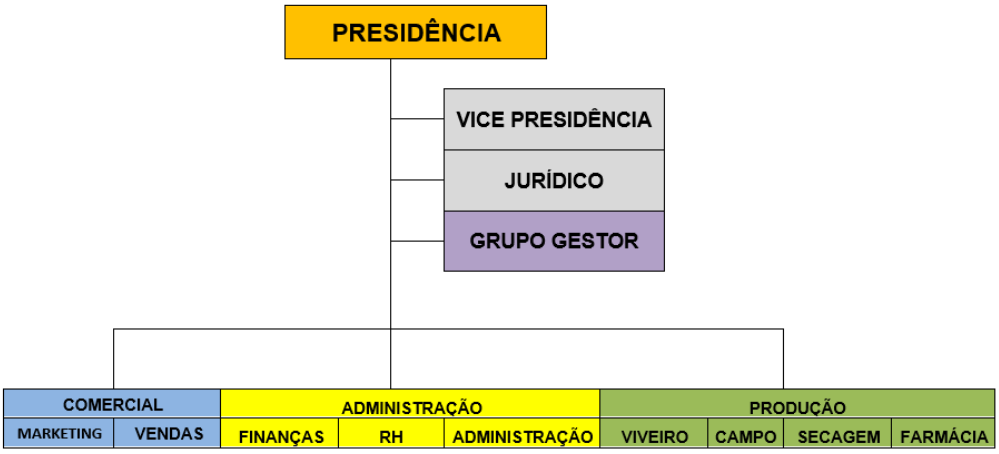
Portanto, a seguir será apresentado todas as informações levantadas referentes aos processos de negócio da cooperativa, destacando as práticas administrativas da cooperativa relevantes para o desenvolvimento do planejamento estratégico de Segurança da Informação dessa empresa.

a) Cooplantas

Como citado a cima, a Cooplantas é uma cooperativa que tem a sua atuação focada na produção de insumos fitoterápicos de qualidade e alimentos funcionais de modo a contribuir com a geração de renda e agregação de valor que será absorvida pelo mercado local e regional.

Com isso, foi extraído nessa visita também, o organograma da Figura 6 que demonstra como a cooperativa se divide:

Figura 6 – Organograma Cooplantas



Fonte: COOPLANTAS, 2018

Portanto, com a visita técnica realizada *in loco* no dia 07 de abril de 2018 a cooperativa, foi possível conhecer todos os processos de produtivos e administrativos da Cooplantas, onde pôde-se notar que todos os controles administrativos da pequena organização eram baseados em planilhas de Excel, que ficavam em apenas alguns

computadores da alta gestão da cooperativa, onde alguns responsáveis ficavam encarregados de alimentar as planilhas para realizar controles administrativos e de campo, bem como: controles de custos, vendas, lucros, compras, pedidos, produção, movimentação financeira e etc.

Além disso, foi informado que, embora essas planilhas fossem alimentadas somente pela alta gestão da cooperativa, algumas dessas planilhas precisavam ser alimentadas também por outras pessoas que participavam dos processos de produção, no entanto, nem todas essas pessoas possuem competências para o uso correto dessas tecnologias, onde pôde-se perceber a necessidade de um treinamento intensivo para essas pessoas.

Outro problema destacado foi a falta de compartilhamento de arquivos entre os computadores da Cooplantas, pois não há uma configuração e muito menos uma infraestrutura de redes de computadores, e como resultado surge a duplicidade de arquivos entre computadores e inconsistência de dados, não havendo qualquer tipo ou controle de backup de arquivos importantes, que não podem em hipótese alguma ser perdidos, roubados ou divulgados.

Então, de acordo com a visita técnica realizada *in loco*, pôde-se perceber a inexistência de qualquer tecnologia complexa utilizada para os seus controles administrativos e de produção, no entanto as tecnologias que lá já existem, exigem níveis de proteção e segurança de suas informações que ainda não foram implantados. Portanto, para esse trabalho, tomou-se a iniciativa de elaborar um plano estratégico de Segurança da Informação para a Cooplantas, baseado nas metodologias citadas no referencial teórico.

PLANEJAMENTO DA SEGURANÇA DA INFORMAÇÃO

Neste capítulo será tratado as etapas do processo de implantação da Segurança da Informação, realizando dessa forma o seu planejamento com cronogramas, custos e tarefas.

a) Reconhecer o ambiente

Nesta etapa será feita toda a identificação do ambiente produtivo e administrativo da cooperativa, sendo feita a exploração e reconhecimento de riscos existentes à Segurança da Informação da empresa, levando em consideração toda a cultura organizacional existente lá, bem como a forma de trabalhar de cada setor.

b) Sensibilizar a alta direção

Neste processo de implantação da Segurança da Informação, será muito importante contar com o apoio da alta direção. Para isso, é necessário que a direção esteja ciente e sensibilizada com a necessidade de realizar a proteção e Segurança da Informação do negócio. Portanto, para alinhamento das ideias, propostas e apresentação dos benefícios que a Segurança da Informação pode trazer adjunto ao negócio da empresa, uma reunião entre o responsável pelo departamento de TI, diretores e presidência da empresa deverá ser realizada.

Nesta reunião, deverão ser abordados os benefícios financeiros e prejuízos evitados já alcançados em outras empresas com a implantação de projetos e programas de Segurança da Informação. Serão apresentados também resultados de pesquisas e relatos de outros profissionais e executivos que implantaram boas práticas de Segurança da Informação alinhada ao negócio, bem como o Retorno Sobre Investimento (ROI) após

a implantação. Além disso, serão apresentados também relatórios demonstrando os riscos de segurança atuais existentes na cooperativa.

A ideia é alcançar com isso o entendimento, aprovação e consentimento da alta direção para iniciar o processo de implantação de boas práticas de Segurança da Informação.

Tabela 5 – Reunião para alinhamento e apresentação da Segurança da Informação

Data	**Participantes**	**Tema**
08/08/2018 às 14hs	Toda a diretoria, presidência e o responsável pelo departamento de TI	Segurança da Informação e seus benefícios

c) Definir o foco do Planejamento de Segurança da Informação

O foco do Planejamento de Segurança da Informação a ser implantado nessa cooperativa será definido em comum acordo com a alta direção da empresa, considerando as suas necessidades e os riscos identificados.

De acordo com a visita realizada na Cooplantas, e com as reuniões feitas durante o desenvolvimento desse trabalho, pôde-se identificar a necessidade da implantação de políticas de backups e controles de acessos a pastas e planilhas, sendo acessadas apenas por usuários autorizados a modificar o conteúdo de informações das mesmas. Outra necessidade identificada seria o compartilhamento desses arquivos e pastas, onde informações inseridas pelo ambiente administrativo devem ser visualizadas pelo ambiente produtivo e vice-versa.

Portanto, Planejamento de Segurança da Informação nessa cooperativa terá o papel de controlar as implantações das práticas de Segurança da Informação e acompanhar e proteger as evoluções e resultados dos processos e recursos de TI do negócio.

d) Definir as responsabilidades e a estrutura do Planejamento Segurança da Informação

De acordo com a avaliação dos processos de negócio da Cooplantas, foi elaborada a Tabela 6 com as responsabilidades básicas do Planejamento de Segurança da Informação.

Tabela 6 - Responsabilidades do Planejamento de Segurança da Informação

Responsabilidades do Planejamento de Segurança da Informação	**Responsável**
Validação das práticas e políticas de Segurança da Informação que forem implantadas.	Gestor de TI
Controle dos riscos.	Gestor de TI
Controle de implementações para melhorias e adaptações do Planejamento de Segurança da Informação.	Gestor de TI
Controle de confidencialidade das informações.	Gestor de TI
Controle de integridade das informações.	Gestor de TI
Controle de disponibilidade das informações.	Gestor de TI
Controle de autenticação das informações.	Gestor de TI
Controle de não repúdio.	Gestor de TI

É importante salientar que todos os direitos decisórios em relação a TI e a Segurança da Informação serão designados ao Gestor de TI e discutidos com a alta direção quando necessário.

e) Definir o escopo básico do Planejamento de Segurança da Informação

De acordo com as informações coletadas na visita *in loco* à cooperativa, o escopo básico do Planejamento de Segurança da Informação da Cooplantas foi definido como mostra a Tabela 7:

Tabela 7 - Escopo básico do Planejamento de Segurança da Informação

1 - Analisar os processos de negócio
1.1 – Observar as atividades
1.2 – Entrevistar os usuários do sistema/computadores/tecnologias
1.3 – Fazer reuniões com responsáveis de áreas
1.4 – Gerar relatório com os resultados da análise
Analisar os processos de negócios da empresa, a fim de encontrar falhas de segurança no sistema/infraestrutura. A atividade deverá ser feita através de observações, entrevistas com os usuários, apontamentos e reuniões com responsáveis de áreas. Após essa primeira etapa, deverá ser feito um ou mais relatórios com os resultados dessa análise.
2 - Definir os conceitos de Segurança da Informação que serão implantados
2.1 - Levantar as metodologias de Segurança da Informação oferecidas pelo mercado
2.2 – Avaliar as metodologias levantadas
2.3 – Discutir internamente em reuniões com a alta direção
2.4 – Definir os conceitos de Segurança da Informação que serão adotados
Nesta etapa será feito um levantamento das metodologias de Segurança da Informação que o mercado oferece, a fim de encontrar a metodologia que melhor se ajusta ao negócio da empresa. Neste levantamento serão feitas avaliações dos conceitos estudados, onde deverá ser discutido internamente com a alta direção, para que assim possam ser definidos os conceitos de Segurança da Informação que serão adotados para proteção e controle dos ativos de TI.
3 - Definir os procedimentos de Segurança da Informação que serão implantados
3.1 – Definir uma padronização de processos de Segurança da Informação
3.2 – Definir responsáveis pela garantia da execução dos procedimentos
3.3 – Apresentar os conceitos com os processos definidos para os cooperados
Será definida uma padronização de processos, para auxiliar na constituição dos controles de Segurança da Informação da Cooplantas. Então, será preciso estabelecer a partir dos conceitos escolhidos, padrões que serão adotados na execução dos processos operacionais e administrativos dos cooperados através do computador/sistema de planilhas. Após definido e estabelecidos, os procedimentos deverão ser apresentados a todos os cooperados.
4 – Implantar e controlar a Segurança da Informação
4.1 - Definir cronograma
4.2 - Estabelecer o início da implantação dos conceitos e procedimentos
4.3 - Delegar tarefas de controles de Segurança da Informação
4.4 - Vistoriar o cumprimento dos procedimentos e cronograma

Após conhecer os processos de negócio da empresa e suas necessidades, e em seguida definir o conceito e os procedimentos que deverão ser adotados, serão feitas as suas implantações. Para isso, será definido um cronograma com tarefas de implantação a serem seguidas pelo responsável de TI e pelos cooperados no geral. Depois desta etapa, deverá ser realizada uma vistoria para validar o cumprimento dos conceitos e procedimentos de Segurança da Informação.

f) Estabelecer um mapa de etapas, considerando ações de curto, médio e longos prazos

Para a execução do Planejamento de Segurança da Informação, será desenvolvido um diagrama de Gantt que abordará de forma detalhada as atividades de Segurança da Informação que deverão ser seguidas nessa cooperativa.. Com isso, será possível ter a visão de todas as etapas a serem seguidas pela equipe de TI e o avanço previsto dentro do cronograma definido. Gerando um controle maior do progresso do cronograma e do planejamento.

g) Elaborar o plano de gerenciamento da mudança da cultura organizacional

Para que o Planejamento de Segurança da Informação seja aplicada de fato, será preciso contar com o engajamento dos cooperados. Então, serão feitas eventuais mudanças na cultura organizacional da cooperativa com o olhar voltado para a Segurança da Informação durante o andamento e progresso do planejamento. Mas para isso, durante a execução das etapas, será necessário realizar a análise do ambiente e a partir disso identificar a cultura atual e definir a desejada. Portanto, torna-se necessário a execução das seguintes etapas:

- Reuniões para entender como funciona a execução do trabalho de todos os cooperados;
- Com base nas reuniões, deverão ser feitas análises comparativas entre a cultura atual e a cultura desejada no olhar do Planejamento de Segurança da Informação;
- Elaborar planos de comunicação entre a cooperativa e os cooperados para mantê-los informados sobre qualquer atualização ou mudança no âmbito de tecnologias e Segurança da Informação e que irão impacta-los, bem como mensagens culturais e informativas nos murais da empresa;
- Definir responsáveis dentro da cooperativa para realizar e apoiar o gerenciamento da mudança de cultura organizacional;
- Realizar palestras para conscientizar e informar a todos sobre do que se trata as mudanças e quais serão os seus benefícios para a cooperativa;
- Enviar e-mails informativos e publicar informações nos murais da empresa;
- Implantar políticas de segurança
- Estabelecer metas a serem atingidas com o engajamento de todos;

h) Revisar e evoluir o Planejamento de Segurança da Informação

Ao final do cronograma de cada etapa, deverá ser feita uma reavaliação do planejamento, para definir se as decisões do Planejamento de Segurança da Informação ainda estão alinhadas ao negócio da Cooplantas, ou se será necessária uma mudança na estratégia do Planejamento de Segurança da Informação.

Isso será feito através de uma avaliação dos erros e acertos cometidos, dos resultados gerados e da análise da evolução do negócio da cooperativa no período em que estas etapas foram implantadas. Dessa forma, serão encontrados pontos a serem aperfeiçoados e mantidos na evolução contínua do planejamento.

CONSIDERAÇÕES FINAIS

O trabalho de planejamento, execução e controle das ações de segurança da informação são, não apenas importantes, como também essenciais para o sucesso de qualquer atividade profissional baseada e suportada por sistemas de informação computadorizados.

Este trabalho propiciou a oportunidade de conhecer na prática as dificuldades inerentes à aplicação de procedimentos de segurança em uma cooperativa. Essas dificuldades acontecem nesse tipo de organização, bem como, em qualquer outro tipo que hoje estão atuando no mundo do trabalho.

Ao longo do processo de desenvolvimento do plano estratégico de TI voltado para a segurança da informação apresentado neste trabalho, outras proposições serão levantadas com o intuito de se criar a ambiência necessária para que os dados e as informações importantes para o negócio da cooperativa estejam protegidos e essa possa continuar competitiva no mercado. Esses dados são fundamentais para que haja o crescimento do negócio e o alcance da expectativa de tantas famílias que há anos aguardam uma melhoria de sua qualidade de vida através do trabalho árduo e honesto desempenhado por todos os cooperados, que, por mais que seja feito de forma correta e dedicada, nem sempre possui o ferramental necessário para a competitividade que o ambiente empresarial exige.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002: Tecnologia da Informação – Técnicas de Segurança – Código de Prática para a Gestão da Segurança da Informação. Rio de Janeiro, 2005.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 17799:2005: Tecnologia da Informação – Técnicas de Segurança – Código de Prática para a Gestão da Segurança da Informação. Rio de Janeiro, 2005.

BRUM, Fernando. **A importância da Informação para Empresas de Sucesso**: Uma abordagem sobre a importância da informação no atual ambiente empresarial, 2011.Disponível em: <http://www.brumconsulting.com.br/2011/08/importancia-informacao-sucesso-empresas.html>. Acesso em: 09 mar. 2018.

CRÚZIO, Helnom de Oliveira. **Como organizar e administrar uma cooperativa.** 1º ed. Rio de Janeiro: FGV, 2000.

FERREIRA, Fernando N. F.; ARAÚJO, T.. **Política de Segurança da Informação:** Guia Prático Para Elaboração e Implementação. 2º ed. **Rio de Janeiro**: Ciência Moderna, 2008.

ISO, (2008). ISO/IEC 27005 Information technology - Security techniques - Information security risk management. International Organization for Standardization

LAUDON, Kenneth C.; LAUDON, Jane P.. **Sistemas de Informação Gerenciais.** 11. ed. São Paulo: Pearson Education do Brasil Ltda., 2015.

LYRA, Maurício Rocha. **Segurança e auditoria em sistemas de informação.** Rio de Janeiro: Ciência Moderna Ltda., 2008.

MARCIANO, João Luiz; LIMA-MARQUES, Mamede. **O enfoque social da Segurança da Informação. Ci. Inf.**, Brasília, v. 35, n. 3, p. 89-98, dez. 2006. Disponível em <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0100-19652006000300009&lng=pt&nrm=iso>. Acesso em 11 abr. 2018.

MATTOS, Antonio Carlos M.. **Sistema de Informação:** Uma visão executiva. 2. ed. São Paulo: Saraiva, 2010.

MAUAD, Marcelo José Ladeira. **As cooperativas de trabalho e sua relação com o direito do trabalho**. Revista da Faculdade de Direitos de São Bernardo do Campo, São Bernardo do Campo, v. 6, n. 1, 2000. Disponível em: <https://revistas.direitosbc.br/index.php/fdsbc/article/download/ 586/448>. Acesso em: 14 Mar. 2018.

MORAES, Giseli Diniz de Almeida; TERENCE, Ana Cláudia Fernandes; ESCRIVAO FILHO, Edmundo. **A tecnologia da informação como suporte à gestão estratégica da informação na pequena empresa**. JISTEM J.Inf.Syst. Technol. Manag. (Online**)**, São Paulo, v. 1, n. 1, p. 27-43, 2004. Disponível em <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1807-17752004000100003&lng=en&nrm=iso>. Acesso em 27 Mar. 2018.

PRATES, Glaúcia Aparecida; OSPINA, Marco Túlio. **Tecnologia da informação em pequenas empresas**: fatores de êxito, restrições e benefícios. **Rev. adm. contemp.**, Curitiba, v. 8, n. 2, p. 9-26, Jun 2004 Disponível em: <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1415-65552004000200002&lng=en&nrm=iso>. access on 27 Mar. 2018.

SÊMOLA, Marcos. **Gestão da Segurança da Informação:** uma visão executiva. Rio de Janeiro: Campus, 2003.