Tecnologia

SEGURANÇA DA INFORMAÇÃO: DA CONSTITUIÇÃO E ATUAÇÃO DO CONSELHO GESTOR DE SEGURANÇA NA ORGANIZAÇÃO MILITAR

GUSTAVO PANIAGUA DOS SANTOS[1],WILBERT CARPI SILVA[2],MARCOS NALIN[3]

Resumo: A necessidade de segurança não está voltada para um departamento ou um ativo em específico, mas sim a tudo que compreende a organização como um todo no seu processo de negócio. É necessário criar um Conselho Corporativo de Segurança da Informação estrategicamente posicionado na hierarquia e dotado de capacidade técnica e política suficientes para implementar ações baseadas em um Modelo de Gestão Corporativa de Segurança, que possibilite manter um processo cíclico e contínuo de planejamento, coordenação, controle e execução de medidas de segurança à informação tornando a organização capaz de auto-gestão sobre novas ameaças e vulnerabilidade decorrentes de alterações de variáveis internas e externas ao seu negócio. realizar a implantação do Conselho Gestor de Segurança da Informação na estrutura de uma Organização Militar. O Conselho Gestor de Segurança passará a ser o principal responsável em identificar o tamanho, a amplitude e complexidade das questões relacionadas Segurança da Informação, atuando na coordenação e controle de diversas ações, construindo assim uma solução às necessidades da Organização Militar.

Palavras-chave: segurança da informação, planejamento, coordenação, controle e execução.

Abstract. The necessity of security should not focus only a department or specific assets, but it should involve the whole organization in its working process. It is essential to create a corporative committee for information security supported by a hierarchical structure and endowed with technical and political capacity, so that the implementations of actions based on a model of corporate security management can keep cyclical and continuous planning process, coordination and execution of security measures related to information. Thus the organization itself can manage threats and vulnerabilities derived from internal and external changes in business scenario. This article intends to help establishment of a management commitee for information security in the organizational structure of the Brazilian Army. The Managing Council of Security comes to be the main body in charge of identifying the size, breadth and complexity of the questions related to information security, working in the coordination and control of various actions and therefore building an integrated solution to the needs of the military organization.

Keywords: information security, planning, coordination, control and execution.

1. Introdução

Uma grande dificuldade que as organizações têm enfrentado é a de controlar e manter a confidencialidade, integridade e disponibilidade das informações dentro e fora dos seus limites físicos, visto o grande fluxo de dados distribuídos e compartilhados na grande rede. Na maioria das vezes, isto ocorre devido à deficiência de percepção do objetivo da segurança da informação dentro da instituição. Controlar o acesso à rede de computadores, gerar cópias de segurança dos dados e outras ações básicas e comuns no meio tecnológico podem ilusoriamente definir a atuação da segurança da informação na organização como satisfatória, o que, segundo Sêmola, causa uma falsa sensação de segurança, ou seja, é a não visualização dos diversos níveis de vulnerabilidades as quais os ativos de uma organização estão sujeitos.

[1] Escola de Administração do Exército (EsAEx), Salvador, Brasil. gpaniagua@ibest.com.br.
[2] Escola de Administração do Exército (EsAEx), Salvador, Brasil. wilbert_carpi@hotmail.com.
[3] Escola de Administração do Exército (EsAEx), Salvador, Brasil. nalin@globo.com.

Com isso, percebemos que falta uma visão corporativa de segurança onde, de um outro nível de percepção, vemos não só os ativos que o departamento de informática visualiza e manipula, mas sim os que circulam por todos os setores da organização.

> O nível de segurança de uma empresa está diretamente associado à segurança oferecida pela "porta" mais fraca. Por isso, é preciso ter uma visão corporativa capaz de viabilizar uma ação consistente e abrangente levando a empresa a atingir o nível de segurança adequado à natureza de seu negócio. (SÊMOLA, 2003)

Diante desse cenário, o desafio da organização, no tocante ao modelo de gestão de segurança da informação, é a necessidade da formação de uma equipe de profissionais, formada por pessoas oriundas de vários setores da organização, responsável em realizar a tomada de ações com o intuito de mapear e identificar a situação geral da empresa, em que se deve identificar as ameaças, vulnerabilidades, riscos e os impactos a fim de que se construa uma solução que possa abranger a organização como um todo. Esta equipe é denominada de Conselho Gestor de Segurança da Informação.

Esse modelo de gestão de segurança já é realidade na comunidade européia, haja vista a criação da ENISA – ***European Network and Information Security Agency*** – que teve início de suas atividades em janeiro de 2004, e que tem por objetivo facilitar e intensificar a coordenação européia no domínio da segurança da informação e, deste modo, proporcionar um nível de segurança suficientemente elevado nos países pertencentes à União Européia (UE). A agência destina-se, portanto, a reforçar a capacidade da comunidade européia e dos países-membros de dar respostas a problemas de segurança das redes de comunicação e da informação.

A NBR ISO/IEC 17799, publicada no ano de 2001, é a norma brasileira que trata da gestão da segurança da informação e esta norma recomenda que seja criada uma estrutura de gerenciamento para iniciar a implementação da segurança da informação dentro da organização.

> Convém que fóruns apropriados de gerenciamento com liderança da direção sejam estabelecidos para aprovar a política de segurança da informação, atribuir as funções da segurança e coordenar a implementação da segurança através da organização.(NBR ISO/IEC 17799, 2001)

Hoje, a utilização da tecnologia da informação é componente essencial da vida diária de qualquer organização militar, da mesma forma a questão segurança da informação tornou-se um assunto de preocupação crescente devido às constantes ameaças de violações que estão sujeitas. Isso fez com que as OM reagissem implementando novas tecnologias para aumentar a segurança e adotando normas e procedimentos internos, como no caso das políticas de segurança. É natural que essas ações sejam diferentes para cada organização, porém é necessário que haja uma padronização no processo de coordenação das atividades voltadas para a segurança da informação, permitindo alcançar uma solução eficaz para os problemas da segurança.

Nesse sentido, vimos propor a realização de implantação do Conselho Gestor de Segurança da Informação dentro da estrutura de uma Organização Militar, demonstrando uma possível constituição e forma de atuação para que se possa garantir um direcionamento claro e um suporte de gestão visível dos envolvidos para as iniciativas de segurança. Para a realização dessa proposta, utilizaremos a metodologia apresentada no livro Gestão da Segurança

da Informação – Uma Visão Executiva, de Sêmola (2003).

2. Ciclo de Vida da Informação

A informação é um bem e o seu valor é perfeitamente possível de ser medido. Portanto, a informação deve ser mantida em segurança, assim como os ambientes e os equipamentos utilizados para o seu processamento. Conforme a NBR ISO/IEC 17799 a informação possui três atributos essenciais: a confidencialidade, a integridade e a disponibilidade. A confidencialidade é a garantia de que a informação é acessível somente para pessoas autorizadas a terem acesso. A integridade é a garantia de que a informação será recebida na íntegra, ou seja, que não foi alterada por pessoas não autorizadas para tal, e a disponibilidade é a garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário. A segurança da informação visa a garantir que a informação não tenha seus atributos essenciais violados.

Por ser um objeto valioso para qualquer organização, os aspectos referentes à segurança da informação devem ser minuciosamente observados como os atributos essenciais descritos anteriormente, e, principalmente, devem ser avaliados todos os momentos que fazem parte do ciclo de vida da informação.

O ciclo de vida da informação pode ser caracterizado pelos momentos em que a informação é colocada em risco, ou seja, quando da existência da possibilidade de perda de pelo menos um de seus atributos essenciais. Estes momentos são vivenciados justamente quando ativos físicos, tecnológicos e humanos fazem uso da informação independentemente da forma como ela é representada, seja na forma eletrônica ou não.

Segundo Marcos Sêmola, o ciclo de vida da informação possui quatro momentos e todos eles merecem a mesma importância pelos profissionais que tratam de segurança da informação. São eles:

> **Manuseio:** Caracterizado pelo instante em que a informação é criada e manipulada, seja ao manusear um relatório impresso, ao utilizar uma senha para obter acesso a um ambiente que necessite autenticação e até mesmo ao digitar informações que irão trafegar em uma rede;
> **Armazenamento:** Momento em que a informação é armazenada para ser utilizada posteriormente, seja em um servidor de banco de dados, em papel, ou ainda em um disquete;
> **Transporte:** Momento em que a informação é transportada do emissor até o destino, ou seja, até o receptor. Neste caso pode ser o encaminhamento de uma mensagem via correio eletrônico, transmissão de fax e até mesmo uma conversa ao telefone;
> **Descarte:** Sendo tão importante como os anteriores, este momento é caracterizado quando a informação é descartada, independente do meio em que ela está armazenada.

Todos os quatro momentos do ciclo de vida da informação vistos acima possuem grande importância para que se preservem os princípios da segurança. Se em um determinado instante, o ativo, que estiver utilizando a informação, deixe de atentar para qualquer um dos momentos previstos, então vulnerabilidades serão expostas e, em conseqüência disso, a informação será um alvo que poderá ser explorado pelas ameaças.

> A visão corporativa da segurança da informação deve ser comparada a uma corrente, em que o elo mais fraco determina seu grau de resistência e

> proteção. A invasão ocorre onde a segurança falha. (SÊMOLA, 2003)

3. A Necessidade de Segurança

Um fator que vem superando o limite da produtividade e da funcionalidade, em qualquer ambiente, é a necessidade de segurança, pois da mesma maneira que a evolução da tecnologia permitiu uma agilização do cumprimento de diversas tarefas, também possibilitou a criação de novos riscos e ameaças que podem resultar em grandes prejuízos para esses sistemas.

Podia-se dizer que, antes da chamada "Era da Informação", o patrimônio de uma organização era mensurado considerando apenas seus bens materiais. Com o progresso da informática juntamente com as redes de comunicação, a informação, que antes era representada na forma de papéis, entra em um novo cenário passando a ser representada eletronicamente. Atualmente, as organizações utilizam a tecnologia da informação com o objetivo de aumentar a agilidade dos processos envolvidos e, com isso, melhorar a produtividade aliada à redução dos custos.

Com isso, o compartilhamento de informações passou a ser considerado uma prática necessária e, nesse contexto, pode-se perceber que as organizações passaram a ter um alto grau da dependência a informação. Por isso, o principal desafio da Segurança da Informação é como disponibilizar informações que sejam íntegras, confiáveis e que garantam também sua "confidencialidade" quando necessária. Uma falha, uma comunicação com informações falsas ou um roubo ou fraude de informações podem trazer graves conseqüências para a organização. Deste modo, a proteção, não só das informações, mas também de todos os recursos envolvidos da infra-estrutura tecnológica utilizada para o seu processamento, deve ser tratada com devida importância. E como a informação é o principal capital das organizações, protegê-la significa proteger seu próprio negócio. Um grande problema, que ainda existe em muitas organizações, é que muitos processos foram desenvolvidos sem o devido enfoque na segurança, e o resultado disso é uma aplicação de "remendos" para os problemas de segurança que vão surgindo constantemente, sem uma estratégia e uma arquitetura que protejam de fato a organização. Essa abordagem de "remendos" cria uma falsa sensação de segurança, o que é muito perigoso, e muitas vezes é pior do que não ter segurança alguma. A superficialidade e a utilização de técnicas parciais e incompletas pode aumentar a vulnerabilidade da organização.

> Devemos compreender que o grande alvo é a informação, e que a mesma circula por toda a organização, alimenta todos os processos do negócio, e está sujeita a variadas ameaças, furos de segurança ou vulnerabilidades que transcendem os aspectos tecnológicos, são alvos também de interferências provocadas por aspectos físicos e humanos. (SÊMOLA, 2003).

Ainda hoje, existe a falta de uma melhor percepção do problema da segurança e uma maior conscientização por parte das pessoas que ocupam posições estratégicas nos setores administrativos das organizações, e isso são fatores que devem ser considerados como barreiras na implantação da segurança da informação dentro das organizações.

Em outubro de 2003, a Módulo Security Solutions, empresa brasileira especializada em segurança da informação, divulgou a 9ª Pesquisa Nacional de Segurança da Informação. Os profissionais que participaram deste estudo foram divididos em vários segmentos, entre eles 17% faziam parte de órgãos do Governo. Diante dessa pesquisa, obteve-se que os três principais obstáculos para implementação da segurança da informação nas empresas

foram: falta de consciência dos executivos (23%), dificuldade em demonstrar o retorno (18%) e custo de implementação (16%). E ainda, 51% dos entrevistados acreditam que os executivos consideram a Segurança da Informação fundamental para a integridade e continuidade de seus negócios, sendo que para 21% é fator vital e para 16% é crítica. Vemos que, apesar dessa visão otimista, a falta de conscientização de executivos ainda é considerada como o principal obstáculo para implementação da Segurança da Informação dentro das organizações.

Assim, pode-se dizer que, na área de segurança da informação, muito mais importante do que utilizar uma determinada tecnologia ou procedimento, é essencial que seja formada, entre os integrantes de uma organização, uma cultura de segurança. O sucesso da disseminação de uma nova cultura é algo que demanda tempo, deve ser trabalhado a médio e longo prazo. E a origem desta nova idéia deve ter princípio no corpo executivo de uma determinada organização. Por isso, implementação da segurança da informação deve-se iniciar no formato *top down*, ou seja, com a conscientização do corpo executivo de uma organização, para atingir os demais integrantes dentro da hierarquia.

4. Modelo de Gestão Corporativa de Segurança

O Conselho Gestor de Segurança da Informação é uma estrutura, que, como em qualquer outro processo corporativo, precisa ser implementado na instituição com a finalidade de promover a garantia da segurança corporativa, ou seja, envolver não só um departamento, mas sim todos os segmentos administrativos.

Sêmola nos propõe um Modelo de Gestão Corporativa de Segurança, onde se enfatiza a importância da criação de mais uma unidade administrativa, bem como do seu envolvimento com as unidades já existentes. O objetivo é a atuação continuada dessa gestão sobre todos os departamentos e processos da organização, buscando a implementação, a administração e a consolidação da segurança corporativa.

Segundo o modelo, esses objetivos podem ser alcançados seguindo uma linha de trabalho baseada em um fluxo seqüencial de etapas, onde existem dados crus ou semiprocessados, que servem de orientação para análise e formalização deste trabalho, e depois de mesclados e processados, obtêm-se resultados que demonstrarão a efetivação do trabalho do conselho. As etapas constituem: Conselho Corporativo de Segurança da Informação; Mapeamento da Segurança; Estratégia de Segurança; Planejamento de Segurança; Implementação de Segurança; Administração de Segurança; e Segurança na Cadeia Produtiva.

A primeira etapa consiste na criação de um conselho responsável pela gestão da segurança. As suas atribuições estão ligadas exclusivamente ao nível de supervisão não devendo atuar diretamente na linha de ação. O seu papel está direcionado à orientação e à administração da segurança corporativa. Os seus objetivos são:

> **Orientar** a organização na implantação da segurança e avaliar os seus resultados;
>
> **Adequar** o plano de ação às diretrizes estratégicas do negócio de forma que haja o máximo de retorno dentro de um investimento apropriado;
>
> **Coordenar** os agentes de segurança em seus Conselhos Interdepartamentais, ou seja, os seus representantes dentro dos diversos departamentos, a fim de manter sincronismo na implantação das ações pré-definidas, bem como na existência de possíveis ajustes no plano de ação;

Administrar e garantir a implantação do Modelo de Gestão Corporativa de Segurança de tal forma que o sucesso seja alcançado em capacitação de auto-gestão podendo compreender novos desafios com autonomia.

Na segunda etapa faremos um mapeamento de toda a necessidade de segurança existente na organização, levando em consideração todos os bens importantes para o negócio, físicos ou não. Relacionamos como tarefas a serem cumpridas:

Identificar processos de negócio e grau de importância para a organização;

Inventariar todos os ativos responsáveis pela manutenção da organização e que sustentam a sua operação, bem como tudo o que causa interferência ou alteração nas estratégias do negócio interna ou externamente;

Elaborar uma Matriz de Riscos, envolvendo ameaças, vulnerabilidades e impactos, possibilitando uma análise detalhada e propondo uma lista de medidas de segurança a serem tomadas;

Relacionar todas as necessidades sobre a informação, no que diz respeito ao seu manuseio, armazenamento, transporte e descarte, a fim de que haja uma orientação mais específica na sua segurança.

Não menos importante, a etapa que se segue consiste em definir elementos comportamentais e necessários para a implantação da segurança. A estratégia de segurança sugere:

Definir um plano de ação de nível corporativo, considerando todas as estratégias de negócio, interesses da organização e todos os seus processos e ativos;

Buscar o poder político necessário para o apoio na execução das ações de segurança através da conscientização dos executivos pela sua importância na manutenção do negócio.

Neste momento temos uma situação que irá facilitar a passagem para a próxima etapa, pois é quando precisamos do envolvimento dos responsáveis dentro dos departamentos, haja vista a concretização de uma vontade política por parte dos executivos. Deve ser elaborado um planejamento de segurança onde se deve:

Alinhar responsabilidades dos Conselhos Interdepartamentais às ações globais do Conselho Corporativo de Segurança da Informação;

Capacitar tecnicamente as pessoas envolvidas na liderança, a fim de torná-las co-responsáveis pelo sucesso do modelo de gestão;

Elaborar uma Política de Segurança da Informação que possa gerar Diretrizes, Normas, Procedimentos e Instruções que servirão de apoio à toda ação executada na organização, sempre de encontro às necessidades estratégicas. O manuseio, o armanezamento, o transporte e o descarte de informações devem ser levantados de forma a atingir o ideal dentro da faixa de risco;

Minimizar a possibilidade de ameaças iminentes levantadas no passo anterior, quando do mapeamento de riscos elaborado para a definição da Política de Segurança da Informação.

Na etapa de implementação de segurança, onde vemos a oficialização da Política de Segurança dentro da organização, podemos observar a execução de alguns passos:

Disseminar a Política de Segurança entre executivos, técnicos e usuários tornando-os práticos no relacionamento da informação;

Treinar os usuários de forma a habilitá-los nas boas práticas de manuseio, armazenamento, transporte e descarte da informação, alertando-os pela responsabilidade na sua execução;

Implementar as técnicas existentes para minimizar ou, se possível, eliminar as vulnerabilidades observadas, a fim de nivelar os riscos, no mínimo, a um ponto de administração e dar segurança para uma boa operação.

A manutenção das medidas estratégicas de segurança e o monitoramento das ações definidas compreendem a parte principal da etapa de administração de segurança. Os passos a serem observados nesta etapa são:

Monitorar os controles implementados observando mudanças decorridas da existência de variáveis internas e externas organização e que possam modificar o grau de vulnerabilidade, ou, até, o aparecimento de novas ameaças;

Calcular o ROI – *Return Over Investment*, ou Retorno sobre o Investimento – utilizando as medições realizadas sobre as ações implementadas, a fim de posicionar estrategicamente os excutivos e responsáveis pelos conselhos interdepartamentais e viabilizar novas necessidades sob demandas do negócio;

Observar o equilíbrio entre o negócio e as normas e regras pertinentes, sejam internas ou externas, devendo manter padrões e respeitar a legislação;

Garantir a continuidade do negócio através da definição de planos de contingência e recuperação de desastres, a fim de estar preparada para o restabelecimento rápido da operacionalidade do negócio;

Administrar a compatibilização dos controles implementados com a Política de Segurança e preparar as suas regras de operação para atender a novas necessidades do negócio.

A última etapa consiste em aplicar as normas de segurança implementadas nas interfaces externas que se relacionam com o negócio da organização, ou seja, a segurança na cadeia produtiva. O passo a ser executado determina:

Equalizar as medidas de segurança adotadas pela organização aos processos de negócio que envolvem parceiros. A necessidade de comunicação com fornecedores, clientes, governo, etc, não deve comprometer o trabalho de controle na segurança da informação, mantendo-a segura nas suas diversas interfaces.

É importante salientar a necessidade de segurança sobre os ativos da organização lembrando que nenhum trabalho de controle e prevenção tem fim, e que este novo processo é cíclico e deve ser de auto-gestão, ou seja, a organização deve ser capaz de administrar os planos de

ação, de política da segurança, planos de continuidade, planos de contingência e todos os documentos normativos, a fim de adequá-los a novas tendências de mercado, a novas ameaças e vulnerabilidades decorrentes de alterações estratégicas do negócio.

A proposta do Modelo de Gestão Corporativa de Segurança da Informação consiste em um processo cíclico e contínuo onde é necessário planejar, coordenar, controlar e executar todas as ações (figura 01) e medidas de segurança necessárias para a manutenção do negócio da organização.

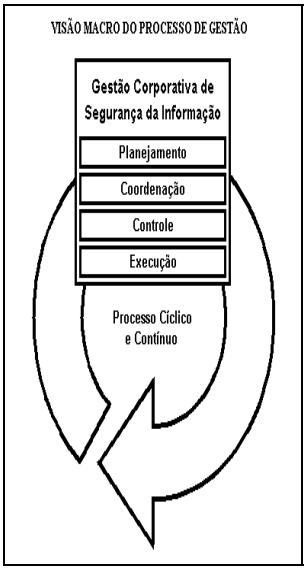

Figura 01

5. Conselho Gestor de Segurança da Informação

É fator crítico de sucesso iniciar a organização de um grupo, convencionalmente chamado de Conselho Corporativo de Segurança.

> A primeira atividade é definir as responsabilidades de planejamento, execução, monitoração, seu posicionamento dentro do organograma da organização, garantindo que tenham acesso a esferas decisivas que possam atuar sobre toda a corporação. Seu principal papel será organizar, concentrar e planejar as ações de segurança que irão interferir em todos os ambientes e processos, tendo a possibilidade de redirecionar os planos de acordo com as mudanças físicas, tecnológicas e humanas que, inevitavelmente, ocorrerão. (SÊMOLA, 2003).

O Conselho Corporativo de Segurança ou Conselho Gestor de Segurança da Informação é ponto central na responsabilidade de fomentar a segurança adequada da informação promovendo a organização e orientação na implantação de um Modelo de Gestão Corporativa de Segurança.

O conselho deve estar estrategicamente posicionado na hierarquia de tal forma a ter respaldo político para fazer executar o modelo nas diversas áreas da organização e em seus diferentes níveis hierárquicos.

Todos os departamentos devem ter o mesmo conceito e conhecimento dessa necessidade e para isso é necessário fazê-los responsáveis pela própria implementação. Deve haver um treinamento que prepare não só os executivos para essa jornada, mas também os chefes das células administrativas da organização, reais responsáveis pelo sucesso na implementação do modelo.

Tem como objetivos definidos:

Administrar e fiscalizar a implementação do Modelo de Gestão Corporativa de Segurança da Informação em todos os segmentos da organização de forma integrada e envolvendo diretamente todos os processos de negócio;

Analisar resultados da implementação interdepartamental, sempre levando em consideração as metas definidas, fazendo um comparativo com os possíveis efeitos desses resultados e, se necessário, adequar o Plano Diretor de Segurança às novas mudanças percebidas nas variáveis internas e externas;

Interagir com os conselhos executivo e de auditoria, a fim de resolver e demonstrar resultados corporativos do conselho de segurança. A troca de informações, baseada nos índices e indicadores de segurança definidos, será a base para se obter essas informações;

Alinhar o trabalho dos conselhos interdepartamentais ao do conselho corporativo, a fim de manter uma implementação uniforme e baseada num único modelo. O chefe de departamento tem a capacidade e o alcance de detalhes que o conselho corporativo não tem, e com isso é possível definir ações mais específicas de forma a atingir os problemas diretamente.

O Modelo de Gestão Corporativa de Segurança da Informação sugere a criação de Conselhos Interdepartamentais, a fim de orientar a implementação pelos segmentos da estrutura organizacional onde há maior representatividade e criticidade. Esses departamentos são considerados Células de Segurança pela formação de equipes locais, que têm a responsabilidade de manter um alinhamento da sua abrangência à dimensão corporativa.

> Com uma esfera de abrangência menor, estes conselhos têm importante papel no modelo de gestão de segurança da informação. Apesar de estarem sendo orientados por diretrizes maiores na esfera do Conselho Corporativo de Segurança, deverão medir os resultados dos ambientes específicos, reportar novas necessidades e situações qe expoham a informação. (SÊMOLA, 2003, p98).

A formação do conselho é baseada na representação política e técnica exercida dentro da organização e é composta por:

Coordenação Geral de Segurança: é responsável pelo envolvimento da organização, mobilizando os diversos segmentos para a execução do modelo. Este modelo irá formar índices e indicadores de segurança e metas a serem alcançadas. É uma função diretamente política e de alta representação organizacional. Pode ser formada por diretores ou por pessoas de alto cargo de chefia;

Coordenação de Segurança: será a executora técnica das etapas do modelo, baseando-se sempre em resultados provenientes das ações tomadas ao longo do processo. Propõe mudanças, medidas e contramedidas, adequando-as às variáveis que contribuem para a dinamicidade do negócio. Essa função é técnica e deve possuir representação organizacional suficiente para a implementação e mobilização dos segmentos envolvidos no processo. Apresentamos aqui a figura do Oficial de Segurança – *Security Officer* – dotado de experiência e conhecimento técnico sobre segurança da informação, ele é o Gestor de Segurança;

Planejamento e Avaliação: apóiam o coordenador geral no desenvolvimento de palestras de conscientização, na elaboração de propostas de projetos de segurança, bem como na elaboração de relatórios de acompanhamento, exibindo resultados alcançados ao longo do processo. Consultores de Segurança e de Contingência, Analistas e Assistentes de Segurança participam da função de Planejamento e Avaliação;

Controle: é uma função que tem por finalidade realizar análises de risco e análises de métricas dos índices e indicadores de segurança, tendo a responsabilidade pelo treinamento na execução do seu

manuseio. O Controle é responsável, também, por exercer funções de auditoria e monitoramento. Encontram-se aqui os Auditores de Segurança, o Gerente de Risco e o Monitor d Segurança;

Execução: é a função de exigir o cumprimento da Política de Segurança na organização, de fornecer resultados dos índices e indicadores e segurança à função Controle, de atender e fornecer informações à auditoria. Mantém a função Controle informada por quebra de segurança e executa medidas e contramedidas de contenção. Administrador de Rede, Gestor de Desenvolvimento, Gestor de Produção, Gestor de Aplicação, Gestor de Segurança Física e Suporte a Tecnologias são as figuras ligadas à função de controle.

É importante fazer menção ao profissional responsável pela gestão de segurança, o *Security Officer*, pois este assume um papel substancial para o sucesso do modelo. O Oficial de Segurança precisa conhecer o negócio da empresa, o segmento de mercado onde ela está inserida e todas as expectativas do Corpo Executivo quanto ao que vai ser desempenhado durante o processo de implantação do modelo.

O Oficial de Segurança encontrará vários desafios que deverão ser tratados com cautela. É necessário conhecer e compreender os limites estruturais da organização observando a autoridade que cada componente possui dentro da hierarquia. Esse especialista precisa conhecer os processos de negócio da organização, ser sensível às mudanças culturais. Qualquer mudança física, tecnológica e humana será gerenciada por ele. Para atender às demandas de segurança do negócio, precisa também identificar profissionais preparados para exercer a função de executor do processo.

> Esta ocupação deve existir oficialmente na organização cujas responsabilidades e habilidades estejam diretamente associadas à liderança do Conselho Corporativo de Segurança e à interação com líderes dos Conselhos Interdepartamentais de Segurança. Perfil técnico aprofundado, visão corporativa e destreza para gestão são elementos fundamentais para que haja uma canalização de esforços de forma coerente com os macro-objetivos da segurança e do próprio negócio. (SÊMOLA, 2003).

6. Implantação e Atuação do Conselho Gestor de Segurança da Informação na Organização Militar

As Organizações Militares do Exército Brasileiro, a cada dia que passa, utilizam-se de recursos tecnológicos e redes de comunicação disponíveis para manipular as informações que trafegam dentro e fora dos perímetros de uma OM. Por isso, o tema Segurança da Informação não é mais novidade nas OM, pois já adotam medidas de segurança de acordo com a peculiaridade de cada uma. Mas ainda existe, por parte dos integrantes de uma OM, uma deficiência de percepção dos riscos que podem despontar durante o manuseio, armazenamento, transporte e descarte das informações.

Por isso, este artigo se propõe apresentar, como modelo de gestão corporativa de segurança , a criação de um Conselho Gestor de Segurança da Informação para atuar dentro de uma Organização Militar.

O Conselho passará a ser o principal elemento que identificará o tamanho, a amplitude e complexidade das questões relacionadas à Segurança da Informação, atuando como uma espécie de maestro, no acompanhando e coordenando as diversas ações, construindo asssim uma solução integrada às necessidades da OM.

De acordo com estudos realizados, vimos que os profissionais que irão compor o Conselho deverão ser oriundos

de diversas áreas estratégicas da organização para que se obtenha visões diferentes da segurança da informação. Sugerimos, portanto, que esses elementos sejam integrantes das seções que compõem o Estado-Maior da OM.

Analisando o contexto da Organização Militar, e levando em consideração a posição estratégica, vemos que o a função do coordenador geral do conselho gestor na segurança da informação poderá ser desempenhada pelo Subcomandante da Unidade, tendo como assessor direto o *Security Officer* que, segundo a proposta de Nascimento, deverá exercer sua atividade na 2ª seção. As demais células de segurança do conselho poderão ser compostas pelas 1ª, 2ª, 3ª e 4ª Seções, incluindo ainda a Seção de Relações Públicas e a Seção de Saúde da Unidade, ou seja, as seções que compõem o Estado-Maior da Unidade.

O *Security Officer* deverá possuir um perfil diferenciado, pois ele necessitará de um maior domínio dos conceitos, métodos e técnicas de segurança. Por isso, o *Security Officer* deverá ser o primeiro integrante do conselho gestor que necessitará estar qualificado e para isto, necessitará realizar o treinamento de capacitação através de cursos especializados e certificados em segurança da informação. A capacitação técnica do militar que estiver atuando como *Security Officer* torna-se um fator essencial, pois ele é o principal integrante do conselho gestor de segurança da informação e o elemento responsável em iniciar o treinamento dos representantes dos conselhos interdepartamentais.

O representante de cada conselho interdepartamental, ou célula de segurança, deverá ser o primeiro a receber o treinamento específico por parte do *Security Officer*. Esse integrante ficará responsável por realizar a disseminação das novas diretrizes de segurança da informação em sua célula de segurança.

O gestor de cada célula de segurança possuirá funções cruciais dentro do contexto da segurança corporativa, pois além de compor o Conselho Gestor de Segurança da Informação, também será o responsável pela disseminação da cultura de segurança da informação dentro da sua respectiva célula de segurança. O gestor da célula deverá possuir uma visão estratégica de segurança da informação, juntamente com o *Security Officer*, quando estiver atuando como integrante do Conselho, também deverá possuir visão tática e operacional quando estiver coordenando atividades dentro de sua célula de segurança específica.

A seguir, a figura 02 simboliza o Estado-Maior de uma Organização Militar, e mostra uma possível estrutura do Conselho Gestor de Segurança da Informação.

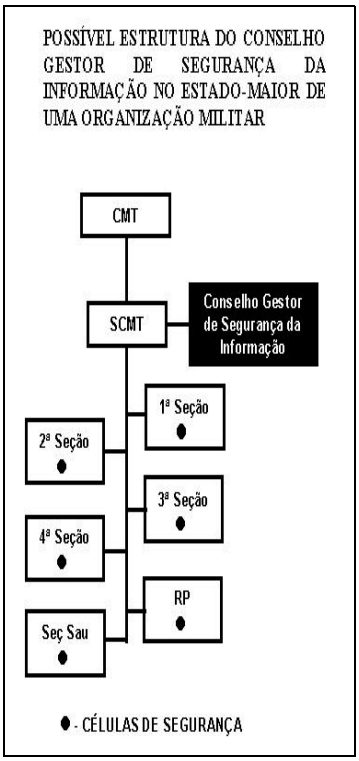

Figura 02

7. Conclusão

A segurança da informação é essencial para vida de qualquer organização, ainda mais que os

procedimentos adotados até hoje, e que são considerados seguros, podem ser quebrados a todo instante tanto pelos ativos que manipulam as informações quanto pelas novas tecnologias que vão surgindo. Por isso, é necessário que a organização tome as ações adequadas, e de forma constante, com o objetivo de buscar o aprimoramento das medidas de segurança. Porém, atingir um nível desejado de segurança não é possível sem a participação de todos os integrantes de uma determinada organização e, infelizmente, prevenção e segurança não fazem parte da cultura de nossa sociedade. Apesar da constante falta de tempo, a tarefa de disseminação da cultura de segurança não é algo que podemos estipular em curto prazo, isso demanda tempo. Incutir uma nova idéia de segurança em pessoas que até então achavam que isso era um assunto que nunca seria de seu interesse é uma tarefa que deve ser planejada para médio e longo prazos.

A visão estratégica da segurança ficará a cargo do Conselho Gestor de Segurança da Informação, que será o responsável em disseminar essa nova cultura dentro da Organização Militar. Além de planejar, aplicar e atualizar as medidas relativas à Segurança da Informação para cada Unidade, também será responsável pelo processo de conscientização de todos os integrantes, onde terá como principal objetivo mostrar que cada elemento, dentro de sua esfera de atribuição, é responsável pela segurança da informação de toda a organização. A visão tática e operacional do processo e o alcance de uma maturidade desse estado de consciência serão trabalhados essencialmente pelos representantes do Conselho Gestor da Segurança da Informação dentro de cada célula, ou seja, nos conselhos interdepartamentais de segurança.

Devemos ter em mente que para obter sucesso nas ações de segurança, requer esforços de médio e longo prazo, e que tem como principal objetivo provocar a mudança de cultura de nossa sociedade.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **Norma Brasileira Registrada – NBR ISO/IEC 17799**: tecnologia da informação – Código de prática para a gestão da segurança da informação. Rio de Janeiro: ABNT, 2001.

NASCIMENTO, Emerson da Rocha. **A importância do security officer na Organização Militar:** EsAEx, Salvador, 2003.

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