Modelo de Maturidade e Capacidades para a Defesa Cibernética

Sylvio André Diogo Silva – Instituto Tecnológico de Aeronáutica e Edgar Toshiro Yano – Instituto Tecnológico de Aeronáutica

***Resumo* — Uma implantação efetiva de um Sistema de Defesa Cibernética requer esforços coordenados de capacidades fundamentais: Governança, Comando e Controle, Mecanismos de Defesa e Supervisão da Defesa. A partir dessas capacidades fundamentais foi desenvolvido um modelo de capacidades que identifica os requisitos essenciais de um Sistema de Defesa Cibernética. A partir desse modelo foi concebido um modelo de maturidade de capacidades. O modelo proposto pode ser usado para avaliar e planejar a implantação de um sistema Defesa Cibernética.**

***Palavras-Chave* — defesa cibernética, modelos de capacidades e de maturidade.**

I. INTRODUÇÃO

A crescente dependência das organizações nos sistemas computacionais e a crescente integração desses sistemas por intermédio das redes de computadores tornam o chamado ciberespaço [1] num ambiente suscetível a combates de grandes proporções ou a uma guerra cibernética.

Na guerra cibernética os atacantes concentram seus esforços para atingir alvos governamentais e organizacionais com a intenção de sabotar, infiltrar, roubar e atacar, produzindo efeitos que podem proporcionar uma vantagem significativa frente ao oponente. Esse novo cenário de conflito tem levado a grandes investimentos em vários países em defesa cibernética a fim de garantir a integridade, disponibilidade, confidencialidade e disponibilidade dos seus sistemas mais críticos.

A Defesa Cibernética emprega as mesmas técnicas da Segurança da Informação. A diferença está na finalidade, motivação e emprego das metodologias. A Defesa Cibernética visa à proteção da missão de uma organização ou de ativos[1] críticos contra ataques que possuem motivações políticas e sociais e que podem afetar uma nação como um todo. A disponibilidade de recursos para os atacantes pode ser ilimitada. Quanto a metodologias, a Defesa Cibernética requer o uso de técnicas de comando e controle com o desenvolvimento e aprimoramento contínuo de estratégias e táticas. Na Defesa Cibernética os efeitos de um ataque podem afetar severamente uma organização causando prejuízos, por vezes, difíceis de mensurar e as medidas corretivas podem exigir grandes esforços da organização. Assim sendo é necessário um monitoramento e controle contínuo das ameaças e o emprego rápido de ações defensivas coordenadas e estabelecidas conforme um planejamento estratégico e tático.

Estabelecer um Sistema de Defesa Cibernética eficaz é um empreendimento complexo e requer esforços coordenados em gestão de processos, pessoal e tecnologia. Assim é desejável o uso de modelos que possam ser utilizados para identificar atividades e recursos necessários bem como para a avaliação dos esforços realizados. Modelos de maturidade tais como o CMMI[2] e CobiT[3] tem sido empregados com sucesso para a Governança de Tecnologia de Informação. Através desses modelos as organizações conseguem identificar o estado corrente quanto ao emprego de melhores práticas, o estado desejável e os passos a serem seguidos para alcançar esse estado. A motivação para esta pesquisa é criar um modelo de maturidade para defesa cibernética que possa ser utilizado para apoiar o planejamento, a implantação e a avaliação de sistemas de defesa cibernética.

Este artigo aborda a concepção de um modelo de maturidade de capacidades para defesa cibernética. Através desse modelo uma organização, com ativos susceptíveis a ameaças do ciberespaço, poderá identificar qual é o nível de desempenho corrente das capacidades de defesa, avaliar essas capacidades para enfrentar as ameaças e definir direções para a melhoria do sistema de defesa como um todo.

A estratégia utilizada para a concepção do modelo foi dividida em duas fases. Na primeira fase foi desenvolvido um modelo de capacidades para a defesa cibernética. Capacidades descrevem o que é realizado por uma função de negócio e o desempenho esperado. Uma capacidade abstrai recursos, atividades e pessoal requerido para a execução da função. Modelos de capacidades descrevem o que é realizado por uma organização para atender seus objetivos. A descrição de como a organização executa as capacidades não são analisadas nesses modelos. Na segunda fase foi identificado um modelo de níveis de maturidade. Um nível de maturidade representa um estado do domínio da organização quanto às capacidades requeridas para a defesa cibernética. O avanço nos níveis de maturidade traz o aprimoramento dessas capacidades na organização. Assim um modelo de níveis de maturidade descreve uma estratégia para a melhoria das capacidades.

O artigo apresenta conceitos de modelos de capacidade e de maturidade, descreve um modelo de capacidades para defesa cibernética e um modelo de maturidade para evolução dessas capacidades em uma organização. Através de cenários de uso é explicada a utilização do modelo de maturidade. Na

[1]Ativo – Qualquer coisa que tenha valor para organização. [ISO/IEC 13335-1:2004].

última seção são apresentadas conclusões e propostas para trabalhos futuros.

II. MODELO DE CAPACIDADES

Modelos de negócios são normalmente baseados em processos (como fazer?) alinhados com o objetivo estratégico e político de uma organização. Um modelo de capacidades ao invés de analisar os negócios por meio de processos, faz a análise por capacidades (o que fazer?). Uma capacidade descreve o que uma função de negócio faz, sem descrever como essa função é executada. São mais estáveis do que os processos, pois, os processos de negócio estão em constante modificação devido a mudanças organizacionais ou de tecnologia. Uma capacidade é constituída de processos, pessoas e ativos físicos ou a combinação de dois ou mais elementos conforme ilustrado na Fig. 1 [4].

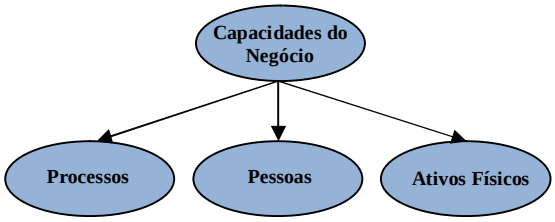

Fig. 1 Elementos de uma Capacidade

O modelo de capacidades pode ser representado por uma taxonomia ilustrando as capacidades de uma organização em diversos níveis de abstração. As taxonomias das capacidades (Fig. 2) são divididas hierarquicamente em níveis sendo o primeiro nível caracterizado pelas capacidades fundamentais subdivididas em operacionais e ambientais. As operacionais incluem todas as capacidades que uma organização possui. As capacidades ambientais são todas as capacidades externas ao negócio que influem na forma como a organização gera valor [4].

As capacidades do segundo nível (ou Grupo de Capacidades) representam o primeiro nível de detalhamento de cada capacidade fundamental. Grupos de capacidades são geralmente importantes, pois, refletem as capacidades que serão atribuídas a unidades funcionais da organização. Essas capacidades possuem níveis de serviço, restrições e limitações. Os Grupos de Capacidades são desmembrados por sua vez em capacidades de terceiro nível ou capacidades de negócio. Eventualmente, algumas capacidades de negócio podem ser desmembradas em novas capacidades de negócio, até o ponto de serem mapeadas diretamente a um processo de negócio [4].

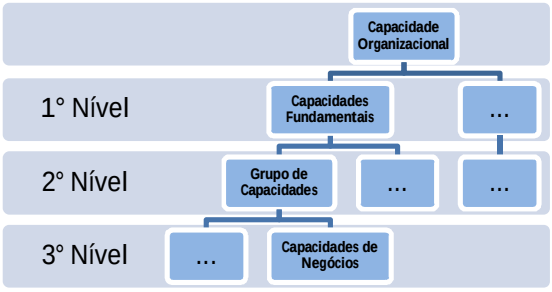

Fig. 2 – Taxonomia Hierárquica das Capacidades

III. MODELAGEM DE CAPACIDADES PARA DEFESA CIBERNÉTICA

As capacidades fundamentais são ambientais e operacionais. As ambientais representam as capacidades externas que interagem com as capacidades operacionais. Para a defesa cibernética, o ambiente são os ativos a serem protegidos e as fontes de ameaças interessadas em causar danos nos ativos da organização. Assim as capacidades ambientais representam os ativos da organização e as fontes de ameaças para estes ativos. As capacidades operacionais devem proteger os ativos da Organização das Fontes de Ameaça conforme ilustrado na Fig. 3.

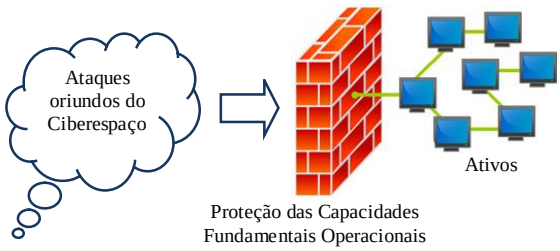

Fig 3. Emprego das Capacidades Fundamentais Operacionais

Essas capacidades operacionais foram identificadas a partir dos elementos fundamentais de um sistema de defesa cibernética conforme O. Sami Saydjari [5]. Esses elementos são: sensores e exploração; percepção da situação; mecanismos de defesa; comando e controle; estratégicas e táticas e ciência e engenharia. Sensores e exploração representam os "olhos" do sistema e identificam as capacidades, intenções e ações dos adversários; percepção da situação interpreta os dados avaliando possíveis impactos e efeitos; mecanismos de defesa é a tecnologia utilizada para conter ameaças; o comando e controle é o processo de tomar e executar decisões a partir de opções oferecidas pela percepção da situação; estratégias e táticas é o conhecimento que apóia as boas decisões para m se ter uma melhor proteção contra ataques; a ciência e engenharia são os princípios empregados na concepção, desenho, construção e manutenção de sistemas.

Cada um desses elementos pode ser atendido pelas seguintes capacidades operacionais fundamentais, visualizadas na Fig. 4: Governança; Comando e Controle; Mecanismos de Defesa e Supervisão da Defesa. Essas capacidades são explicadas a seguir no item A.

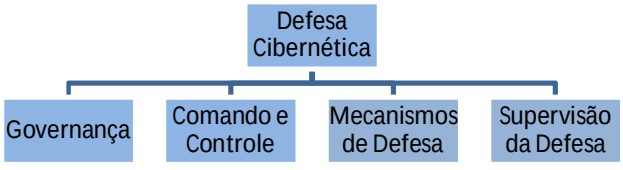

Fig. 4: Taxonomia das Capacidades Fundamentais para Defesa Cibernética

A. Capacidades Fundamentais Operacionais

1) Governança

A Governança de um sistema visa garantir que este sistema irá atender as metas de negócios da organização. A governança para defesa cibernética visa estabelecer e aprimorar as políticas, as estratégias e as táticas da organização frente às ameaças existentes no espaço cibernético. A idéia central dessa capacidade é o constante aprimoramento do pessoal, processos e tecnologia para a defesa cibernética da organização, de modo que, as melhores decisões sejam sempre tomadas e a organização faça uso de estratégias e táticas previamente avaliadas e testadas.

Uma política de defesa cibernética consiste num conjunto formal de regras que devem ser seguidas pelos diferentes membros e colaboradores da organização. Políticas de Defesa descrevem requisitos globais de segurança e retratam valores da organização, experiências passadas e melhores práticas. As políticas de defesa fornecem princípios a serem obedecidos pelas estratégias e táticas de defesa de cibernética[6].

As Estratégias de Defesa tem por finalidade orientar a aplicação de recursos, métodos e procedimentos utilizados para a defesa da missão da organização quanto às ameaças do ciberespaço. Uma estratégia estabelece um plano de defesa para um determinado cenário de ataque. Dado a necessidade de rapidez de resposta contra os ataques é fundamental que a organização tenha previamente elaborada e testada estratégias para os principais cenários de ataque[5].

As Táticas de Defesa são os procedimentos e métodos empregados nas diferentes capacidades da defesa cibernética e que devem estar alinhados com a política e as estratégias da organização. As táticas são como ferramentas que precisam ser constantemente avaliadas e testadas quanto a sua eficácia em diferentes cenários de ataque[5].

A capacidade Governança é desmembrada nos seguintes Grupos de Capacidades:

1.1 Políticas de Defesa: definição da política do sistema de defesa em termos da missão e valores da organização. Na política devem ser definidos os objetivos de segurança e estabelecido um direcionamento global e princípios a serem empregados para a Defesa Cibernética[5].

1.2 Monitoramento e Avaliação de Estratégias e Táticas: As estratégias e táticas de defesa são monitoradas e avaliadas de modo a identificar deficiências e necessidades de aprimoramento[5].

1.3 Gestão de Problemas: Deficiências recorrentes nas capacidades de defesa são analisadas com profundidade de modo a encontrar soluções definitivas[7].

1.4 Gestão de Conhecimento: Deve ser mantido e disponibilizado um repositório com casos de sucesso, falhas, ações corretivas, melhores práticas, etc[6].

2) Comando e Controle

Essa capacidade fundamental provê a análise da situação corrente; tomada de decisões a partir de uma compreensão de opções e uma comunicação das decisões e acompanhamento da execução de forma precisa e confiável [5]. As decisões de defesa cibernética envolvem tanto ações de efeito imediato tais como a desativação de serviços e instalação de backups de segurança, como também de ações de longo prazo tais como a implementação de novos serviços para mitigar impactos de vulnerabilidades. A capacidade de comando e controle deve estar fortemente alinhada com a missão da organização, de modo que, as decisões tomadas estejam sempre de acordo com um modelo de riscos do negócio. A capacidade de Comando e Controle é desmembrada nos seguintes Grupos de Capacidades:

2.1 Consciência Situacional: Essa capacidade provê uma análise do estado corrente de segurança frente aos riscos envolvidos. A partir dessa análise são identificadas opções de decisões a serem tomadas. A consciência situacional deverá oferecer um comportamento pró-ativo da organização frente aos riscos[5].

2.2 Comando: Decisões são tomadas a partir de opções estabelecidas pela consciência situacional. As decisões do comando devem estar alinhadas com os interesses da alta gerência da organização.

2.3 Controle: A execução das ações deve ser comunicada e monitorada. O controle deve exercer também a gestão operacional da defesa cibernética.

3) Mecanismos de Defesa

A capacidade de Mecanismos de Defesa provê processos e tecnologia de segurança para proteger os ativos da organização contra ataques do ciberespaço[5]. Essa capacidade é desmembrada nos seguintes Grupos de Capacidades:

3.1 Serviços de Segurança: tem por finalidade prover serviços de segurança (autenticação, autorização, confidencialidade, integridade e disponibilidade) para os ativos digitais de acordo com os riscos envolvidos[7].

3.2 Segurança Física: visa garantir que os equipamentos e instalação física estão adequadamente protegidos de acordo com os riscos envolvidos[6].

3.3 Segurança de Pessoal: visa garantir que controles pessoais apropriados estão ativos antes da contratação, durante o contrato e após contrato para todo pessoal incluindo terceiros[7].

3.4 Desenvolvimento, Operação e Manutenção Segura: visa garantir que os sistemas são adquiridos, instalados, operados e mantidos seguindo processos adequados ao nível de risco envolvido[6].

4) Supervisão da Defesa

A defesa cibernética requer o monitoramento e acompanhamento constante da eficácia dos mecanismos de defesa. Essa capacidade analisa os incidentes ocorridos, a capacidade e possíveis intenções dos atacantes, bem como identifica e analisa as vulnerabilidades correntes através de testes de invasão e auditorias. Essa capacidade é desmembrada nas seguintes capacidades:

4.1 Monitoramento de mecanismos de defesa: executa o monitoramento dos mecanismos de defesa instalados de modo a identificar possíveis intrusões ou novas vulnerabilidades[5].

4.2 Gestão de Incidentes: analisa incidentes reportados, propõe e acompanha a implementação de medidas corretivas**[6].**

4.3 Testes de Invasão: testes de avaliação são periodicamente executados de modo a avaliar a robustez dos mecanismos de defesa instalados.

4.4 Auditoria[6]: auditorias são periodicamente executadas de modo a verificar se os processos recomendados e boas práticas estão sendo empregadas.

B. Níveis de Desempenho

Os Grupos de Capacidades representam capacidades que podem ser alocadas a unidades funcionais da organização e possuem funcionalidades e níveis de desempenho. Foi estabelecido para todas as capacidades do segundo nível seis níveis de desempenho. Esses níveis de desempenho foram estabelecidos de acordo com os níveis de maturidade do modelo de maturidade selecionado. Os níveis de desempenho estabelecidos são:

0: Inexistente – A organização não reconhece a importância da capacidade, ou a capacidade é implementada de modo informal;

1: Inicial – Há evidências de que a organização reconhece que a capacidade é importante e que as necessidades devem ser endereçadas. Entretanto não há um processo padronizado e o gerenciamento é caso a caso e desorganizado;

2: Repetitível, mas intuitivo – A capacidade é implementada de acordo com um planejamento estabelecido conforme riscos identificados. Há forte dependência do conhecimento individual e existe alguma documentação;

3: Definido - Os processos são padronizados, documentados e comunicados conforme um modelo da organização;

4: Gerenciado - O desempenho da capacidade é monitorado conforme um modelo quantitativo. Ações de melhoria são feitas conforme este modelo. Ferramentas automatizadas são empregadas na execução da capacidade.

5: Otimizado: Os processos são aprimorados e novas tecnologias são empregadas de modo a atingir metas quantitativas para a melhoria. Os fluxos de trabalho são automatizados e ferramentas para aumentar a qualidade e efetividade dos processos estão disponíveis.

Para cada um dos Grupos de Capacidades foram identificados níveis de desempenho de acordo com a escala de níveis selecionada. De forma a ilustrar esta atividade são apresentados, nas tabelas de I a III, os níveis de desempenho das capacidades Política de Defesa da Capacidade Fundamental de Governança, Consciência Situacional da Capacidade Fundamental de Comando e Controle e Serviços de Segurança da Capacidade Fundamental de Mecanismos de Defesa.

TABELA I - POLÍTICA DE DEFESA

Nível	Descrição
0	Não existe uma política para defesa cibernética
1	Não existe uma política formalmente estabelecida
2	Existe uma política que é seguida no planejamento das atividades de defesa cibernética.
3	Uma política é estabelecida e mantida de acordo com um modelo da organização.
4	A eficácia da política é avaliada de forma quantitativa.
5	A Política é aprimorada de acordo com um modelo quantitativo.

TABELA II - CONSCIÊNCIA SITUACIONAL

Nível	Descrição
0	Inexistente
1	Atividades de análise são realizadas por iniciativas ad-hoc.
2	Atividades de análise são implementadas de acordo com um planejamento e integradas ao comando e controle.
3	Impactos e tendências são analisadas de acordo com processos e procedimentos da organização.
4	Impactos e tendências são analisadas de forma quantitativa.
5	O Aprimoramento da capacidade de consciência situacional é realizado de acordo com resultados quantitativos.

TABELA III – SERVIÇOS DE SEGURANÇA

Nível	Descrição
0	Inexistente
1	Os serviços de Segurança são realizados por iniciativas isoladas e individuais (ad-hoc).
2	Os serviços são realizados de acordo com um planejamento estabelecido para tratar riscos da organização, mas com dependência de conhecimento individual.
3	Os serviços de segurança são realizados de forma organizada e sistemática pela organização.
4	Os serviços são monitorados e a sua efetividade é medida em termos de desempenho quantitativo.
5	Os serviços são monitorados, avaliados e refinados até alcançar as melhores práticas conforme desempenho quantitativo.

IV. MODELO DE MATURIDADE PARA DEFESA CIBERNÉTICA

Os modelos de maturidade permitem a uma organização avaliar o grau de domínio e a experiência da organização na adoção de melhores práticas para a implementação de capacidades, e também identificar direções a serem seguidas para melhorar esse grau de domínio.

Existem diversos modelos para medição de maturidade de sistemas de informação. A abordagem proposta neste trabalho é a utilizada no Modelo de Governança de TI chamado CobiT[3] que permite que a gerência tenha condições de: mapear a situação atual da organização, comparar com a situação das melhores organizações no segmento, comparar com padrões internacionais e estabelecer e monitorar passo a passo as melhorias dos processos rumo ao estado de melhoria contínua.

Percorrer os níveis de maturidade significa que a organização deverá passar por diferentes estágios de comportamento até se atingir o estágio de melhoria contínua onde a organização tem controle sobre os processos e tecnologia empregados e é capaz de estabelecer ações de melhoria com metas quantitativas. Para a defesa cibernética os níveis de maturidade foram estabelecidos de acordo com os seguintes atributos:

- Percepção e tratamento de riscos: Ativos, vulnerabilidades, ameaças e riscos são identificados e as ações de defesa são planejadas e implantadas de acordo com os riscos envolvidos.
- Implantação de Comando e Controle: a execução e a efetividade das ações de defesa são coordenadas por um grupo formalmente estabelecido, com recursos e nível de autoridade apropriado.
- Implantação de um Modelo de Governança: políticas, estratégias e táticas são desenvolvidas, implantadas e aprimoradas de acordo com modelos da organização.

Conforme estes atributos foram estabelecidos os seguintes níveis de maturidade:

0 - Inexistente: a organização não possui capacidades de defesa cibernética reconhecidas. Riscos são identificados e tratados de forma subjetiva. Não existem responsáveis formalmente indicados para a Defesa Cibernética.

1 - Inicial: a organização reconhece a importância das capacidades de defesa cibernética. Mas as capacidades são

implantadas de forma ad-hoc sem planejamento e organização. Riscos são identificados, mas são tratados sem um processo formal, onde ações de defesa são dimensionadas e implantadas de acordo com os riscos envolvidos.

2 - Repetitível: As capacidades de defesa cibernética são planejadas, implantadas e controladas de acordo com os riscos envolvidos. Existem responsáveis formalmente estabelecidos para a coordenação das ações de defesa. As capacidades de defesa são implantadas caso a caso sem levar em conta um modelo da organização. Ações de defesa são executadas de forma reativa. A coordenação entre os sistemas de defesa da organização é realizada de forma ad-hoc.

3 - Definido: A implantação de capacidades de defesa é feita de acordo com modelos da organização. Modelos da organização são continuamente avaliados e aprimorados. A capacidade de comando e controle de defesa é coordenada em toda a organização. Ações de defesa são executadas de forma pró-ativa. Políticas, estratégias e táticas são desenvolvidas e implantadas conforme um modelo mantido pela organização.

4 - Gerenciado: Riscos e a eficácia de capacidades de defesa são compreendidos de forma quantitativa.

5 - Otimizado: Ações de melhoria de capacidades de defesa são estabelecidas e implantadas com metas quantitativas. Modelos da organização são continuamente aprimorados conforme metas quantitativas.

V. CENÁRIOS DE USO DO MODELO

O modelo proposto deve atender os seguintes cenários de uso:

- Identificação do estado corrente das capacidades de defesa;
- Identificação do estado desejável; e
- Planejamento de passos para se atingir o estado desejável.

A. Identificação do Estado Corrente

A identificação do estado corrente das capacidades de defesa pode ser feita por uma equipe de avaliadores interna ou externa devidamente treinada no uso do modelo. O primeiro passo é estabelecer o escopo da avaliação. O escopo é definido pelos ativos da organização que requerem proteção. Todos os sistemas de defesa para os ativos selecionados formarão o sistema de defesa cibernética da organização a ser avaliada.

Os avaliadores deverão, a partir de leitura de documentos dos sistemas de defesa, questionários e entrevistas com responsáveis, identificar o nível de desempenho para os diferentes Grupos de Capacidades. O nível de desempenho dos Grupos de Capacidades irá definir o nível de maturidade da organização. Foi definida a seguinte regra para a atribuição de níveis de maturidade: Uma organização tem nível de maturidade N se todos os Grupos de Capacidades tiverem nível de desempenho maior ou igual a N.

B. Identificação do Estado desejável

O estado desejável depende dos níveis de risco das ameaças aos ativos protegidos. Níveis de risco elevado são devido a ameaças com impacto elevado e/ou uma grande probabilidade de ocorrência. Impactos elevados trazem custos inaceitáveis tais como perdas de vidas humanas e gastos financeiros elevados.

O tratamento de riscos pode ser de forma reativa ou de forma pró-ativa (com antecipação de ações). No comportamento reativo está implícito que uma ameaça está ocorrendo e ações de mitigação são aplicadas para reduzir o impacto. Por exemplo, um servidor foi invadido e ele ficará temporariamente fora do ar.

No comportamento pró-ativo, as ações são executadas de forma antecipada. Isto é, ações de mitigação são executadas antes que a ameaça ocorra. Para o comportamento pró-ativo, a organização deverá ter capacidades de comando e controle que permitam a identificação precisa de tendências de ameaças, estratégias e táticas apropriadas para tratar essas ameaças de forma coordenada.

De acordo com o perfil dos riscos envolvidos é possível deduzir o nível de maturidade desejável para a organização. Uma garantia para riscos que possam ser tratados de forma reativa é obtida ao se atingir o nível 2 de maturidade, quando riscos são identificados e as capacidades são dimensionadas para atender esses riscos. Entretanto, neste nível de maturidade não há garantias de coordenação da organização para se ter uma capacidade pró-ativa para tratamento de riscos.

Para riscos que requerem antecipação de ações (risco elevado) é necessário que a organização responsável esteja enquadrada pelo menos no nível 3. Com um modelo de riscos da organização aprimorado de acordo com experiências passadas e melhores práticas e uma coordenação entre os diferentes grupos é possível a execução de ações pró-ativas efetivas.

O nível de maturidade 4 é requerido para organizações que desejam não apenas um comportamento pró-ativo mas também um controle quantitativo do desempenho das ações de defesa.

No nível de maturidade 5 a organização possui pleno controle das suas capacidades de defesa e de forma pró-ativa estabelece metas quantitativas de melhoria das capacidades.

C. Planejamento para se atingir o estado desejável

Identificado o estado (ou nível de maturidade) desejável, é necessário definir os passos para se alcançar esse estado. O avanço nos níveis de maturidade é evolucionário. Isto é, a organização deverá passar em todos os níveis intermediários até se atingir o nível desejável. Estar em um nível de maturidade implica não apenas em processos, procedimentos e responsáveis formalmente designados, mas que todo o pessoal envolvido esteja capacitado para operar os processos e tecnologia conforme o nível de maturidade.

De modo a auxiliar o planejamento para se alcançar o nível de maturidade desejado, podemos utilizar os seguintes marcos a serem alcançados em cada nível:

Nível 1: A organização reconhece formalmente a importância da Defesa Cibernética.

Nível 2: As capacidades de defesa cibernética são implantadas de acordo com um plano que considera os riscos para os ativos a serem protegidos. Os planos são desenvolvidos, caso a caso, sem adotar modelos da organização.

Nível 3: As capacidades de defesa cibernética são implantadas de acordo com um modelo adotado e mantido pela organização. Existe forte coordenação entre os grupos. O comportamento para tratamento de riscos é pró-ativo.

Nível 4: As capacidades de defesa cibernética são compreendidas de forma quantitativa.

Nível 5: As capacidades e os modelos da organização são aprimorados de acordo com metas quantitativas.

VI. CONCLUSÕES

Uma defesa cibernética efetiva requer uma vigilância contínua das ameaças que podem ser originadas de mudanças nos processos, pessoal, tecnologia e no ambiente social e de negócios onde a organização está inserida. Assim é necessário que as capacidades que compõem a defesa cibernética não sejam apenas concebidas para atender o cenário corrente de ameaças, mas também que elas estejam sendo continuamente aprimoradas de modo que possam enfrentar novas ameaças ou as evoluções das ameaças existentes.

De modo a atender a demanda de aprimoramento contínuo das capacidades de defesa, neste artigo apresentamos um Modelo de Maturidade de Capacidades de Defesa Cibernética. Utilizando este modelo, uma organização pode identificar o nível de desempenho corrente do seu sistema de defesa, identificar o nível de desempenho desejável frente aos riscos envolvidos e definir um plano para aprimoramento das capacidades correntes para se alcançar o nível de desempenho estabelecido.

O modelo proposto independe de tecnologias ou de metodologias específicas e pode ser utilizado por qualquer organização que possua ativos a serem protegidos de ameaças do ciberespaço. Essa proposta descreve uma estratégia de emprego das melhores práticas estabelecidas em padrões internacionais, entretanto, ela ainda está em processo de validação por intermédio de casos reais. Os resultados a serem obtidos deverão ser publicados para uma futura avaliação pela comunidade científica.

REFERÊNCIAS

[1]- William Gibson . Neuromancer. 1984. 20th Anniversary Edition. New York: Ace Books, 2004

[2] - CMMI-DEV, CMMI for Development, V1.2 model, CMU/SEI- 2006-TR-008. Software Engineering Institute, 2006. Disponível em http://www.sei.cmu.edu/reports/ 06tr008.pdf . Acesso em Julho de 2010.

[3] – COBIT - Framework for IT Governance and Control. Disponível em http://www.isaca.org/knowledge-center/ cobit/Pages/Overview.aspx . Acesso em junho de 2010.

[4] - Business-Capability Mapping: Staying Ahead of the Joneses. Disponível em http://msdn.microsoft.com/en-us/library/bb402954.aspx . Acesso em junho de 2010.

[5] – SAYDJARI, O. Sami. Cyber Defense: Art to Science, Communications of the ACM, v.47, n.3, pp52-57. 2004

[6] - ABNT NBR ISO/IEC 27002:2006. Técnicas de Segurança – Código de Prática para a Gestão de Segurança da Informação.

[7] - NIST (2010). Guide for assessing the security controls in federal information systems and organizations. Special Publication 800-53A Revision 1, Consistent with NIST SP 800-53, Revision 3, National Institute of Standards and Technology, Gaithersburg, MD 20899-8930.