

# Proposta de Norma de Segurança da Informação para o Gerenciamento dos Ativos e Direitos de Acesso dos Militares Transferidos do 3º Centro de Telemática de Área

Ricardo Hisao Watanabe  
Centro de Educação Tecnológica Paula Souza – São Paulo – Brasil  
ricawat@hotmail.com

Marília Macorin de Azevedo  
Centro de Educação Tecnológica Paula Souza – São Paulo – Brasil  
mmacorin@radial.br

Napoleão Verardi Galegale  
Centro de Educação Tecnológica Paula Souza – São Paulo – Brasil  
nvg@galegale.com.br

**Resumo** - No 3º Centro de Telemática de Área (3º CTA) é comum ocorrerem transferências de militares para outras Organizações Militares (OM) ou para a reserva. Por ocasião dessas transferências, muitas vezes não são revisadas as questões de permissões de acessos à rede interna bem como aos sistemas de informação da OM. A observância às Normas de Segurança existentes na literatura pode dar subsídios para que sejam instituídos processos de revisão de direitos de acesso do militar transferido.

**Palavras-chave:** Segurança da Informação, Exército Brasileiro, Controle de Acesso.

**Abstract** - The people's movement to another Military Organizations (MO) are common in 3º Centro de Telemática de Área (3º CTA). When it happens, for many times are not reviewed the questions about permissions of access to internal net and information systems of MO. The observation to Security Rules under literature can give us subsidize for details process of review of rights of access of military moved.

**Key-words:** Information Security, Brazilian Army, Control access.

## 1. Introdução

O 3º CTA é uma OM do Exército Brasileiro (EB) e um dos órgãos de execução do Centro Integrado de Telemática do Exército (CITEx), a quem compete operar os Sistemas de Informática e Comunicações de interesse do Sistema de Comando e Controle do Exército na área do Comando Militar do Sudeste (CMSE) [1]. É uma OM voltada para a tecnologia e está interligada à Rede Privativa Corporativa do Exército (EBnet), que interliga os Grandes Comandos<sup>1</sup> (G Cmdo) e muitas OM localizadas em várias regiões do Brasil.

Em todas as organizações do EB são comuns e constantes as movimentações de pessoal, e estas ocorrem por razões estratégicas, nivelamentos<sup>2</sup>, promoções, reserva, aposentadorias e também por questões particulares do próprio militar. A movimentação

---

<sup>1</sup> É a denominação genérica dada a qualquer comando da Força Terrestre, privativo de oficial-general.

<sup>2</sup> É o resultado da operação que visa equilibrar o pessoal distribuído pelas várias OM do Exército Brasileiro.

de militares, principalmente entre as organizações usuárias dos serviços da EBnet e a não observância das devoluções de ativos e da revisão dos direitos de acesso à rede e aos sistemas de informação, podem acarretar em acessos indevidos, riscos à preservação da confidencialidade, da integridade e da disponibilidade dos vários tipos de Sistemas de Informação, não somente do 3º CTA, como de todas as demais OM interligadas a EBnet.

O presente trabalho pretende, a partir da literatura e normas existentes, propor uma política de gerenciamento dos ativos e dos direitos de acesso aos recursos de processamento de informações, por parte dos militares transferidos, a fim de salvaguardar os ativos da organização e de minimizar ou até extinguir a possibilidade de acessos indevidos.

## **2. Desenvolvimento**

### **2.1. O 3º Centro de Telemática de Área**

O 3º CTA é uma OM do EB voltada para a tecnologia da informação, com várias atribuições, dentre as quais destacamos a instalação, operação, produção e manutenção (Hardware e Software) dos sistemas de informação que compõem o Sistema Estratégico na área do CMSE. Na área de segurança, o 3º CTA tem como atribuição o estabelecimento das medidas de segurança dos Subsistemas de Informática e de Comunicações, e ainda, deve fomentar a cultura de utilização das modernas Tecnologias de Informação em sua área de atuação [1].

Atualmente, sua estrutura organizacional se divide em Chefia, Subchefia e quatro divisões:

- Divisão Administrativa: responsável pelo patrimônio, pelas questões financeiras e materiais;
- Divisão de Pessoal: trata dos assuntos relacionados com pessoas. Recursos Humanos (RH);
- Divisão Técnica: voltada para o desenvolvimento de sistemas, treinamentos em informática, manutenção e suporte de sistemas; e,
- Divisão de Operações: mantém os serviços de redes, comunicações, manutenção de equipamentos, suporte, operação de sistemas, servidores, telefonia, servidores, instalação de software, gerenciamento de usuários e senhas.

Para atendimentos dos requisitos de segurança, a rede interna é acessada por senhas individuais, com privilégios de acesso dependentes da função que o militar exerce. A rede disponibiliza serviços de impressão, áreas para backup e trocas de arquivos, acesso aos sistemas de informação internos, voltados para controles de patrimônio, de pessoal e de documentação, nos vários níveis de confidencialidade.

Outra característica da rede interna do 3º CTA é que ela está integrada à Internet em conformidade com as Normas para o Controle da Utilização dos Meios de Tecnologia da Informação no Exército (NORTI) [2]. Convém ressaltar que o objetivo das NORTI é controlar o conteúdo das informações ou dados armazenados nos dispositivos de TI de propriedade do EB a fim de coibir conteúdos considerados ilícitos, contrários à disciplina, que viole qualquer direito de terceiros, ou que ainda afete à moral e os bons costumes.

As NORTI, apesar de orientarem os militares e servidores civis na utilização correta dos recursos de TI, não trata dos procedimentos relativos ao encerramento de atividades, devolução de ativos, retirada de direitos de acesso por ocasião das movimentações de pessoal.

Além da Internet, a rede interna do 3º CTA está integrada à EBnet, através da qual é possível, a partir de usuários e senhas autorizados, acessar conteúdos de outras OM integradas à rede.

### 3. Embasamento Teórico

#### 3.1. Segurança da Informação

A informação é um ativo importante e essencial para as necessidades de negócios de uma organização e precisa ser adequadamente protegida. A informação pode existir em várias formas, tais como documentos impressos ou escritos em papel, armazenada eletronicamente, transmitida por correio eletrônico, filmes, apresentações ou falada em conversas [3].

Para que a informação receba um nível adequado de proteção é necessário que esta seja classificada conforme o seu nível de sensibilidade e de criticidade. A segurança da Informação (SI) ainda deve atender os seguintes requisitos básicos [3,4]:

- 1) **Confidencialidade:** Garantir que o acesso à informação seja obtido somente por pessoas autorizadas.
- 2) **Integridade:** Salvar a exatidão e a completeza da informação e dos métodos de processamento.
- 3) **Disponibilidade:** Garantir que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

A informação poderá ter uma classificação inicial e reclassificação ao longo do tempo, conforme a política de segurança adotada. É conveniente que o responsável pelo ativo defina a classificação, analisando-o a intervalos regulares a fim de verificar se esta se encontra no nível apropriado [3].

#### 3.2. Importância da SI

A importância da SI para a organização, tanto para os setores públicos como privados, é que, além de proteger as suas infra-estruturas, viabiliza os negócios, evita ou reduz os riscos relevantes.

A SI se torna cada vez mais necessária na medida em que se aumentam as interconexões de redes públicas e privadas, pois os controles e acessos às informações ficam expostos a um grande número de ameaças tais como:

- Fraudes, espionagem, sabotagens e vandalismos;
- Hackers;
- Outros tipos de ataques que estão se tornando cada vez mais comuns, ambiciosos e sofisticados.

Outro aspecto relacionado à SI é que muitos sistemas não são projetados para serem seguros e não têm como serem protegidos por meios técnicos. Uma das maneiras de minimizar tais riscos está na elaboração de Políticas de Segurança da Informação (PSI) que pode possibilitar a gestão e os procedimentos apropriados. [3].

### **3.3. Normas e legislações**

A 9ª Pesquisa Nacional de Segurança da Informação [5], realizada no primeiro semestre de 2003 pela empresa Módulo Security Solutions S.A., da qual participaram cerca de 50% das 1000 maiores empresas do Brasil, nos diversos segmentos tais como governo, indústria e financeiro, mostra que 63,5% dos entrevistados utilizam a norma ISO 17799 para norteamento das ações de segurança de suas organizações, ficando 37% para as publicações do Governo Federal (decreto 4553 e outros), 30% as publicações do Banco Central (resolução 2554 e outras), 27% a Regulamentação da ICP-Brasil, 20% o COBIT e 20% as Publicações da CVM (Resolução 358 e outras).

A norma NBR ISO/IEC 17799:2005 tem como objetivo o estabelecimento de diretrizes e princípios gerais para iniciação, implantação, manutenção e melhoria da gestão de SI em uma organização. Pode ainda servir como um guia prático para o desenvolvimento dos procedimentos de segurança, das práticas eficientes de gestão da segurança e para ajudar a criar a confiança nas atividades interorganizacionais.

Esta norma, ainda pode ser considerada como um ponto de partida para que cada organização desenvolva suas diretrizes específicas, visto que nem todos os controles e diretrizes nela contidas podem ser aplicadas. Além disso, podem ser necessários controles adicionais.

Na pesquisa mencionada anteriormente, em relação às legislações, normas e regulamentações que norteiam as organizações, destacam-se ainda as publicações do Governo Federal, em particular, o Decreto 4.553 [6] que trata da salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, bem como das áreas e instalações onde tramitam.

Para o EB, o Comandante do Exército aprovou as IG 20-19 - Instruções Gerais de Segurança da Informação para o Exército Brasileiro [4], com a finalidade de orientar o planejamento e a execução das ações relacionadas à SI. As IG 20-19 definem responsabilidades, orientações gerais, e têm como objetivo servir de referência básica para todas as documentações normativas versando sobre segurança, deixando o detalhamento de processos de SI para serem especificadas por outras normas.

### **3.4. Vulnerabilidades**

Vulnerabilidade [7] é o ponto onde qualquer sistema é suscetível a um ataque; trata-se de uma fraqueza encontrada em determinados recursos, processos e configurações. Essa condição pode ser causada pela ausência ou ineficiência das medidas de proteção utilizadas para salvaguardar os ativos da organização.

As vulnerabilidades, entre outras, podem ser:

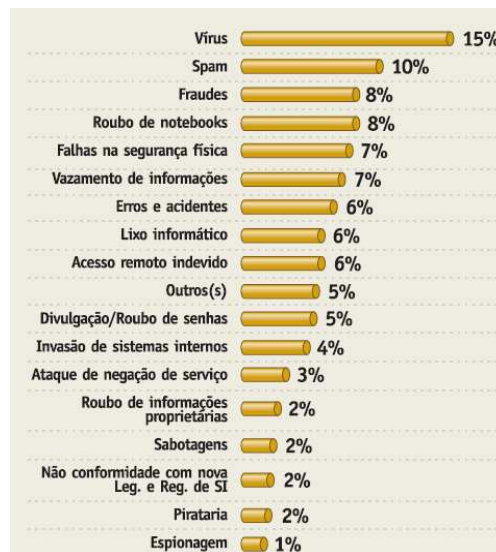
- 1) Hardware: ausência de firewall e dispositivos de armazenamento ineficazes.
- 2) Software: equipamentos não configurados corretamente, antivírus não atualizado.

- 3) Humanas: falta de treinamento, compartilhamento indevido de informações, funcionários mal intencionados.
- 4) Naturais: podem se constituir em desastres naturais como inundações, terremotos.
- 5) Físicas: instalações inadequadas, fios elétricos e cabos de rede distribuídos de forma incorreta, ausência de extintores ou extintores inadequados.

As vulnerabilidades se constituem em pontos sensíveis a ataques, fraudes, invasões e, conforme a 10ª Pesquisa Nacional de Segurança da Informação, realizada em 2006, 33% das organizações não sabem quantificar as perdas ou sequer identificar os responsáveis pelo problema devido à falta de um planejamento formal de segurança [8].

As dificuldades em apontar responsáveis, levam as empresas a se dedicarem, muitas vezes, em apenas corrigir as falhas, porém, quando descobrem as causas, verificam que 24% das falhas são causadas pelos próprios funcionários e 20% por hackers, ou seja, problemas de origem humana; já os problemas com vírus 15%, spam 10% e fraudes 8% são os que mais causam danos financeiros para a organização conforme mostra a **Figura 1**.

**Figura 1 – Problemas que Geraram Perdas Financeiras**



Fonte: Módulo Security Solutions S.A. (2003).

A pesquisa ainda revela que 56% das organizações governamentais são as que menos quantificaram as perdas causadas por problemas de segurança e que quando conseguiram identificar os causadores dos problemas, apontaram funcionários e hackers como responsáveis.

### 3.5. Estabelecimento de Controles de Segurança

A norma NBR ISO/IEC 17799:2005 oferece um modelo para o estabelecimento e a seleção de controles a partir da identificação dos requisitos de SI da organização. Esses controles são considerados como ponto de partida para a implementação da SI.

Os requisitos de SI são identificados a partir de três fontes:

- 1) Análise/avaliação de riscos para a organização: identificação das ameaças aos ativos e as vulnerabilidades;
- 2) Legislação vigente, regulamentações, contratos;
- 3) Objetivos e requisitos do negócio.

A identificação dos requisitos de segurança e dos riscos resulta na seleção de controles apropriados para assegurar que os riscos sejam reduzidos a um nível aceitável. A NBR ISO/IEC 17799:2005 sugere que os controles podem ser selecionados a partir dela, e que também podem ser criados novos controles para atendimento de necessidades específicas.

### 3.6. Segurança em Recursos Humanos

As pessoas são um importante fator para a SI nas organizações. Segundo a pesquisa [8], 55% das organizações apontam a falta de conscientização de executivos e de usuários um dos principais obstáculos para a sua implementação.

A NBR ISO/IEC 17799:2005 estabelece controles voltados para funcionários, fornecedores e terceiros:

- 1) Antes da contratação: entendimento e aceitação das responsabilidades e papéis, reduzindo o risco de roubo, fraude ou mau uso dos recursos;
- 2) Durante a contratação: consciência das ameaças e preocupações relativas à SI, apoio à PSI nos seus trabalhos normais e conseqüente redução do risco humano;
- 3) Encerramento ou mudança de contratação: assegurar que as pessoas deixem a organização ou mudem de trabalho de forma ordenada.

### 3.7. Encerramento ou mudança da contratação

Por ocasião do encerramento ou mudança de contratação de funcionários, fornecedores e terceiros, convém que as responsabilidades estejam definidas a fim de que esse processo seja feito de modo controlado e que a devolução dos ativos e a retirada de todos os acessos sejam concluídas [3].

- 1) **Encerramento das atividades:** este controle busca a clara definição dos responsáveis para a realização do encerramento ou da mudança de um trabalho onde, geralmente a área de RH juntamente com o gestor da pessoa que está saindo são os responsáveis pelo processo global.
- 2) **Devolução de ativos:** controle da devolução de todos os ativos da organização que estejam em posse da pessoa após o encerramento de suas atividades.
  - Equipamentos, documentos corporativos e software;
  - Dispositivos de computação móvel, cartões de acesso, manuais, mídias;
  - Documentação dos conhecimentos da pessoa que são considerados importantes para a organização.
- 3) **Retirada de direitos de acesso:** controle da retirada dos direitos de acesso aos ativos associados com os sistemas de informação e serviços. Incluem-se também:
  - Acesso físico tais como chaves, cartões de identificação;

- Alteração das senhas de acesso que a pessoa utilizava.

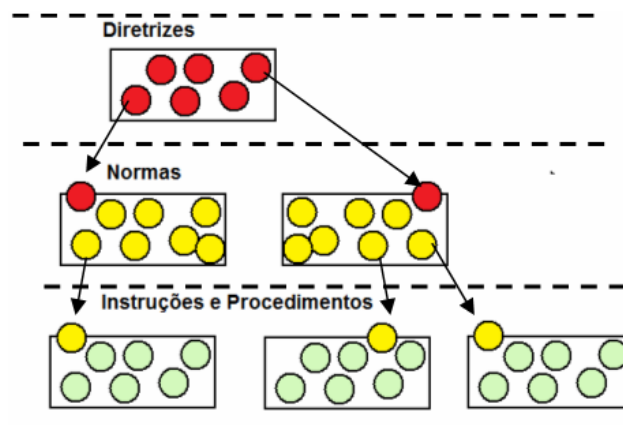
O acesso aos ativos de informação e aos recursos pode ser reduzido ou retirado antes mesmo do encerramento da atividade.

### 3.8. Política de Segurança da Informação

As PSI são um conjunto de documentos que resumem os princípios de SI que a organização reconhece como sendo importantes e que devem estar presentes no dia-a-dia de suas atividades. Conforme mostrado na Figura 2, os documentos de uma PSI são divididos em três categorias: [9]

- **Diretrizes:** Regras de alto nível que representam os princípios básicos de acordo com a visão estratégica da organização. São básicas para a criação das Normas e Procedimentos;
- **Normas:** Especificação das escolhas tecnológicas e dos controles que deverão ser implementados para atingir a estratégia definida nas Diretrizes;
- **Instruções e Procedimentos:** As Instruções detalham as configurações de produtos ou funcionalidades. Os Procedimentos detalham atividades passo a passo e normalmente envolvem a interação de áreas e pessoas.

**Figura 2 – Estrutura dos documentos da PSI**



Fonte: Guia Oficial para Formação de Gestores em SI [9]

Para a norma NBR ISO/IEC 17799:2005, convém que as PSI sejam claras, alinhadas com os objetivos do negócio e devem prover uma direção e apoio para a SI em conformidade com os riscos do negócio e com as leis e regulamentações relevantes.

## 4. Proposta de uma norma para o pessoal transferido

Este item constitui-se na razão do trabalho proposto, a sua motivação e o processo de elaboração da norma com base no referencial teórico.

A escolha da norma proposta por este trabalho teve como motivações:

- Seu caráter imprescindível para a segurança das informações e dos ativos da OM como já explanado no referencial teórico;
- As pesquisas mostram que nas empresas governamentais, a maioria dos problemas de segurança, quando identificados, apontam para os próprios funcionários e hackers;

- A nova norma constitui-se em um modelo e ponto de partida para elaboração de outros controles, visto que a diretriz básica abre campo para elaboração de outras normas;
- Pode ser perfeitamente adicionada ao processo administrativo de transferência de pessoal já existente;
- Com algumas adaptações (estrutura organizacional da OM) pode ser adotada por qualquer OM do EB.

Para a construção da nova norma, seguindo-se o referencial teórico e a estrutura dos documentos de uma PSI, buscou-se a partir das IG 20-19 [4], a diretriz básica para a elaboração das normas e dos procedimentos para os militares transferidos.

#### **4.1. Diretriz**

“Para todo tipo de serviço corporativo de rede de comunicações, seja no contexto local ou remoto, devem existir mecanismos de defesa contra ataques aos referidos sistemas.” (Art. 17 das IG20-19 [4]).

#### **4.2. Norma**

“A saída de militares ou funcionários civis da OM, por motivos de transferência para reserva, para outra organização ou exclusão, deve ser feita de modo controlado a fim de que a devolução de todos os equipamentos e a retirada de todos os direitos de acesso seja concluída.”

#### **4.3. Instruções e Procedimentos**

##### **4.3.1. Encerramento das atividades:**

**Instrução:** A partir da confirmação da transferência do militar ou funcionário civil para outra OM, para reserva ou exclusão, convém que sejam observados os procedimentos necessários para fins de devolução de ativos e retirada de direitos de acesso. A movimentação de militares e funcionários civis deve ser coordenada pela Divisão de Pessoal que tem as atribuições de RH.

##### **Procedimentos:**

- A Divisão de Pessoal deve comunicar o fato à Divisão gestora do transferido;
- A Divisão de Pessoal deve comunicar à Divisão de Operações, caso esta não seja a gestora do transferido.
- A Divisão de Pessoal deve comunicar à Divisão Administrativa para fins de verificação do material em poder do transferido.

##### **4.3.2. Devolução dos ativos:**

**Instrução:** Todos os ativos da OM em poder do militar ou funcionário civil transferido devem ser devolvidos, mediante documento formal, após o encerramento de suas atividades na organização.

##### **Procedimentos:**

- A Divisão de Pessoal, ao comunicar ao militar ou funcionário civil a respeito de seu desligamento da OM, deve fornecer um documento no qual as Divisões Administrativa, Operacional e a gestora, confirmem, mediante

assinatura, as devoluções de ativos que porventura estavam em posse do transferido.

- A Divisão Administrativa deve verificar as devoluções, conferir e assinar o documento de devolução;
- A Divisão de Operações deve verificar as devoluções, conferir e assinar documento de devolução;
- A Divisão gestora do transferido deve:
  - Verificar as devoluções dos ativos;
  - Documentar possíveis conhecimentos do transferido que são considerados importantes para as atividades da Divisão;
  - Conferir e assinar documento de devolução;
- A Divisão de Pessoal deve conferir as assinaturas dos responsáveis e arquivar o documento.

#### **4.3.3. Retirada de direitos de acesso:**

**Instrução:** Todos os direitos de acesso às informações e aos recursos de informação da OM em poder do militar ou funcionário civil transferido devem ser retirados após o encerramento de suas atividades.

#### **Procedimentos:**

- A Divisão de Operações deve retirar todos os acessos aos ativos e aos recursos de processamento da informação dos militares e funcionários civis transferidos, assim que for informada do encerramento de suas atividades por parte da Divisão de Pessoal.
- O mesmo procedimento deve ser adotado pela Divisão gestora do transferido, caso este tenha acesso a algum ativo ou recurso de processamento interno.

## **5. Conclusões**

A literatura nos mostra que os desafios de SI aumentam a cada dia e, conseqüentemente, demandam que as organizações instituem suas Políticas de Segurança da Informação.

Nesse sentido, o comando do EB instituiu as “Instruções Gerais de Segurança da Informação para o Exército Brasileiro (IG 20-19)”, onde um dos objetivos é dotar o Exército de uma referência básica para a elaboração de documentos normativos sobre SI.

A fim de se elaborar uma norma de gerenciamento dos ativos e direitos de acesso do pessoal transferido, foi definida a partir das IG 20-19, a diretriz voltada para as questões de segurança necessárias para todo tipo de serviço corporativo de rede. Para o desenvolvimento das instruções e procedimentos, consultou-se a norma NBR ISO/IEC 17799:2005 e o Guia Oficial para Formação de Gestores em Segurança da Informação [9].

Escolheu-se a NBR ISO/IEC 17799:2005 como base para elaboração da norma, tendo em vista que a 9ª Pesquisa Nacional de Segurança da Informação, da qual participaram cerca de 50% das 1000 maiores empresas do Brasil, apontou a utilização da norma por 63,5% dos entrevistados, para nortear as ações de segurança de suas organizações.

Observa-se que em todas as OM já existem processos administrativos referentes ao pessoal transferido, voltados para o controle de materiais, documentação e transferências de responsabilidades.

Finalmente, a norma proposta neste trabalho, constitui-se em um ponto de partida para a implementação da SI em qualquer OM, podendo ser facilmente adaptada ao processo administrativo de transferência de pessoal já existente.

## **6. Referências**

### **6.1. Sites da Internet**

- [1] 3º Centro de Telemática de Área de São Paulo. Disponível em: [www.3cta.eb.mil.br](http://www.3cta.eb.mil.br). Acesso em 04/07/2008.
- [5] Módulo Security Solutions S.A. 9ª Pesquisa Nacional de Segurança da Informação. Rio de Janeiro, 2003. Disponível em: [http://www.modulo.com.br/media/9a\\_pesquisa\\_nacional.pdf](http://www.modulo.com.br/media/9a_pesquisa_nacional.pdf). Acesso em 04/07/2008.
- [8] MÓDULO Technology for GRC. Governance Risk and Compliance. 10ª Pesquisa Nacional de Segurança da Informação. 2006. Disponível em: [http://www.modulo.com.br/media/10a\\_pesquisa\\_nacional.pdf](http://www.modulo.com.br/media/10a_pesquisa_nacional.pdf). Acesso em 04/07/2008.

### **6.2. Documentos Oficiais**

- [2] Brasil. Exército Brasileiro. Portaria nº 006-DCT, de 05 de fevereiro de 2007. Normas para o Controle da Utilização dos Meios de Tecnologia da Informação no Exército (NORTI). Departamento de Ciência e Tecnologia, 2007.
- [4] Brasil. Exército Brasileiro. Instruções Gerais de Segurança da Informação para o Exército Brasileiro (IG 20-19). Portaria nº 483, de 20 de setembro de 2001. Exército Brasileiro, 2001.
- [6] Brasil. Decreto nº 4.553, de 27 de dezembro de 2002. Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências. **Lex:** Diário Oficial da União de 30 de dezembro de 2002, P. 6. Legislação Federal e marginalia.

### **6.3. Livros e Teses**

- [7] Moreira, Nilton Stringasci. Segurança Mínima. Rio de Janeiro: Axcel Books, 2001.
- [9] Ramos, Anderson (org.). Guia Oficial para Formação de Gestores em Segurança da Informação. Porto Alegre, RS: Editora Zouk, 2006.

### **6.4. Normas**

- [3] Associação Brasileira de Normas Técnicas. ABNT NBR ISO/IEC 17799:2005 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão

da segurança da informação. Associação Brasileira de Normas Técnicas – Rio de Janeiro: ABNT, 2005.

**Contato**

Ricardo Hisao Watanabe

Subtenente do Exército Brasileiro

End. Av Manoel da Nóbrega, 754 – Jd Adalgisa – Osasco SP

Tel: 9975 5210 Res: 3698 5832

Email: ricawat@hotmail.com