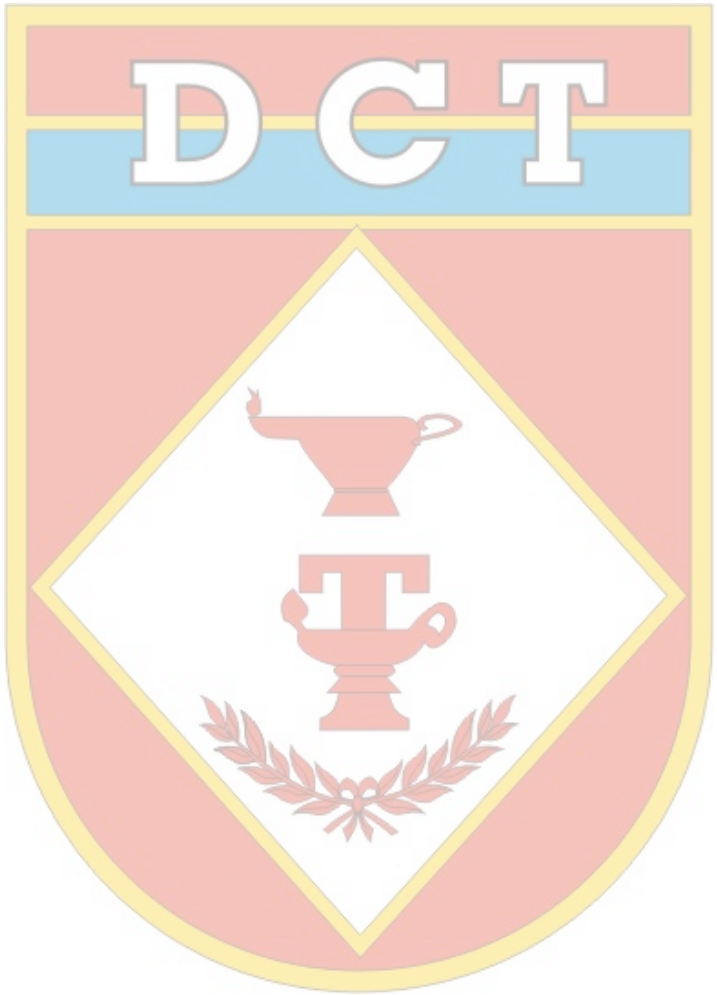


Exército Brasileiro

Braço Forte Mão Amiga

Cartilha Emergencial de Segurança

Tecnologia da Informação e Comunicações

Exército Brasileiro

Departamento de Ciência e Tecnologia

"Presente e Futuro se encontram aqui"

Versão 1.0 - 2011

Cartilha Emergencial de Segurança de Tecnologia da Informação e Comunicações

Sumário

Cartilha Emergencial de Segurança de Tecnologia da Informação e Comunicações

A não observância das medidas previstas nesta publicação de emergência implicará em imputação de responsabilidade pessoal, caso haja violação dos Sistemas de Tecnologia da Informação e Comunicações (TIC) do Exército Brasileiro.

1 INTRODUÇÃO

1.1 A inserção das ferramentas de TI nos ambientes de trabalho das Instituições e Empresas veio acompanhada de uma exigência altamente prioritária, que já existia, sob outras condições, em situações convencionais: **A SEGURANÇA DOS SISTEMAS.**

1.2 O assunto é de tal relevância para as atividades administrativas e operacionais, que o Exército implantou recentemente o **Núcleo do Centro de Defesa Cibernética (NuDCiber)**, cuja missão é a de definir o arcabouço de um ambiente de segurança corporativa de alto nível, estabelecendo o arsenal de medidas, tecnologias e marcos regulatórios destinados a manter a integridade da sua infraestrutura de TI, em qualquer cenário.

1.3 **Esta Cartilha Emergencial sobre Segurança de TIC**, destina-se a implantar, desde já, procedimentos de segurança básicos, de baixo custo e complexidade, muitos dos quais já previstos e adotados pelas OM. As recomendações contidas nesta publicação **são de caráter impositivo**, cabendo aos Comandantes, Chefes e Diretores a responsabilidade pelo seu cumprimento.

- Instruções Reguladoras Sobre Análise de Risco para Ambientes de Tecnologia da Informação do Exército Brasileiro – IRRISC (IR-13-10);
- Instruções Reguladoras sobre Segurança da Informação nas Redes de Comunicação e de Computadores do Exército Brasileiro – IRESER (IR 13-15);
- Instruções Reguladoras sobre Segurança da Infraestrutura de Chaves Públicas do Exército Brasileiro – IRESICP (IR 80-05);
- Instruções Reguladoras para Práticas de Certificação da Autoridade Raiz do Exército Brasileiro – IRESRAIZ (IR 80-06);
- Instruções Reguladoras para Práticas de Certificação da Autoridade Certificadora do Exército Brasileiro – IRESPCAC (IR 80-07); e
- Portaria 111 – DCT, de 29MAR10 – Plano de Padronização do Ambiente e Migração para Software Livre no Exército Brasileiro.

Cartilha Emergencial de Segurança
de Tecnologia da Informação e Comunicações

1.4 As ações contidas neste documento baseiam-se na experiência dos profissionais responsáveis pelos Sistemas de Telemática do Exército, ao longo dos últimos anos, e nos ensinamentos obtidos junto aos mais importantes órgãos de Segurança de Informação, constituindo-se em uma coletânea das melhores práticas.

1.5 Por fim, ressalta-se que além de preservação dos Sistemas de TIC, as medidas de segurança contribuem para resguardar a imagem da Instituição, dificultando a violação desses sistemas e a obtenção de informações sensíveis por intermédio de ações criminosas.

2 REGRAS BÁSICAS DE SEGURANÇA COMPUTACIONAL AOS CMT OM

2.1 Cada OM deverá organizar, publicando em Boletim Interno, um Comitê permanente de auditoria interna das medidas de segurança preconizadas na regulamentação vigente, constantes ao final desta Cartilha e parcialmente abordadas no texto, cabendo ao DCT a realização de verificações externas de caráter programado ou inopinado, como autoridade validadora dos níveis de segurança dos sistemas sustentados pela TI do Exército Brasileiro.

2.2 Controlar o acesso à Internet na OM, restringindo-o, apenas, às estações de trabalho que efetivamente necessitarem de tal acesso. Ainda assim, devem ser bloqueados os sítios que reduzam a produtividade, ou que sejam incompatíveis com a seriedade e a responsabilidade esperada no ambiente de trabalho.

2.3 Estabelecer uma rotina de permanente conscientização dos integrantes da organização quanto ao emprego adequado dos recursos de Tecnologia da Informação e Comunicações (TIC) à disposição da OM.

2.4 Solicitar o apoio técnico à OM de Telemática do Exército (CTA ou CT) que atende à OM considerada, sempre que houver dúvidas.

2.5 **Proibir** a utilização de dispositivos móveis de armazenamento (*pendrives*, HD externos ou cartões de memória), particularmente em ambientes onde operam máquinas com dados sensíveis. Quando absolutamente necessário, liberar o acesso de tais dispositivos, **sob supervisão**, somente nas máquinas com antivírus configurado para verificar, automaticamente, qualquer dispositivo removível conectado ao computador.

Cartilha Emergencial de Segurança
de Tecnologia da Informação e Comunicações

9 LEGISLAÇÃO DE REFERÊNCIA

Abaixo, segue a legislação que regula a atividade de TIC no EB. Consultá-la sempre que necessário. Em caso de dúvidas, consultar o CTA/CT de sua área.

- Instruções Gerais de Segurança da Informação para o Exército Brasileiro (IG-20-19);
- Instruções Gerais para Salvaguarda de Assuntos Sigilosos (IG-10-51);
- Normas para o Controle da Utilização dos Meios de Tecnologia da Informação no Exército – NORTI - 3ª Edição, BE 034, de 22 Ago 08;
- Instruções Reguladoras para Utilização da Rede Mundial de Computadores (Internet) por Organizações Militares e Militares do Exército (IR-20-26);
- Instruções Reguladoras para o Emprego Sistêmico do Serviço de Correio Eletrônico no Exército Brasileiro - IRESCE (IR 13-06);
- Instruções Reguladoras para Emprego Sistêmico da Informática no Exército Brasileiro - IREMSI (IR 13-07);
- Instruções Reguladoras Sobre Auditoria de Segurança de Sistemas de Informação do Exército Brasileiro – IRASEG (IR 13-09);

8.3.2 Desconsiderar **todos os *e-mails*** de supostas instituições bancárias ou governamentais, solicitando atualização de cadastro ou instalação de programas;

8.3.3 Ficar atento a *e-mails* ou telefonemas solicitando dados pessoais (números de cartão, senhas, etc.) ou dados sobre a tecnologia que está sendo utilizada (sistema operacional, antivírus, etc.).

Cartilha Emergencial de Segurança
de Tecnologia da Informação e Comunicações

2.6 Manter o sigilo das senhas utilizadas nos sistemas computacionais. As senhas são pessoais, não podendo, portanto, ser compartilhadas. Os cadastros de usuários que acessam os sistemas devem ser **mantidos atualizados e supervisionados pela contra-inteligência da OM.**

2.7 Estabelecer uma política clara e supervisionada relativa ao **descredenciamento** de usuários que tenham sido transferidos de OM ou de função.

2.8 Divulgar com regularidade o cumprimento das diretrizes, manuais, instruções e normas em vigor no âmbito do Exército que tratam da Segurança da Informação e Comunicações (SIC).

3 COMPUTADORES DA OM

3.1 Utilizar somente ***software*** original e licenciado e os constantes no Anexo E ao Plano de Padronização do Ambiente e Migração para Software Livre no Exército Brasileiro publicado na separata ao BE Nr 17 de 30ABR10.

3.2 Adotar os seguintes tipos de programas de segurança em todos os computadores da OM, utilizando ***software*** adquirido ou padronizado pelo Exército:

3.2.1 ***Antivírus:*** para evitar a propagação de vírus de computador;

3.2.2 ***Antispyware*****:** para manter a máquina protegida de programas espiões;

3.2.3 ***Antispam*****:** para evitar o tráfego de mensagens de correio eletrônico indesejadas; e

3.2.4 ***Firewall pessoal***: para proteger a máquina de acessos remotos ao seu equipamento e furto de dados.

3.3 Manter permanentemente atualizados e com as mais recentes correções de segurança, todos os programas instalados. Os atos hostis exploram as vulnerabilidades conhecidas que, normalmente, são corrigidas nas versões mais recentes. Recomenda-se a adoção de ferramentas como CACIC ou ***OCS Inventory*** para gerenciamento de atualizações.

Cartilha Emergencial de Segurança
de Tecnologia da Informação e Comunicações

8 PROTEÇÃO CONTRA SPAM

8.1 Não utilizar a conta de correio corporativo funcional em cadastros de sítios na Internet. Se necessário, manter uma conta em provedor público (Gmail, Yahoo, Hotmail, etc) para esta finalidade.

8.2 DISPOSITIVOS DE ARMAZENAMENTO REMOVÍVEIS

8.2.1 Configurar o antivírus para verificar automaticamente todos os dispositivos de armazenamento removíveis (CD, DVD, *pendrive*, cartão de memória, HD externo etc.) conectados ao computador.

8.2.2 Desabilitar a execução automática de quaisquer dispositivos móveis.

8.2.3 **Não permitir o uso descontrolado de qualquer tipo de dispositivo de armazenamento removível no ambiente de trabalho.**

8.3 PROTEÇÃO CONTRA FRAUDES VIA INTERNET

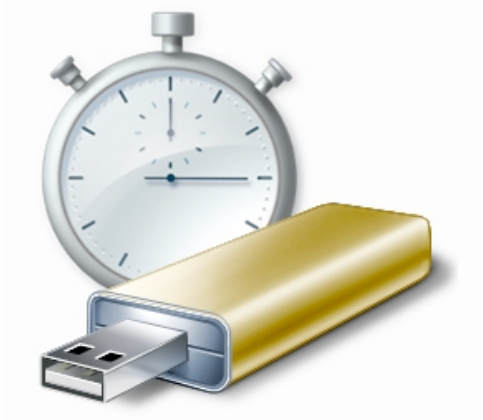
8.3.1 Não clicar em *links* ou abrir arquivos recebidos por *e-mail*, a menos que se tenha absoluta certeza da origem e integridade do mesmo. Ter em mente que um arquivo enviado por uma pessoa de confiança pode não ter sido realmente enviado por ela;

6.2 Retirar os equipamentos comprometidos da rede, **mas preservar as evidências para posterior análise forense** por pessoal especializado, mantendo-o, inclusive, ligado.

7 TELEFONIA e VIDEO-CONFERÊNCIA NA OM

7.1 As comunicações telefônicas e por videoconferência devem tratar somente de assuntos ostensivos.

7.2 São vedadas teleconferências, ainda que de assuntos ostensivos, utilizando-se de serviços não homologados pelo Exército, por intermédio do DCT.



Cartilha Emergencial de Segurança
de Tecnologia da Informação e Comunicações

4 REDE DA OM

4.1 Quando a OM possuir acesso à Internet disponibilizado pelo CITEx ou pelo CTA/CT da sua área, **não deve haver contratação** de outros acessos junto às empresas provedoras do serviço. O DCT está atualizando e ampliando o provimento de serviços necessários às atividades institucionais.

4.2 **Na imperiosa necessidade de contratação de acesso à Internet**, **não permitir** que as estações conectadas à rede mundial estejam, simultaneamente, conectadas também à EBNet.

4.3 **Utilizar exclusivamente o correio eletrônico corporativo** para troca de mensagens relativas ao serviço.

4.4 Os servidores e os sistemas que armazenam dados corporativos devem conter mecanismos fortes de autenticação, conforme prevê o Art. 47 das IR 13-15.

4.5 Utilizar serviços criptográficos para o intercâmbio de informações (correio eletrônico corporativo, transferência de arquivos, etc.).

4.6 Proteger os ativos de rede para evitar o furto de equipamentos que armazenem informações ou a interceptação do tráfego da rede (*sniffers*). Mesmo equipamentos obsoletos e descarregados podem

armazenar dados sensíveis, facilmente recuperáveis. A mesma recomendação vale para equipamentos que deixarão a OM para manutenção. **Os discos deverão ser retirados** e, se for o caso, formatados com *software* que elimine, definitivamente, os dados existentes (técnicas de *wipe*).

4.7 Solicitar ao CTA/CT de apoio a verificação de vulnerabilidades em sistemas disponibilizados na Internet.

4.8 Executar rigoroso controle das máquinas e dos usuários que podem ter acesso à rede de computadores da OM. **Não permitir** que máquinas de visitantes sejam conectadas à rede local.

4.9 Evitar a utilização de redes sem fio (*wireless*). Se for imprescindível seu emprego, adotar protocolos de proteção seguros (WPA ou superior) e só permitir o acesso dos equipamentos previamente cadastrados (controle de endereços MAC). No caso de instalação dessa solução, solicitar apoio técnico do CTA/CT da área.

Cartilha Emergencial de Segurança
de Tecnologia da Informação e Comunicações

5 PÁGINA DE INTERNET DA OM

5.1 Priorizar a segurança da página: elaborar páginas simples, utilizando componentes de origem confiável, homologados pelo Departamento de Ciência e Tecnologia, observando o previsto nas IR 20-26.

5.2 Observar as normas de contra-inteligência: não divulgar dados pessoais ou informações sobre a rotina da OM.

5.3 Hospedar a página exclusivamente nos servidores do CITEx ou do CTA/CT que apoia a OM.

6 INCIDENTES DE SEGURANÇA

6.1 Na ocorrência de qualquer **violação de segurança** aos recursos de TIC da OM, o fato deverá ser imediatamente comunicado, pelo meio mais rápido, à Seção de Tratamento de Incidentes de Rede (STIR) do CTA/CT de sua área, que determinará as medidas exigidas para cada caso. A OM atingida, obrigatoriamente, será objeto de uma auditoria técnica por parte da STIR correspondente. O Relatório decorrente deverá ser encaminhado ao CITEx e DCT pelo CT/CTA para análise e para que sejam tomadas as medidas complementares, inclusive em relação às responsabilidades da OM.