PORTARIA Nº 004-DCT, DE 31 DE JANEIRO DE 2007.

Aprova as Instruções Reguladoras Sobre Segurança da Informação nas Redes de Comunicação e de Computadores do Exército Brasileiro - IRESER (IR 13-15).

O CHEFE DO DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA, no uso da atribuição que lhe confere o art. 14, inciso III, do Regulamento do Departamento de Ciência e Tecnologia (R-55), aprovado pela Portaria do Comandante do Exército nº 370, de 30 de maio de 2005, combinado com o disposto no art. 112 das Instruções Gerais para a Correspondência, as Publicações e os Atos Administrativos no Âmbito do Exército (IG 10-42), aprovada pela Portaria do Comandante do Exército nº 041, de 18 de fevereiro de 2002, resolve:

Art. 1º Aprovar as Instruções Reguladoras Sobre Segurança da Informação nas Redes de Comunicação e de Computadores do Exército Brasileiro - IRESER (IR 13-15).

Art. 2º Estabelecer que esta Portaria entre em vigor na data de sua publicação.

INSTRUÇÕES REGULADORAS SOBRE SEGURANÇA DA INFORMAÇÃO NAS REDES DE COMUNICAÇÃO E DE COMPUTADORES DO EXÉRCITO BRASILEIRO IRESER - (IR 13-15)

ÍNDICE DOS ASSUNTOS

Art.

Anexos

INSTRUÇÕES REGULADORAS SOBRE SEGURANÇA DA INFORMAÇÃO NAS REDES DE COMUNICAÇÃO E DE COMPUTADORES DO EXÉRCITO BRASILEIRO IRESER - (IR 13-15)

TÍTULO I
DAS GENERALIDADES

Art. 1º As presentes instruções, elaboradas em observância aos artigos 17 e 20 e ao inciso XIV do artigo 31 das Instruções Gerais de Segurança da Informação para o Exército Brasileiro (IG 20-19), têm por finalidade regular as condições de segurança da informação a serem satisfeitas pelas redes de comunicação e de computadores no âmbito do Exército Brasileiro.

Art. 2º São objetivos destas Instruções:

I - estabelecer regras gerais de segurança para os ambientes de rede do Exército nas áreas:

a) documentação normativa;

b) riscos;

c) mecanismos de defesa contra violações de segurança da rede;

d) monitoração e registro de eventos referentes aos serviços corporativos de rede;

e) a verificação da efetividade das ações de segurança da informação (auditora da segurança da informação) relativos aos serviços de rede;

f) contingência (continuidade de serviços) para os serviços de rede corporativos;

g gestão de incidentes de rede;

h) gestão da segurança.

II - orientar as OM do Exército na composição de suas normas internas de segurança de redes;

III - prover referenciais doutrinários sobre segurança da informação no que tange à segurança de redes;

IV - Estabelecer as principais responsabilidades no processo de segurança da informação no ambiente de redes Exército.

TÍTULO II
DEFINIÇÕES BÁSICAS

Art. 3º Para a aplicação destas Instruções, deve-se adotar a seguinte conceituação:

I - RECURSO DE REDE - são todos os meios tecnológicos pelos quais é possível processar, enviar, receber ou armazenar dados em uma rede. Exemplos: computadores e seus periféricos, concentradores (**hubs, switches** e roteadores), modens, interfaces de rede.

II - RECURSO CRÍTICO - recurso de rede cuja violação física ou lógica implica em uma violação de segurança com repercussões negativas, no mínimo, para a OM a que pertence o recurso.

III - COMPROMETIMENTO DE RECURSO DE REDE - violação de segurança de um recurso de rede que tenha como conseqüência a perda de um ou mais dos atributos de integridade, da disponibilidade e da confidencialidade dos dados da rede;

IV - CONTINGÊNCIA - situação excepcional com desdobramentos danosos às informações de um sistema de informação;

V - CONTINUIDADE DE SERVIÇOS - conjunto de ações que, durante a ocorrência de situações de violação da segurança, visam garantir a continuidade dos serviços de uma rede e o processo de retorno à normalidade.

VI - CONTROLES - Para aplicação destas Instruções, devem ser considerados como controles todos as formas que definam limites ou atuem como limitadores de qualquer ação que influa na confidencialidade, na integridade ou na disponibilidade dos dados de uma rede.

VII - EFETIVIDADE DAS AÇÕES DE SEGURANÇA - eficácia e eficiência de uma ação de segurança.

VIII - MECANISMO DE DEFESA **-** ação, automatizada ou não, capaz de prevenir, interromper ou neutralizar um ataque à rede.

IX - ARQUITETURA DO **FIREWALL** OU DO SISTEMA DE DETECÇÃO DE INTRUSÃO - configuração da disposição física e lógica dos elementos que compõem o **firewall** ou o sistema de detecção de intrusão na rede.

X - CÓDIGOS MALÉFICOS OU MALICIOSOS - programas cuja finalidade é violar a segurança de um serviço, computador ou rede. Exemplos desses códigos são os vírus de computador, os cavalos de tróia (**trojans**), os vermes (**worms**), programas espiões (**por exemplo, spywares e keyloggers**) etc.

XI - MONITORAÇÃO DE EVENTOS DE REDE - processo em que um sistema de gerência de rede acessa, acompanha a evolução e interpreta os registros dos eventos ocorridos num **hardware** ou **software** da rede.

XII - PONTOS DE CONTATO - elementos que devem ser acionados em caso de comprometimento de algum recurso da rede e que sejam as pessoas mais habilitadas a lidar com a correção do problema.

XIII - PROCESSOS DE AUTENTICAÇÃO - processo pelo qual é possível aferir se o originador de um processo automatizado, por exemplo, o envio de uma mensagem eletrônica, é realmente quem alega ser.

XIV - REGISTRO DE EVENTOS DE REDE - conjunto de informações que listam as ocorrências durante o funcionamento de um **hardware** ou **software** instalado na rede.

XV - VIOLAÇÃO DA SEGURANÇA DA INFORMAÇÃO - eventos que violem a integridade, a disponibilidade e a confidencialidade da informação.

XVI - INCIDENTE DE REDE - ocorrência de um evento de violação da segurança da rede, seja de origem intencional ou não, que atinja recursos de infra-estrutura física, lógica ou de alimentação elétrica, **hardware**, meios de armazenamento, protocolos, dados, serviços, **softwares** ou qualquer outro recurso de rede cujo o comprometimento atinja a integridade, a disponibilidade ou a confidencialidade da informação.

XVII - GERÊNCIA DA REDE – processo pelo qual o funcionamento da rede pode ser monitorado, em particular nos parâmetros referentes as áreas de configuração, falhas, performance, contabilização e segurança, com a possibilidade de adequação dos valores desses parâmetros pela intervenção do gerente da rede.

TÍTULO III

DAS REGRAS GERAIS DE SEGURANÇA

CAPÍTULO I

DA DOCUMENTAÇÃO NORMATIVA

Art. 4º Todas as redes de dados ou comunicação do Exército devem possuir documentação normativa de segurança da informação, as quais devem definir as regras de segurança e responsabilidades necessárias para a proteção das informações nessas redes.

Art. 5º A documentação normativa básica de segurança da informação de qualquer rede do Exército deve seguir o modelo definido no ANEXO A.

Art. 6º A documentação normativa deve ser desdobrada em mais de uma norma, caso a complexidade da rede seja tal que os responsáveis pela elaboração dos documentos julguem esse desdobramento recomendável. Desta forma, pode-se ter uma norma principal de segurança da informação para a rede e, por exemplo, outras duas normas específicas para o serviço de correio eletrônico e outra para o **firewall**.

Art. 7º As normas de redes devem abordar os temas que sejam de relevância para a OM onde a rede está implementada, porém nessas normas deverão constar regras de segurança nas seguintes áreas básicas:

I - REGRAS GERAIS - regras de segurança de caráter geral e voltadas para medidas de segurança dos dados, informações e conhecimentos armazenados, processados ou disseminados nos enlaces ou equipamentos da rede;

II - SEGURANÇA DOS SERVIÇOS, SISTEMAS, APLICATIVOS E SISTEMAS OPERACIONAIS DE REDE - regras de segurança referentes aos procedimentos de instalação, configuração e uso de:

a) serviços, tais como correio eletrônico ou WEB;

b) sistemas corporativos específicos do Exército;

c) aplicativos de uso geral, tais como suítes de escritório;

d) sistemas operacionais de rede.

III - SEGURANÇA DO **HARDWARE** - regras de segurança referentes aos procedimentos de instalação, configuração e uso de:

a) computadores servidores;
b) computadores de uso específico;
c) computadores de uso geral;
d) periféricos de rede;
e) equipamentos de interligação de rede (roteadores, **switches**, **hubs**, modem, repetidores);
f) centrais telefônicas;
g) equipamentos rádio.

IV - SEGURANÇA DAS INFRA-ESTRUTURA DE REDE - regras de segurança relativas às estruturas de:

a) interligação lógica e seus elementos constituintes, tais como cabeamentos, dutos, documentação da instalação (descrição da rede, plantas etc) cabeamentos, pontos de acesso de redes sem fio etc;

b) alimentação elétrica, e seus elementos constituintes, tais como fiação elétrica, dutos, quadros de distribuição, estabilizadores, **nobreak** etc.

V - SEGURANÇA DAS ÁREAS E INSTALAÇÕES - regras de segurança relativas a ao controle de acesso e a adequação das áreas e instalações onde se encontram equipamentos críticos da rede;

VI - PLANO DE CONTINGÊNCIA - regras de segurança relativas às medidas de contingência para a rede;

VII - SEGURANÇA DO PESSOAL - regras de segurança relativas aos comportamentos adotados pelo pessoal que lida com as redes, seja no nível gerencial, de manutenção ou usuário final;

VIII - GERENCIAMENTO DA REDE - regras de segurança relativas às ações de gerência da rede, ou seja, monitoração e adequação de parâmetros referentes às áreas de configuração, desempenho, falhas e contabilização;

IX - INCIDENTES DE REDES – regras para procedimentos no caso de ocorrerem incidentes de rede (violações da segurança da rede).

Art. 8º O processo necessário para elaboração das normas é o seguinte:

I - nomeação em BI da equipe que elaborará o(s) documento(s) e o militar condutor do processo;

II - elaboração do plano de ação necessário para elaborar a norma, definindo objetivos, tarefas, responsabilidades, recursos e cronograma;

III - realização de uma análise de riscos na rede, conforme Instruções vigentes;

IV - elaboração de uma primeira versão conforme modelo constante destas Instruções;

V - refinamento da primeira versão por meio de discussões e sugestões apresentadas pela equipe até que se obtenha uma versão considerada satisfatória para o grupo. Um fluxograma do processo está representado na figura 1.

CAPÍTULO II

DA ANÁLISE DE RISCOS

Art. 9º Todas as ações que impliquem em atualização, reconfiguração, acréscimo de **hardware** ou **software** ou qualquer outro rearranjo na composição da rede, em particular se a modificação for em um elemento de segurança, devem ser precedidas de uma análise de riscos nos moldes definidos nas Instruções do Exército sobre o assunto.

§ 1º Caso não seja possível a aplicação prévia de uma análise de risco, deve-se realizá-la no menor prazo possível de modo a se aferir o grau de risco introduzido pela modificação no ambiente da rede.

§ 2º O nível de detalhamento do processo da análise de riscos a ser realizada dependerá da dimensão da modificação que ocorra, mantendo-se o mecanismo básico da análise previsto nas Instruções do Exército vigentes sobre riscos. As ameaças básicas em um ambiente de rede são as seguintes:

I - escuta passiva (sem atingir a integridade do dado) ou ativa (atingindo a integridade do dado) de dados em trânsito na rede;

II - acesso passivo (sem reconfiguração) ou ativo (com reconfiguração) de programas computador da rede por outro computador da rede ou fora dela;

III - acesso passivo (sem atingir a integridade do dado) ou ativo (atingindo a integridade do dado) de dados por outro computador da rede ou fora dela;

IV - inserção de mensagens na rede, falsificando a sua autoria;

V - reuso de uma mensagem autêntica já utilizada anteriormente na rede;

VI - bloqueio de tráfego de uma ramificação específica ou de toda a rede;

VII - execução remota de programa não autorizado.

§ 3º As modificações no ambiente da rede e decisões advindas da aplicação da análise de risco devem ser registradas em relatório, conforme modelo constante do ANEXO B, que deverá ser arquivado juntamente com os demais documentos da rede e, se necessário for, a documentação gerada deverá receber classificação sigilosa.

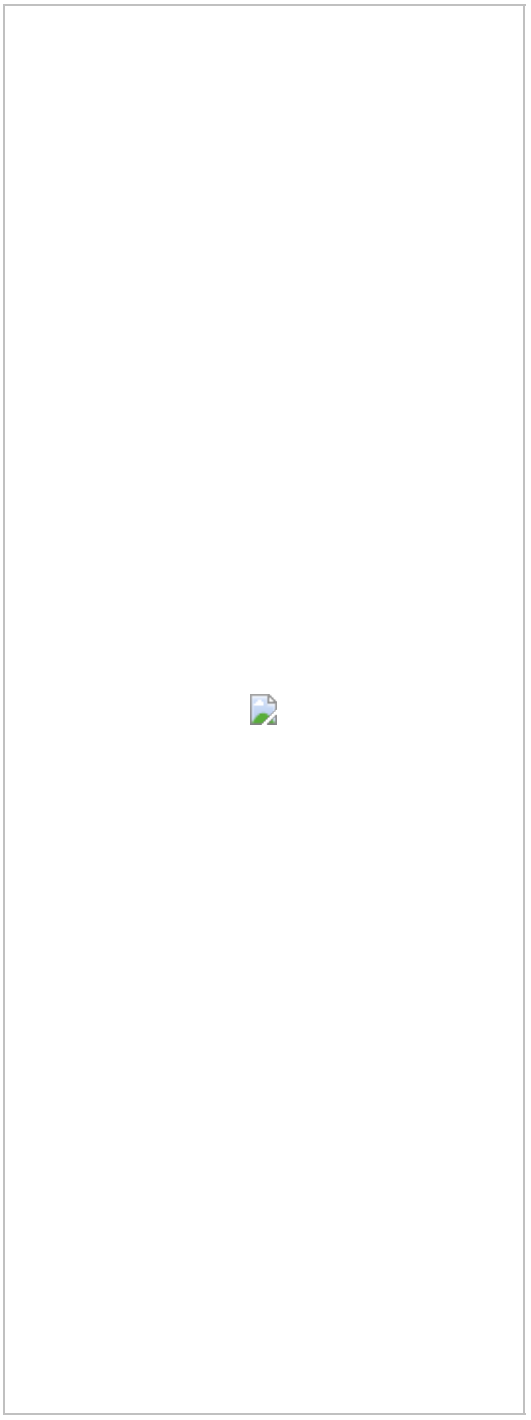


Fig nº 1: Processo para elaboração de normas de segurança

CAPÍTULO III

DAS TÉCNICAS E TIPOS DE PRODUTOS TECNOLÓGICOS

Seção I

Da Criptografia

Art. 10. A criptografia é um mecanismo que deve ser utilizado na cifração de dados a serem transmitidos ou armazenados nas redes do Exército sempre que houver necessidade de preservação do sigilo desses dados e em compatibilidade com as regras se segurança de salvaguarda de assuntos sigilosos em vigor.

Art. 11. A adoção do uso de criptografia para proteção de sigilo de dados deve ser precedida de uma análise de riscos que justifique a escolha da solução a ser usada.

Parágrafo único. A análise de riscos deve seguir as recomendações contidas nas documentações normativas do Exército sobre esse tema.

Art. 12. As soluções criptográficas utilizadas na Força devem ser ter um das seguintes origens:

I - ser uma solução de concepção e implementação realizados pelo DCT;

II - ser uma solução de concepção do DCT e implementação controlada por esse Departamento;

III - ser uma solução de concepção de empresa privada, especialmente desenvolvida para o Exército e com o processo de

desenvolvimento e implementação controlados pelo DCT;

IV - ser uma solução de concepção de empresa privada, com algoritmos proprietários, de concepção e desenvolvimentos não controlados pelo DCT;

V - ser uma solução baseada em padrões comerciais e notoriamente conhecidos.

Parágrafo único. As soluções enquadradas nos incisos IV e V só poderão ser adotadas para os casos em que for inviável técnica ou administrativamente ser enquadradas em um dos três primeiros incisos e a análise de riscos realizada para o caso indicar que os riscos gerados por essa opção são toleráveis.

Art. 13. Os sistemas criptográficos implementados nas redes do Exército devem atender aos seguintes requisitos:

I - utilizar algoritmos criptográficos comprovadamente robustos e compatíveis com o risco associado ao seu emprego;

II - devem utilizar mecanismos de geração e gerenciamento de chaves criptográficas comprovadamente robustos e compatíveis com o risco associado ao seu emprego;

III - utilizar chaves cujo o tamanho seja compatível com o nível de segurança desejado contra ataques de força bruta;

IV - ser, preferencialmente, de origem nacional;

V - devem ter o seu uso disciplinado por regras contidas nas normas de segurança da rede em que for empregado.

Parágrafo único. A robustez da solução deve ser reconhecida e atestada pelo Departamento de Ciência e Tecnologia, portanto, para a adoção em caráter permanente de um sistema criptográfico, as OM do Exército devem consultar o DCT para obter informações quanto à adequação da escolha.

Art. 14. As regras relativas ao uso de criptografia contidas nas normas de segurança da rede em uma OM devem conter, no mínimo, diretivas relativas ao seguinte:

I - situações em que devem e as que não devem ser utilizados ferramentas criptográficas automatizadas;

II - procedimentos para uso e gerência das chaves criptográficas (geração, configuração, validade, armazenamento, descarte, substituição, transmissão, procedimentos em caso de violação ou perda etc);

III - algoritmos passíveis de utilização;

IV - formas de trato (armazenamento, classificação sigilosa, formato etc) de documentação gerada com o uso da criptografia (**log** de eventos, relatórios, análise de riscos para escolha da solução etc).

Art. 15. As OM que fazem uso de sistemas criptográficos em suas redes devem notificar o DCT, em documento classificado, sobre as características e o tipo de uso desses sistemas para fins de conhecimento e verificação da adequação do uso. Os itens a serem informados são os seguintes:

I - finalidade do sistema;

II - tipos de criptografia possíveis (simétrica ou de chave pública);

III - tipos de algoritmo criptográficos usados;

IV - algoritmos de geração das chaves criptográficas;

V - tamanho das chaves criptográficas que podem ser usadas;

VI - uso que está sendo feito na rede da OM (tipos de dados que estão sendo protegidos);

VII - formas de segurança para as chaves criptográficas;

VIII - versão do **software**, ou do **firmware,** se for o caso, que implementa a solução;

IX - se foram ou não utilizados critérios para julgar se o algoritmo criptográfico e o mecanismo de geração e gerenciamento das chaves criptográficas é robusto o suficiente para atender o grau de risco envolvido com o uso da solução e quais forma esses critérios.

Parágrafo único. Caso haja dificuldade em obter as informações listadas nesse artigo, a OM deverá encaminhar ao DCT o máximo de informações possíveis sobre a solução para que seja possível aferir os parâmetros de relevância para que o Departamento possa prover a orientação sobre a adequação da solução.

Art. 16. Para a escolha de um sistema de criptografia a ser empregado em redes da Força e nos casos em que houver a impossibilidade de satisfazer na íntegra o uso de soluções nacionais, deve-se buscar compor a solução de tal modo que seus elementos constituintes possam ser substituídos por soluções nacionais, quando estas estiverem disponíveis e tecnologicamente confiáveis, desde que tais substituições não comprometam a robustez da solução global.

Art. 17. Todo parâmetro crítico, como chaves criptográficas, cuja exposição indevida comprometa a segurança do sistema criptográfico usado na rede da OM, deve ser armazenado em forma cifrada, sendo essa cifração realizada com chaves armazenadas em mídias removíveis.

Art. 18. A manipulação das chaves criptográficas utilizadas nos sistemas criptográficos da das redes do Exército deverá ser restrita a um número mínimo e essencial de pessoas assim como deve estar submetida a mecanismos de controle estipulados nas normas de segurança e monitorados pela gerência da rede.

Art. 19. O processo de remessa de chaves criptográficas e demais parâmetros do sistema de criptografia deve assegurar o sigilo desses parâmetros por meio de canais seguros.

Art. 20. O uso de criptografia só deve ser utilizado em mensagens de serviço e que devidamente enquadradas nas normas internas da OM e do Exército sobre a matéria.

Seção II
Do Acesso Remoto Seguro (Redes Privadas Virtuais - RPV)

Art. 21. As OM que não tenham acesso à rede EBNet, mas possuam Internet devem fazer uso do acesso remoto seguro para efetivar esse acesso. Para obter o acesso seguro, a seguinte sistemática deve ser realizada:

I - A OM deverá encaminhar solicitação ao CITEx, de acordo com o modelo representado no ANEXO C, justificando a necessidade do acesso remoto via Internet e declarando não possuir acesso à EBNet, seja por meio da prestadora de serviço ou da Rede Metropolitana.

II - O documento deverá conter uma lista de usuários por OM, devidamente autorizados a receber o acesso remoto, por intermédio da Internet.

III - Para cada usuário deverá ser fornecido:

a) o nome completo;

b) posto ou graduação;

c) número da identidade;

d) telefone de contato; e

e) se for o caso, a solicitação de uma senha (para o caso de usuários não cadastrado para acesso ao Correio Eletrônico Corporativo).

IV - Após o cadastramento, o CITEx deverá notificar à OM as senhas temporárias, o endereço do sítio da Internet e instruções para obter o **software** necessário ao acesso remoto e as orientações de instalação.

Seção III
Do Firewall e dos Sistemas de Detecção de Intrusão

Art. 22. As OM que tiverem suas redes conectadas à EBNet e que estiverem conectadas à Internet ou a outras redes inseguras devem fazer uso de **firewall** para proteger essa conexão.

Parágrafo único. As regras de filtragem implementadas no **firewall** da OM deverão ser compatíveis com as regras configuradas no **firewall** do CITEx.

Art. 23. As ferramentas de **firewall** e de detecção de intrusão devem ser adquiridas prevendo-se, no processo de compra, a inclusão de treinamento para uso do produto e com a contratação de serviço pós-venda, no qual o fabricante ou seu representante legalmente reconhecido esteja formalmente comprometido em prover suporte técnico e a atualização do produto.

Art. 24. As OM que fizerem uso de ferramentas de **firewall** ou sistemas de detecção de intrusão devem incluir em seus planejamentos financeiros a previsão de recursos para atualização técnica do pessoal que operava as ferramentas.

Art. 25. As redes onde dados corporativos são armazenados em servidores específicos devem utilizar mecanismos de detecção de intrusão nesses servidores.

Art. 26. Os **firewalls** e sistemas de detecção de intrusão devem estar em funcionamento e regidos por normas de segurança, cujo modelo esteja de acordo com o ANEXO D, que definam:

I - seu uso (que sistemas protegem);

II - configuração lógica (serviços permitidos e proibidos; usuários ou grupos e seus privilégios de acesso; tipos de tráfego, serviço, protocolo ou usuários permitidos ou proibidos; configuração do registro de logs; relações de confiança com outras redes; serviços de criptografia e antivírus, se for o caso; etc);

III - configuração da instalação física (arquitetura do **firewall** ou do sistema de detecção de intrusão);

IV - manutenção (atualização e verificação da normalidade de operação);

V - ações de contingências (**firewall "backup"**, procedimentos em caso de violação e restauração de serviços);

VI - cópias de segurança (configuração e registros de eventos - **logs**);

VII - tipo de controle de acesso;

VIII - tipo de processo de autenticação que é necessário, assim como outras regras que estejam de acordo com as peculiaridades da rede.

IX - pessoal autorizado a acessar e configurar os **softwares**;

X - periodicidade de revisão da norma.

Parágrafo único. As normas que especifiquem a configuração dos **firewalls** ou sistemas de detecção de intrusão devem ter classificação sigilosa e ser mantidas conforme as Instruções que trata de salvaguarda de assuntos sigilosos em vigor no Exército.

Art. 27. Os sistemas de **firewalls**, os sistemas de detecção de intrusão e outros mecanismos de segurança considerados críticos devem ser instalados em equipamentos exclusivamente dedicados ao seu uso, ou seja, não se deve utilizar o mesmo equipamento para instalar serviços de segurança e outros serviços como, por exemplo, correio eletrônico ou serviço para acesso a Internet.

Parágrafo único. Nos casos em que forem utilizadas aplicações de segurança cuja finalidade é monitorar uma ou mais aplicações, como no caso dos **Host Intrusion Detection Systems** (HIDS) é admissível e necessário a convivência do serviço de segurança com outros serviços no mesmo computador.

Art. 28. Serviços e funcionalidades adicionais que não sejam necessárias para proteção da rede ou que permitam privilégios de gerência e acesso que não sejam previstos nas regras de segurança não devem ser instalados ou ativados tanto nas ferramentas quanto nos sistemas operacionais que as sustentam.

Art. 29. Tanto as ferramentas de segurança utilizadas quanto os sistemas operacionais que as sustentam devem ser mantidos atualizados com as correções e atualizações de segurança conforme esses módulos forem disponibilizados pelo fabricante.

Art. 30. Para efeito de verificação da conformidade entre a norma de segurança do **firewall** ou do sistema de detecção de intrusão, devem ser utilizadas ao menos duas técnicas básicas:

I - comparação das regras que estão configuradas no **firewall** ou no sistema de detecção de intrusão com as regras previstas nas normas;

II - teste de violação das regras configuradas por meio da tentativas de se efetuar ações que, a princípio, se espera que sejam impedidas pela segurança do sistema.

Art. 31. A gerência remota de um sistema de **firewall** de nível de aplicação ou sistemas de detecção de intrusão pode ser realizada desde que os dados sejam cifrados por método criptográfico recomendado pelo DCT e com processo de autenticação baseado em certificação digital.

Art. 32. Qualquer ocorrência de tentativa ou violação de segurança ocorrida no **firewall** ou no sistema de detecção de intrusã imediatamente notificada à Seção de Tratamento de Incidentes de Redes, no CITEx ou CT/CTA correspondente à Região Militar a que a OM onde ocorreu o fato está vinculada.

Art. 33. O DCT manterá, por meio da página eletrônica do CITEx, informações sobre sugestões de configurações lógicas e físicas dos diversos tipos de **firewall** e sistemas de detecção de intrusão, assim como o nível de segurança que, em princípio, cada um proporciona.

Seção IV

Da Segurança Contra Códigos Maléficos

Art. 34. O uso de **software** em qualquer computador do Exército deve estar em conformidade com as suas licenças de uso.

Art. 35. Todo computador conectado à EBNet deve executar diariamente um **software**, preferencialmente homologado pelo DCT, para verificação de contaminação por vírus ou outro código maléfico.

Art. 36. A base de dados do **software** antivírus deve ser mantida atualizada de modo que sejam minimizadas as possibilidades de um código maléfico ser instalado e executado no computador que o antivírus protege.

Art. 37. Todos os computadores servidores devem estar protegidos por **softwares**, devidamente atualizados, de antivírus e demais códigos maliciosos. Particular atenção deve ser dada aos servidores de dados corporativos e os de correio eletrônico.

Art. 38. Os **softwares** antivírus e códigos maléficos devem ser adquiridos mediante a garantia de atualização contínua da base de dados sobre vírus de computador, assim como de outros códigos maliciosos.

Art. 39. As aplicações de proteção contra códigos maléficos antivírus deverão estar configuradas de tal modo a registrar, por meio da função de **log,** qualquer ocorrência desses códigos.

Parágrafo único. Os relatórios fornecidos pela própria aplicação deverão ser remetidos ao CITEx para fins de análise. A periodicidade desse envio será estabelecida conforme a capacidade de acompanhamento do CITEx e será notificada na página eletrônica do CITEx.

Art. 40. O uso de **softwares** contra códigos maléficos deve ser regido por regras de segurança, as quais devem figurar nas normas de segurança da rede do OM, cujo modelo encontra-se no ANEXO A.

Parágrafo único. As regras relativas à proteção contra códigos maléficos variarão conforme a realidade tecnológica corrente, assim como do tipo de demanda de proteção que o ambiente exigir, no entanto, devem-se adotar as seguintes regras como ponto de partida para um conjunto de regras a ser aplicado a ambientes específicos:

I - quaisquer arquivos ou macros anexados a uma mensagem eletrônica proveniente de uma fonte desconhecida, suspeita ou não confiável nunca devem ser abertos e sim totalmente apagados;

II - arquivos ou macros anexados a uma mensagem eletrônica proveniente de fonte conhecida só devem ser abertos após a verificação de sua integridade;

III - mensagens de **spam**, cadeias e outras mensagens coletivas devem ser excluídas sem realizar o encaminhamento (**forwarding**);

IV - arquivos de fontes desconhecidas ou suspeitas nunca devem ser transferidos para o computador por qualquer que seja o serviço de acesso a esses arquivos (WWW, FTP, chat etc);

V - o compartilhamento do disco da máquina local com acesso de leitura e escrita deve ser evitado, a menos que haja a necessidade absoluta do serviço para fazê-lo e, neste caso, a permissão de acesso deve ser concedida apenas àqueles que necessitam da informação e deve ser mantida apenas pelo tempo necessário para que o dado seja acessado;

VI - antes da utilização de informações em mídias removíveis, tais como disquetes, CD, **flash cards, pendrives,** discos **zip** etc, sempre se deve realizar verificação da integridade dos arquivos para se ter certeza de que não estão contaminados por vírus ou outro código maléfico.

VII - caso haja necessidade de temporariamente desativar o **software** de proteção para fins de testes, manutenções especiais, incompatibilidades específicas ou outra razão inevitável, é necessário adotar o seguinte procedimento:

a) deve-se executar o **software** de proteção para assegurar que o computador esteja isento de vírus ou outros tipos de infecções;

b) desabilitar o **software** de proteção;

c) realizar apenas o procedimento que se fez necessário e nunca acionar outros serviços notoriamente conhecidos pela sua capacidade de propagação de códigos maléficos, tais como o correio eletrônico.

VIII - o computador para o qual seja constatada a contaminação de um ou mais de seus arquivos por vírus ou outro código maléfico deverá ser imediatamente desconectado da rede até a remoção do código;

IX - a utilização de **softwares** aplicativos, utilitários ou sistemas operacionais só poderá ser realizada com o conhecimento do

responsável pela gerência da rede e se o **software** for de origem conhecida e legal.

Seção V
Dos Mecanismos de Autenticação e Controle de Acesso

Art. 41. O acesso aos dados e serviços corporativos de rede no Exército, seja em conexões locais ou remotas, só pode ser concedido mediante a verificação da autenticidade da identificação do usuário por meio de técnicas de autenticação de rede.

Art. 42. Dentre as regras de segurança que compõem a norma de segurança de rede, cujo modelo encontra-se no ANEXO A, deverão estar incluídas regras sobre as formas de autenticação e de controle de acesso peculiares à rede para qual a norma será elaborada.

§ 1º Dentre os aspectos básicos de autenticação a serem considerados para constar da norma de segurança da rede devem figurar regras sobre:

I - política de senha (regras que definem os caracteres utilizáveis, tamanho, tempo de validade, número de tentativas de conexão, senhas "fracas" a serem evitadas, periodicidade admissível para troca, características de salvaguarda e procedimentos em caso de violação);

II - conexão (**logon**) à rede;

III - conexão (**logon**) a serviços locais ou remotos específicos;

IV - uso para certificados digitais;

V - assinatura digital;

VI - uso de **smart cards** e **tokens**;

VII - uso de mecanismos biométricos;

VIII - demais mecanismos de autenticação não especificados.

§ 2º Dentre os aspectos básicos de controle de acesso a serem considerados para constar da norma de segurança da rede devem figurar regras sobre:

I - privilégios de grupos de usuários ou usuários individuais;

II - definição de privilégio, se for o caso, que pode ser concedido a elementos externos, tais como serviços terceirizados ou de manutenção;

III - definição de privilégios especiais para usuários internos, tais como o gerente da rede ou o pessoal que realiza a manutenção dos equipamentos;

IV - retirada de privilégio para pessoal desligado ou transferido;

V - uso de termo de compromisso e manutenção de sigilo.

Art. 43. O controle de acesso aos equipamentos de interconexão (roteadores**, switches**, **hubs** e demais equipamentos de interligação de computadores) deve ser disciplinado por regras contidas na norma de segurança da rede e deve contemplar os seguintes aspectos:

I - identificação e autenticação de acesso;

II - configurações para roteamentos específicos, segmentação física e lógica devido a requisitos de segurança do ambiente (pode implicar em classificação da norma);

III - desconexão por inatividade;

IV - condições para configuração remota.

Art. 44. Os serviços de certificação digital usados nas redes do Exército devem estar de acordo com as orientações e regras vigentes da Infra-Estrutura de Chaves Públicas do Brasil (ICP-Brasil).

Art. 45. Nas redes em que for utilizada certificação digital, a salvaguarda do certificado é de responsabilidade única e exclusiva do seu possuidor.

Art. 46. O serviço de assinatura digital deve ser implementado por meio do uso de certificados digitais.

Art. 47. É recomendável que os computadores servidores que armazenem dados corporativos, provejam serviços de sistemas corporativos ou, ainda, provejam serviços de segurança tais como **firewall** e sistema de detecção de intrusão, devem contar com mecanismos fortes de autenticação, associados às tradicionais técnicas baseadas em senha, para identificar aqueles que acessem esses recursos.

Parágrafo único. Os mecanismos fortes devem estar baseados em técnicas de autenticação reconhecidamente robustas tais como: certificação digital, reconhecimento biométrico, utilização de **smartcards** ou dispositivos similares (**tokens**) ou combinação dessas técnicas.

Seção VI
Da Monitoração e Registro dos Eventos

Art. 48. As normas de segurança da informação internas às OM devem conter regras relativas ao modo de monitoração e registro de eventos de rede considerados críticos.

Art. 49. Todos os computadores servidores e equipamentos de rede que contenham dados ou executem serviços identificados pela análise de risco como sendo elementos que necessitem proteção específica devem manter o seu serviço de registro (**logs**) de eventos ativado.

Parágrafo único. Considerando o fato de que, em geral, ativar o serviço de registro de eventos em sua plenitude pode incorrer no armazenamento de dados desnecessários, deve-se, a princípio, configurar a monitoração apenas dos eventos considerados essenciais e, à medida que a experiência e a necessidade demonstrarem, outros eventos deverão ser acompanhados.

Art. 50. A conclusão de que eventos devam ser registrados devem resultar, preferencialmente, de análises de risco. Como eventos relevantes a serem considerados, sugere-se a seguinte lista:

I - identificação dos usuários;

II - data e hora de entrada e saída no sistema;

III - número de tentativas de conexão;

IV - origem ou localização do equipamento está requisitando a conexão;

V - concessões e cancelamentos de privilégios de usuários;

VI - concessões e cancelamentos de conta e senha para acesso à rede local;

VII - concessões e cancelamentos de acesso às redes externas via rede local;

VIII - endereços externos acessados por meio da rede local;

IX - acessos aos servidores;

X - desconexão ou conexão de estações e servidores;

XI - modificações nas configurações das barreiras de proteção externa (**firewall**) e de cada computador (**firewall** de estação ou de servidor);

XII - modificações na configuração de sistemas de detecção de intrusão ou de prevensão de intrusão (**intrusion detection systems** - IDS / **intrusion prevention systems –** IPS / **host intrusion detection systems** - HIDS);

XIII - modificações nas configurações de roteadores, switches ou outros equipamentos de redes passíveis de serem configurados remotamente;

XIV - acesso a informações sobre o volume de tráfego de informações que circulam internamente na rede local; e

XV - acesso a informações sobre o volume de tráfego de informações que são trocadas com redes externas.

Art. 51. Os computadores de uma rede devem ter seus relógios sincronizados para que os registros de eventos mantenham sua credibilidade, logo, as estações devem ser sincronizadas com o servidor da rede, que, por sua vez, deve estar ajustado com um padrão local de tempo.

Art. 52. Os registros de eventos devem ser periodicamente auditados para fins de verificação do correto funcionamento do equipamento ou **software**.

Parágrafo único. O período de auditagem deve ser estipulado conforme a categoria da rede e critérios adicionais de cada OM.

Art. 53. Os arquivos contendo a informação sobre os eventos devem ser periodicamente gravados sobre algum tipo de suporte de **backup** e armazenados de acordo com as normas para salvaguarda de documentação sigilosa previstas na legislação.

Seção VII

Das Cópias de Segurança (Backup)

Art. 54. Toda rede do Exército deve normatizar e aplicar procedimentos para execução periódica de cópias de segurança para salvaguardar os dados da Unidade, assim como viabilizar a recuperação desses dados em situações de violação dos originais.

Art. 55. As cópias de segurança devem ser armazenadas em locais fisicamente distantes de onde foram gerados de modo a não haver a possibilidade de que danos à instalação principal possa destruir os dados e suas cópias. Entenda-se por "distante" uma instalação física que, no mínimo, esteja em uma edificação diferente de onde estão os arquivos originais.

Art. 56. As condições ambientais de armazenamento, assim como a periodicidade de renovação e descarte das mídias, devem obedecer às recomendações do fabricante do material, de modo a minimizar o risco da perda dos dados da cópia de segurança por deterioração da mídia utilizada.

Art. 57. As cópias de segurança devem ser preservadas por mais de uma geração, sendo o número mínimo de duas versões.

Art. 58. A recuperação dos dados deve ser testada periodicamente para que se tenha a certeza da sua disponibilidade e integridade.

Art. 59. As normas de segurança de rede de cada OM devem conter regras que disciplinem os procedimentos de produção, armazenamento, preservação, teste, atualização e descarte das cópias de segurança.

Art. 60. Além das regras relativas aos procedimentos de gerenciamento das cópias de segurança, devem ser elaboradas duas outras documentações: procedimentos operacionais padrão (POP) relativos aos procedimentos de **backup** e relatórios que informem os eventos associados a cada procedimento do processo (data-hora, arquivos copiados, operador, tipo de cópia realizada etc).

Seção VIII

Das Comunicações e da Telefonia

Art. 61. Dentre as regras de segurança que compõem a norma de segurança de rede, cujo modelo encontra-se no ANEXO A, deverão estar incluídas regras sobre a utilização das redes de comunicação e de telefonia, levando-se em consideração, os aspectos das instalações físicas onde se encontram, a manutenção dos equipamentos, os protocolos e serviços utilizados e prerrogativas de uso e manutenção.

Art. 62. Os procedimentos de segurança nas comunicações rádio deverão estar de acordo com a doutrina de segurança das comunicações vigentes no Exército.

Subseção IX

Das Redes Rádio

Art. 63. Em aplicações de operação real, as operações rádio, seja da rede estratégica ou de uma rede tática, deverão realizar as comunicações de forma controlada pelos instrumentos normativos adequados como as Instruções Padrão de Comunicações (IPCOM) e as Instruções de Emprego das Comunicações (IECom).

Art. 64. Nos processos de aquisição de material de comunicações para as redes rádio do Exército, deve-se buscar as implementações com possibilidade de uso de criptografia aprovada pelo Exército, em particular aquelas de desenvolvimento próprio, sendo que, na impossibilidade, deve-se buscar produtos para os quais seja viável realizar as adaptações de **hardware** e **software** necessárias desde que tais adaptações não comprometam a funcionalidade do produto.

Art. 65. Nos casos em não seja possível utilizar soluções de criptografia aprovadas no Exército nos rádios já em emprego, deve-se realizar análises de risco para avaliar que tipo de configurações são admissíveis e em que tipo de operação pode ser empregado, sendo que o resultado dessas análises deve ser refletidos nas normas que disciplinem o uso dos rádios envolvidos.

Subseção X

Das Redes de Telefonia

Art. 66. As comunicações telefônicas que necessitem ser tratadas com preservação de sigilo do seu teor (telefone seguro) devem ser efetuadas apenas pelo equipamentos destinados para este fim e obedecendo-se as orientações da seção de inteligência da OM previstas pela para seu uso e manutenção.

Art. 67. A infra-estrutura de cabeamento telefônico seja para transmissão de dados ou uso de voz deve estar instalada de acordo com as normas sobre cabeamento estruturado utilizadas em projetos de obras militares executadas ou fiscalizadas pelas Comissões Regionais de Obras, assim como a documentação técnica, incluindo as plantas das instalações devem estar atualizadas e disponíveis para consulta do pessoal credenciado.

Subseção XI

Das Redes Sem Fio

Art. 68. As redes sem fio são categorizadas conforme a abrangência da área de cobertura, cada qual com requisitos de segurança próprios, desta forma todas as soluções a serem adotadas para uso na Força devem ser previamente preparadas de tal modo que as configurações de segurança sejam adequadamente ajustadas, em particular, os aspectos de identificação e autenticação do usuário e da criptografia dos dados.

Art. 69. As OM usuárias de redes sem fio, ainda que em termos experimentais, devem averiguar quais dados estão acessíveis pela rede e adequar as configurações segurança dos dispositivos, conforme as funcionalidades que o equipamento e o padrão de rede sem fio implementado, uma vez que é possível que elementos estranhos ao serviço monitorem e até acessem os dados dos equipamentos da rede a partir de pontos localizados de algumas dezenas até algumas centenas de metros, dependendo do padrão de rede utilizado.

Art. 70. Nos dispositivos baseados no padrão IEEE 802.15 ou equivalente devem ser utilizados apenas no manuseio de dados de natureza ostensiva, ainda assim, para garantia de condições mínimas de integridade da informação e autenticidade de usuário, os devidos ajustes das configurações dos parâmetros criptográficos, tais como extensão da chave, o algoritmo escolhido, identificadores não óbvios e o tempo de uso, devem ser previamente ajustados.

Art. 71. Nos dispositivos baseados no padrão IEEE 802.11 ou equivalentes, os de tipos vulnerabilidades são semelhantes ao padrão IEEE 802.15, ou seja, as maiores preocupações estão voltadas para o problema da autenticação e do sigilo, assim, tanto nas normas da rede quanto nas implementações propriamente ditas, deve-se atentar para os seguintes aspectos:

I - habilitação do protocolo de segurança e efetuar a mudança de seus parâmetros com freqüência;

II - efetuar freqüentemente a mudança dos parâmetros de identificação da rede para fins de autenticaç;ão de usuário;

III - evitar o uso da rede no padrão de autenticação aberta;

IV - desabilitar **broadcasting** de parâmetros de autenticação;

V - modificar a senha padrão do administrador;

VI - não permitir pontos de acesso à rede indiscriminadamente e sim com rígido controle;

VII - não fazer uso de conexões de equipamentos ligados à redes sem fio a redes corporativas;

VIII - fazer uso, caso a funcionalidade esteja disponível, filtragem baseada em endereços físicos;

IX - desligar pontos de acesso em horários fora do expediente;

X - realizar auditorias e análises de risco com freqüência nas redes sem fio;

XI - explorar as funcionalidades de segurança adicionais que existam no produto, em especial às relacionadas aos padrões de segurança IEEE 802.11i IEEE 802.11x, respeitados os demais requisitos do sistema;

XII - realização de testes de “vazamento” de sinal.

Seção IX

Da Infra-estrutura de Alimentação Elétrica

Art. 72. O sistema de alimentação elétrica que as redes das OM fazem uso devem estar de acordo com as recomendações e normas utilizados no Exército pelas Comissões Regionais de Obras (CRO).

Art. 73. Os computadores servidores que armazenem dados corporativos, provejam serviços de sistemas corporativos e para os quais seja considerada crítica a sua indisponibilidade devem contar com proteção para interrupção de fornecimento de alimentação elétrica (**nobreak**).

Art. 74. Os computadores nos quais estejam instalados os **softwares** que implementam serviços de segurança para a rede, tais como **firewall** e sistema de detecção de intrusão devem contar com proteção para interrupção de fornecimento de alimentação elétrica (**nobreak**).

Art. 75. Na norma de segurança de redes de uma OM deverão constar procedimentos periódicos de verificação das:

I - condições de estabilidade;

II - identificação de pontos de alimentação;

III - quadro de distribuição;

IV - aterramento;

V - estado das baterias dos sistemas para proteção contra interrupção de energia (**nobreak**);

VI - estado dos estabilizadores de energia, assim como outros equipamentos existentes na rede e com função no sistema de alimentação elétrica.

Seção X

Da Configuração da Rede

Art. 76. Os ambientes de redes do Exército devem fazer uso de produtos tecnológicos, técnicas de gerência e metodologias de segurança de forma combinada para assegurar a proteção dos dados armazenados, em trânsito ou em processamento na rede.

Art. 77. A combinação dos elementos de segurança para proteção das redes é específica para cada caso, porém como requisitos básicos, tanto para as redes de computadores quanto as redes de comunicações e telefonia, seguintes recomendações devem ser adotadas:

a) adoção das regras de segurança dispostas nestas Instruções que sejam compatíveis com o ambiente da rede da OM;

b) adoção das soluções de segurança conforme os requisitos de segurança do ambiente da rede da OM;

c) documentação descritiva da rede contendo como informações básicas: o mapa lógico e físico da rede (indicação de tipos de equipamento e segmentações); o inventário da rede (**hardware** e **software**);

d) definir a estrutura de gestão da segurança tomando por base os seguintes elementos:

- normas de segurança que definam as regras de segurança gerais;

- o processo de gerenciamento de riscos (que pode ser a aplicação das normas vigentes no Exército sobre esse tema ou uma personalização delas para o ambiente da rede e, além disso, deve ser definido em documento, podendo estar no corpo da norma ou em documento separado);

- a estruturação lógica e física dos equipamentos e **softwares** de segurança ou que possuam funcionalidades de segurança (pode requerer um documento com classificação sigilosa) e respectivas regras de segurança e POP - procedimentos operacionais padrão - para manter, adequar, monitorar e aplicar contingência a essa estrutura;

- o plano de contingência da rede;

- documentação da segurança orgânica da OM.

e) POP sobre os processos de monitoração das falhas, da performance, da configuração, da segurança e, se for o caso, da contabilização (taxação do uso de recursos da rede);

f) histórico das violações de segurança da rede (documento de classificação sigilosa).

CAPÍTULO IV

DOS SERVIÇOS, SISTEMAS OPERACIONAIS E APLICATIVOS DE REDE

Seção I

Dos Serviços de Rede

Art. 78. Os serviços de rede oferecidos nas redes locais ou na rede corporativa do Exército devem ser regulados por normas específicas ou em capítulos próprios de normas elaboradas para cada ambiente de rede em particular. As regras de segurança básicas para os esses serviços devem considerar, no mínimo, os seguintes aspectos:

I - configuração do serviço;

II - controle de acesso para administração do serviço;

III - entrada no sistema (**log on)**;

IV - configuração do servidor onde o serviço está instalado;

V - configuração do sistema operacional sobre o qual o serviço está instalado;

VI - procedimentos preventivos contra ameaças advindas de vírus de computador e demais códigos maliciosos;

VII - procedimentos em caso de detecção de violação da segurança do serviço

VIII - procedimentos em caso de corrompimento ou interrupção do funcionamento de um serviço de rede em função de uma violação de segurança;

IX - procedimentos para **backup** de informações do serviço;

X - procedimentos para **backup** dos **log** de eventos;

XI - detecção de violações no serviço;

XII - detecção da ação de códigos maléficos;

XIII - integridade dos dados gerados, processados ou enviados;

XIV - procedimentos de atualização e correção do serviço para fins de segurança.

Parágrafo único. Nas situações em que a descrição das configurações do serviço ou das demais características listadas neste artigo contenham informações cuja exposição possa comprometer a segurança da rede, a norma de verá ser convertida em um documento classificado.

Art. 79. Os serviços de rede cujos dados processados contenham informações cujo teor seja considerado "sensível" devem ser executados em segmentos isolados da rede, sendo que o isolamento pode ser físico ou lógico conforme o grau do risco envolvido. Considere-se informação sensível aquela que, ainda que não seja classificada, não convém que trafegue na mesma rede juntamente com dados administrativos.

Art. 80. O planejamento de serviços ou sistemas corporativos para uso em redes deve prever, dentre os requisitos do sistema, a inclusão de controles que permitam testes de auditoria para verificação da efetividade das funcionalidades do serviço ou sistema, assim como o registro de eventos ocorridos.

Seção II

Dos Sistemas Operacionais de Rede

Art. 81. Os sistemas operacionais de rede devem ser instalados, configurados e administrados de modo a permitir apenas os privilégios

mínimos necessários para atender aos requisitos da rede.

Art. 82. Os sistemas operacionais de rede devem funcionar de forma atualizada, com as últimas correções de segurança fornecidas pelo seu fabricante. O DCT, por meio de publicação em página eletrônica do Centro Integrado de Telemática do Exército, disponibilizará informações sobre as atualizações necessárias.

Art. 83. As regras administrativas relativas aos sistemas operacionais de rede em uso no Exército devem considerar os seguintes aspectos:

I - identificação de usuário e autenticação desta identificação;

II - controle de acesso;

III - compartimentalização de privilégios de controle de acesso para administração do sistema;

IV - proteção contra reuso de objetos relacionados à segurança, tais como senhas, informações de histórico de operações de configuração etc.

V - contabilização do uso dos recursos do sistema;

VI - armazenamento de informações de histórico sobre os eventos ocorridos no sistema;

VII - comunicação remota (para fins de administração) segura (conexão e enlace);

VIII - detecção de intrusão

IX - registro de eventos do sistema.

Seção III
Dos Aplicativos de Rede

Art. 84. Aplicativos de rede que contenham funcionalidades de segurança devem fazer uso dessas funcionalidades, exceto nos casos em outras proteções específicas de segurança sejam utilizadas e tornem desnecessárias ou contraproducentes as medidas adicionais do aplicativo.

§ 1º Este artigo trata de funcionalidades de segurança do aplicativo e não de correções de segurança necessárias disponibilizadas pelo fabricante. Essas correções são de instalação e ativação obrigatórias.

§ 2º Nos casos em que a funcionalidade de segurança do aplicativo seja redundante em relação a outras proteções da rede, cabe ao gerente da rede a decisão sobre a necessidade ou não da ativar a funcionalidade.

§ 3º Nos casos em que a funcionalidade de segurança do aplicativo complemente a proteção existente na rede ou seja a única proteção contra riscos à informação, sua ativação é obrigatória e deve ser documentada nas normas de segurança da rede.

Seção IV
Dos Bancos de Dados

Art. 85. Os dados corporativos armazenados em bando de dados devem contar com ferramentas de segurança, sejam inerentes ao produto que implementa o banco ou implementadas por produtos de segurança externos ao banco, que garantam a integridade, a disponibilidade e, se for o caso, a confidencialidade dos dados, assim como controlem as formas de autenticação e os privilégios de acesso de quem acesse o banco.

Art. 86. Os serviços essenciais de segurança dos bancos de dados corporativos devem:

I - ser ativados de modo compatível com os riscos envolvidos;

II - estarem disciplinados em regras de segurança da norma interna de rede;

III - ter o acesso aos dados viabilizado sempre por alguma técnica de autenticação adequada;

IV - ter o controle de acesso ativado e configurado de tal modo a propiciar apenas os privilégios de acesso necessários para realização das operações de cada tipo de usuário;

V - ter os registros de eventos (**log** de eventos) ativados e configurados de tal modo a registrar as ocorrências definidas como essenciais nas regras de segurança da norma interna da OM;

VI - garantir a disponibilidade dos dados tanto em relação ao acesso via rede ou por meio da recuperação de cópias de segurança para os usuários com privilégio de acesso;

VII - garantir da integridade de dados pelo uso das funcionalidades de detecção e correção de erros;

VIII - realizar cópias de segurança (**backup**) periódicas;

IX - armazenar dados sigilosos cuja classificação o permita na forma criptografada;

X - ativar e configurar de modo compatível com a norma de segurança da rede as funcionalidades de gerência, se ferramenta oferecer esse recurso.

CAPÍTULO V
DAS INSTALAÇÕES FÍSICAS

Art. 87. A segurança das instalações onde se encontram os equipamentos e as mídias de transmissão dos dados da rede deve estar

disciplinada por regras que, preferencialmente, estarão definidas na documentação da segurança orgânica da OM, podendo, dependendo das particularidades do ambiente físico da rede, constar da norma de segurança de redes.

Art. 88. O acesso físico aos equipamentos onde serviços de segurança da informação ou outros serviços considerados críticos estejam instalados deve ser restrito ao mínimo necessário de usuários autorizados.

Art. 89. Os pontos de rede disponíveis nas áreas da OM devem ser ativados apenas conforme a necessidade para prevenir tentativas de conexões não autorizadas de computadores portáteis.

Art. 90. O acesso físico, de pessoal que não seja usuário de recursos críticos da rede, às dependências onde esses recursos estão instalados deve ser controlado.

CAPÍTULO VI
DAS CONTINGÊNCIAS

Art. 91. As redes do Exército devem contar com planos de contingência especificamente elaborados para seus ambientes de modo que esteja previsto como se deve agir em situações de perda de um ou mais dos atributos de segurança da informação, quais sejam, integridade, disponibilidade ou confidencialidade.

Parágrafo único. A perda de integridade, disponibilidade ou confidencialidade da informação em uma rede, dentre outras diversas possibilidades, ocorre quando:

I - são efetivados ataques diretos aos dados em trânsito, armazenados ou em processamento na rede;

II - são efetivados ataques diretos aos recursos de **hardware**, **software**, infra-estruturas lógica e elétrica por meio dos quais os dados da rede são processados;

III - situações imprevistas, resultantes de imperfeições nos processos pelos quais as informações críticas passam, seja através do **hardware**, do **software**, da infra-estrutura lógica e da alimentação elétrica;P>

IV - acidentes advindos por imperícia, imprudência, negligência ou, ainda, por má fé quem opera um recurso de **software** ou **hardware** pelo qual dados críticos passam;

V - acidentes advindos de catástrofes naturais.

Art. 92. O Plano de Contingência da rede deve seguir o modelo descrito no ANEXO E.

Art. 93. Dependendo da sua complexidade, o Plano de Contingência da rede pode compor uma parte da norma de segurança ou uma documentação à parte.

Art. 94. A execução do plano de contingência da rede deve ser testada periodicamente para que seja verificada a sua efetividade.

Art. 95. O período de que trata este artigo deve ser atribuído de acordo com as características de cada OM e sua estipulação está a cargo do Comandante, mediante proposta a ser apresentada pelo responsável pela segurança da informação na OM.

Art. 96. O processo para elaboração, manutenção e atualização do Plano de Contingência é o seguinte:

I - identificação dos processos administrativos críticos para a missão da OM e que dependam em algum grau de ferramentas de tecnologia da informação;

II - identificação de recursos e serviços críticos que implementam a parte tecnológica dos processos administrativos que se refere o item anterior; como exemplos de recursos e serviços se tem:

a) computadores;

b) **softwares**;

c) equipamentos de rede;

d) componentes da infra-estrutura de alimentação elétrica;

e) componentes da infra-estrutura de cabeamento lógico;

f) equipamentos de comunicações;

g) pessoal.

h) serviços de rede;

i) sistemas corporativos.

III - análise de riscos sobre os recursos e serviços identificados no item anterior para que se tenha uma medida da sua importância, seu grau de vulnerabilidade, as chances de violação e o impacto gerado por essa violação;

IV - identificação dos serviços e recursos que necessitam de contingências para garantir a continuidade dos processos críticos para a OM;

V - identificação das ações necessárias para implementar a contingência do serviço conforme o tipo de categoria de violação da informação que é processada no recursos ou pelo serviço (categoria de violação: violação da confidencialidade, violação da integridade, violação da disponibilidade)

VI - identificação dos recursos necessários para implementar as ações identificadas;

VII - identificação do pessoal, conforme as competências necessárias e disponíveis para implementar as ações;

VIII - estabelecimentos dos processos para lidar com cada tipo de categoria de violação;

IX - redação do plano de contingência conforme modelo do ANEXO E;

X - teste da efetividade do plano;

XI - aprovação por meio de publicação em BI;

XII - simulação periódica do plano para aferir sua efetividade e o adestramento do pessoal;

XIII - elaboração de relatório sobre os fatos observados nos testes;

XIV - revisão e atualização do plano conforme a demanda identificada nos relatórios.

Parágrafo único. O mesmo tratamento deverá ser aplicado aos arquivos eletrônicos que originaram a documentação em pauta.

Art. 98. O Comandante, Chefe ou Diretor deverá designar, por publicação em boletim interno, militares da OM para aturem como “pontos de contato” nas situações de acionamento de contingências.

Art. 99. Os pontos de contato deverão ser de tantos tipos quanto forem necessários ao tratamento das possíveis situações de contingências devendo haver, pelo menos, dois tipos:

I - gerência da rede da OM: responsável(is) pelas primeiras medidas para lidar com os problemas de segurança ocorridos na rede de comunicações ou de computadores e que tenham reflexos no contexto da própria rede;

II - operação técnica: responsável(is) pelas primeiras medidas para lidar com os problemas de segurança ocorridos em recursos específicos da rede nos quais é especialista.

Art. 100. Em casos em que as características das áreas e instalações, além das condições ambientais, forem tais que existam riscos para a rede da OM, a elaboração do plano de contingência deve levar em consideração situações de desastre, tais como:

a) incêndios na sala de servidores ou equipamentos críticos;

0.1cm; line-height: 120%; orphans: 2"> b) inundação;

c) infiltrações;

d) desabamento;

e) explosões.

Art. 101. O Plano de Contingência deve ser testado periodicamente, em períodos não superiores a seis meses. As técnicas empregadas podem variar conforme as peculiaridades da rede e seus serviços, sendo consideradas como básicas as seguintes:

I - testes de recuperação das cópias de segurança (**backup**);

II - testes de reativação de serviços críticos (ativação de uma instalação alternativa em outro servidor ou reinstalação e reconfiguração do serviço);

III - teste da atualização dos contatos com as pessoas envolvidas;

IV - teste da destreza e eficácia das tarefas desempenhadas pelos diversos grupos.

CAPÍTULO VIII
DA VERIFICAÇÃO DA EFETIVIDADE

Art. 102. As normas de segurança de rede devem conter regras relativas aos controles necessários para verificar a efetividade das medidas de segurança implementadas para proteger a rede e os dados nela processados.

Art. 103. Os controles básicos para verificação da efetividade são:

I - legislação vigente;

II - as normas de segurança da rede;

III - a documentação da segurança orgânica da OM;

IV - outras normas de segurança que tenham aplicação no ambiente de rede;

V - configurações de segurança de **hardware** e **software**, tanto dos sistemas que tenha funcionalidades de segurança, quanto dos sistemas específicos de segurança.

Art. 104. A verificação da efetividade é um processo que pode ter caráter preventivo ou de investigação de acordo com a necessidade.

Art. 105. A verificação da efetividade com caráter de investigação busca esclarecer as razões de uma violação de segurança e a auditoria de caráter preventivo verifica a conformidade e efetividade das ações de segurança.

Art. 106. A técnica básica a ser empregada para a verificação é a das "listas de verificação", as quais podem ser obtidas por meio do acesso à página eletrônica do CITEx.

§ 1º A aplicação das listas de verificação deve obedecer ao modelo do ANEXO F.

§ 2º A aplicação de técnicas mais sofisticadas, em relação às listas de verificação, passíveis de serem utilizadas na rede serão usadas em auditorias externas realizadas por CT ou CTA, podendo ser usadas pelo pessoal interno, desde de que especializado na técnica e, se for o caso, na ferramenta que a implementa.

Art. 107. A verificação de efetividade deve ser um processo aplicado periodicamente no ambiente de rede da OM.

Parágrafo único. O período de verificação deve ser estipulado de acordo com as peculiaridades da rede, no entanto, esse período não deverá exceder a seis meses.

Art. 108. Ao término de qualquer processo de verificação de efetividade, deverá ser gerado um relatório conforme o modelo do ANEXO G.

Parágrafo único. Caso haja a constatação de violações de segurança, o relatório deverá receber classificação sigilosa e encaminhado ao CITEx para fins de registro de histórico sobre violações de segurança para a equipe de pronta resposta a incidentes do Exército.

Art. 109. O processo básico de verificação de efetividade deve seguintes etapas:

I - levantamento de informações sobre a caracterização da rede a ser verificada;

II - identificação dos pontos de controle específicos da rede (equipamentos e/ou serviços) sob auditoria;

III - escolha dos controles necessários;

IV - avaliação dos pontos de controle selecionados por meio da aplicação da técnica de listas de verificação (auditoria interna);

V - (se for o caso) avaliação dos pontos de controle selecionados por meio da aplicação de técnicas específicas selecionada pela equipe de auditoria (auditoria externa - CITEX/CTA/CT);.

VI - Preenchimento do relatório de auditoria conforme modelos constantes das normas de auditoria da segurança da informação vigentes no Exército;

VII - Encaminhamento do relatório para os responsáveis pela gerência da rede (nos casos de auditoria externa);

VIII - Encaminhamento do relatório para o CITEX para fins de estatística e aprimoramento das formas de respostas ao incidentes de segurança.

Art. 110. Todas as ações relativas à verificação de efetividade deverá estar em conformidade com as Instruções relativas à auditoria da segurança da informação.

CAPÍTULO IX
DO GERENCIAMENTO DA SEGURANÇA

Seção I
Do Processo de Gerenciamento

Art. 111. A gerência da segurança da rede deve atuar nas seguintes áreas:

I - DOCUMENTAÇÃO NORMATIVA DE SEGURANÇA DA INFORMAÇÃO - A documentação normativa de segurança da informação compreende todas publicações oficiais do Exército sobre o temas "segurança da informação", salvaguarda de assuntos sigilosos e contra-inteligência (Instruções Gerais, Reguladoras ou Provisórias, Manuais, Normas etc) passíveis de serem aplicadas no ambiente da rede;

II - GESTÃO DE RISCOS - A gestão de riscos é o processo que identifica que recurso informacional está sob risco, as chances do risco se concretizar, o impacto causado por essa concretização e as medidas de abrandamento do risco. Esse processo está definido em Instruções específicas do Exército e deve ser usado na gestão da rede para subsidiar a escolha, a aquisição, o uso, a configuração, a expansão, a atualização dos recursos da rede, além outras situações que causem impactos nesses recursos;

III - PRODUTOS TECNOLÓGICOS DE SEGURANÇA DA INFORMAÇÃO - Produtos tecnológicos de segurança da informação compreendem os equipamentos e soluções de **software** e de infra-estrutura física que compõem a proteção de segurança da rede;

IV - FUNCIONALIDADES DE SEGURANÇA DE UM PRODUTO OU SERVIÇO - Mecanismos de segurança presentes em produtos não destinados prioritariamente a prover segurança compreendem todas as funcionalidades de segurança passíveis de serem configuradas nesses produtos e que agregam proteção à informação;

V - MECANISMOS DE CONTINGÊNCIA E CONTINUIDADE DE SERVIÇOS - Mecanismos de contingência e continuidade de serviços são as normas, processos e medidas implementadas por meio do plano de contingência;

VI - AUDITORIA DE SEGURANÇA DA INFORMAÇÃO - Auditoria de segurança da informação é o processo de verificação da conformidade entre o que é estabelecido para a aplicar a segurança da informação e o que é implementado de fato. Esse processo está definido em Instruções específicas do Exército;

VII - RECURSOS HUMANOS - O aspecto relativo aos recursos humanos, no que diz respeito ao seu comportamento na operação do recursos de TI, enfoca o pessoal que: gerencia os processos de segurança, opera os produtos de segurança e o usuário final;

VIII - ÁREAS E INSTALAÇÕES ONDE OS RECURSOS DE INFORMAÇÃO ESTÃO - Áreas e instalações compreendem as áreas onde os recursos de informação a ser protegida estão, ou por onde passam ou são armazenados os dados e informações;

IX - PROCESSO DE GERENCIAMENTO DA SEGURANÇA DA INFORMAÇÃO - O processo de gerenciamento da segurança da informação de redes é mecanismo que define as ações de planejamento, monitoração e adequação das medidas de segurança da informação na rede;

X - TRATAMENTO DE INCIDENTES E PRESERVAÇÃO DE EVIDÊNCIAS - O tratamento de incidentes lida com a forma com a qual se deve reagir ou prevenir incidentes de segurança, enquanto a preservação de evidência está relacionada a salvaguarda de registros de eventos, assim como estados de configurações de serviços e equipamentos que tenham sido modificados de forma ilegítima e violando a segurança para fins de investigação e apuração de responsabilidades.

112. O processo básico de gerenciamento da segurança da informação em redes é o seguinte:

I - identificação dos processos administrativos da OM;

II - identificação dos serviços de rede que automatizam ou apóiam os processos administrativos da OM;

III - estabelecimento (estrutura de rede a ser implantada) ou reconhecimento (estrutura de rede já implantada) da finalidade da rede e seus objetivos específicos, ou seja, estabelecimento ou reconhecimento da finalidade e os objetivos do conjunto dos serviços de rede que automatizam ou apóiam os processos administrativos da OM;

IV - identificação dos requisitos que impõem como deve ser conduzido o processo de segurança na rede (processos administrativos que a segurança deve proteger, regras estabelecidas em normas de seguranca ou de contra-inteligência, requisitos de equipamentos ou **softwares**, normas técnicas, ordens do Comandante, obrigações contratuais, legislação do País, demandas do serviço ou do usuário etc);

V - implementação das regras existentes na documentação normativa nos serviços de rede;

VI - registros das regras que não puderam ser atendidas, os motivos da impossibilidade e a comunicação do fato ao Comandante, em documento que indique linhas de ação para adequação da situação;

VII - análise de riscos do ambiente da rede, de acordo com a metodologia definida nas Instruções específicas sobre riscos;

VIII - implementação das medidas de abrandamento do risco resultantes da análise de risco;

IX - monitoração contínua dos resultados das medidas de segurança para aferição da sua efetividade, sendo que, periodicamente, devem-se realizar processos de auditoria para averiguar mais precisamente as condições de segurança;

X - adequação das medidas de segurança como resultado da monitoração, da auditoria, das inovações tecnológicas, das novas orientações normativas etc, para manter o risco de violação da segurança em patamares aceitáveis.

Parágrafo único. O processo de que trata este artigo está representado na figura 2.

Seção II

Das Ações Administrativas

Art. 113. As ações administrativas do gerenciamento da segurança da informação abrangem os aspectos não eminentemente de tecnologia da informação, mas que são relevantes para a manutenção das ações de segurança. Estão entre essas ações, as seguintes:

I - trâmite de documentação contendo informação que necessita de proteção;

II - cumprimento de contratos de fornecimento, suporte ou outros serviços pós-venda;

III - gestão de licenças de uso de **software**;

IV - especificação de material, equipamentos e **softwares** para aquisição em processos licitatórios;

V - recebimento de material, equipamentos e **softwares** de segurança adquiridos;

VI - manutenção de equipamentos que contenham dados sensíveis;

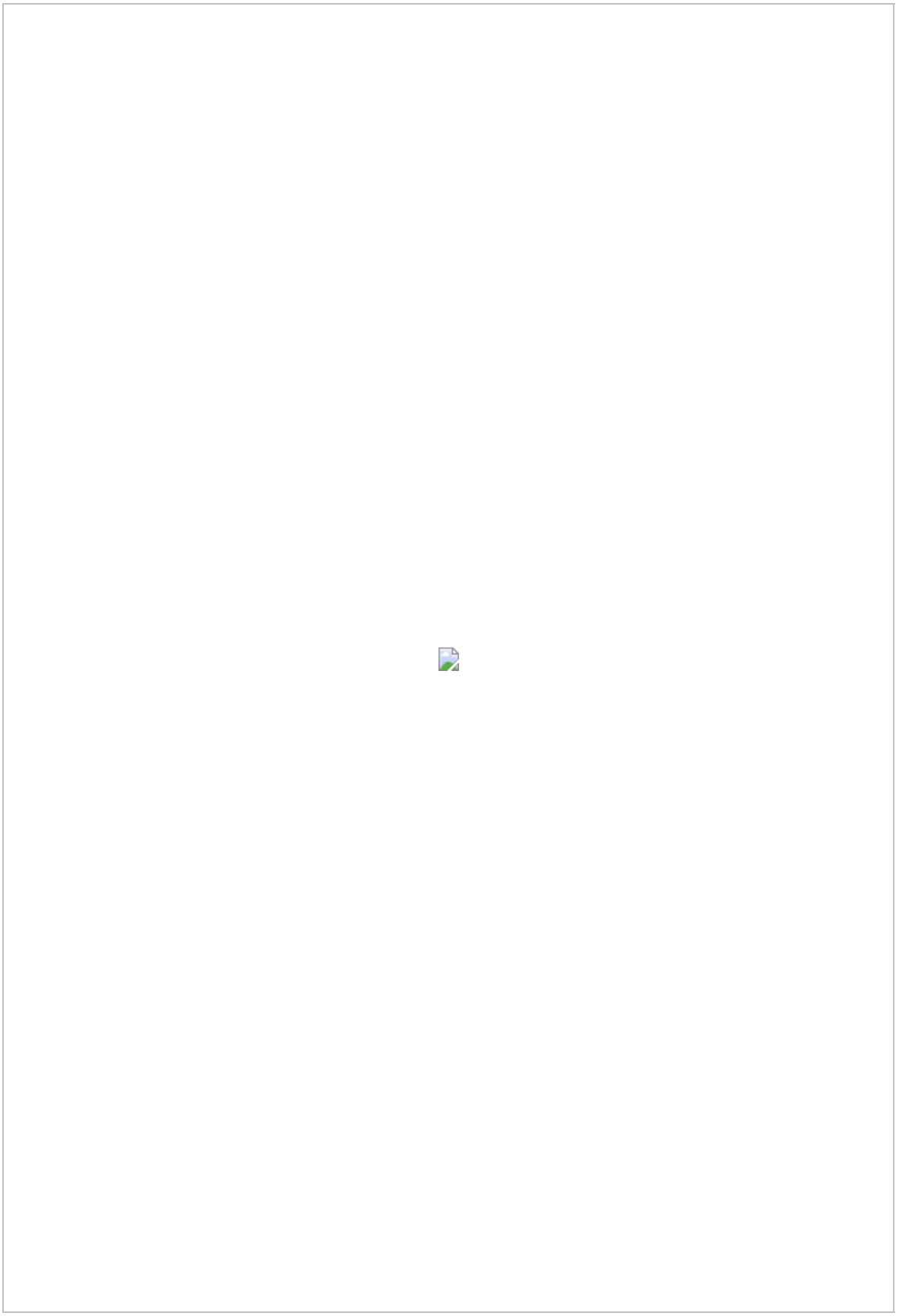
VII - seleção, treinamento e conscientização de pessoal para atuar com equipamentos, **softwares** ou diretamente com dados que necessitam de segurança;

VIII - obtenção de informações sobre boas práticas, alertas e estado da arte sobre segurança da informação.

Art. 114. O cumprimento de contratos, quando atingem a segurança da informação, devem ser acompanhados pela responsável pela segurança da informação da OM, que deverá manter o Comandante informado sobre o cumprimento ou não das cláusulas contratuais que atinjam a segurança.

Art. 115. A manutenção, realizada em instalações externas à OM, de equipamentos onde estão instalados serviços utilizados para segurança da rede deve ser precedida pela realização de cópias de segurança (**backup**) dos arquivos que contenham registros de eventos e outros dados sensíveis e, a seguir, os arquivos originais devem ser destruídos por meio de sucessivos processos de sobrescrita e apagamento.

orphans: 2"> Parágrafo único. Caso não seja possível realizar a operação de destruição dos dados de que trata este artigo, caberá ao Comandante, assessorado pelo seu corpo técnico, decidir se o equipamento ou parte dele poderá sofrer a manutenção fora da OM.



margin-top: 0.2cm; margin-bottom: 0cm">Fig nº 2: Processo de gestão de segurança de rede.

Art. 116. Toda violação da segurança da informação na rede da OM que comprometa a sua missão deverá ser notificado ao Comandante da OM que deverá julgar se é ou não matéria sigilosa.

§ 1º Violações de segurança da informação devem ser notificadas mensalmente ao CITEx para fins de análise e adequação de medidas de defesa contra o tipo de violações ocorrida, estatística e aprimoramento da doutrina de segurança da informação. A notificação deve ser feita pelo contato disponível na página eletrônica daquele Centro.

§ 2º Violações consideradas graves, tais como vírus de computador que causem perda de dados, invasões feitas por **hackers**, sabotagem do sistema de informação da OM, fraudes etc, devem ser imediatamente notificadas ao CITEx para fins de resposta ao incidente de segurança surgido.

§ 3º Dependendo das possíveis repercursões da violação, a comunicação deve ser feita por meio de documento com classificação

sigilosa.

Art. 117. As OM que não possuam, no seu efetivo, militares com a capacitação técnica para elaborar as normas de segurança da informação devem solicitar apoio aos CT ou CTA correspondentes a Região Militar a que pertencem.

Art. 118. As violações de segurança que atinjam quaisquer das redes internas da Força e com reflexos fora do contexto do Exército só poderão ser comentadas para o público externo e imprensa pelo CComSEx ou conforme critério estabelecido pelo Comandante da Força.

Art. 119. Os responsáveis pela segurança da informação da rede da OM deverá estar atualizado quanto aos incidentes de segurança da informação para melhor desempenho de sua função. O ponto de partida para obter essa orientação é acessar a informações sobre respostas a incidentes de segurança existentes na página eletrônica do CITEx.

Art. 120. As normas relativas ao gerenciamento de segurança da informação de uma rede devem ser classificadas. O ANEXO H define o modelo a ser utilizado.

Art. 121. O uso de meios de Tecnologia da Informação por pessoal do Exército, seja civil ou militar, assim como por elementos pertencentes a outras organizações, públicas ou privadas, poderá estar condicionado a assinatura de termo de compromisso de manutenção de sigilo de acordo com modelo constante das Instruções Gerais para Salvaguarda de Assuntos Sigilosos, ou instrumento legislativo que o valha.

§1º O pessoal de outras organizações que, por força da necessidade, tiver acesso a assuntos classificados, deverá assinar termo de compromisso de manutenção de sigilo;

§ 2º O pessoal pertencente ao Exército que, por força da necessidade, tiver acesso a assuntos classificados, poderá ou não assinar termo de compromisso de manutenção de sigilo, cabendo ao Comandante da OM definir quais os casos pertinentes.

STYLE="margin-top: 0.4cm; margin-bottom: 0.1cm; orphans: 2; page-break-after: avoid"> **Seção III**

Dos Aspectos Técnicos

Art. 122. Os aspectos técnicos da gestão da segurança da informação em redes devem abranger as ações gerenciais, seja de monitoração ou intervenção direta no funcionamento de equipamentos e **softwares**, que garantam a manutenção das regras de segurança estabelecidas em normas ou planos de segurança ou que venham a adequá-las para uma efetiva proteção da rede.

Art. 123. As ações gerenciais devem surgir como resultado dos requisitos de segurança de cada ambiente de rede, no entanto, os seguintes aspectos devem ser considerados quando da realização da análise de riscos e da elaboração das normas de segurança:

I - elaboração, aplicação e atualização das políticas;

II - direitos e privilégios no controle de acesso a dados;

III - uso de criptografia;

IV - assinatura digital;

V - certificação digital;

VI - identificação e autenticação de usuários da rede;

VII - acesso remoto;

VIII - uso de mais de serviço de rede em um só computador;

IX - senhas;

X - contas de acesso à rede de usuários (particular atenção deve ser dada às contas do pessoal em férias, transferidos, convidados e anônimos);

XI - cópias de segurança (**backup**);

XII - ativação e armazenamentos de **log** de eventos;

XIII - atualização dos sistemas operacionais;

XIV - conteúdo de sítios Internet das OM;

XV - configuração e uso de aplicativos ou plataformas de gerencia de rede.

Art. 124. Os sistemas operacionais dos computadores onde estiverem instalados **softwares** de defesa contra ataques à rede devem ter sua instalação configurada de modo a prover o mínimo possível de privilégios aos usuários do equipamento, assim como todos as atualizações disponibilizadas pelo fabricante devem ser instaladas no menor prazo possível.

Art. 125. O POP da gerência deve prever procedimentos para checar as atualizações.

Art. 126. A transmissão e armazenamento de arquivos contendo documentos com classificação sigilosa nas redes internas e para externas deve ser controlada em todas as categorias de rede conforme o previsto nas IG 10-51.

Art. 127. Devem ser realizadas cópias de segurança (**backup**) de dados e configurações de sistema de uma forma regular e deve-se realizar o armazenamento dessas cópias de segurança em local seguro e em instalações físicas distintas de onde os dados originais estão.

Art. 128. Ferramentas específicas para quebra de segurança não devem ser utilizadas, exceto por pessoal autorizado e de forma controlada pelo responsável pela administração da rede para fins de teste de segurança da rede.

Seção V

Dos Aspectos do Pessoal

Art. 129. O pessoal responsável pela operação e gestão da segurança deve estar treinado e atualizado no manuseio e condução do processo de gestão da segurança, logo as OM deverão incluir em seus planejamentos financeiros recursos para esse fim.

Seção VI

Dos Aspectos de Tratamento de Incidentes e Preservação de Evidências

Art. 130. A gerência da rede deverá proceder ao tratamento de incidentes de segurança priorizando: a preservação das evidências sobre a autoria e razões da violação de segurança, a continuidade dos serviços e o processo de recuperação da condição de normalidade.

Art. 131. Os incidentes de segurança devem ser documentados e armazenados juntamente com os registros dos eventos que os caracterizam e a documentação resultante deve ser remetida ao CITEx para fins de histórico e providências cabíveis no tocante a resposta ao incidente.

Parágrafo único. A onde ocorrer o incidente OM deverá notificar o CTA ou CT estiver vinculada caso esses Centros já possuam Seções de Tratamento de Incidentes.

Art. 132. O processo de preservação de evidências, pode demandar serviços especializados de checagem e averiguação dos recursos violados, o que poderá implicar na solicitação de apoio do CITEx ou de um CT ou CTA ao qual a OM estiver vinculada.

Art. 133. A gerência da OM deverá realizar os procedimentos relativos aos registros de eventos e continuidade de serviços contidas nestas Instruções, assim como outras providências dispostas nestas regras e ficar em condições de passar por processos de auditagem por parte da estrutura do CITEx organizada para essa tarefa.

TÍTULO IV

DAS RESPONSABILIDADES

CAPÍTULO I

DO DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA

Art. 134. Compete ao Departamento de Ciência e Tecnologia:

I - propor ao EME norma de especificação, uso, manutenção de equipamentos e **softwares** criptográfico para o Exército;

JUSTIFY STYLE="text-indent: 2.5cm; margin-top: 0.3cm; margin-bottom: 0.1cm; orphans: 2"> II - propor ao EME uma estrutura funcional necessária para gerir a segurança da informaç;ão nas redes do Exército;

III - estabelecer os requisitos para:

a) especificação, teste, aquisição, uso, manutenção de ferramentas de **software** e o **hardware** para segurança da informação em redes de dados e de comunicação;

b) implementação de sistemas corporativos com mecanismos de segurança;

c) aplicação de procedimentos de auditagem das OM pelos CTA e CT;

d) planejamento, implementação e aplicação de métodos e produtos para respostas à incidentes e preservação de evidências em situações de violação de segurança.

IV - definir a sistemática de treinamento e atualização de pessoal para manuseio adequado das ferramentas e **hardware** de segurança em redes;

V - especificar o formato e a periodicidade que as informações de eventos de segurança registrados nos sistemas do CITEx para fins de histórico e estatísticas;

VI - estabelecer as métricas e, em casos específicos, cotas para os indicadores de segurança das rede corporativas;

VII - fomentar a pesquisa e o desenvolvimento e a aplicação de soluções criptográficas;

VIII - manter a atualizada a doutrina relativa à segurança da informação em ambiente de rede definidas nestas Instruções;

IX - prever no planejamento orçamentário as necessidades de recursos destinados à segurança da informação das redes corporativas do Exército;

X - acompanhar o estado da arte nas áreas metodológica, de **hardware** e de **software** para segurança da informação em redes;

XI - acompanhar o cumprimento das atribuições destas Instruções;

XII - auditar a efetividade do cumprimento destas Instruções no âmbito das suas OMDS;

XIII - realizar, por meio de suas OMDS, verificações de rotina ou inopinadas da eficácia das proteções das redes das OM do Exército, visando aprimorar o processo de proteção nas redes da Força;

XIV - prover ao CITEx os dados necessários para atualizar as informações sobre configuração de ferramentas de segurança para publicação na página eletrônica da EBNet daquele Centro para orientação das OM do Exército;

XV - orientar o CITEx na consecução periódica de análise de riscos na Rede Rádio Estratégica e, a partir do resultado da análise, diagnosticar quais os riscos envolvidos na rede;

XVI - orientar o CITEx na consecução de análise de riscos para o uso de Redes Rádios Táticas e, a partir do resultado da análise, diagnosticar quais os riscos envolvidos nas redes;

line-height: 113%; orphans: 2"> XVII - realizar a gestão estratégica dos assuntos referentes a incidentes da rede corporativa, tendo por órgão operacional o CITEx, por meio da Seção de Tratamento de Incidentes de Rede, podendo:

a) notificar uma OM, a partir da qual estejam sendo originados eventos de violação de segurança na rede corporativa, para as devidas providências de neutralização do problema;

b) suspender temporariamente a conexão de rede de uma OM à Rede Corporativa do Exército nos casos extremos em sejam identificados ataques à essa rede considerados graves (implantação de dados corporativos falsos, substituição, destruição ou reuso de dados corporativos lícitos,

falsificação de acesso de usuários com privilégios especiais, violação de chaves criptográficas de uso real, vazamento de informações do Sistema de Inteligência, além de outros que possam ser identificados) enquanto a ameaça perdurar.

XVIII - criar demanda, a partir das necessidades da Força, a respeito das atividades de pesquisa a serem desenvolvidas pelo Grupo Finalístico de Segurança da Informação.

CAPÍTULO II

DO CENTRO DE DESENVOLVIMENTO DE SISTEMAS

Art. 135. Compete ao Centro de Desenvolvimento de Sistemas:

I - especificar as soluções de **software** e **hardware** de segurança da informação para uso nas redes do Exército conforme os requisitos estabelecidos pelo DCT;

II - desenvolver sistemas corporativos com recursos de segurança da informação conforme requisitos estabelecidos pelo DCT;

III - acompanhar, por meio de atividades de prospecção na área de segurança, as novidades metodológicas e tecnológicas relacionadas à segurança da informação;

IV - pesquisar os requisitos dos serviços da rede corporativa do Exército e propor ao DCT as normas de segurança para esses serviços;

V - realizar prospecção sobre as melhores práticas a respeito do uso de ferramentas de segurança, tais como **firewall** e sistemas de detecção ou prevenção de intrusão;

VI - propor ao DCT, de forma periódica e em intervalos de tempo não superiores a um ano, sugestões quanto ao aprimoramento destas Instruções com base no conhecimento advindo do acompanhamento das novidades metodológicas e tecnológicas no setor.

CAPÍTULO III

DO CENTRO INTEGRADO DE TELEMÁTICA DO EXÉRCITO

Art. 136. Compete ao Centro Integrado de Telemática do Exército:

I - aplicar e gerenciar as soluções de segurança da informação especificadas para uso na rede corporativa do Exército;

II - informar o DCT as necessidades de especialização e tipos treinamento para o pessoal diretamente envolvido na operação dos mecanismos de segurança da informação;

III - manter a Estrutura de Tratamento de Incidentes de Redes, tendo sua Seção de Tratamento de Incidentes de Redes como órgão central da estrutura;

IV - registrar e manter armazenados os eventos ocorridos nos equipamentos e sistemas que devem estar configurados para registrar essas informações;

V - remeter ao DCT, em períodos e formatos estabelecidos por esse Departamento, as informações de eventos registrados;

VI - disseminar, por meio das suas OMDS e na área de atuação de cada uma, a doutrina contida nestas Instruções;

VII - manter atualizada e divulgar, através das páginas eletrônicas do Exército e do CITEx, listas de verificação passíveis de utilização na elaboração de planos de contingência nas redes do Exército, assim como a periodicidade para notificação de ocorrências de ações de código maléficos;

VIII - manter em sua página eletrônica informações sobre atualizações de segurança para os sistemas operacionais em utilização na Força;

IX - atualizar as listas de verificação a cada seis meses, ou a qualquer momento que a necessidade obrigar, e informar o DCT das mudanças ocorridas;

X - publicar em sua página eletrônica na EBNet, a partir de orientações do DCT, as informações sobre configuração de ferramentas de segurança para orientação das OM do Exército;

XI - executar periodicamente, conforme orientação do DCT, análises de riscos nas Redes Rádio Estratégica e Tática e, a partir do resultado da análise, diagnosticar quais os riscos envolvidos e levantar as informações necessárias para interpretar as evidências de violação de segurança;

XII - exercer a monitoração de incidentes na Rede Corporativa por meio da sua Seção de Tratamentos de Incidentes e notificar o DCT sobre os incidentes identificados e estabelecer uma rotina de interação com com os demais Centros de Tratamentos de Incidentes Brasileiros e Internacionais de interesse do Exército;

XIII - propor ao DCT, de forma periódica e em intervalos de tempo não superiores a um ano, sugestões quanto ao aprimoramento da doutrina de auditoria de segurança da informação com base no conhecimento adquirido nas atividades de gerenciamento das rede de dados e comunicações.

CAPÍTULO IV

DO INSTITUTO MILITAR DE ENGENHARIA

Art. 137. Compete ao Instituto Militar de Engenharia:

I - incluir, dentre os trabalhos de tema dirigido, iniciação científica, projetos de fim de curso, dissertações de mestrado e teses de doutorado, temas relacionados à segurança da informação em redes de comunicação e de dados;

II - Disseminar aos membros do Grupo Finalístico de Segurança da Informação o conteúdo dos trabalhos no artigo I;

III - propor ao DCT, de forma periódica e em intervalos de tempo não superiores a um ano, sugestões quanto ao aprimoramento da doutrina

de auditoria de segurança da informação com base no conhecimento adquirido com os resultados dos trabalhos de graduação e pós-graduação realizados sobre o tema.

CAPÍTULO V

DO DIRETORIA DE SERVIÇO GEOGRÁFICO

Art. 138. Compete à Diretoria de Serviço Geográfico:

I - implementar nas informações geográficas sob sua gestão as proteções necessárias, conforme as análises de riscos que forem realizadas no âmbito da Diretoria;

II - propor ao DCT, de forma periódica e em intervalos de tempo não superiores a um ano, sugestões quanto ao aprimoramento da doutrina de auditoria de segurança da informação com base nas necessidades da área do serviço geográfico.

CAPÍTULO VI

DO CENTRO INTEGRADO DE GUERRA ELETRÔNICA

Art. 139. Compete ao Centro Integrado de Guerra Eletrônica:

I - informar o DCT as necessidades de especialização e tipos treinamento para o pessoal diretamente envolvido na operação de mecanismos tecnológicos de segurança da informação em redes das atividades de Guerra Eletrônica;

II - manter-se em condições de disseminar a doutrina de segurança da informação em redes na área de sua atuação a partir do apoio do DCT;

III - disseminar, por meio dos seus cursos, a doutrina contida nestas Instruções, com as adaptações julgadas pertinentes para a área de Guerra Eletrônica.

CAPÍTULO VII

DO GRUPO FINALÍSTICO DE SEGURANÇA DA INFORMAÇÃO

Art. 140. Compete ao Grupo Finalístico de Segurança da Informação, por intermédio do seu Chefe:

I - realizar atividades de pesquisas e desenvolvimento de segurança da informação segundo a orientação do DCT;

II - propor ao DCT, de forma periódica e em intervalos de tempo não superiores a dois anos, sugestões quanto ao aprimoramento da doutrina de segurança da informação em redes com base no conhecimento adquirido com os resultados dos trabalhos de graduação e pós-graduação realizados sobre o tema.

CAPÍTULO VIII

DAS OM DO EXÉRCITO

Art. 141. Compete às OM do Exército, por intermédio do seu Comandante:

I - manter inventário dos recursos componentes do seu sistema de informação conforme modelo constante das NARMCEI;

II - manter seus sistemas de informação em conformidade com o previstos nestas Instruções e, assim, estar em condições adequadas para a realização de auditorias;

III - nomear a equipe técnica que procederá a auditoria interna da segurança da informação;

IV - zelar para que estas Instruções sejam aplicadas no ambiente desta rede;

V - informar o CITEx sobre incidentes de rede ocorridos no seu ambiente de rede;

VI - comunicar ao DCT os casos em que forem identificadas eventuais incompatibilidades entre a doutrina de segurança disseminada pelo DCT e a doutrina de contra-inteligência.

CAPÍTULO IX

DOS USUÁRIOS DAS REDES

Art. 142. Compete aos usuários do Exército:

I - manter a confidencialidade dos dados sob sua responsabilidade, assim como sua senha pessoal de acesso à rede ou a serviços específicos;

II - informar ao chefe imediato quaisquer violações de segurança que vier a observar;

III - alterar quaisquer uma de suas senhas em caso de suspeita ou constatação de ela foi exposta ou descoberta;

IV - encerrar sessões de trabalhado, ativar algum mecanismo de bloqueio de acesso da conexão a rede ou a serviços específicos de seu acesso sempre que se ausentar do computador em que está operando;

V - evitar instalar qualquer programa seu sem a ciência e aprovação do responsável pela gerência da rede;

VI - procurar se informar sobre as normas de segurança a que o desempenho de sua função está ligada;

VII - evitar editar arquivos de documentos sigilosos em computadores particulares, em especial se conectados à Internet;

VIII - ao transportar arquivos de trabalho para seu computador particular, procurar realizar procedimento de verificação antivírus antes de reinserir o documento no computador de trabalho;

IX - na elaboração de documentação com classificação sigilosa, ou não classificado mas cuja publicação prematura seria inconveniente, procurar não deixar o documento exposto no computador quando tiver de se afastar do equipamento e nem permitir que, quando da impressão do documento em impressora que estiver numa localização física distante do computador, as folhas impressas fiquem expostas a outros usuários;

X - salvaguardar mídias de armazenamento, tais como disquetes, CD ROM, **pendrive**, **flash card** etc, que contenham informações que demandem cuidados de proteção especiais, em especial as que forem de natureza sigilosa.

ANEXO A

MODELO DE NORMA DE SEGURANÇA PARA REDES DO EXÉRCITO

MINISTÉRIO DA DEFESA

a

EXÉRCITO BRASILEIRO

OM

"NORMAS PARA SEGURANÇA DA INFORMAÇÃO DA REDE DE DA OM"

EXÉRCITO BRASILEIRO

OM

"NORMAS PARA SEGURANÇA DA INFORMAÇÃO DA REDE DE DA OM"

(Deve-se transcrever a finalidade do documento, por exemplo: "A finalidade desta norma é estabelecer as regras de segurança para proteção das informações contidas na rede de computadores e de comunicações da OM XX".)

2. OBJETIVOS

(Deve-se transcrever os objetivos a serem atingidos pela aplicação da norma e que, em conjunto, cumpram a finalidade estabelecida.)

3. CONCEITOS E PRESSUPOSTOS BÁSICOS

(Conceitos: deve-se transcrever neste item as terminologias específicas relacionadas ao uso e gerência da rede necessárias para facilitar o entendimento do documento. Pressupostos: item opcional, caso se julgue necessário estabelecer que, para aplicação das Instruções, certas condições devem ser previamente atendidas e consideradas vigentes.)

4. REGRAS DE SEGURANÇA

(Deve-se transcrever todas as regras de segurança julgadas necessárias e, se a complexidade do documento assim o exigir, separar grupos de regras em categorias, como ocorre nestas Instruções.)

a. Regras Gerais (regras de segurança de caráter geral e voltadas para medidas de segurança dos dados, informações e conhecimentos armazenados, processados ou disseminados nos enlaces ou equipamentos da rede)

b. Segurança dos Serviços, Sistemas, Aplicativos e Sistemas Operacionais de Rede (regras de segurança referentes aos procedimentos de uso de: serviços, tais como correio eletrônico ou WEB; sistemas corporativos específicos do Exército; aplicativos de uso geral, tais como suítes de escritório; sistemas operacionais de rede).

1) Dos Serviços de Rede (subtítulo referente aos serviços);

2) Dos Sistemas Aplicativos (subtítulo referente aos sistemas corporativos);

3) Dos Aplicativos de Rede (subtítulo referente aos **softwares** aplicativos);

4) Dos Sistemas Operacionais de Rede (subtítulo referente aos sistemas operacionais utilizados).

c. Segurança do **Hardware** (regras de segurança referentes aos procedimentos de uso de computadores servidores, computadores de uso específico, computadores de uso geral, periféricos de rede, equipamentos de interligação de rede - roteadores, **switches**, **hubs**, modem, repetidores).

1) Computadores servidores;

2) Computadores de uso específico;

3) Computadores de uso geral;

4) Periféricos de rede;

5) Equipamentos de interligação de rede;

6) Outros equipamentos.

d. Segurança das Áreas e Instalações (regras de segurança relativas ao controle de acesso e a adequação das áreas e instalações onde se encontram equipamentos críticos da rede);

e. Cópias de Segurança **(Backup)** (regras de sobre produção, armazenamento, teste, atualização, substituição e descarte de cópias de segurança no nível de usuário final);

f. Segurança do Pessoal (regras de segurança relativas aos aspectos de sensibilização e treinamento do pessoal que lida com as redes no nível de usuário final);

5. **RESPONSABILIDADES**

(Deve-se transcrever as obrigações de cada seção/assessoria/função da OM envolvida com a aplicação das normas de segurança.)

6. **PRESCRIÇÕES DIVERSAS**

(Deve-se fazer uso deste item, caso existam particularidades do contexto da OM que não se enquadrem nos itens anteriores, mas que sejam julgados importantes para a norma.)

Cidade, (DD) de (MM) de (AAAA)

Assinatura Comandante

ANEXO B

MODELO DE RELATÓRIO DE MUDANÇAS NA REDE

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
OM

RELATÓRIO DE MODIFICAÇÕES NA REDE DA OM XXXX

1. FINALIDADE

(finalidade do documento)

2. ASSUNTO

(descrição sumária da modificação em pauta)

3. DATA DA MODIFICAÇÃO

(data em que ocorreu a modificação; caso a mudança ocorra num período que abranja mais de um dia, o período, destacando-se a data de início e fim, deve ser explicitado)

4. DESCRIÇÃO DA MODIFICAÇÃO

(descrição detalhada da modificação necessária e do processo de como a modificação foi feita)

5. RESPONSÁVEIS

(registro de quem efetuou a mudança e que acompanhou ou fiscalizou)

6. DOCUMENTAÇÃO ENQUADRANTE

(se for o caso, deve ser citada a documentação normativa ou contratual sob a qual o processo de mudança foi realizado)

7. REGISTROS ADICIONAIS

(deve-se registrar informações adicionais julgadas pertinentes, em particular a respeito de análises de risco realizadas)

Cidade, (DD) de (MM) de (AAAA)

Oficial responsável

Assinatura Comandante

ANEXO C

MODELO DE SOLICITAÇÃO PARA ACESSO REMOTO

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO

XXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXX

Local, ___ de _____ de 200_.

Of nº

Do

Ao Sr Chefe do Centro Integrado de Telemática do Exército

Assunto: Cadastro no Acesso Remoto Seguro

1. Expediente versando sobre solicitação de cadastro de usuários desta OM no Acesso Remoto Seguro à EBNet.

2. Informo a V Exa que há necessidade que esta OM acesse o sistema de Acesso Remoto Seguro, pelos seguintes motivos:

a. ...

b. ...

3. Esta OM não possui acesso à EBNet (ou somente possui acesso à EBNet por intermédio de linha discada, o que implica em alto custo para as chamadas telefônicas).

4. Em conseqüência, solicito à V Exa autorizar que os seguintes militares, em ordem de prioridade, tenham o Acesso Remoto à EBNet:

PRIORIDADE	POSTOGRAD	NOME COMPLETO (Negritar Nome de Guerra)	IDENTI-DADE	DESEJA CADASTRAR NOVA SENHA	TELEFONE
1	Ten	.....	.....	Sim	(xx).....
2	Sgt	.....	.....	Não	(xx).....

_____

Cmt OM

ANEXO D

MODELO DE NORMA DE SEGURANÇA PARA FIREWALLS/IDS/IPS

CLASSIFICAÇÃO

MINISTÉRIO DA DEFESA

EXÉRCITO BRASILEIRO

OM

"**NORMAS PARA DE SEGURANÇA PARA FIREWALLS ..... DA OM**"

1. FINALIDADE

(Deve-se transcrever a finalidade do documento.)

2. OBJETIVOS

(Deve-se transcrever os objetivos a serem atingidos pela aplicação da norma e que, em conjunto, cumpram a finalidade estabelecida.)

3. NORMAS DE REFERÊNCIA

(Relação de normas relacionadas e que possam complementar ou respaldar o uso da norma de **firewall**.)

4. REGRAS DE SEGURANÇA

(Deve-se transcrever todas as regras de segurança julgadas necessárias.)

a. Regras Gerais (regras de segurança de caráter geral para o **firewall**.)

b. Arquitetura do **Firewall**/IDS (descrição da disposição física e lógica que os componentes do **firewall** estão - roteadores , computadores servidores e Zonas desmilitarizadas - esquemas gráficos devem ser utilizados)

c. Regras para cada componente do **Firewall**

1) Roteador(es) externos (regras relativas ao (s) roteador(es) que estão como interface entre a rede e o mundo exterior)

1.1) Regras de filtragem de pacote (tipos de filtros implementados);

1.2) Rotas específicas (rotas estabelecidas de maneira forçada, por motivo de segurança)

2) Roteador(es) internos (regras relativas ao (s) roteador(es) que estão como interface entre as redes internas ou entre segmentos da rede)

2.1) Regras de filtragem de pacote (tipos de filtros implementados);

2.2) Rotas específicas (rotas estabelecidas de maneira forçada, por motivo de segurança).

2.3) Sistemas Operacionais (regras referentes aos sistemas operacionais utilizados nos roteadores, se for o caso).

2.4) Configuração para registro de eventos (**logs**).

CLASSIFICAÇÃO

CLASSIFICAÇÃO

3) **Firewalls** de Aplicação (**software** e computador - regras relativas ao **software** de **firewall** implementado em um computador dedicado - se houver mais de um desses conjuntos, cada um terá um item na norma descrevendo suas regras)

3.1) Regras de filtragem de pacote (tipos de filtros implementados)**;**

3.2) Rotas específicas (rotas estabelecidas de maneira forçada, por motivo de segurança).

3.3) Regras de filtragem de aplicações e serviços (serviços e aplicações de rede permitidas, seu sentido [dentro para fora da rede ou vice-versa], em que parte ou segmento da rede é permitido, usuários permitidos, tipo de autenticação requerida etc)

3.4) Sistemas Operacionais (regras referentes ao(s) sistema(s) operacional(is) utilizado(s) no(s) servidor(es) onde está(ão) instalado(s) o **software**(s) de **firewall**).

3.5) Configuração para registro de eventos (logs).

d. Contingências (procedimentos par o caso de indisponibilidade de um, mais de um componente ou até todo o sistema de **firewall**, formas alternativas de manter o serviço de **firewall** ou procedimento de interrupção, se for o caso.)

e. Testes de efetividade (regras sobre os testes par a verificação da eficácia e eficiência do sistema de **firewall** e sua periodicidade).

f. Segurança das Áreas e Instalações (regras de segurança relativas ao controle de acesso e a adequação das áreas e instalações onde se encontram os componentes do **firewall**);

g. Cópias de Segurança **(Backup)** (regras de sobre produção, armazenamento, teste, atualização, substituição e descarte de cópias de segurança das informações de configuração ou outros considerados importantes);

5. RESPONSABILIDADES

(Deve-se transcrever as obrigações de cada responsável pela operação, gerência e manutenção do **firewall**.)

6. PRESCRIÇÕES DIVERSAS

(Deve-se fazer uso deste item, caso existam particularidades do contexto da OM que não se enquadrem nos itens anteriores, mas que sejam julgados importantes para a norma.)

Cidade, (DD) de (MM) de (AAAA)

Assinatura Comandante

CLASSIFICAÇÃO

ANEXO E

MODELO DE PLANO DE CONTINGÊNCIA

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
OM

(Este modelo se refere ao caso genérico com várias possibilidades para composição do Plano de Contingência, NÃO SENDO OBRIGATÓRIO a reprodução todos os itens. Assim, é recomendável que sejam confeccionadas as partes realmente necessárias e que a elaboração do documento e sua vigência sejam feitas gradualmente, elegendo-se escopos considerados prioritários e para esses escopos sejam realizadas as versões correspondentes.)

1. FINALIDADE

Transcrição da finalidade do plano. (Exemplo: A finalidade deste plano é descrever os procedimentos necessários para lidar com situações emergenciais de indisponibilidade dos serviços de informática e de comunicações necessárias à continuidade dos serviços da OM "...".)

2. OBJETIVOS

Transcrição dos objetivos necessários para cumprir a finalidade do plano. (Exemplo: A fim de cumprir a finalidade anunciada, os seguintes objetivos são estipulados: definição dos grupos envolvidos na condução do processo, assim como as respectivas responsabilidades; descrição dos procedimentos na ativação e desenvolvimento do plano para lidar com situações emergenciais; e descrição dos procedimentos para propiciar a restauração das condições operacionais normais.)

3. PERÍODO DE VIGÊNCIA

(data da última atualização, período de vigência do plano e periodicidade do treinamento do plano).

4. SERVIÇOS (OU PROCESSOS) A SEREM PRESERVADOS

Esta relação deverá estar organizada conforme as conveniências do ambiente para o qual o plano de contingência é elaborado. Algumas categorias podem se demonstrar como convenientes, por exemplo, os serviços podem estar organizados em grupos, separados por critérios: de criticidade, ou instâncias administrativas etc.

Neste item deve constar a descrição dos serviços considerados críticos e, portanto, para os quais as medidas de contingência estão voltadas. A descrição deve ser detalhada, sendo que o grau de detalhamento obedecerá aos critérios estabelecidos pelos elaboradores do plano. O mesmo raciocínio deve ser aplicado ao item 5 (Recursos).

Alguns exemplos (genéricos) são os seguintes:

a. Serviço 1: (denominação e descrição sumária da finalidade do serviço).

1) Configuração do serviço: (descrição de como o serviço deve estar configurado para operar).

2) Computador onde está instalado: (identificação do computador e configuração do **hardware**).

3) O sistema operacional utilizado no computador onde o serviço está instalado: (nome do sistema, versão, **service packs** ou **patches** instalados e configuração do sistema).

4) Serviços adicionais instalados no mesmo computador: (identificação do(s) **software**(s), versão, **service packs** ou **patches** instalados e configuração do(s) **software**(s)).

5) Localização física: (local onde está instalado o computador no qual o serviço está instalado).

6) Localização física dos **softwares** necessários (localização e forma de aceso aos **softwares** necessários para reativar o serviço).

7) Responsáveis pela manutenção e operação: (relação nominal do pessoal a ser acionado nas situações de crise e formas de contato).

8) POP para ativar a contingência: (procedimentos operacionais básicos (POP) necessários para acionar os meios alternativos para manter o serviço ativo, tais meios deverão abranger aspectos humanos, materiais, instrumentais, computacionais, de instalações físicas etc).

9) POP para as ações que deverão vigorar durante a contingência: (POP necessários para manter o serviço ativo, tais meios deverão abranger aspectos humanos, materiais, instrumentais, computacionais, de instalações físicas etc).

10) POP retorno à normalidade (reinstalação e reativação): (procedimentos operacionais básicos (pop) para reinstalar e configurar todo o conjunto (**hardware** e **software**) como se fosse a primeira instalação)

b. Serviço 2: (idem o anterior)

:

:

:

:

RECURSOS A SEREM PRESERVADOS (recursos de equipamentos ou lógicos não diretamente ligados aos serviços - tópico anterior -, mas que tenham sido considerados relevantes, por exemplo: computadores, roteadores, switches etc)

c. Recurso 1: (denominação e descrição sumária da finalidade do recurso).

1) Configuração do recurso: (descrição de como o recurso deve estar configurado para operar).

2) Computador onde está instalado (se for o caso): (identificação do computador e configuração do **hardware**).

3) O sistema operacional utilizado (se for o caso) no recurso: (nome do sistema, versão, **service packs** ou **patches** instalados e configuração do sistema

).

4) Localização física: (local onde está instalado o recurso).

5) Localização física dos **softwares** necessários (localização e forma de aceso aos **softwares** necessários para reativar o recurso).

6) Serviços adicionais instalados no mesmo recurso (se for o caso) : (identificação do(s) **software**(s), versão, **service packs** ou **patches** instalados e configuração do(s) **software**(s)).

7) Responsáveis pela manutenção e operação: (relação nominal do pessoal a ser acionado nas situações de crise e formas de contato).

8) POP para ativar a contingência: (procedimentos operacionais básicos (POP) necessários para acionar os meios alternativos para manter o recurso utilizável, tais meios deverão abranger aspectos humanos, materiais, instrumentais, computacionais, de instalações físicas etc).

9) POP para as ações que deverão vigorar durante a contingência: (POP necessários para manter o recurso utilizável, tais meios deverão abranger aspectos humanos, materiais, instrumentais, computacionais, de instalações físicas etc).

10) POP para retorno à normalidade (reinstalação e reativação): (procedimentos operacionais básicos (pop) para reinstalar e configurar todo o conjunto (**hardware** e **software**) que compõe o recurso como se fosse a primeira instalação).

11) POP de reinstalação: (procedimentos operacionais básicos (pop) para reinstalar e configurar todo o conjunto (**hardware** e **software**) como se fosse a primeira instalação).

d. Recurso 2: (idem o anterior)

:

:

:

:

RELAÇÃO DO PESSOAL (relação do pessoal envolvido na aplicação do plano)

Posto /Graduação/ NOME (destaque para o nome de guerra)	Grupo (se for o caso)	Formas de Contato					
		Endereço comercial e residencial	Telefones: Res/Trab/ Ramal	Celular	Pager	e-mail	Outros contatos

5. ESTRUTURAÇÃO DOS GRUPOS

A seguir são apresentados os grupos responsáveis pelas diversas fases e etapas do desenvolvimento e ativação do plano de contingência. Os grupos exemplificados buscam oferecer variadas opções, no entanto, não se pretendeu impor uma lista mínima ou que esgotasse as opções.

O modelo adotado pela OM deve estar de acordo com as suas peculiaridades. Em conseqüência, em algumas OM a estruturação do plano poderá ser mais simples que este modelo, podendo haver até mesmo supressão ou aglutinamento de um ou mais itens ou subitens. Por outro lado, se necessário for, em algumas OM, a estruturação do plano poderá ser mais complexo, o que implicará no acréscimo de itens adicionais.

a. Grupo de Coordenação

1) Exerce a coordenação geral do plano de contingência. Composto por:

2) Comandante;

3) Subcomandante;

4) Estado-Maior;

5) Oficiais de comunicações e de informática;

6) Inteligência;

7) Segurança de informações;

8) outros (a ser definido conforme a necessidade em função das características de cada OM).

b. Apoio Administrativo

Provê o apoio administrativo necessário para a execução do plano de contingência. Composto por:

1) Seção de Pessoal ou equivalente.

c. Serviços de Rede de Comunicações e de Computadores

Gerencia os serviços de rede durante a contingência. Composto por membros das seguintes áreas:

1) comunicações;

2) informática;

3) administração de banco de dados;

4) suporte técnico ou o que o equivalha

5) administração da rede;

6) outros (conforme particularidades da rede da OM).

d. **Hardware**

Provê apoio na área de equipamentos. Composto por membros das seguintes áreas:

1) suporte técnico ou o que o equivalha;

2) manutenção de equipamentos rádio e de informática.

e. **Software**

Provê apoio na área de **software** básico (sistemas operacionais e aplicativos administrativos), de apoio (**softwares** de manutenção ou diagnóstico) e sistemas corporativos Composto por membros das seguintes áreas:

1) comunicações e de informática;

2) suporte técnico ou o que o equivalha.

f. Comunicações

Provê apoio na manutenção e operacionalização da estrutura de comunicações rádio necessária ao plano de contingência. Composto por membros das seguintes áreas:

1) comunicações;

2) suporte técnico ou o que o equivalha.

3) informática.

6. RESPONSABILIDADES DOS GRUPOS

a. Grupo de Coordenação

1) Permanentes:

1.1) identificar as funções e recursos críticos para a OM e, portanto, estabelecer o que deve constar do plano de contingência;

1.2) analisar e definir alternativas para o processamento das funções e recursos críticos para o caso da sua indisponibilidade;

1.3) definir os recursos financeiros e materiais necessários para viabilizar o plano;

1.4) coordenar as atividades dos demais grupos;

1.5) elaborar o plano de contingência e normas correlacionadas e julgadas necessárias;

1.6) revisão periódica do plano de contingência;

1.7) distribuição de cópias do plano e normas a todos os envolvidos;

1.8) organizar e coordenar a execução das simulações do plano;

1.9) dar apoio a todos os envolvidos;

1.10) resolver conflitos entre os diversos grupos;

1.11) estabelecer qual a infra-estrutura de **hardware** e **software** de comunicações e computacional alternativa com a qual se deve contar durante a ativação do plano de contingência, assim como sua localização física;

1.12) informar aos demais envolvidos quanto às atualizações sofridas pelos sistemas e recursos críticos;

1.13) definir, com o grupo de aplicativos, as atividades envolvidas com os sistemas críticos.

1.14) definir e montar a estrutura de retorno à normalidade;

1.15) manter atualizado os procedimentos para operacionalizar o plano de contingência.

2) Na ativação do plano de contingência:

2.1) coordenar a ativação do plano de contingência;

2.2) coordenar as atividades dos demais grupos.

3) Durante a execução do plano de contingência

3.1) coordenar as atividades do plano de contingência;

3.2) estabelecer diretrizes para situações imprevistas.

4) Retorno à normalidade:

4.1) coordenar as atividades de retorno à normalidade.

b. Apoio Administrativo

1) Permanentes:

1.1) manter atualizados as listas de contatos para comunicação com os envolvidos no plano (números de telefone, fax, e-mail etc.);

1.2) divulgar aos membros do plano de contingência as listas de contatos de todos os envolvidos;

1.3) providenciar a requisição dos recursos necessários para operacionalizar o plano.

2.) Durante a contingência

2.1) fornecer local apropriado para um "Centro de Operações de Contingência";

2.2) suprir o local com as facilidades de comunicação.

2.3) fornecer os suprimentos básicos (lápis, papel, mesa, cadeira, armário);

2.4) fornecer meios de transporte de pessoas e materiais.

c. Serviços de Rede

1) Permanentes

1.1) desenvolver os procedimentos específicos destinadas aos serviços de redes considerados críticos;

1.2) manter atualizadas todos os procedimentos para manutenção do funcionamento dos serviços de redes;

1.3) manter atualizadas e em lugar seguro cópias da documentação dos sistemas de **hardware** e **software** que constituem os serviços de redes críticos;

1.4) prever e desenvolver procedimentos para atender a todas as condições de retorno à normalidade, para as rotinas de contingência.

1.5) providenciar local livre de riscos e guardar as cópias de segurança dos sistemas necessários para a contingência;

1.6) estabelecer procedimentos de operação em caso de emergência;

2) Na ativação da contingência

2.1) ativar a contingência, conforme os serviços atingidos;

3.) Durante a contingência

3.1) solucionar problemas imprevistos relacionados aos serviços de redes;

3.2 efetuar os acertos que se fizerem necessários nos serviços de rede ativados durante a contingência.

3.3) se for o caso, tornar acessível o(s) local(is) alternativo(s) para operação em caso de contingência;

3.4) operar os sistemas que terão sua contingência ativada em função da emergência que venha a ocorrer.

3.5) gerar e manter as cópias de segurança dos dados necessários ao retorno à normalidade.

4) Retorno à normalidade

4.1) Executar o processo de retorno à normalidade, conforme previsto no plano de contingência.

d. **Hardware**

1) Permanentes:

1.1) manter atualizada o inventário dos equipamentos existentes e a situação de cada um;

1.3) analisar e propor as melhores alternativas de contingência para o **hardware** considerado com crítico para a rede;

1.4) providenciar local livre de riscos e guardar as cópias de segurança dos sistemas necessários para a contingência;

1.5) estabelecer procedimentos de operação em caso de emergência;

1.6) se for o caso, tornar acessível o(s) local(is) alternativo(s) para operação em caso de contingência.

2) Na ativação da contingência:

2.1) comunicar aos envolvidos no plano de contingência quaisquer avarias que possam afetar o processamento dos serviços de rede considerados críticos à missão da OM, fornecendo a previsão para a correção do problema.

3) Durante a contingência:

3.1) providenciar os reparos dos equipamentos danificados;

3.2) providenciar o equipamento alternativo e ativá-lo;

3.3) contatar os fornecedores, se for o caso, visando à reposição de componentes ou dos próprios equipamentos;

3.4) operar os sistemas que terão sua contingência ativada em função da emergência que venha a ocorrer.

3.5) gerar e manter as cópias de segurança dos dados necessários ao retorno à normalidade.

4) No retorno à normalidade:

4.1) concluir as correções e comunicar a todos os envolvidos para se efetuar retorno à normalidade.

e. **Software**

1) Permanentes:

1.1) manter atualizada o inventário de todos os **softwares** e sistemas informatizados disponíveis na OM, identificando sua utilização;

1.2) criar e manter atualizada a estrutura de cópias dos sistemas operacionais e dos aplicativos administrativos nos equipamento alternativos;

1.3) analisar e colocar em prática as melhores alternativas de contingência para os diversos **softwares** e sistemas usados na OM.

2) Na ativação da contingência

2.1) ativar o sistema operacional e os **softwares** de contingência na instalação alternativa.

3) Durante a contingência e no retorno à normalidade

3.1) dar apoio e resolver situações imprevistas relacionadas com **softwares**;

3.2) operar os sistemas que terão sua contingência ativada em função da emergência que venha a ocorrer.

3.3) gerar e manter as cópias de segurança dos dados necessários ao retorno à normalidade.

f. Comunicação

1) Permanentes:

1.1) manter atualizada o inventário dos recursos de **hardware**, **software** e canais que compõem a estrutura de comunicação;

1.2) analisar e viabilizar rotas alternativas para os enlaces de comunicação da OM;

1.3) providenciar local livre de riscos e guardar as cópias de segurança dos sistemas necessários para a contingência;

1.4) estabelecer procedimentos de operação em caso de emergência;

1.5) se for o caso, tornar acessível o(s) local(is) alternativo(s) para operação em caso de contingência.

2) Durante a contingência:

2.1) providenciar a instalação e reconfiguração dos enlaces de comunicação para o local onde se processará a contingência;

2.2) dar apoio e resolver situações imprevistas relacionadas com a estrutura de comunicações;

2.3) operar os sistemas que terão sua contingência ativada em função da emergência que venha a ocorrer.

2.4) gerar e manter as cópias de segurança dos dados necessários ao retorno à normalidade.

7. INFORMAÇÕES COMPLEMENTARES

a. Sobre o Plano de Contingência

1) Quem mantém e atualiza.

2) Quem recebe cópias parciais/totais.

3) Periodicidade de atualização e data da última atualização.

b. Relação de fornecedores, fabricantes, representantes técnicos etc.

Neste item deve constar a relação dos fornecedores, fabricantes, representantes técnicos ou qualquer outra entidade que esteja vinculada formalmente com a manutenção do funcionamento de um recurso crítico ou de parte dele. É recomendável que, no mínimo, constem as seguintes informações:

1) Nome da empresa.

2) Pessoas para contato.

3) Telefones (comercial, residencial, celular).

4) Pager.

5) E-mail.

8. AÇÕES A SEREM IMPLEMENTADAS

A seguir, são apresentados os itens que devem compor o tópico de ações a serem executadas em situações de ativação do plano. O fato do conteúdo desta parte ser específico de cada ambiente faz com que a elaboração de cada caso possa estar aquém ou além daqueles aqui sugeridos.

O objetivo desta parte do plano é descrever o que deve ser feito, de acordo com o tipo de violação de segurança que venha a ocorrer. As tabelas a seguir devem ser utilizadas para definir os POP relativos às fases de ativação e vigência da contingência, assim como da fase de retorno à normalidade.

É recomendável que sejam listados os recursos / serviços computacionais e de comunicações, além de outros considerados críticos e associar a eles as ações correspondentes, com os respectivos responsáveis pela sua execução, de acordo com violações de segurança que atinjam a integridade, a confidencialidade, a disponibilidade da informação ligada ao recurso considerado ou ainda a autenticidade da pessoa que acessa ou tenta acessar a informação ligado ao recurso. Isso pode ser feito, por exemplo, construindo-se uma ou mais tabelas como representado a seguir:

Recurso/Serviço crítico	Violações de segurança	Ações a serem tomadas	Responsáveis pelas ações
Recurso/Serviço crítico1	Violação contra a confidencialidade da informação processada pelo recurso ou serviço 1	Ações relativas às violações de confidencialidade **1) Na ativação da contingência;** **2) durante a contingência;** **3) no retorno à normalidade.**	Responsáveis pelas ações relativas à violação de confidencialidade
	Violação contra a integridade da informação processada pelo recurso ou serviço 1	Ações relativas às violações de integridade: **1) na ativação da contingência;** **2) durante a contingência;** **3) no retorno à normalidade.**	Responsáveis pelas ações relativas à violação de integridade
	Violação contra a disponibilidade da informação processada pelo recurso ou serviço 1	Ações relativas às violações de disponibilidade: **1) na ativação da contingência;** **2) durante a contingência;** **3) no retorno à normalidade.**	Responsáveis pelas ações relativas à violação de disponibilidade
Recurso/Serviço crítico1		Ações relativas às violações específicas:	

	Violações específicas contra a informação processada pelo recurso ou serviço 1	**1) na ativação da contingência;** **2) durante a contingência;** **3) no retorno à normalidade.**	Responsáveis pelas ações relativas à violação específicas
Recurso/Serviço crítico 2	Violação contra a confidencialidade da informação processada pelo recurso ou serviço 2	Ações relativas às violações de confidencialidade **1) na ativação da contingência;** **2) durante a contingência;** **3) no retorno à normalidade.**	Responsáveis pelas ações relativas à violação de confidencialidade
	Violação contra a integridade da informação processada pelo recurso ou serviço 2	Ações relativas às violações de integridade: **1) na ativação da contingência;** **2) durante a contingência;** **3) no retorno à normalidade.**	Responsáveis pelas ações relativas à violação de integridade
	Violação contra a disponibilidade da informação processada pelo recurso ou serviço 2	Ações relativas às violações de disponibilidade: **1) na ativação da contingência;** **2) durante a contingência;** **3) no retorno à normalidade.**	Responsáveis pelas ações relativas à violação de disponibilidade
	Violações específicas contra a informação processada pelo recurso ou serviço 2	Ações relativas às violações específicas: **1) na ativação da contingência;** **2) durante a contingência;** **3) no retorno à normalidade.**	Responsáveis pelas ações relativas à violação específicas
:	:	:	:
Recurso / Serviço crítico n	:	:	:

Os campos a serem preenchidos são: a identificação do serviço ou recurso, as ações a serem implementadas, os responsáveis e as violações específicas. Os itens de violação de atributos (confidencialidade, integridade e disponibilidade), na segunda coluna, não devem ser direcionados para tipos de ataques específicos, pois, para isso, existe o item de violações específicas. Ao contrário, os itens não específicos servem para referenciar simplesmente a

violação do atributo. Por exemplo, no item relativo a "Violação contra a integridade da informação processada pelo recurso ou serviço 1" se refere a perda da integridade da informação (ou conjunto de informações) correspondente ao item, independente de qual violação específica a gerou.

É recomendável que as ações a serem tomadas sejam subdivididas em três categorias: ações que deflagram a execução do plano, ações que perduram durante a aplicação do plano e ações para retorno a normalidade.

ANEXO F

MODELO PARA APLICAÇÃO DE LISTA DE VERIFICAÇÃO

MINISTÉRIO DA DEFESA

EXÉRCITO BRASILEIRO

OM

LEVANTAMENTO DO ESTADO DA REDE BASEADO EM LISTAS DE VERIFICAÇÃO

1. FINALIDADE: (Finalidade a que se destina o documento).

2. OBJETIVO: (Descrição do objetivo da aplicação da técnica de lista de verificação, ou seja, o que se pretende averiguar com a sua aplicação).

3. APLICAÇÃO DA LISTA DE VERIFICAÇÃO:

(item no qual se reproduzirá as listas de verificação julgadas necessárias para a verificação demandada).

Nº Ordem	PERGUNTA / CONTEXTO CONSIDERADO	S(*)	N(*)	N/A (*)	OBSERVAÇÕES
	1. SERVIÇOS DE REDE				
	a. Correio eletrônico (exemplo):				
1)					
2)					
:					
	b. WEB (exemplo):				
1)					
2)					
:					
	c. Firewall (exemplo):				
1)					
2)					
:					
	d. Proteção contra Códigos Maléficos (exemplo):				
1)					
2)					
:					
	2. SERVIDORES (exemplo):				
1)					
2)					
:					
	3. INFRA-ESTRUTURA DE REDEC (exemplo)				
1)					
2)					
:					

*** S: sim; N: não; N/A: não se aplica.**

Cidade, (DD) de (MM) de (AAAA)

Oficial responsável

Assinatura Comandante

ANEXO G

MODELO DE VERIFICAÇÃO DE EFETIVIDADE

MINISTÉRIO DA DEFESA

EXÉRCITO BRASILEIRO

OM

RELATÓRIO DE VERIFICAÇÃO DA EFETIVIDADE SOBRE OS SERVIÇOS DE REDES DA OM XXX

1. SÍNTESE:

(Resumo informativo sobre o corpo do documento explicitando os seus pontos principais de modo a esclarecer rapidamente às autoridades sobre o seu teor)

2. OBJETIVO:

(Descrição do objetivo da auditoria e, se necessário for, de objetivos secundários ou específicos)

3. PERÍODO DA VERIFICAÇÃO:

(período em que a auditoria foi realizada)

4. EQUIPE RESPONSÁVEL:

(lista do pessoal que executou a auditoria e as respectivas atribuições)

5. METODOLOGIA ADOTADA:

(Método adotado para executar a verificação. O método mais simples é o da conferência da conformidade baseada em listas de verificação. Outros métodos; tais como análise de **logs**, entrevistas, questionários, simulações, análise de programa fonte etc; variarão conforme a necessidade e a capacitação do pessoal envolvido)

6. OBJETO:

(Elemento(s) sobre o(s) qual(is) a verificação será focada)

7. CONTEXTO:

(descrição sumária sobre o ambiente verificado, esclarecendo sobre serviços, **hardware**, **software**, infra-estruturas e pessoal relevante)

8. FATOS RELEVANTES:

(descrição detalhada dos fatos relevantes no que diz respeito à conformidade entre as ações implementadas e as recomendadas ou estabelecidas e, se necessário for, com subdivisões por assunto; comentários dos auditores sobre as causas e conseqüências do que foi constatado; e as recomendações pertinentes)

9. CONCLUSÃO:

(A conclusão deve ser objetiva e, preferencialmente do tipo resumo, ou seja, destacando pontos principais e as recomendações)

Local, data

Assinatura do responsável pela verificação

10. PARECER:

(parecer da autoridade competente aprovando o relatório ou não e o despacho correspondente)

CLASSIFICAÇÃO

ANEXO H

MODELO DE NORMA DE GERENCIAMENTO DA SEGURANÇA DE REDE

MINISTÉRIO DA DEFESA

EXÉRCITO BRASILEIRO

OM

"NORMAS PARA GERENCIAMENTO DA SEGURANÇA DA INFORMAÇÃO DA REDE DE ..... DA OM"

1. FINALIDADE

(Deve-se transcrever a finalidade do documento, por exemplo: "A finalidade desta norma é estabelecer as regras para o gerenciamento da segurança da informação na rede de computadores e de comunicações da OM XX".)

2. OBJETIVOS

(Devem-se transcrever os objetivos a serem atingidos pela aplicação da norma e que, em conjunto, cumpram a finalidade estabelecida.)

3. CONCEITOS E PRESSUPOSTOS BÁSICOS

(Conceitos: devem-se transcrever neste item as terminologias específicas relacionadas ao uso e gerência da rede para facilitar o entendimento do documento. Pressupostos: item opcional, caso se julgue necessário estabelecer que, para aplicação das Instruções, certas condições devem ser previamente atendidas.)

(Devem-se transcrever todas as regras de segurança julgadas necessárias e, se a complexidade do documento assim o exigir, separar grupos de regras em categorias, como ocorre nestas Instruções.)

a. Regras Gerais (regras de segurança de caráter geral e voltadas para medidas de segurança dos dados, informações e conhecimentos armazenados, processados ou disseminados nos enlaces ou equipamentos da rede);

b. Gerenciamento da Rede (regras de segurança relativas às ações de gerência da rede, ou seja, monitoração e adequação de parâmetros referentes às áreas de configuração, desempenho, falhas e contabilização; considerando que pode haver casos em que estas regras devam ser tratadas como informação classificadas, é possível que este item gere um documento a parte).

CLASSIFICAÇÃO
CLASSIFICAÇÃO

1) Configuração dos Privilégios para administração da rede

1.1) Contas (regras relativas à concessão, configuração, suspensão e verificação de segurança de senhas de acesso à rede);

1.2) Senhas (regras relativas às configurações para escolha, periodicidade e expiração de senhas);

1.3) Configuração de privilégios (regras relativas às configurações dos privilégios de usuários e grupos e o controle de acesso);

1.4) Inventário da rede (regras relativas ao controle do inventário do **software** e **hardware** da rede);

1.5) Registro de operações (regras relativas aos registros das operações ocorridas nos sistemas da rede)

1.6) Registros de violações (regras relativas ao registro das violações de segurança ocorridas na rede);

1.7) Acesso Remoto para Administração (regras relativas à configuração do serviço de conexão remota para fins administração da rede);

2) Serviços, Sistemas, Aplicativos específicos de segurança (regras relativas aos serviços, sistemas e aplicativos específicos de segurança, por exemplo f**irewall**, antivírus etc;)

2.1) **Firewall** (subtítulo referente às regras de segurança do **firewall**) ;

2.2) Sistema de Detecção a Intrusão (subtítulo referente às regras de segurança do sistema de detecção de intrusão);

2.3) Aplicações de Criptografia (subtítulo referente às regras de segurança de aplicações de criptografia);

2.4) Uso de Certificados Digitais (subtítulo referente às regras de para a gestão de certificados digitais);

3) Códigos maliciosos (subtítulo referente às regras de segurança de uso e configuração do serviço de detecção de códigos maliciosos);

4) Documentação de Sistemas (regras de segurança relativas à guarda e proteção das documentações dos sistemas em funcionamento na rede).

c. Segurança dos Serviços, Sistemas, Aplicativos e Sistemas Operacionais de Rede (regras de segurança referentes aos procedimentos de instalação, configuração e uso de: serviços, tais como correio eletrônico ou WEB; sistemas corporativos específicos do Exército; aplicativos de uso geral, tais como suítes de escritório; sistemas operacionais de rede).

1) Dos Serviços de Rede (subtítulo referente aos serviços);

2) Dos Sistemas Aplicativos (subtítulo referente aos sistemas corporativos);

3) Dos Aplicativos de Rede (subtítulo referente aos **softwares** aplicativos);

4) Dos Sistemas Operacionais de Rede (subtítulo referente aos sistemas operacionais utilizados).

CLASSIFICAÇÃO

CLASSIFICAÇÃO

d. Segurança do **Hardware** (regras de segurança referentes aos procedimentos de instalação, configuração e uso de computadores servidores, computadores de uso específico, computadores de uso geral, periféricos de rede, equipamentos de interligação de rede (roteadores, **switches**, **hubs**, modem, repetidores).

1) Computadores servidores;

2) Computadores de uso específico;

3) Computadores de uso geral;

4) Periféricos de rede;

5) Equipamentos de interligação de rede;

6) Outros equipamentos.

e. Segurança da Infra-estrutura de Rede (regras de segurança relativas às estruturas de: interligação lógica e seus elementos constituintes, tais como cabeamentos, dutos, documentação da instalação (descrição da rede, plantas etc) cabeamentos; e alimentação elétrica, e seus elementos constituintes, tais como fiação elétrica, dutos, quadros de distribuição, estabilizadores, **nobreak** etc)

1) Infra-estruturas lógicas;

2) Infra-estrutura de alimentação elétrica.

f. Segurança das Áreas e Instalações (regras de segurança relativas ao controle de acesso e a adequação das áreas e instalações onde se encontram equipamentos críticos da rede);

g. Contingência (regras de segurança relativas às medidas de contingência para a rede);

1) **Backup** (regras de sobre produção, armazenamento, teste, atualização, substituição e descarte de cópias de segurança no nível gerencial);

2) Plano de Contingência (descrição do plano de contingência da rede - pode requerer um documento separado).

h. Segurança do Pessoal (regras de segurança relativas aos aspectos de sensibilização e treinamento do pessoal que lida com as redes nos níveis gerencial e de manutenção).

i. Documentação de Sistemas (regras de segurança relativas à guarda e proteção das documentações dos sistemas em funcionamento na rede).

5. RESPONSABILIDADES

(Devem-se transcrever as obrigações de cada seção/assessoria/função da OM envolvida com a aplicação das normas de segurança.)

6. PRESCRIÇÕES DIVERSAS

(Deve-se fazer uso deste item, caso existam particularidades do contexto da OM que não se enquadrem nos itens anteriores, mas que sejam julgados

importantes para a norma.)

Cidade, (DD) de (MM) de (AAAA)

Assinatura Comandante

CLASSIFICAÇÃO