MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
SECRETARIA-GERAL DO EXÉRCITO

Boletim do Exército

Nº 09/2007

Brasília - DF, 2 de março de 2007.

BOLETIM DO EXÉRCITO
Nº 09/2007
Brasília - DF, 2 de março de 2007.

ÍNDICE

1ª PARTE
LEIS E DECRETOS

Sem alteração.

2ª PARTE
ATOS ADMINISTRATIVOS

COMANDANTE DO EXÉRCITO

DEPARTAMENTO-GERAL DO PESSOAL

DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA

3ª PARTE
ATOS DE PESSOAL

ATOS DO PODER EXECUTIVO

MINISTÉRIO DA DEFESA

SECRETARIA DE ORGANIZAÇÃO INSTITUCIONAL

COMANDANTE DO EXÉRCITO

SECRETARIA-GERAL DO EXÉRCITO

4ª PARTE
JUSTIÇA E DISCIPLINA

Sem alteração.

1ª PARTE
LEIS E DECRETOS

Sem alteração.

2ª PARTE
ATOS ADMINISTRATIVOS

COMANDANTE DO EXÉRCITO

PORTARIA Nº 074, DE 23 DE FEVEREIRO DE 2007.

Aprova o Plano de Inspeções e Visitas do Exército para o primeiro semestre de 2007, e dá outras providências.

O **COMANDANTE DO EXÉRCITO**, no uso das atribuições que lhe conferem o art. 4º da Lei Complementar nº 97, de 9 de junho de 1999, e o inciso XIV do art. 20 da Estrutura Regimental do Comando do Exército, aprovada pelo Decreto nº 5.751, de 12 de abril de 2006, e de acordo com que propõe o Estado-Maior do Exército, resolve:

Art. 1º Aprovar o Plano de Inspeções e Visitas do Exército (PIV) para o primeiro semestre de 2007, que com esta baixa.

Art. 2º Determinar que:

I - na execução do PIV para o primeiro semestre de 2007, sejam respeitados os limites impostos pela Administração Federal; e

II - o Estado-Maior do Exército e os órgãos de direção setorial adotem, em suas áreas de competência, as providências decorrentes.

Art. 3º Estabelecer que esta Portaria entre em vigor na data de sua publicação.

DEPARTAMENTO-GERAL DO PESSOAL

PORTARIA Nº 019-DGP, DE 23 DE FEVEREIRO DE 2007.

Fixa as vagas para o Estágio de Instrução e de Preparação para Oficiais Temporários (EIPOT), em 2007.

O **CHEFE DO DEPARTAMENTO-GERAL DO PESSOAL**, no uso da atribuição que lhe foi conferida pelo art. 8º das Instruções Gerais para a Convocação, Estágios, as Prorrogações de Tempo de Serviço, as Promoções e o Licenciamento dos Integrantes da Reserva de 2ª Classe (IG 10-68), aprovadas pela Portaria do Comandante do Exército nº 462, de 21 de agosto de 2003, resolve:

Art. 1º Fixar o número de vagas para o Estágio de Instrução e de Preparação para Oficiais Temporários (EIPOT) em 2007, de acordo com o quadro abaixo:

RM	VAGAS – ARMA / QUADRO / SERVIÇO							TOTAL
	INF	CAV	ART	ENG	COM	QMB	INT	
1ª	10	06 (a)	04	05 (b)	03	05	05	38
2ª	12	04 (c)	03	07 (d)	04 (e)	09 (f)	10 (g)	49
3ª	12	06	06	08	06	04	14	56

RM	VAGAS – ARMA / QUADRO / SERVIÇO							TOTAL
	INF	CAV	ART	ENG	COM	QMB	INT	
4ª	05	00	02	02 (h)	00	00	04 (i)	13
5ª	18	00	06	03	00	09(j)	11	47
6ª	03	00	00	00	00	00	00	03
7ª	01	00	03	04 (l)	02 (m)	00	05 (n)	15
8ª	12	00	00	00	00	00	00	12
9ª	04	07 (o)	00	00	00	00	00	11
10ª	00	00	00	00	00	00	00	00
11ª	05	00	04	00	00	00	00	09
12ª	33	00	00	00	00	00	07(p)	40
TOTAL	115	23	28	29	15	27	56	293

Legenda:

(a) 04 (quatro) vagas para a 1ª RM, 02 (duas) vagas para a 12ª RM;
(b) 03 (três) vagas para a 1ª RM, 02 (duas) vagas para a 12ª RM;
(c) 02 (duas) vagas para a 2ª RM, 02 (duas) vagas para a 4ª RM/4ª DE;
(d) 03 (três) vagas para a 2ª RM, 04 (quatro) vagas para a 9ª RM;
(e) 03 (três) vagas para a 2ª RM, 01 (uma) vaga para a 4ª RM/4ª DE;
(f) 06 (seis) vagas a 2ª RM, 03 (três) vagas para a 4ª RM/4ª DE;
(g) 07 (sete) vagas para a 2ª RM, 03 (três) vagas para 11ª RM;
(h) 02 (duas) vagas para a 12ª RM;
(i) 04 (quatro) vagas para a 11ª RM;
(j) 07 (sete) vagas para a 5ª RM/5ª DE, 02 (duas) vagas para a 11ª RM;
(l) 02 (duas) vagas para 7ª RM, 02 (duas) vagas para a 12ª RM;
(m) 01 (uma) vaga para a 7ª RM/DE, 01 (uma) vaga para 12ª RM;
(n) 01 (uma) vaga a 7ª RM/7ª DE, 01 (uma) vaga para a 6ª RM e 03 (três) vagas para 11ª RM;
(o) 05 (cinco) vagas para a 9ª RM, 02 (duas) vagas para a 11ª RM; e
(p) 06 (seis) vagas a 12ª RM, 01 (uma) vaga para a 8ª RM/8ª DE;

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

DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA

PORTARIA Nº 002-DCT, DE 31 DE JANEIRO DE 2007

Aprova as Instruções Reguladoras Sobre Análise de Riscos para Ambientes de Tecnologia da Informação do Exército Brasileiro - IRRISC (IR 13 -10).

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 Análise de Riscos para Ambientes de Tecnologia da Informação do Exército Brasileiro - IRRISC (IR 13 -10).

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

INSTRUÇÕES REGULADORAS SOBRE ANÁLISE DE RISCOS PARA AMBIENTES DE TECNOLOGIA DA INFORMAÇÃO DO EXÉRCITO BRASILEIRO – IRRISC (IR 13-10)

ÍNDICE DOS ASSUNTOS

Anexos:

INSTRUÇÕES REGULADORAS SOBRE ANÁLISE DE RISCOS PARA AMBIENTES DE TECNOLOGIA DA INFORMAÇÃO DO EXÉRCITO BRASILEIRO - IRRISC (IR 13-10)

TÍTULO I
DAS GENERALIDADES

Art. 1º As presentes instruções, elaboradas em observância aos art. 15, 16 e ao inciso VI do art. 31 das Instruções Gerais de Segurança da Informação para o Exército Brasileiro (IG 20-19), têm por finalidade regular as condições para o emprego de uma metodologia básica de avaliação de risco a ser aplicada nas OM do Exército Brasileiro, na área de segurança da informação.

Art. 2º São objetivos destas Instruções:

I - Gerar critérios para tomada de decisão sobre investimentos em segurança da informação.

II - Prover referenciais doutrinários sobre segurança da informação no que tange à gestão de riscos.

III - Orientar a execução de processos de análises de risco qualitativas nos ambientes de sistemas de informação do Exército.

IV - Prover um mecanismo útil na aplicação de processos de auditoria de segurança da informação.

V - Estabelecer as principais responsabilidades no processo de análise de riscos da informação no Exército.

TÍTULO II
DAS DEFINIÇÕES BÁSICAS

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

I - SISTEMA DE INFORMAÇÃO (SI) - Sistema que obtenha, produza, armazene, processe e transmita informações. Para aplicação destas IR, deve ser considerado que, em sua forma mais simples, um SI pode ser constituído de um sistema corporativo informatizado, assim como, em sua forma mais complexa, um SI pode ser constituído de um conjunto de redes de computadores e de comunicação, com seus **softwares**, equipamentos, usuários e processos administrativos.

II - RECURSO DE UM SISTEMA DE INFORMAÇÃO - são todos os elementos que podem ser considerados como meios para viabilizar a constituição e o funcionamento de um Sistema de Informação (SI), ou seja, a sua capacidade de obter, processar, armazenar e transmitir informações. Exemplos: computadores e seus periféricos, **softwares** de aplicação em rede, interfaces de rede, equipamentos de interligação dos nós da rede, elementos da infra-estrutura de cabeamento lógico e infra-estrutura de alimentação elétrica de rede etc.

III - RECURSO OU DADO CRÍTICO – recurso de um sistema de informação ou dado cuja violação física ou lógica implica em uma violação de segurança com repercussões significativas, no mínimo, para a OM a que pertence o recurso ou o dado.

IV - IMPACTO - efeito negativo sobre informações ou recursos de um SI em razão de uma violação de segurança.

V - VULNERABILIDADE - ponto fraco existente em um SI que, se explorado, pode vir a causar um impacto ao sistema. Por exemplo, uma vulnerabilidade comum é a não existência ou não atualização de **softwares** antivírus em computadores.

VI - RISCO - possível evento que representa uma ameaça em potencial aos recursos de um sistema de informação e que pode se concretizar por meio da exploração de uma ou mais vulnerabilidades do sistema, causando impacto nos objetivos do SI e, por conseguinte, à missão das OM que dele dependam. Por exemplo, a possibilidade de uma instalação de um programa espião para gravação de informações digitadas, como nomes de usuários e senhas, é um risco que computadores correm.

VII - ANÁLISE DE RISCOS - análise realizada sobre os recursos de um sistema de informação cuja primeira etapa é descobrir quais os recursos críticos desse sistema e, em relação a esses recursos, determinar: as vulnerabilidades de segurança; os riscos que o sistema corre; os impactos que a missão da OM pode sofrer se a segurança for comprometida; as chances de ocorrerem comprometimentos de segurança; e a magnitude dos riscos reconhecidos. Essa análise pode ser quantitativa ou qualitativa dependendo da metodologia empregada.

VIII - ESTIMATIVA DO VALOR DO RISCO - processo que associa um valor ao risco identificado na análise de riscos.

IX - MATRIZ DE RISCOS - Matriz que relaciona uma associação de valores de impacto e chances de concretização de uma ameaça com um valor de risco.

X - GESTÃO DE RISCOS - processo que visa manter os riscos em patamares aceitáveis para o SI a que é aplicado e que é realizada por meio dos seguintes processos: análise de riscos; concepção e aplicação das medidas de eliminação ou abrandamento do risco; e monitoração do risco no decorrer do tempo.

XI - IDENTIFICAÇÃO DO RISCO - processo que visa identificar os riscos que um sistema de informações está correndo.

XII - ESPECIALISTA DE ÁREA - especialista em tecnologia ou produto utilizado em um sistema de informação, seja por vivência prática na operação ou por possuir cursos específicos ou, ainda, por formação acadêmica de graduação ou pós-graduação na área da qual se necessita atuar.

XIII - ANÁLISE QUALITATIVA DE RISCOS - análise de riscos que estima o valor dos riscos por meios não estatísticos, ou seja, por estimativas fornecidas por especialistas de área.

XIV - ANÁLISE QUANTITATIVA DE RISCOS - análise de riscos que conta com dados em quantidade e qualidade tal que seja possível utilizar técnicas estatísticas para calcular e interpretar o risco.

TÍTULO III
DO PROCESSO DE ANÁLISE DE RISCOS

CAPÍTULO I
DO PROCESSO DE ANÁLISE DE RISCOS

Art. 4º Para fins de aplicação destas Instruções, o processo de análise de riscos é definido como a seguir:

I - DESIGNAÇÃO DO PESSOAL - escolha, designação e credenciamento do pessoal envolvido no processo.

II - PLANEJAMENTO DA ANÁLISE DE RISCOS - fase em que são estabelecidas as ações a serem realizadas para identificar os riscos de um sistema de informação.

III - CARACTERIZAÇÃO DO SISTEMA A SER ANALISADO - identificação do escopo de abrangência do sistema; suas funções e objetivos; seus recursos e dados críticos; as pessoas, grupos ou organizações responsáveis pela sua gestão e manutenção; os controles já existentes para minimizar os riscos; a documentação do sistema e as normas de segurança que estejam relacionadas ao seu uso.

IV - IDENTIFICAÇÃO DAS VULNERABILIDADES E DOS RISCOS - identificação das fragilidades do SI sob análise e dos riscos associados.

V - ESTIMATIVA DAS CHANCES DA CONCRETIZAÇÃO DOS RISCOS - processo em que são estimadas as chances ou as probabilidades de ocorrerem eventos que explorem as vulnerabilidades do sistema e redundem na concretização dos riscos identificados.

VI - ANÁLISE DE IMPACTOS - estimativa dos impactos que podem ocorrer devido a concretização dos riscos identificados.

VII - IDENTIFICAÇÃO DOS RISCOS - processo no qual, a partir dos valores estimados para impacto e as chances da concretização de uma ameaça, se constata qual o valor correspondente do risco, consultando-se, para isso, a Matriz de Risco.

VIII - RELATO DA SITUAÇÃO - fase em que são registradas em documento as informações que consolidam o que foi constatado com a análise de riscos e que lista as recomendações necessárias para lidar com os riscos.

Art. 5º O processo de análise de riscos é representado na figura 1.

CAPÍTULO II
DA DESIGNAÇÃO E CREDENCIAMENTO DE PESSOAL

Art. 6º O pessoal envolvido no processo deverá ser selecionado e credenciado de acordo com o prescrito nas Instruções Gerais para Salvaguarda de Assuntos Sigilosos e nas Normas para Concessão de Credencial de Segurança ou instrumento normativo e legal o valha, além de outras legislações ou documentos normativos internos que se façam necessários.

Parágrafo único. O Comandante, assessorado pelo seu Estado-Maior, identificará os assuntos que, em razão de um processo de análise de riscos, possam ser expostos aos aplicadores do processo e, em conseqüência, poderá requerer que os responsáveis pela análise assinem um termo de compromisso e manutenção de sigilo, conforme modelo (ou adaptação, conforme o caso) disponível nas Instruções Gerais para Salvaguarda de Assuntos Sigilosos.

Art. 7º O pessoal técnico designado para aplicar o processo de análise de riscos deverá ser escolhido conforme o perfil técnico necessário.

Parágrafo único. O Comandante da OM onde será realizada a análise de riscos deverá designar um militar que fará os levantamentos iniciais para identificar o perfil técnico necessário às situações específicas a serem abordadas no processo de análise e, assim, tornar precisa a indicação dos técnicos que executarão o processo.

CAPÍTULO III
DO PLANEJAMENTO DA ANÁLISE DE RISCOS

Art. 8º Para o planejamento e execução da análise de riscos, devem ser estabelecidas, no mínimo, as seguintes responsabilidades:

I - gerente ou coordenador do processo;

II - integrantes da equipe que executará o processo e que sejam representantes das áreas diretamente inseridas no escopo da análise de riscos a ser aplicada.

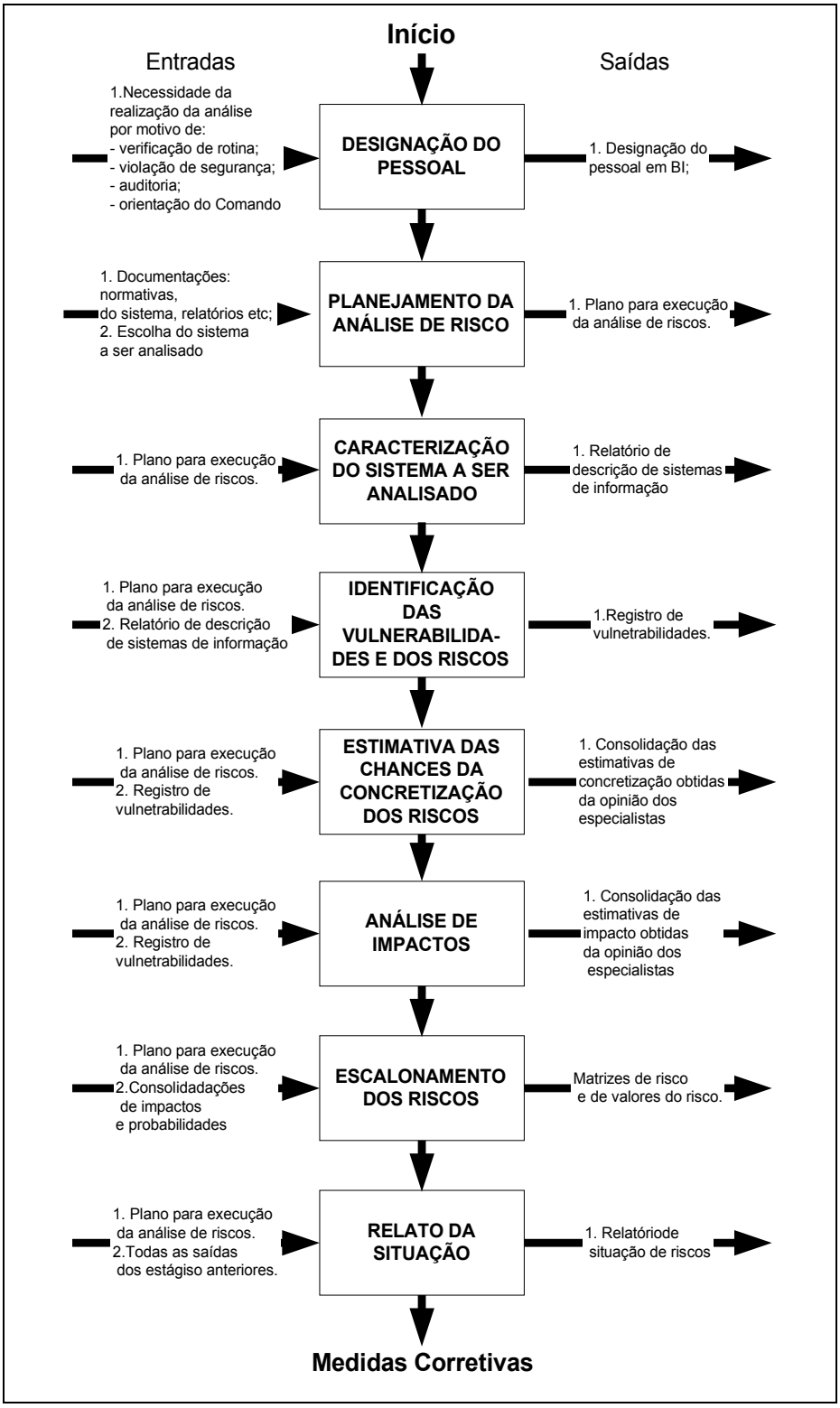

Fig nº 1 - Processo de Analise de Riscos

Art. 9º Para subsidiar a elaboração do planejamento da análise de riscos, devem ser levados em consideração todos os documentos que sejam reconhecidos como relevantes ao processo. A lista básica recomendada é a seguinte:

I - documentação relativa à segurança da informação ou contra-inteligência que esteja relacionada ao escopo escolhido para a análise (Instruções, Manuais, Políticas, Normas, Plano de Segurança Orgânica, demais publicações internas julgadas pertinentes etc);

II - documentação normativa de segurança aplicável ao Exército, mas de origem externa e que esteja relacionada ao escopo escolhido para a análise;

III - documentação técnica de produtos tecnológicos empregados no escopo escolhido para análise de riscos;

IV - documentos administrativos, técnicos ou de outra natureza e que estejam relacionados ao escopo escolhido para a análise;

V - relatórios ou outros documentos onde estejam registrados os resultados de análises de riscos, ou processo similares, que tenham sido realizados anteriormente no escopo onde será desenvolvida a análise de riscos em planejamento;

VI - literaturas acadêmicas e outras literaturas especializadas.

Parágrafo único. Caso existam relatórios de análises de riscos anteriores, os critérios adotados para interpretar os valores do risco devem ser analisados para se verificar se as margens anteriores continuam válidas ou devem ser revistas na análise em andamento.

Art. 10. As técnicas a serem empregadas para a elaboração do planejamento devem ser estabelecidas conforme as particularidades das OM em que a análise é planejada e aplicada, no entanto, é recomendável que sejam empregadas, no mínimo, práticas de reuniões entre os gerentes e os representantes das áreas envolvidas.

Art. 11. O planejamento da análise de riscos deve estabelecer as tarefas relativas a cada fase do processo definido no art. 4º.

Art. 12. O planejamento da análise de riscos deve ser consolidado em um documento que deverá seguir o modelo descrito no ANEXO A.

CAPÍTULO IV
DA EXECUÇÃO DO PLANO

Seção I
Da Caracterização do Sistema a ser Analisado

Art. 13. O gerente ou coordenador do processo deverá fazer o levantamento prévio das características do sistema. Devem ser levadas em consideração, com especial cuidado, as seguintes categorias:

I - dados e informações;

II - processos que definem o trâmite dos dados e informações no(s) sistema(s) de informação(ões);

III - serviços automatizados;

IV - **software**;

V - **hardware**;

VI - **hardware** de conexão à outras redes;

VII - infra-estrutura de cabeamento de rede;

VIII - infra-estrutura de alimentação elétrica (equipamentos e instalações)

IX - pessoal responsável pela gerência, manutenção ou uso final do sistema;

X - conjunto de documentos técnicos ou normativos para uso, gerência e segurança do sistema.

Art. 14. Para obtenção das informações a respeito da caracterização do sistema, o gerente ou coordenador do processo deverá lançar mão das técnicas que julgar adequadas em relação às características do ambiente do sistema. As técnicas básicas são:

I - estudo da documentação do sistema;

II - entrevistas individuais com gerentes e usuários do sistema;

III - reuniões com gerentes e usuários do sistema.

Art. 15. As características do sistema devem ser registradas em relatório conforme modelo constante do ANEXO B.

Seção II
Da Identificação das Vulnerabilidades

Art. 16. O processo de busca da identificação das vulnerabilidades deve considerar todos os aspectos que compõe o sistema.

Art. 17. Para fins de organização e facilitação do trabalho de identificação de vulnerabilidades, devem ser estabelecidas algumas áreas que norteiem o levantamento. A escolha das áreas é decorrente das características de cada sistema, sendo que, dentre as que devem ser levadas em consideração no ambiente dos SI do Exército, estão:

I - dados;

II - sistemas corporativos;

III - **softwares**;

IV - serviços de rede;

V - **hardware** computacional;

VI - **hardware** de interligação entre redes;

VII - **hardware** de comunicação;

VIII - infra-estrutura de rede de dados;

IX - infra-estrutura de rede de comunicação;

X - infra-estrutura de rede de alimentação elétrica;

XI - áreas e instalações dos componentes do sistema;

XII - condições ambientais (vulnerabilidades oriundas de condições naturais do ambiente e que possam ameaçar o SI);

XIII - pessoal usuário e gestor do sistema;

XIV - pessoal externo (parceiros ou possíveis intrusos – "**hackers**");

XV - processos administrativos relacionados ao sistema;

XVI - normas de segurança vigentes;

XVII - projetos de SI, abrangendo desde sua concepção até sua implementação.

XVIII - processos contratuais ou de outra natureza que envolvam parcerias ou trabalhos conjuntos com outras organizações ou empresas.

Art. 18. Para cada área ou grupos de áreas escolhidas ou estipuladas, deve-se registrar as vulnerabilidades encontradas e as ações necessárias para explorá-las. No ANEXO C, consta um modelo de tabela para tal registro.

Art. 19. As técnicas que devem ser utilizadas para preenchimento das tabelas que registrarão as vulnerabilidades são diversas, sendo as básicas a serem utilizadas nos sistemas de informação do Exército:

I - REUNIÕES DE **BRAINSTORM**. O gerente ou condutor do processo dirigirá uma discussão na qual gerentes, especialistas, usuários, além de outros integrantes da organização poderão, sem críticas dos demais participantes, falar sobre o que identificam como vulnerabilidades.

Essas vulnerabilidades são registradas e, posteriormente o gerente fará a sua consolidação com o aval do grupo. As fases da aplicação da técnica de **brainstorm** são:

a) escolha do condutor do processo (preferencialmente o militar mais antigo, de modo a melhor controlar as discussões);

b) escolha das categorias de vulnerabilidades as quais serão trabalhadas;

c) escolha dos participantes (escolhidos conforme seu conhecimento no sistema de informação sob foco ou na área de conhecimento necessária);

d) estabelecimento de quem fará as anotações das idéias que serão geradas;

e) realização de reunião na qual a técnica será aplicada;

f) explicação da técnica para os participantes;

g) se o grupo for considerado numeroso pelo condutor dos trabalho e as áreas a serem abordadas forem estanques, devem ser formados grupos distintos com seus relatores;

h) o tempo de geração de idéias deve ser estipulado e o processo ser iniciado e rigorosamente encerrado quando do término do tempo (o tempo a ser escolhido variará conforme a complexidade do tempo e o número de pessoas, um exemplo é que um grupo de cinco pessoas, tratando de segurança física poderia gerar idéias por um período entre 30 e 50 minutos);

i) TODAS as idéias devem ser anotadas, conforme modelo constante do ANEXO D, por mais absurdas que possam parecer a princípio (essa observação é extremamente importante);

j) as idéias anotadas devem ser passadas a limpo, no mesmo documento representado no ANEXO D, atentando-se para que a redação seja clara e não deturpe a idéia original e o título seja modificado para "VERSÃO CONSOLIDADA DO **BRAINSTORM";**

k) o grupo deve estudar a redação "limpa" e eliminar redundâncias e idéias consideradas, após discussões do grupo, sem relevância;

l) o resultado definitivo deve ser registrado nas tabelas de vulnerabilidades, representadas no ANEXO C.

II - REVISÃO CRÍTICA DE DOCUMENTAÇÃO. Pesquisa e análise dos processos e procedimentos documentados, relativos ao escopo analisado, e de documentações relativas a outras análises de risco já realizadas, devendo ser dada especial atenção às medidas de tratamento do risco que foram estabelecidas e o seu cumprimento. A revisão tem como objetivo descobrir informações sobre características importantes do sistema e que podem gerar algum tipo de vulnerabilidade. As possíveis vulnerabilidades devem ser anotadas e verificadas na realidade e, se confirmadas, devem ser registradas nas tabelas de vulnerabilidades, cujo modelo está no ANEXO C.

III - LISTAS DE VERIFICAÇÃO. Esta técnica faz uso de listagens onde estão registrados, em geral, em forma de perguntas, os estados em que devem estar as informações ou recursos informacionais críticos. O objetivo desta técnica é, por meio da aplicação da lista de verificação, verificar se as vulnerabilidades aventadas pelas perguntas se confirmam. Em caso positivo, as vulnerabilidades encontradas devem ser registradas nas tabelas de vulnerabilidades, representadas no ANEXO C. Exemplos dessas listas estão publicados na Internet pelo portal do Exército e na Intranet pela página do CITEx.

IV - TÉCNICA DE **DELPHI**. Esta técnica é baseada na busca de um consenso entre especialistas de área (conforme conceituado nestas Instruções) que opinam, por meio de questionários, sobre o escopo analisado. Esta técnica tem por objetivo estimar as chances de uma vulnerabilidade ser explorada e ocorrer uma violação de segurança ou estimar o impacto que pode advir da concretização de uma ou mais ameaças que explorem vulnerabilidades. O modelo de questionário está representado no ANEXO E. As etapas de aplicação da técnica são os seguintes:

a) um grupo de especialistas no tema a ser estudado é formado e um coordenador ou condutor é escolhido.

b) o coordenador formula um questionário com perguntas que devem ser respondidas de forma objetiva, de acordo com opções ou valores referente a uma escala, como, por exemplo, números, datas, porcentagem etc.

c) envia-se o questionário para os especialistas e solicita-se a eles as respostas acompanhadas de justificativas.

d) após a recuperação dos questionários respondidos e justificados, procede-se um tratamento estatístico dos dados para obtenção de tendências centrais e variâncias (é provável que, na maioria das ocorrências, não haja dados em número suficiente para tratamento estatístico, assim, o condutor do processo observará as tendências das escolhas feitas pelos especialistas e julgará se é possível um tratamento dos dados apenas pelos valores médios).

e) caso não haja uma clara convergência das respostas, procede-se uma segunda rodada de aplicação dos mesmos questionários, acompanhados dos estudos estatísticos ou ajustes possíveis que foram realizados e de um sumário das justificativas para cada pergunta. Solicita-se, então, que os respondentes, considerando as justificativas dos demais e as tendências reveladas nos estudos, revejam ou não a sua posição.

f) repetem-se os procedimentos 4 e 5 até que haja uma convergência de opiniões em torno de valores médios;

g) caso a não ocorra a convergência aludida, o condutor do processo deverá estudar a possibilidade de refazer o estudo modificando a abordagem.

V - ENTREVISTAS. Contato direto do gerente ou coordenador do plano com quem detém as informações necessárias. Esta técnica tem por objetivo melhor caracterizar pontos do sistema. As anotações resultantes da entrevista deve compor o conteúdo do relatório de descrição do sistema de informação constante do ANEXO B.

VI - VULNERABILIDADES NOTIFICADAS PELO FABRICANTE. Pesquisa sobre vulnerabilidades notificadas pelos fabricantes dos componentes do SI analisado. Esta técnica visa identificar vulnerabilidades específicas de produtos utilizados no SI e seus resultados devem ser anotados no registro de vulnerabilidades constante do ANEXO C.

VII - PESQUISA DE VULNERABILIDADES NOTIFICADAS. Pesquisa nas bases de dados de entidades especializadas em vulnerabilidades de SI e, caso existam, bases de dados internas e que contenham lições aprendidas sobre o assunto. Esta técnica tem o mesmo objetivo da técnica anterior e deve receber o mesmo tratamento.

VIII - IDENTIFICAÇÃO DE VULNERABILIDADES POR USO DE **SOFTWARES** DE APOIO. Esta técnica visa identificar a utilização de ferramentas automatizadas de gerência de rede ou específicas de busca de vulnerabilidades.

Art. 20. O resultado desta fase do processo de execução da análise de riscos é um conjunto de tabelas com as informações sobre as vulnerabilidades encontradas. Esse conjunto deverá compor o relatório de situação cujo modelo se encontra no ANEXO F.

Seção III
Da Identificação do Risco

Art. 21. A identificação do risco visa caracterizar o evento que, em decorrência da exploração de uma vulnerabilidade, pode redundar em um impacto negativo ao SI. Logo, essa identificação está diretamente ligada ao processo de identificação das vulnerabilidades.

Art. 22. Como etapa inicial do processo para a identificação dos riscos, é necessária a sua categorização. A divisão dos escopos possíveis em que os riscos devem ser abordados visa facilitar o processo da análise de riscos.

Parágrafo único. As categorias de que tratam este artigo devem ser escolhidas conforme as particularidades de cada ambiente em que a análise de riscos é aplicada, mantendo sempre a coerência com as áreas escolhidas na identificação de vulnerabilidades. Como referencial inicial, deve-se levar em conta as seguintes categorias:

I - TÉCNICOS - esta categoria abrange as áreas abordadas nos incisos I a XI do art. 17.

II - HUMANOS - categoria que leva em consideração os riscos à informação ou aos recursos informacionais advindos de atos humanos, abrangendo os incisos XIII e XIV do art. 17.

III - AMBIENTAIS - categoria referente aos riscos ambientais, ou seja, condições das instalações físicas e do ambiente no qual essas instalações se encontram, abrangendo o inciso XII do art. 17.

IV - ADMINISTRATIVOS - categoria que leva em consideração os riscos à informação ou aos recursos informacionais advindos da má condução ou definição de processos administrativos organizacionais, abrangendo o inciso XV e XVIII do art. 17;

V - PROJETOS - categoria que leva em consideração os riscos à informação ou aos recursos informacionais advindos das fases de planejamento e implementação de um projeto;

VI - EXTERNOS - categoria que leva em consideração os riscos à informação ou aos recursos informacionais advindos de fatores externos à atividade da OM em que a análise de riscos estiver sendo aplicada. Por exemplo, pode-se citar as mudanças de orientação, por parte do escalão superior, sobre determinado trabalho em andamento.

Art. 23. As técnicas passíveis de aplicação para identificar o risco são inúmeras, o que faz com que a escolha da técnica seja resultante das particularidades do ambiente analisado, assim como a experiência dos condutores do processo.

Parágrafo único. Considerando que o processo de identificação do risco pode ser executado concomitantemente com o processo de identificação das vulnerabilidades, as técnicas listadas para aquela fase do processo de execução do Plano podem ser usadas para identificação do risco.

Art. 24. Além da identificação do risco, é útil a identificação de outro elemento que é necessário para a percepção prévia de que um risco está por se concretizar. São os “sinais de advertência” ou “sintomas de risco” e que são identificados de maneira idêntica ao descrito na seção referente às vulnerabilidades. Após o registro desses "sintomas", o seu tratamento que deve ser tal qual fossem vulnerabilidades, ou seja, identificam-se os riscos associados e aplica-se o restante do processo como descrito nas seções a seguir. O modelo de registros de sintomas de risco está descrito no ANEXO G.

Seção IV
Da Estimativa das Chances da Concretização dos Riscos

Art. 25. A estimativa das chances ou probabilidade da concretização de um risco pode ser tratada tanto do ponto de vista qualitativo quanto da perspectiva quantitativa.

Parágrafo único. Nestas Instruções é enfatizado o aspecto qualitativo. A metodologia a ser empregada está descrita na seção VII.

Art. 26. Para aplicação destas Instruções, os valores recomendados como referência para a estimativa das probabilidades (p) estão dispostos na tabela 1.

Valor de (p) [escalas cardinal e ordinal]		**Descrição/Interpretações possíveis**
Cardinal	**Ordinal**	
7	**Sempre**	Ocorrerá todas as vezes.
6	**Freqüente**	Ocorre freqüentemente. Continuamente experimentado. Ocorre quase sempre.
5	**Provável**	Ocorrerá várias vezes. Ocorrência freqüente; é comum. Ocorre muitas vezes.
4	**Ocasional**	Ocorrerá pelo menos uma vez. Ocorrerá algum dia. Ocorrência esporádica.
3	**Remoto**	Improvável, mas poderá ocorrer. Raro, mas pode ser esperado. Pode ocorrer, porém não é provável.
2	**Improvável**	Improvável que ocorrerá. Pode ocorrer, porém é muito improvável.
1	**Extremamente Improvável**	Pode ocorrer, porém as chances são ínfimas.
0	**Nunca**	Certamente não ocorrerá.

Tabela 1: valores recomendados como referência para a estimativa das probabilidades (p)

Seção V
Da Análise de Impactos

Art. 27. A análise de impactos é um processo que visa associar um valor ao impacto (I) sobre os objetivos do SI decorrente de um risco que se concretize.

Art. 28. O valor a ser associado ao impacto dependerá das características do SI analisado. O escalonamento mais simples de valores é baixo, médio e alto, sendo que, para efeito de aplicação destas Instruções, recomenda-se o uso dos valores constantes da tabela 2.

Art. 29. A técnica básica para proceder a análise de impacto é a coleta das opiniões dos especialistas no escopo enfocado, sejam eles técnicos ou administradores, sobre o valor (conforme a escala previamente arbitrada) do impacto.

Valor de (I) [escalas cardinal e ordinal]		**Conseqüência estimada/Interpretações possíveis**
Cardinal	**Ordinal**	
6	**Inaceitável**	- Perda da informação ou dado sem chance de recuperação. - Indisponibilidade definitiva dos recursos informacionais (**hardware** e **software**) envolvidos. - Altíssima chance de perda de vidas para os recursos humanos envolvidos na missão. - Perda da confiança na Instituição pela sociedade.
5	**Grave**	- Destruição ou dano severo aos dados ou informações, ou, ainda, aos recursos informacionais (**hardware** e **software**), porém, com possibilidade de recuperação com custos financeiros e materiais inalcançáveis em prazo oportuno para cumprimento da missão. - Gera processo jurídico. - Mancha a imagem da Instituição.
4	**Crítico**	- Destruição ou dano severo aos dados ou informações, ou, ainda, aos recursos informacionais (**hardware** e **software**), porém, com poucas chances de recuperação em prazo oportuno para cumprimento da missão e a custos financeiros e materiais onerosos. - Pode gerar processo jurídico. - Pode manchar a imagem da Instituição.
3	**Mediano**	- Destruição ou dano aos dados ou informações, ou, ainda, aos recursos informacionais (**hardware** e **software**), porém, com grandes chances de recuperação em prazo oportuno para cumprimento da missão e a custos financeiros e materiais moderados. - Pode gerar processo jurídico. - Pode manchar a imagem da Instituição.
2	**Secundário**	- Destruição ou dano aos dados ou informações, ou, ainda, aos recursos informacionais (**hardware** e **software**), porém, com certeza de recuperação em prazo oportuno para cumprimento da missão e a custos financeiros e materiais baixos. - Gera processo administrativo. - Dificilmente atingirá a imagem da Instituição.
1	**Desprezível**	- Destruição ou dano aos dados ou informações, ou, ainda, aos recursos informacionais (**hardware** e **software**), porém, com certeza de recuperação em prazo oportuno para cumprimento da missão e a custos do emprego da manutenção orgânica. - Pode gerar processo administrativo. - Não atingirá a imagem da Instituição.
0	**Nulo**	- Destruição ou dano aos dados ou informações, ou, ainda, aos recursos informacionais (**hardware** e **software**), porém, com certeza de recuperação imediata ou a curtíssimo prazo e sem custos significativos.

Tabela 2: os valores recomendados como referência para a estimativa dos impactos (I)

Seção VI
Do Escalonamento dos Riscos

Art. 30. O escalonamento do risco visa estipular faixas de valores de risco para fins de sua interpretação.

Art. 31. Os possíveis valores associados ao risco variarão de acordo com os valores estipulados ou calculados para o impacto e a probabilidade de ocorrência de um risco.

Art. 32. Os valores calculados para o risco podem ser retirados de uma matriz, chamada matriz de risco, que é construída a partir dos valores de Impacto e Probabilidade de ocorrência.

Parágrafo único. A matriz de risco gerada pelos valores de referência para os valores de p e I recomendados nestas Instruções se encontra na figura 2. O ANEXO H retrata um exemplo de aplicação.

Seção VII
Da Análise de riscos Qualitativa

Art. 33. O processo de aplicação da análise de riscos qualitativa é como se segue:

I - Estima-se as chances de um risco se concretizar (p). Para essa estimativa são utilizados os pesos preestabelecidos na tabela 1.

§ 1º A escolha dos valores associados às probabilidades são totalmente arbitrários e dependem da experiência e juízo de valor daqueles que aplicarem a análise de riscos.

Probabilidade / Impacto	Nunca	Extremamente Improvável	Improvável	Remoto	Ocasional	Provável	Freqüente	Sempre
Inaceitável	T(0)	I (6)	I (12)	I (18)	I (24)	I (30)	I (36)	I (42)
Grave	T(0)	A(5)	A(10)	A(15)	A(20)	I (25)	I (30)	I (35)
Crítico	T(0)	M(4)	M(8)	M(12)	A(16)	A(20)	I (24)	I (28)
Médio	T(0)	T(3)	M(6)	M(9)	M(12)	M(15)	A(18)	A(21)
Secundário	T(0)	T(2)	T(4)	T(6)	M(8)	M(10)	A(12)	A(14)
Desprezível	T(0)	T(1)	T(2)	T(3)	T(4)	T(5)	M(6)	M(7)
Nulo	T(0)	T(0)	T(0)	T(0)	T(0)	T(0)	T(0)	T(0)

Figura 2: Matriz de valores de risco de referência para o método descrito nestas Instruções.
Legenda para o Risco: I- Intolerável ; A-Alto ; M-Médio ; B - Baixo ; T - Tolerável

§ 2º As técnicas que podem ser utilizadas para a escolha dos valores são: técnica de **Delphi**, caso se conte com mais de um especialista de área, ou entrevista com o(s) especialista(s) que opera(m) o sistema;

II - Estima-se o tipo de impacto sobre o escopo analisado (I). De forma análoga ao que ocorre na estimativa da probabilidade, é utilizada a tabela 2 para a escolha do valor impacto.

Parágrafo único. As técnicas que podem ser utilizadas para a escolha dos valores são as mesmas mencionadas para estimar as probabilidades.

III - A estimativa do valor do risco (R) é calculada pelo produto pxI, sendo que os valores possíveis de serem calculados podem ser retirados da matriz de valores de risco, conforme a figura 2.

IV - Após o cálculo dos valores possíveis para o risco, deve-se identificar na matriz de valores do risco, figura 2, qual o grau de severidade do risco, sendo as opções possíveis, conforme disposto nestas Instruções: I- Intolerável; A-Alto; M-Médio; B - Baixo; T - Tolerável.

V - A partir da identificação da posição que o valor do risco está na matriz de valores do risco, constata-se o seu grau de severidade. A síntese das informações a respeito da situação que envolve o risco é feita pela elaboração da Matriz de Riscos conforme modelo representado no ANEXO H. Os documentos onde as matrizes de riscos estiverem representadas devem ser organizadas conforme a categoria do risco. É extremamente importante ressaltar que a classificação do risco NÃO está associada aos valores numéricos em uma escala crescente, ou seja, pode-se ter um risco classificado como "Intolerável" cujo valor associado seja menor que um risco classificado como "Médio".

VI - A partir dos resultados das Matrizes de Riscos geradas, destacam-se aqueles cujos os valores estão acima do aceitável e dá-se o tratamento adequado para cada de modo a atenuá-lo ao máximo, ou seja, colocá-los no patamar "Aceitável" ou tão próximo quanto possível, por meio de um processo de reavaliação das proteções existentes. As ações relativas a esse controle do risco estão definidas no TÍTULO V.

VII - A escolha dos valores das probabilidades de ocorrência e dos impactos são sujeitos a imprecisões correspondentes ao juízo de valor do especialista que fez a estimativa, logo, devem ser revistos por outros membros da equipe que executa a análise de riscos de modo a diminuir as chances de ocorrerem escolhas sobreestimadas ou subestimadas.

VIII - O fecho da análise de riscos qualitativa fornece a lista dos riscos estimados, com destaque para aqueles que forem considerados prioritários, assim como aqueles que devam passar por análises adicionais, como a análise de riscos quantitativa.

Art. 34. No ANEXO I, encontra-se um modelo de análise de riscos simplificada.

Seção VIII
Da Análise de Riscos Quantitativa

Art. 35. O processo de aplicação da análise de riscos quantitativa faz uso de técnicas estatísticas e pode ser empregado quando os dados disponíveis são em número suficiente para tratamento estatístico e, em especial, em situações em que a análise de riscos qualitativa se revele insuficiente.

Parágrafo único. Estas normas foram elaboradas baseadas no pressuposto que as análises de risco que se façam necessárias aplicar no ambiente do Exército sejam, na sua maior parte, qualitativas. Em casos específicos, em que uma abordagem quantitativa deva ser realizada, o Departamento de Ciência e Tecnologia (DCT) deve ser consultado para a devida orientação.

Seção IX
Do Relatório de Situação de Riscos

Art. 36. O relatório de situação de riscos deverá informar as vulnerabilidades encontradas, as estimativas das chances (probabilidade) da ocorrência da exploração dessas vulnerabilidades, os impactos esperados e os riscos encontrados, de acordo com as áreas em que foram detectados. No ANEXO F, encontra-se o modelo de relatório.

Art. 37. Todo o processo de análise de riscos deverá ser documentado e comporá um processo, no qual deverá estar registrado o histórico das ações do processo.

Parágrafo único. A documentação pertencente ao processo de análise de riscos deverá ser organizada em um ou mais volumes que deverão ser classificados conforme a sensibilidade da informação nele contida e armazenados em conformidade com o prescrito nas Instruções Gerais para Salvaguarda de Assuntos Sigilosos ou instrumento legal que o valha.

TÍTULO V
DO CONTROLE DO GRAU DE RISCO

CAPÍTULO I
DAS MEDIDAS DE CONTROLE

Art. 38. Cada risco detectado deve ser tratado de acordo uma das seguintes estratégias:

I - NEUTRALIZAÇÃO - consiste na modificação do uso ou do tipo de recurso informacional, nas condições ambientais ou qualquer outros fatores que tenham como conseqüência a eliminação da causa que está gerando o risco.

II - TRANSFERÊNCIA - consiste na transferência da responsabilidade da gestão do risco para outra instância administrativa ou mesmo para entidade externa ou contratada.

III - MITIGAÇÃO - consiste em medidas que diminuam o impacto e/ou as chances de um risco se concretizar.

IV - ACEITAÇÃO - consiste na aceitação do risco tal como foi estimado sem medidas adicionais para seu controle. O fato de não haver "medidas adicionais de controle" não significa necessariamente que o nível de controle é baixo ou inexistente. Há situações em que o controle pode ser forte e, em conseqüência, não haver necessidade de medidas adicionais.

Art. 39. Seja qual for a estratégia escolhida, deve-se levar em consideração a relação custobenefício para que o custo da proteção não ultrapasse o custo do prejuízo advindo da concretização do risco. Deve-se levar em consideração não só o custo financeiro, mas outros de natureza gerencial, técnica, intangíveis e outros que se façam necessários para que a aceitação seja uma decisão consistente e claramente justificável.

Art. 40. A seqüência de ações para efetuar o controle apropriado deverá ser a seguinte:

I - a partir dos resultados da análise de riscos contidos no relatório, estabelecer quais os tipos de estratégias serão implementadas para cada risco detectado;

II - as responsabilidades pela execução das ações devem ser formalmente atribuídas em Boletim Interno;

III - estabelecimento das prioridades para tratamentos dos riscos conforme seu grau de severidade;

IV - identificação das medidas de controle possíveis;

V - avaliação da viabilidade técnica e financeira, assim como outro critério que se faça necessário, das medidas de controle possíveis;

VI - escolha das medidas de controle;

VII - as medidas decorrentes devem ser colocadas em prática;

VIII - verificações sobre os resultados das medidas de abrandamento dos riscos devem ser realizadas, podendo ser novas análises de risco, processos de auditoria ou procedimentos simples de verificação, conforme cada caso.

Art. 41. As decisões quanto ao tipo de estratégia para abrandamento do risco devem ser registradas em relatório a ser encaminhado à autoridade competente para ciência do fato e ser mantido em arquivo para servir como informação de histórico de processos de análise de riscos futuros e de auditoria da segurança da informação. O relatório de que trata este artigo tem como modelo o ANEXO F.

CAPÍTULO II
DA MONITORAÇÃO DO RISCO

Art. 42. Os riscos identificados e tratados no processo de gestão do risco devem ser monitorados continuamente para fins de percepção da sua evolução do decorrer do tempo.

Art. 43. Os instrumentos de monitoração principais são: análises de risco periódicas e processos de auditoria de segurança da informação.

Parágrafo único. A periodicidade das análises de risco deverão ser estabelecidas de acordo com a realidade de cada ambiente da OM, projetos ou outros tipos de trabalhos ou contexto e caberá ao Comandante da OM ou responsável pelo processo em andamento a escolha do período.

TÍTULO VI
DAS RESPONSABILIDADES

CAPÍTULO I
DO DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA

Art. 44. Compete ao Departamento de Ciência e Tecnologia:

I - disseminar o teor dessas Instruções no âmbito do Exército;

II - estabelecer os requisitos para especificação, aquisição, distribuição e atualização das ferramentas de **hardware** e **software** necessárias para realizar análises de riscos;

III - definir a sistemática de treinamento e atualização de pessoal para manuseio adequado das ferramentas de análise de riscos;

IV - estabelecer os requisitos para pesquisa na área de gestão de riscos para o ambiente do Exército;

V - elaborar a metodologia de análise de riscos quantitativa para aplicações específicas;

VI - manter a atualizada a doutrina relativa a análise de riscos definidas nestas Instruções;

VII - manter o registro dos relatórios sobre as análises de riscos realizadas nas OM do Exército para fins de aprimoramento da doutrina de análise de riscos;

VIII - prever no planejamento orçamentário as necessidades de recursos destinados à análises de riscos nos sistemas de informação do Exército;

IX - planejar, em conjunto com o CITEx e demais OM envolvidas, a aplicação de análises de riscos nas OM do Exército, estipulando cronograma para aplicação, prioridade, data, duração e responsabilidades;

X - acompanhar o cumprimento das atribuições destas Instruções, informando ao Chefe do DCT, por meio de relatórios;

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

XII - promover a integração com as atividades de análise de risco aplicadas no Sistema de Inteligência do Exército para buscar a compatibilidade dos métodos utilizados.

CAPÍTULO II
DO CENTRO DE DESENVOLVIMENTO DE SISTEMAS

Art. 45. Compete ao Centro de Desenvolvimento de Sistemas:

I - especificar as soluções de **software** e **hardware** para análises de riscos conforme os requisitos estabelecidos pelo DCT;

II - desenvolver aplicativos específicos de análise de riscos conforme requisitos estabelecidos pelo DCT;

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

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

CAPÍTULO III
DO CENTRO INTEGRADO DE TELEMÁTICA DO EXÉRCITO

Art. 46. Compete ao Centro Integrado de Telemática do Exército:

I - apoiar, por meio das suas OMDS, a realização dos processos de análise de riscos nas OM do Exército, conforme planejamento, priorização e cronograma estabelecido pelo DCT;

II - informar o DCT as necessidades de especialização e tipos treinamento para o pessoal diretamente envolvido na realização de análises de risco e disseminação da doutrina;

III - manter-se em condições de disseminar a doutrina de análise de riscos na área de sua atuação a partir do apoio do DCT;

IV - manter-se em condições de aplicar as técnicas de análise de riscos necessárias aos sistemas de informação existentes em sua área de atuação;

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

VI - manter atualizada e divulgar, através das páginas eletrônicas do Exército e do CITEx, listas de verificação passíveis de utilização em processos de análise de riscos no ambiente dos sistemas de informação do Exército;

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

VIII - remeter ao DCT os relatórios sobre as análises de risco realizadas para fins de acompanhamento por aquele Órgão Setorial;

IX - propor ao DCT, de forma periódica e em intervalos de tempo não superiores a um ano, sugestões quanto ao aprimoramento da doutrina de análise de riscos com base no conhecimento adquirido com a aplicação dos processos de gestão de risco.

CAPÍTULO IV
DO INSTITUTO MILITAR DE ENGENHARIA

Art. 47. 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 análises de riscos nos sistemas de informação do Exército;

II - remeter ao DCT cópias dos trabalhos de fim de curso e pós-graduação sobre o tema ou que apliquem métodos de análise de risco a fim de disseminar e compartilhar o conhecimento na área;

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

CAPÍTULO V
DO DIRETORIA DE SERVIÇO GEOGRÁFICO

Art. 48. Compete à Diretoria de Serviço Geográfico:

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

CAPÍTULO VI
DO CENTRO INTEGRADO DE GUERRA ELETRÔNICA

Art. 49. Compete ao Centro Integrado de Guerra Eletrônica:

I - informar o DCT as necessidades de especialização e tipos treinamento para o pessoal diretamente envolvido na realização de análises de riscos e disseminação da doutrina no âmbito das atividades de Guerra Eletrônica;

II - manter-se em condições de disseminar a doutrina de gestão de riscos na área de sua atuação a partir do apoio do DCT;

III - manter-se em condições de aplicar as técnicas de gestão de riscos necessárias aos sistemas de informação existentes em sua área de atuação;

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

V - propor ao DCT, de forma periódica e em intervalos de tempo não superiores a um ano, sugestões quanto ao aprimoramento da doutrina de gestão de riscos com base nas necessidades da área de Guerra Eletrônica.

CAPÍTULO VII
DO GRUPO FINALÍSTICO DE SEGURANÇA DA INFORMAÇÃO

Art. 50. Compete ao Grupo Finalístico de Segurança da Informação:

I - monitorar o surgimento de demandas para estudo e geração de conhecimento na área de gestão de riscos no contexto da segurança da informação do Exército e, se for o caso, desenvolver as ferramentas e metodologias que se fizerem necessárias;

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

CAPÍTULO VIII
DO CENTRO DE INTELIGÊNCIA DO EXÉRCITO

Art. 51. Compete ao Centro de Inteligência do Exército:

I - realizar os processos de análise de riscos nos sistemas de informação componentes do Sistema de Inteligência do Exército (SIEx);

II - atuar em parceria com com o DCT, para fins de compartilhamento de informações e aprendizado, a respeito de mecanismos utilizados em violações de segurança da informação identificadas no SIEx, as quais potencialmente representem ameaça a outros Sistemas do Exército.

CAPÍTULO IX
DAS OM DO EXÉRCITO

Art. 52. 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 análises de risco.

III - solicitar ao DCT, via canal de Comando, apoio na realização de análises de riscos em seus ambientes de rede.

ANEXO A
MODELO DE PLANO DE ANÁLISE DE RISCOS

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
OM

ANÁLISE DE RISCOS NR ____/

PLANO DE ANÁLISE DE RISCOS

1. FINALIDADE

Transcrição da finalidade do plano. (Exemplo: A finalidade deste plano é descrever os procedimentos necessários para executar uma análise de riscos referente ao ambiente de rede local da OM "...".).

2. OBJETIVOS

Transcrição dos objetivos necessários para cumprir a finalidade do plano. (Exemplo: A fim de cumprir a finalidade enunciada, os seguintes objetivos são estipulados: definição dos grupos envolvidos na condução do processo, assim como as respectivas responsabilidades; descrição dos procedimentos para aplicação das técnicas escolhidas para execução da análise de riscos.).

3. ESCOPO

Identificação do escopo abrangido pela análise. Este elemento é de crucial importância por restringir os limites da análise. (Exemplo: Esta análise de risco abrangerá o sistema de banco de dados da OM X e suas interfaces com outros sistemas que se interligam a ele.).

4. METODOLOGIA

Identificação de quais metodologias serão empregadas e em que fase do processo. Por exemplo:

a. Caracterização do Sistema: Entrevistas e pesquisa documentária;

b. Identificação das vulnerabilidades e riscos: **BrainStorm** (os procedimentos da aplicação da técnica, além de dados como data e hora da aplicação, nome do pessoal envolvido e função etc, são descritos nestas Instruções);

c. Estimativa das probabilidades de concretização do risco: Técnica de **Delphi** (o questionário e a relação dos respondentes, além das ações para remeter e recuperar os questionários são descritos nestas Instruções);

d. Análise de impactos: (procedimentos para levantar as estimativas do impacto junto aos especialistas);

e. Escalonamento dos riscos: Arbitramento de valores para o risco (cálculo dos valores do risco, em função dos valores arbitrados para a probabilidade de ocorrerem uma violação de segurança e dos valores arbitrados para representar o impacto);

f. Relatório da situação de riscos: Descrição conforme modelo.

5. ATRIBUIÇÕES E RESPONSABILIDADES

Identificação das atribuições e responsabilidades no processo de acordo com o estabelecido por estas IR. Exemplo:

a. Gerente do Processo: Oficial "..."

b. Grupo de trabalho: "lista dos representantes das áreas envolvidas"

6. GASTOS

Possíveis gastos do processo.

7. PERIODICIDADE DE APLICAÇÃO

Estipula-se, conforme as particularidades da OM, a periodicidade com a qual a análise de riscos deve ser repetida.

8. MÉTRICAS, COTAS E CRITÉRIOS PARA ESTIMATIVA OU CÁLCULO DO RISCO

Métricas e pesos e correspondentes interpretações usados para caracterizar o risco (valores possíveis para: as probabilidades da ocorrência da exploração de uma vulnerabilidade; impacto da exploração de uma vulnerabilidade; e matriz de valores de risco).

9. TRATAMENTO DO RISCO

Possíveis tratamentos que sejam considerados pertinentes ao ambiente da análise conforme as opções existentes nestas Instruções.

10. CRONOGRAMA

Descrição das fases do processo em formato de cronograma.

Local, data

Assinatura do responsável(eis) pela elaboração do Plano

ANEXO B
MODELO DE RELATÓRIO DE DESCRIÇÃO DE SISTEMAS DE INFORMAÇÃO

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
OM

ANÁLISE DE RISCOS NR ____/

RELATÓRIO DE CARACTERIZAÇÃO DE SISTEMAS DE INFORMAÇÃO DA OM XXX

1. APRESENTAÇÃO:

(Resumo informativo sobre as características do sistema de informação, contendo o nome do sistema, sua abrangência de aplicação e sua finalidade).

2. OBJETIVO:

(Enunciar os objetivos específicos, se for o caso, em que se desdobra a finalidade do sistema.)

3. PROCESSOS ADMINISTRATIVOS A QUE O SISTEMA DE INFORMAÇÃO ANALISADO ATENDE:

(Processos que as soluções implementadas nos sistemas de informação sob análise sustentam.).

4. INFORMAÇÕES CRÍTICAS:

(Informações importantes para o cumprimento da finalidade do sistema. Essas informações podem ser dados de um banco de dados, arquivos produzidos por qualquer **software** e arquivados nos computadores dos usuários do sistema, e-mails, documentação oficial em forma digital ou impressa, minutas de documentos, informações sobre configurações do sistema etc.).

5. SERVIÇOS OFERECIDOS:

(descrição dos serviços automatizados oferecidos pelo sistema de informações e suas configurações)

6. SOFTWARES UTILIZADOS:

(lista dos **softwares** utilizados na implementação dos serviços, assim como sua localização, ou seja, equipamentos onde estão instalados e as mídia dos **softwares** originais).

7. HARDWARE UTILIZADO:

(lista dos equipamentos da infra-estrutura computacional e de redes utilizados na implementação do sistema de informação, assim como sua configuração e localização física).

8. INFRA-ESTRUTURA LÓGICA:

(descrição da infra-estrutura lógica de cabeamento de rede, sua configuração lógica e arquitetura física, devendo esta descrição contar com esquemas gráficos, para melhor visualização da descrição).

9. INFRA-ESTRUTURA DE ALIMENTAÇÃO ELÉTRICA:

(descrição da infra-estrutura de alimentação elétrica, devendo constar a distribuição de pontos de alimentação, localização dos quadros de distribuição, tipo e capacidade dos disjuntores principais e esquemas gráficos para melhor visualização da infra-estrutura).

10. PESSOAL:

(descrição do tipo de usuário que utiliza o sistema de informação - gerentes, usuários e manutenção - e o seu grau de privilégio em relação ao uso ou configuração do sistema).

11. NORMAS APLICÁVEIS:

(conjunto de normas de segurança, técnicas ou administrativas aplicáveis ao sistema de informação sob auditoria).

12. PROCEDIMENTOS OPERACIONAIS PADRÃO:

(conjunto de pop relacionados à gestão, uso e manutenção do sistema de informação em uso).

13. RELATÓRIOS DE ANÁLISES DE RISCO ANTERIORES:

(conjunto de relatórios sobre riscos e auditorias realizadas antes da auditoria em andamento)

Local, data

Assinatura do responsável(eis) pela descrição do sistema de informação

14. PARECER:

(parecer do Comandante contando observações adicionais que sejam necessários)

Assinatura do Comandante da OM onde o sistema de informação está implementado

ANEXO C
MODELO PARA REGISTRO DE VULNERABILIDADES

(EXEMPLO)

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
OM

ANÁLISE DE RISCOS NR ____/

ÁREA INVESTIGADA: XXX (por exemplo, **SOFTWARE**)

SOFTWARE ANALISADO	**VULNERABILIDADES**	**FONTE DA AMEAÇA (coluna opcional)**	**AÇÃO NECESSÁRIA PARA EXPLORAR A VULNERABILIDADE**
1. Sistema Operacional de redes XXX, versão yyy, em uso para autenticação de usuários na rede.	1.1 os registros do sistema podem permitir a um intruso modifica-los remotamente. 1.2.	1.1. **Hacker**; 1.2. Elemento interno insatisfeito. 1.3. ...	1.1. Os registros do sistema operacional podem ser editados por quem tiver o privilégio de administrador e modificados para permitir controle externo. 1.2.
2. ...	2.1. .... 2.2. ...	2.1. ... 2.2. ...	2.1. ... 2.2. ...
3. ...	3.1. .... 3.2. ...	3.1. ... 3.2. ...	3.1. ... 3.2. ...
:	:	:	:
:	:	:	:
:	:	:	:

Local, data

Assinatura do responsável(eis) pela elaboração do documento

ANEXO D
MODELO DE FORMULÁRIO PARA BRAINSTORM

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
OM

ANÁLISE DE RISCOS NR ____/

FORMULÁRIO PARA BRAINSTORM (EXEMPLO)

ASSUNTO:XXX (por exemplo: VULNERABILIDADES SOBRE SISTEMAS OPERACIONAIS)

NR	IDÉIA	AUTOR
1.	Sistema operacional de redes não possui todas as correções e atualizações disponibilizadas pelo fabricante	.....
2.	Sistema operacional das estações não possui a possibilidade de configurar restrições de acesso às pastas dos arquivos	.....
3.	Sistema operacional do servidor de correio eletrônico não é compatível com os requisitos da norma de segurança da informação	.....
4.	Sistema operacional da estação do Chefe "trava" muito (SUGESTÃO APARENTEMENTE IRRELEVANTE, MAS, A PRINCÍPIO, DEVE SER CONSIDERADA)	....
5.	Sistema operacional do computador da segunda seção não é automaticamente reconfigurado após o estabelecimento de nova versão de política de segurança (SUGESTÃO APARENTEMENTE IRREAL, MAS, A PRINCÍPIO, DEVE SER CONSIDERADA)	...
6.	:	...
7.	:	...
8.	:	...
9.	:	...
10.	:	...

Local, data

Assinatura do responsável(eis) pela condutor do processo de aplicação da técnica

ANEXO E
MODELO DE QUESTIONÁRIO PARA TÉCNICA DELPHI

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
OM

ANÁLISE DE RISCOS NR ____/

QUESTIONÁRIO PARA TÉCNICA DELPHI (EXEMPLO)

ASSUNTO:XXX (por exemplo: VULNERABILIDADES SOBRE SISTEMAS OPERACIONAIS)

NR	**AMEAÇA**	**CHANCES DE OCORRER (p)**	**IMPACTO (I)**	**JUSTIFICATIVA**
1.	Hacker aproveitar que o sistema operacional de rede não possui todas as correções e atualizações disponibilizadas pelo fabricante	2	3	**(p):** há ligação dos computadores com a Internet, viabilizando ligações entre equipamentos fora da rede e os servidores. **(I)**: a rede poderá ficar indisponível.
2.	.....	.....	.....	
3.	.....	.....	.....	
4.	.....	.....	.....	

Legenda:

a. Probabilidades possíveis (p) do exemplo:
   1) 1, baixa probabilidade;
   2) 2, média probabilidade;
   3) 3, probabilidade.

b. Impactos possíveis (I):
   1) 1, baixo impacto;
   2) 2, médio impacto;
   3) 3, alto impacto.

Local, data

Assinatura do responsável(eis) pela condutor do processo de aplicação da técnica

ANEXO F
MODELO DE RELATÓRIO DE SITUAÇÃO DE RISCOS

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
OM

ANÁLISE DE RISCOS NR ____/

RELATÓRIO DE SITUAÇÃO DE RISCOS 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 análise de riscos realizada e, se necessário for, de objetivos secundários ou específicos)

3. DESCRIÇÃO DO PROCESSO:

(descrição detalhada das fases do processo de análise de riscos do ambiente analisado conforme subitens a seguir e que correspondem as fases de execução descritas nestas IR)

a. Caracterização do Sistema a ser Analisado
b. Identificação das Vulnerabilidades
c. Identificação do Risco
d. Estimativa das Chances da Concretização dos Riscos
e. Análise de Impactos
f. Escalonamento dos Riscos

4. RISCOS DETECTADOS:

(descrição detalhada dos riscos encontrados e, se necessário for, com subdivisões por assunto; suas prioridades; e as recomendações sobre as medidas para tratar o risco que sejam pertinentes)

5. MEDIDAS DE TRATAMENTO DO RISCO:

(Descrição da estratégia de tratamento do risco e as medidas a serem adotadas)

6. CONCLUSÃO:

(A conclusão deve ser objetiva e, preferencialmente do tipo resumo, ou seja, destacando os riscos prioritários e as recomendações correspondentes)

Local, data

Assinatura do responsável pela análise

PARECER:

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

ANEXO G

MODELO PARA REGISTRO DE "SINTOMAS DE RISCOS"

(EXEMPLO)

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
OM

ANÁLISE DE RISCOS NR ____/

CATEGORIA: _____

ÁREA INVESTIGADA: XXX (por exemplo, **SOFTWARE**)

SOFTWARE ANALISADO	**SINTOMA**	**FONTE DA AMEAÇA (se for identificada)**	**AÇÃO QUE PROVAVELMENTE PROVOCOU O SINTOMA**
1. Sistema Operacional de redes XXX, versão yyy, em uso para autenticação de usuários na rede	1.1 os registros do sistema não estão configurados como previsto. 1.2.	1.1. Hacker; 1.2. ... 1.3. ...	1.1. A senha do administrador foi descoberta e os registros foram trocados pelo uso ilícito dos privilégios do administrador. 1.2. ...
2. ...	2.1. .... 2.2. ...	2.1. ... 2.2. ...	2.1. ... 2.2. ...
3. ...	3.1. .... 3.2. ...	3.1. ... 3.2. ...	3.1. ... 3.2. ...
:	:	:	:
:	:	:	:
:	:	:	:

Local, data

Assinatura do responsável(eis) pela condutor do processo de aplicação da técnica

ANEXO H
EXEMPLO DE MATRIZ DE RISCO

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
OM

ANÁLISE DE RISCOS NR ____/

MATRIZ DE RISCO
(demonstra os valores do risco para cada caso, ou seja, para cada vulnerabilidade identificada em um determinado escopo)

Neste exemplo, as probabilidades e impactos possíveis são as mesmas do exemplo da matriz de valores do risco, a qual, num processo real, precederá a elaboração da matriz de risco.

ÁREA INVESTIGADA: XXX (por exemplo, **software, hardware, pessoal, instalações etc.**)

Vulnerabilidade	**Probabilidade**	**Impacto**	**VALOR DO RISCO**
Vulnerabilidade 1	5 (provável)	4 (crítico)	(provável) x (crítico) =A(20) (risco alto)
Vulnerabilidade 2	1(desprezível)	1(Extremamente improvável)	(desprezível)x(extremamente improvável)=T(1) (risco tolerável)
Vulnerabilidade 3	4 (ocasional)	3 (Médio)	(ocasional)x(médio)= A(12) (risco alto)
:	**:**	**:**	**:**

Obs: 1. é recomendável que a seja elaborada uma matriz de risco para cada grupo de vulnerabilidades classificadas em grupos semelhantes como são tratadas no ANEXO C.

2. A classificação do risco NÃO está associada aos valores numéricos em uma escala crescente, ou seja, pode-se ter um risco classificado como "Inaceitável" cujo valor associado seja menor que um risco classificado como "Médio".

Local, data

Assinatura do responsável(eis) pela condutor do processo de aplicação da técnica

ANEXO I
METODOLOGIA SIMPLIFICADA DE ANÁLISE DE RISCOS

Os objetivos deste exemplo simplificado são os seguintes: descrever a seqüência de procedimentos para: identificar as vulnerabilidades (pontos fracos) mais prováveis de um sistema de informações; estimar o impacto associado a essas vulnerabilidades; e propor as ações necessárias para eliminar ou abrandar seus efeitos.

As técnicas básicas utilizadas nesta metodologia simplificada são **brainstorm** e entrevistas. Essas técnicas são utilizadas, respectivamente, para identificação das vulnerabilidades, estimativa da ocorrência de ameaças e estimativa de impactos dos riscos.

1. PRIMEIRA ETAPA (ESCOLHA DOS PARTICIPANTES E DEFINIÇÃO DO ESCOPO DA ANÁLISE):

a. o Comandante escolherá o gerente/coordenador do processo, o qual deverá ter conhecimento do método descrito nestas Instruções e noções sobre segurança da informação;

b. o gerente/coordenador do processo deverá, de acordo com a necessidade, definir o escopo sobre o qual a análise de riscos será desenvolvida (por exemplo: ambiente de rede; protocolos; ambiente Internet; instalações físicas etc.);

c. o gerente/coordenador, de acordo com o escopo escolhido, selecionará os participantes da análise (devem participar da aplicação do método os especialistas envolvidos no assunto, segmento, aplicação ou área a ser analisada. Para condução dos trabalhos deve haver um facilitador e um relator).

2. TERCEIRA ETAPA (obtenção da documentação do sistema):

a. o gerente ou coordenador, de acordo com o escopo escolhido, obter toda a documentação técnica e administrativa julgada necessária ao processo.

3. SEGUNDA ETAPA (EXPOSIÇÃO DA METODOLOGIA DE TRABALHO AOS PARTICIPANTES - responsável: gerente ou coordenador do processo):

a. explicação do método contido nestas Instruções;

b. explicação sobre a aplicação das técnicas básicas;

4. QUARTA ETAPA (IDENTIFICAÇÃO DAS VULNERABILIDADES):

a. Utilização da técnica de **brainstorm**, conforme descrito nestas Instruções, para identificação das vulnerabilidades e dos riscos associados a cada aspecto de segurança (integridade, sigilo e disponibilidade);

b. Para auxiliar na identificação das vulnerabilidades, utilizar questões do tipo:

1) Que evento ou acidente poderia afetar a disponibilidade ou causar dano ao serviço? Que fragilidade do sistema permite que isso ocorra?

2) Que evento poderia afetar a integridade ou confidencialidade da informação ou dado relacionados ao serviço de rede? Que fragilidade do sistema permite que isso ocorra?

3) Que evento poderia afetar a integridade da informação a ser protegida se o **hardware** (**software**, serviço, instalação física, instalação elétrica ou de cabeamento de dados, pessoas) for comprometido? Que fragilidade do sistema permite que isso ocorra?

c. Todos os riscos devem ser registrados, mesmo os que já possuam medidas de redução de riscos.

5. IDENTIFICAÇÃO DOS IMPACTOS E DAS PROBABILIDADES ASSOCIADAS AOS RISCOS

a. Utilização da técnica de entrevista com os responsáveis, gerentes e especialistas no objeto do escopo analisado, fazendo uso das escalas definidas nestas instruções.

6. IDENTIFICAÇÃO DOS RISCOS

a. Calcula-se o valor do risco, conforme os valores estimados para as probabilidades (p) e os correspondentes valores para os impactos (I);

b. Verifica-se em que posição da Matriz de Valores do Risco (definida nestas Instruções) onde o valor calculado está e qual a interpretação deve ser dada ao seu grau de severidade. Note-se que pode haver coincidência de valores numéricos, porém a interpretação é qualitativa, ou seja, conforme a classificação de cada vulnerabilidade (..., remoto, provável,...) e cada impacto (..., desprezível, secundário,...);

c. o produto dessa atividade é uma tabela, como representado a seguir, relacionando os riscos, prioridades e medidas de segurança.

Vulnerabilidade	**Probabilidade de ocorrência**	**Impacto**	**VALOR DO RISCO**	**Medidas de Segurança**
Vulnerabilidade 1	p	I	PxI	.....
:	:	:	:	:
:	:	:	:	:

7. CONCLUSÃO

É elaborado o relatório de consolidação de riscos e contramedidas que deverá conter, além da lista de riscos e contramedidas, um plano de ações e um cronograma de atividades conforme modelo contidos nestas Instruções.

PORTARIA Nº 003-DCT, DE 31 DE JANEIRO DE 2007

Aprova as Instruções Reguladoras Sobre Auditoria de Segurança de Sistemas de Informação do Exército Brasileiro - IRASEG (IR 13-09).

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 Auditoria de Segurança de Sistemas de Informação do Exército Brasileiro - IRASEG (IR 13-09).

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

INSTRUÇÕES REGULADORAS DE AUDITORIA DE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO DO EXÉRCITO BRASILEIRO - IRASEG (IR 13 - 09)

ÍNDICE DOS ASSUNTOS

Art.

Anexos:

INSTRUÇÕES REGULADORAS SOBRE AUDITORIA DE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO DO EXÉRCITO BRASILEIRO - IRASEG (IR 13 - 09)

TÍTULO I
DAS GENERALIDADES

Art. 1º As presentes instruções, elaboradas em observância ao inciso V do art. 31 das Instruções Gerais de Segurança da Informação para o Exército Brasileiro (IG 20-19), têm por finalidade regular as condições para a implantação de um sistema de auditoria de segurança de Sistemas de Informação nas OM do Exército Brasileiro.

Art. 2º São objetivos destas Instruções:

I - Estabelecer os referenciais normativos para definição do sistema de auditoria de segurança de sistemas de informação do Exército;

II - Propiciar aos Comandantes, Chefes, Diretores e Secretários das OM do Exército orientação sobre a aplicação dos processos de auditoria em seus sistemas de informação.

III - Prover referenciais doutrinários sobre segurança da informação no que tange à auditoria da segurança de sistemas de informação.

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

TÍTULO II
DAS DEFINIÇÕES BÁSICAS

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

I - SISTEMA DE INFORMAÇÃO (SI) - Sistema que obtenha, produza, armazene, processe e transmita informações. Para aplicação destas IR, deve ser considerado que, em sua forma mais simples, um SI pode ser constituído de um sistema corporativo informatizado, assim como, em sua forma mais complexa, um SI pode ser constituído de um conjunto de redes de computadores e de comunicação, com seus **softwares**, equipamentos, usuários e processos administrativos.

II - CONTROLES - Para aplicação destas Instruções, devem ser considerados como controles todas as formas que definam limites ou atuem como limitadores de qualquer ação que influa na confidencialidade, na integridade ou na disponibilidade das informações de um sistema de informação.

Duas categorias que exemplificam controles são: a documentação normativa e os mecanismos de configuração de **hardware** ou **software**. Exemplos (que não esgotam as possibilidades) dessas duas categorias são os seguintes:

a) documentação normativa:

- Políticas;
- Diretrizes;
- Instruções;
- Manuais;
- Normas;
- Planos de Segurança Orgânica (PSO);
- Normas Gerais de Ação (NGA);
- projetos;
- procedimentos operacionais padrão;
- documentação técnica de sistemas;
- correspondências oficiais do Exército;
- Boletins Internos;
- documentos normativos, emitidos oficialmente e de acordos com os modelos existentes;
- demais documentos internos, oficialmente firmados;
- contratos com outras organizações ou empresas.

b) Mecanismos de configuração:

- conjunto de configurações de um sistema operacional;
- conjunto de configurações do sistema de **firewall**;
- conjunto de configurações de um **software** aplicativo;
- conjunto de configurações de **hardware** (seja ele qual for).

III - CONFORMIDADE - estado em que se constata a coerência esperada entre o previsto num controle e um elemento auditado.

IV - EFETIVIDADE - eficácia e nível de eficiência de uma ação de segurança, considerados em conjunto, ou seja, denota se a segurança foi atingida (eficácia) e o grau de otimização do processo necessário para atingí-la (eficiência).

V - AUDITORIA DA SEGURANÇA DA INFORMAÇÃO - processo em que é verificada a conformidade entre os controles estabelecidos e o estado dos elementos auditados e, além disso, o grau de efetividade dos processos analisados pela auditoria.

VI - SISTEMA DE AUDITORIA DE SEGURANÇA DE SISTEMA DE INFORMAÇÃO - sistema formado pelas normas, pessoal especializado, processos e recursos computacionais necessários para planejar e executar auditorias de segurança da informação em sistemas de informação.

VII - PONTO DE CONTROLE - elemento que será avaliado em um sistema de informação sob auditoria, podendo ser uma característica específica ou um conjunto de estruturas desse sistema. Exemplos possíveis: uma funcionalidade de um **software**, um aplicativo de computador, um microcomputador, um serviço de rede ou, ainda, um determinado segmento de uma rede.

VIII - TESTE DE INTRUSÃO OU INVASÃO - teste no qual um especialista em técnicas de invasão tenta subverter as proteções e ganhar acesso às partes do sistema de informação sob teste e tem como objetivo descobrir vulnerabilidades nas proteções implementadas.

IX - ESPECIALISTA DE ÁREA - especialista em tecnologia ou produto utilizado em um sistema de informação, seja por vivência prática na operação ou por possuir cursos específicos ou, ainda, por formação acadêmica de graduação ou pós-graduação na área na qual se necessita atuar.

TÍTULO III
DOS CONTROLES

CAPÍTULO I
DAS CATEGORIAS

Art. 4º Para aplicação destas IR, os controles são categorizados como a seguir:

I - CONTROLES ESTRATÉGICOS - são as publicações do Exército de caráter estratégico e que têm reflexos sobre o tratamento dado à informação na Força e, em conseqüência, sobre a segurança da informação. Como exemplo, tem-se a Política de Informação do Exército e as Diretrizes Estratégicas;

II - CONTROLES NORMATIVOS - são as publicações do Exército relativas à segurança da informação ou contra-inteligência e cujas regras são de caráter tático ou operacional e, portanto, passíveis de serem verificadas nos sistemas de informação auditados. Podem ser: de abrangência geral, por exemplo, as Instruções Gerais de Segurança da Informação para o Exército Brasileiro (IG 20 - 19); de aplicação restrita a uma OM, por exemplo, norma interna de segurança da informação; ou um grupo de OM, como o Plano Básico de Ciência e Tecnologia;

III - CONTROLES LEGAIS - são as legislações vigentes no país e passíveis de aplicação no contexto de segurança dos sistemas de informação do Exército. Como exemplo, tem-se a legislação vigente que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos;

IV - CONTROLES ADMINISTRATIVOS - são as definições referentes aos processos e procedimentos administrativos de uma OM, formalmente estabelecidas por meio de publicação em Boletim Interno (BI) . Como exemplo, tem-se os regimentos e regulamentos internos, as notas para BI, Normas Gerais de Ação, determinações específicas do Comandante, expressas em Boletim Interno etc;

V - CONTROLES TÉCNICOS-NORMATIVOS - são as documentações técnicas-normativas, publicadas por organizações externas, que abordem a segurança da informação e que podem servir como referencial para aplicação nos sistemas de informação do Exército ou documentação técnica sobre os produtos tecnológicos utilizados nos sistemas de informação do Exército elaboradas pelo fabricante. Um exemplo é a norma técnica NBR ISO/IEC 17799, sobre gestão de segurança da informação;

VI - CONTROLES CONTINGENCIAIS - documentação que disponha sobre o procedimentos para garantir a continuidade da captação, processamento, armazenamento, transmissão e uso da informação em situações de desastre ou violação da segurança da informação. Como exemplo, tem-se o Plano de Contingência ou de Continuidade de Serviços que deve compor a documentação relativa à segurança da informação sobre a rede da OM;

VII - CONTROLES DE RISCO - é a documentação que define os processos e os procedimentos relativos à gestão de risco. O exemplo é a publicação interna relativa às Instruções do Exército que dispõe sobre o assunto;

VIII - CONTROLES DE PESSOAL - documentação que define atribuições, responsabilidades, orienta ou estabelece referenciais para disciplinar o comportamento do pessoal interno ou, eventualmente, externo, em relação ao trato com a informação de um SI do Exército. Um exemplo é o Regulamento Interno e dos Serviços Gerais (R-1);

IX - CONTROLES DE SEGURANÇA ORGÂNICA - documentação que estabelece os procedimentos para salvaguarda das áreas e instalações onde as informações a serem protegidas são armazenadas, processadas, transmitidas ou usadas. Um exemplo é o Plano de Segurança Orgânica (PSO) ou instrumento normativo que o substitua;

X - CONTROLES DE GERENCIAMENTO DE SEGURANÇA - documentação que estabelece os procedimentos e processos relativos ao planejamento, execução e controle da gestão da segurança da informação, nos níveis estratégico, tático e operacional, sendo, um possível exemplo, as normas internas (no nível do OM) de segurança da informação.

XI - CONTROLES TÉCNICOS - mecanismos automatizados que monitoram o funcionamento de um **hardware** ou de um **software** ou, ainda, mecanismos configurados para limitar ações que influam nesses elementos. Como exemplos se tem: registros de eventos (**log** de eventos), **softwares** de gerência de dispositivos ou rede, funcionalidades de segurança par configuração de sistemas operacionais etc.

Art. 5º É possível que existam situações nas quais ocorram superposições entre alguns dos controles ou que haja controles que não se enquadrem nas categorias relacionadas, mas que sejam úteis para auditoria de segurança de sistemas de informação específicos. Cabe aos responsáveis pela aplicação do processo de auditoria dirimir qual interpretação deve ser dada a cada caso.

CAPÍTULO II
DOS REQUISITOS BÁSICOS DE CADA CONTROLE

Art. 6º Os sistemas de informação em uso no Exército devem ser documentados.

§ 1º Para verificação da efetividade e conformidade dos controles de um sistema de informações de uma OM, ou em uma parte específica desse sistema, é necessário que existam documentações que descrevam o sistema, assim como as regras que disciplinem seu uso e gerência, sendo que, a sua inexistência deve ser considerada uma distorção a ser corrigida.

§ 2º Toda OM que possua ou faça uso de um sistema de informação deverá possuir, em seu acervo normativo, as documentações necessárias para orientar ou regular o uso do SI. Essa documentação deverá ser mantida atualizada e, quando da aplicação do processo de auditagem, estar disponível para a equipe de auditoria.

§ 3º O rol mínimo de documentos que devem existir é o seguinte:

a) documentação que descreva o sistema de informação sob auditoria conforme ANEXO A;

b) normas de segurança da informação ou contra-inteligência do Exército, ou internas da OM, que regem o sistema de informação ou parte dele;

c) documentos que regram procedimentos relativos ao sistema de informação que tenham sido publicadas em BI;

d) normas técnicas ou de segurança externas que sejam aplicadas no sistema de informação sob auditoria;

e) procedimentos operacionais básicos (pop) referente às ações de utilização e gestão (se for o caso) do sistema de informação sob auditoria;

f) demais documentos que estejam relacionados ao sistema de informação sob auditoria e que se enquadrem nas categorias de controles constantes destas Instruções.

Seção I
Dos Controles Estratégicos

Art. 7º O objetivo dos procedimentos de auditoria baseados nos controles estratégicos é verificar a conformidade e a efetividade entre as orientações e ordens do Comando da Força, Estado Maior do Exército ou constantes nas publicações do Exército, a respeito do trato à informação, e as ações tomadas pelos respectivos responsáveis que devam atender a essas ordens e orientações.

Parágrafo único. As referências doutrinárias básicas a que se refere este artigo são a Política de Informação do Exército e as Diretrizes Estratégicas dela derivadas.

Art. 8º Os requisitos básicos dos controles estratégicos são:

I - ser documentações pertencentes ao conjunto de publicações oficiais do Exército ou ordens e orientações do Comando do Exército ou EME disseminadas pelos canais oficiais da Instituição;

II - ser publicações que abranjam o trato ou gestão da informação e que, portanto, geram necessidade de medidas de segurança da informação.

Seção II
Dos Controles Normativos

Art. 9º O objetivo dos procedimentos de auditoria baseados nos controles normativos é verificar a conformidade entre as características do sistema de informação sob auditoria com os documentos normativos do Exército que regem o seu uso e gerência, assim como a efetividade das medidas de segurança no sistema.

§ 1º As referências doutrinárias básicas a que se refere este artigo são as Instruções Gerais relativas à segurança da informação no Exército e à salvaguarda de assuntos sigilosos, assim como a documentação normativa relativa ao Ramo da Contra-Inteligência que estiverem vigentes no âmbito da Força.

§ 2º Das referências doutrinárias básicas, podem se desdobrar outras, mais específicas, versando sobre temas da segurança da informação ou correlatos, tais como:

a) gestão de riscos;

b) meios de tecnologia da informação (segurança em redes de computadores ou de comunicação);

c) auditoria da segurança da informação;

d) pessoal;

e) áreas e instalações;

f) material;

g) documentação;

h) contingência ou continuidade de serviços;

i) gestão de segurança da informação;

j) contra-inteligência.

Art. 10. Os requisitos básicos dos controles normativos são:

I - ser documentos cujo o tipo esteja enquadrado como uma das publicações oficiais do Exército ou que sigam os modelos específicos contidos nessas publicações;

II - quando de aplicação estritamente interna à OM, serem documentos aprovados pelo Comandante em BI e mantidos atualizados, com revisões periódicas e ajustes que reflitam as mudanças nas condições de operação e nos riscos;

III - quando se tratar de normas de caráter operacional, devem:

a) conter regras que estabelecem como o sistema de informação deve estar protegido contra violações de segurança, detalhando as configurações dos recursos computacionais (**hardware** e **software**) e de redes (dados e comunicação);

b) as normas de caráter operacional devem ter classificação sigilosa e receber o tratamento conforme as Instruções do Exército correspondentes;

c) estar de acordo com o modelo sugerido no ANEXO B.

IV - definir as responsabilidades de segurança nos seguintes níveis: de usuários dos recursos de informação; do pessoal de processamento de dados e manutenção; dos gestores do sistema e de sua segurança; e das chefias e Comando.

Seção III
Dos Controles Legais

Art. 11. O objetivo dos procedimentos de auditoria baseados nos controles legais é verificar a conformidade do uso dos recursos do sistema de informação auditado com legislação vigente no país.

Art. 12. O requisito básico dos controles legais é que devem ser legislações de nível federal que versem, ou que estejam relacionadas, ao escopo da segurança da informação e seu assuntos correlatos.

Seção IV
Dos Controles Administrativos

Art. 13. O objetivo dos procedimentos de auditoria baseados nos controles administrativos é verificar a conformidade e a efetividade do que é estabelecido e realizado para a vida administrativa de uma OM e que tenha impacto sobre a proteção da informação dos seus sistemas de informação.

Art. 14. Os requisitos básicos dos controles administrativos são:

I - ser documentos cujo teor seja legitimado por autoridade de Comando ou por responsável técnico, obedecendo aos ritos administrativos do Exército;

II - os documentos que devam constituir o rol dos controles administrativos são:

a) publicações em BI;

b) relatórios;

c) memórias;

d) pareceres;

e) ordem de serviços;

f) projetos;

g) documentos pertencentes ao conjunto de correspondências oficiais do Exército, conforme normas em vigor.

Seção V
Dos Controles Técnicos-Normativos

Art. 15. O objetivo dos procedimentos de auditoria baseados nos controles técnico-normativos é verificar a conformidade e a efetividade em duas situações possíveis:

I - entre o que é estabelecido na documentação técnica elaborada pelo fabricante e as características de configuração e uso do produto em sua aplicação. Os requisitos correspondentes são:

a) ser constituídos de documentações técnicas elaboradas pelo fabricante, ou pelos seus representantes autorizados, sobre os seus produtos que são usados nos sistemas de informação do Exército;

b) abranger todos os produtos de **hardware**, **software** e infra-estruturas lógicas de rede e de alimentação elétrica em uso nos sistemas de informação do Exército.

II - entre as exigências constantes nos documentos normativos de origem externa ao Exército e que disciplinam ou definem o uso e a gestão do sistema de informação sob auditoria. Os requisitos correspondentes são:

a) ser publicações cuja aplicação no âmbito do Exército advenha do fato de serem originadas em:

- órgão da Administração Pública Federal com competência normativa específica no tema abordado no documento que define o controle;

- Associação Brasileira de Normas Técnicas (ABNT);

- órgão normativo internacional, o qual estabeleça normas técnicas necessárias para o uso e proteção do sistema sob auditoria e para as quais não existam equivalentes no país.

Art. 16. As OM cujos sistemas de informação forem projetados de acordo com as exigências técnicas de documentações normativas não pertencentes ao conjunto de publicações do Exército, tais como as normas da ABNT, devem ser possuir essa documentação e disponibilizá-la à equipe de autoria, quando da realização dos processos de auditoria.

Seção VI
Dos Controles Contingenciais

Art. 17. O objetivo dos procedimentos de auditoria baseados nos controles de contingência é verificar a conformidade e a efetividade entre o que é estabelecido no plano de contingência, elaborado para manter a continuidade do serviço em situações de desastre ou violação da segurança, e as ações tomadas para sua efetivação prática.

Art. 18. Os requisitos básicos dos controles contingenciais são:

I - estar materializado na forma de um plano de contingência;

II - estar atualizados de acordo com a periodicidade estipulada (no seu próprio texto) para sua aplicação, a qual deverá ser baseada na realidade do seu uso;

III - estipular uma sistemática para treinamento e simulação de aplicação do plano de contingência.

IV - os requisitos gerados pelas análises de risco realizadas no ambiente do sistema de informação sob auditoria devem conduzir a elaboração do plano de contingência;

V - prever no plano de contingência:

a) forma de reação aos incidentes de segurança;

b) as responsabilidades cabíveis para cada etapa do plano, ou seja: constatação do problema, notificação dos responsáveis pelos procedimentos de reação, o tratamento do problema e o retorno a normalidade;

c) formas de localizar e contatar os pontos de contato para lidar com violações de segurança.

VI - no caso de plano de contingência para redes, deve-se utilizar o modelo previstos nas Instruções que tratam de segurança em redes.

Seção VII
Dos Controles de Risco

Art. 19. O objetivo dos procedimentos de auditoria baseados nos controles de risco é verificar a conformidade e a efetividade entre o que é estabelecido nas conclusões das análises de risco realizadas para os sistemas de informação sob auditoria e as providências decorrentes para cada caso.

Parágrafo único. O requisitos básicos dos controles de risco são aqueles resultantes das análises de risco realizadas para o sistema de informação sob auditagem e que devem constar dos relatórios correspondentes cujas orientações para sua elaboração se encontram nas Instruções Reguladoras sobre risco.

Seção VIII
Dos Controles de Pessoal

Art. 20. O objetivo dos procedimentos de auditoria baseados nos controles de pessoal é verificar a efetividade das ações de conscientização e treinamento do pessoal para a segurança da informação, assim como a conformidade entre essas ações e a documentação que estabelece a referências sobre o assunto.

Art. 21. Os requisitos básicos dos controles de pessoal são:

I - estabelecer normas de conduta para o pessoal, interno e externo, que minimizem os riscos quanto a violações de segurança da informação advindas de atos de negligência, imprudência, imperícia, acidentais ou má-fé.

II - seguir os moldes estabelecidos na doutrina de contra-inteligência;

III - quando de nível de estratégico, definir diretrizes sobre formação de recursos humanos na área de segurança da informação;

IV - quando de nível de tático ou operacional, estar voltados para treinamento de pessoal para o uso de **hardware** ou **software** computacional ou de comunicações para segurança da informação;

V - quando versarem sobre preparo de recursos humanos, devem existir programas de treinamento ou conscientização sobre as documentações normativas de segurança que abranjam tanto o pessoal iniciante quanto o treinamento periódico de atualização, assim como os registros das atividades desses programas ou treinamentos.

Art. 22. Devem existir controles que prevejam a existência de segregação de funções de modo que seja evitado que um indivíduo venha a controlar todos os estágios de um processo de manuseio de informação crítica para o sistema.

§ 1º As descrições das atribuições dos cargos devem refletir os princípios de segregação de funções.

§ 2º As responsabilidades por restringir o acesso de usuários a atividades críticas de operação e programação devem estar claramente definidas, divulgadas e aplicadas.

Seção IX
Dos Controles de Instalações Físicas, Materiais e Documentação

Art. 23. O objetivo dos procedimentos de auditoria baseados nos controles de instalações físicas, Materiais e Documentação é verificar a conformidade e a efetividade entre o que é estabelecido para a proteção das: áreas e instalações onde os suportes da informação se encontram; dos materiais de natureza sensível para a segurança das informações; e da documentação oficial da OM.

Parágrafo único. O requisito básico dos controles de instalações físicas é que devem ser baseados na documentação de segurança orgânica da OM a respeito de áreas e instalações.

Seção X
Dos Controles de Gerenciamento de Segurança

Art. 24. O objetivo dos procedimentos de auditoria baseados nos controles de gestão da segurança é verificar a conformidade e a efetividade entre o estabelecido nas atribuições de responsabilidades para gerir a segurança da informação constantes nas Instruções sobre segurança vigentes e as ações realizadas.

Art. 25. Os requisitos básicos dos controles de gerenciamento de segurança devem definir as responsabilidades da função de gestão de segurança da informação para o sistema de informação sob auditoria por meio da descrição dos procedimentos operacionais básicos, no mínimo, nas seguintes áreas:

I - normas utilizadas na gestão do sistema de informação;

II - elaboração, uso e atualização da documentação do sistema;

III - relatórios de gestão do risco;

IV - plano de contingência;

V - segurança da áreas e instalações;

VI - relatórios de auditorias;

VII - procedimentos de gestão do sistema de informação sob auditoria.

TÍTULO IV
DA VERIFICAÇÃO DA CONFORMIDADE E DA EFETIVIDADE

CAPÍTULO I
DOS PROCEDIMENTOS DE VERIFICAÇÃO

Art. 26. Os procedimentos de verificação devem buscar aferir se os controles escolhidos como referência para o processo de auditoria estão sendo satisfeitos (conformidade) e se há eficiência e eficácia nos processos auditados (efetividade).

Art. 27. Para a aferição dos controles devem ser empregadas as técnicas de auditoria que se façam necessárias conforme o tipo de recurso ou sistema auditado. No CAPÍTULO II, deste TÍTULO, estão listadas algumas das técnicas consideradas básicas.

§ 1º A técnica mais direta e simples para aferição da conformidade é de "listas de verificação". Exemplos destas listas, classificadas de acordo com os controles definidos nestas IR, estão publicados na Internet pelo portal do Exército e na Intranet pela página do CITEx.

§ 2º As listas de verificação não se restringem à técnica em si, mas podem ser utilizados como subsídios para emprego de outras técnicas de auditoria.

Art. 28. O processo de auditoria empregado deve ter sua sistemática definida como de um destes dois tipos: avaliação do sistema tipo I e tipo II.

§ 1º A avaliação tipo I é aquela na qual os sistemas são avaliados segundo critérios básicos de funcionamento de seu componentes que estejam sob auditoria. Em geral, a avaliação pode ser feita por pessoal não especializado no sistema, desde que paute o trabalho em um planejamento previamente elaborado e de acordo com estas Instruções.

§ 2º A avaliação tipo II é aquela na qual os componentes do sistema que esteja sob auditoria são avaliados segundo critérios detalhados e específicos. A avaliação deve ser feita por um especialista de área e que esteja familiarizado com as características técnicas do sistema avaliado.

Art. 29. Um inventário dos recursos do sistema de informação sob auditoria deve estar disponível e atualizado e elaborado conforme modelo constante das Normas Administrativas Relativas ao Material de Comunicações Estratégicas, Eletrônica, Guerra Eletrônica e Informática (NARMCEI) ou outras normas que venham a substituí-las.

Art. 30. Devem existir ferramentas e procedimentos definidos para o ambiente sob auditoria que viabilizem a salvaguarda dos dados e configurações do sistema durante o processo de auditoria.

Art. 31. para evitar transtornos decorrentes da suspensão parcial ou total dos serviços providos por um sistema de informação ou um de seus componentes durante o processo de auditoria, a aplicação desse processo deve:

a) contar com um planejamento prévio, no qual tarefas, responsabilidades e recursos sejam registrados;

b) que o contexto auditado e o nível de detalhamento dos testes sejam discutidos previamente com a gerência do sistema;

c) que os testes, preferencialmente, sejam limitados ao acesso e leitura de dados;

d) que sejam utilizados meios de registrar o que as ferramentas de auditoria utilizadas no processos realizem ou acessem nos recursos do sistema auditado.

Art. 32. No caso específico em que seja realizado um teste de invasão no sistema, é necessário que:

a) antes da aplicação do teste, os procedimentos básicos a serem empregados sejam registrados em um documento e comunicados formalmente ao Comandante da OM onde o sistema está implementado;

b) o Comandante da OM onde o teste será realizado deve ser comunicado com antecedência para que sejam providenciadas ações de salvaguarda de dados que possam ser indevidamente expostos ou acidentalmente corrompidos durante o teste.

Art. 33. Devem existir procedimentos registrados:

a) que garantam que a configuração dos sistemas corporativos e suas modificações subseqüentes sejam autorizadas e testadas antes de sua implementação;

b) de controle e documentação das alterações nos sistemas corporativos e motivo de sua realização;

c) sobre os procedimentos de revisão, aprovação, controle e edição de dados de entrada, para garantir sua integridade e prevenir erros;

d) sobre detecção de erro e correção.

CAPÍTULO II
DAS TÉCNICAS DE VERIFICAÇÃO

Art. 34. As técnicas listadas nestas Instruções devem servir como um referencial inicial para os responsáveis pela auditoria interna dos sistemas de informações do Exército, não esgotando as possibilidades.

Parágrafo único. As possíveis técnicas para verificação, assim como os critérios para a escolha da técnica adequada variam conforme as características do ambiente auditado. Cabe ao auditor tomar as decisões necessárias.

Art. 35. As técnicas básicas a serem consideradas nas auditorias de segurança de sistemas de informação do Exército são as seguintes:

I - ESTUDO DA DOCUMENTAÇÃO DO SISTEMA - análise da documentação técnica do sistema sob auditoria.

II - LISTAS DE VERIFICAÇÃO - técnica que se baseia na utilização de listas previamente elaboradas em função das características do ambiente auditado e que serve para aferição direta se um controle está ou não implementado, se é eficaz e eficiente.

III - VERIFICAÇÃO POR APLICATIVO DE COMPUTADOR - técnica baseada no uso de um **software** que verifica alguns pontos-chave do sistema auditado. Pode ser uma ferramenta que busca vulnerabilidades em serviços de rede ou em programas específicos, tais como sistemas operacionais.

IV - QUESTIONÁRIOS - conjunto de perguntas que os responsáveis pela auditoria aplicam aos responsáveis pelo ambiente auditado, a fim de levantarem informações sobre o atendimento ou não dos controles.

V - SIMULAÇÃO DE DADOS - técnica em que um conjunto de dados fictícios é submetido ao sistema auditado para que sejam criticadas as suas saídas.

VI - VISITA ÀS INSTALAÇÕES DO AMBIENTE AUDITADO - técnica na qual o auditor vai até as instalações do ambiente auditado observar os processos do uso do sistema auditado. Em geral, essa técnica é aplicada em conjunto com a técnica da entrevista.

VII - MAPEAMENTO DE PROGRAMAS - técnica com a qual se faz um levantamento estatístico do uso de serviços, programas ou rotinas de programas e visa, dentre outros objetivos, identificar processos em desuso ou fraudes. Em geral, necessita de **software** específico para sua aplicação ou utilitários existentes em sistemas operacionais de rede ou em aplicativos de gerência de redes.

VIII - ENTREVISTAS - reunião entre auditores e os responsáveis pelos sistemas auditados onde, por meio de perguntas preestabelecidas, busca-se obter informações sobre o atendimento ou não dos controles.

IX - ANÁLISE DE **LOG** - técnica que consiste na análise dos registros de eventos (l**ogs**) ocorridos em um sistema de informação ou um de seu componentes com a finalidade de identificar comportamentos que atentem contra a segurança.

X - ANÁLISE DE PROGRAMA FONTE - leitura direta do código fonte do programa.

XI - ANÁLISE DE RISCOS - análise realizada sobre os recursos de um sistema de informação cuja finalidade é estimar valor do risco que as informações de um sistema de informações estão correndo. Para um melhor entendimento sobre a aplicação deste tipo de análise, podem ser consultadas as Instruções do Exército sobre este tema.

TÍTULO V
DO PROCESSO DE AUDITORIA

CAPÍTULO I
DAS RESPONSABILIDADES ESPECÍFICAS E ETAPAS

Art. 36. A auditoria dos sistemas de informação do Exército deve ser periódica, cabendo ao Gabinete do Comandante, no caso dos seus órgãos subordinados; EME, para suas Subchefias; ODS e Grandes Comandos, para suas OM subordinadas, a responsabilidade de estipular, em consonância com orientações do Departamento de Ciência e Tecnologia, a periodicidade de auditoria de seus sistemas.

Art. 37. As etapas básicas que definem o processo de auditoria são os seguintes:

I - designação e credenciamento do pessoal a realizar o processo;

II - elaboração do plano da auditoria a ser realizada;

III - levantamento das informação sobre o sistema a ser auditado;

IV - identificação dos pontos de controle do sistema sob auditoria;

V - escolha dos controles necessários;

VI - seleção de quais pontos de controle serão verificados e a prioridade entre eles;

VII - avaliação dos pontos de controle selecionados;

VIII - reavaliação (repetição de algumas etapas para verificar acertos), se for o caso;

IX - conclusão da auditoria com emissão de relatório de auditoria, conforme ANEXO E.

CAPÍTULO II
DA DESIGNAÇÃO E CREDENCIAMENTO DE PESSOAL

Art. 38. O pessoal envolvido no processo deverá ser selecionado e credenciado de acordo com o prescrito nas Instruções Gerais para Salvaguarda de Assuntos Sigilosos e nas Normas para Concessão de Credencial de Segurança ou instrumento normativo e legal o valha, além de outras legislações ou documentos normativos internos que se façam necessários.

Parágrafo único. O Comandante, assessorado pelo seu Estado-Maior, identificará os assuntos que, em razão de um processo de auditoria, possam ser expostos aos aplicadores do processo e, em conseqüência, poderá requerer que os responsáveis pela auditoria assinem um termo de compromisso e manutenção de sigilo, conforme modelo (ou adaptação, conforme o caso) disponível nas Instruções Gerais para Salvaguarda de Assuntos Sigilosos .

Art. 39. O pessoal técnico designado para aplicar o processo de auditoria deverá ser escolhido conforme o perfil técnico necessário.

Parágrafo único. O Comandante da OM que realizará ou onde será realizada a auditoria, conforme o caso, deverá designar um militar que fará os levantamentos iniciais necessários para identificar o perfil técnico necessário às situações específicas a serem abordadas no processo de auditoria e, assim, tornar precisa a indicação dos técnicos que executarão o processo.

CAPÍTULO III
DA ELABORAÇÃO DO PLANO DE AUDITORIA

Art. 40. O plano de auditoria deverá definir o escopo coberto pela auditoria, os objetivos a serem alcançados, os recursos e as tarefas necessários à realização do processo de auditoria, assim como o cronograma de eventos.

Parágrafo único. Os recursos a serem demandados no processo de auditoria variam conforme a necessidade de cada sistema, sendo os mais comuns: humanos, tecnológicos, materiais, administrativos e financeiros.

Art. 41. A equipe que realiza a auditoria deve ser dividida em dois grupos: coordenação e execução.

§ 1º O grupo de coordenação deve ser responsável pela elaboração do plano, acompanhamento da execução, interpretação dos resultados e emissão do relatório de auditoria. Esse grupo deve ser composto pelos elementos de gerência dos sistemas envolvidos na auditoria e pelo gerente do próprio processo de auditoria.

§ 2º O grupo de execução deve ser responsável pela execução das tarefas previstas para a auditoria e deve ser constituído pelos especialistas de área que estão capacitados para aplicar as técnicas previstas no planejamento.

§ 3º Os trabalhos dos grupos de auditoria devem começar por uma reunião na qual devem ser definidos os objetivos e as tarefas do processo.

Art. 42. Os planos de auditoria devem levar em consideração os relatórios de auditorias realizadas anteriormente no escopo a ser analisado para fins de aprendizado e otimização dos procedimentos.

Art. 43. O plano de Auditoria deve seguir o modelo constante do ANEXO C.

CAPÍTULO IV
DO LEVANTAMENTO DAS INFORMAÇÕES

Art. 44. Cabe ao grupo de execução, a tarefa de levantamento de informações sobre o sistema a ser auditado.

Art. 45. O objetivo do levantamento de informações é caracterizar o sistema a ser auditado e prover os subsídios necessários à identificação dos pontos de controle.

Art. 46. As técnicas básicas para esse tipo de levantamento são: estudo de documentação, entrevistas, questionários e visita às instalações do ambiente auditado.

Parágrafo único. Por serem citadas como “básicas”, essas técnicas são indicadas para o caso geral, cabendo ao grupo de execução, sob os auspícios do grupo de coordenação, decidir quais técnicas devem ser mais adequadas conforme o caso.

Art. 47. O levantamento de informações deve enfocar não só as características do sistema, mas, também, as interfaces com outros sistemas de modo a prevenir testes em áreas não pertencentes ao contexto previamente definido.

Art. 48. A consolidação das informações levantadas devem ser feitas por meio de relatório a ser encaminhado à equipe de coordenação.

§ 1º As informações devem estar representadas tanto da forma descritiva quanto gráfica, de acordo com o que exprimir maior clareza da informação.

§ 2º O modelo do relatório pode seguir o estabelecido no ANEXO A, sendo que esse relatório pode já estar disponível na documentação da OM, como recomendado nestas Instruções, e caberá a equipe de execução decidir se o grau de detalhamento será o suficiente para a auditoria em andamento.

CAPÍTULO V
IDENTIFICAÇÃO DOS PONTOS DE CONTROLE

Art. 49. A identificação física dos pontos de controle é realizada pela equipe de execução.

Art. 50. Caso o ambiente a ser auditado já tenha passado por outros processos de auditoria, a documentação referente ao processo anterior deve estar a disposição da equipe de execução para fins de facilitação da identificação dos pontos de controle.

Art. 51. Os pontos de controle identificados devem ser relacionados e ter suas características principais registradas em relatório.

Art. 52. O modelo do relatório de caracterização dos pontos de controle deve seguir os moldes do ANEXO D, o qual é uma adaptação do ANEXO A.

Art. 53. A caracterização de cada ponto de controle deve conter, no mínimo, as seguintes informações:

I - Objetivos e funções do ponto de controle no sistema sob auditoria.

II - Parâmetros que permitam calcular ou estimar valores associados ao tipo de ponto de controle (se for o caso).

III - Tipos de configurações (lógicas e físicas, se for o caso) envolvidas.

IV - Vulnerabilidades que estejam aparentes.

V - Técnicas de auditoria julgadas adequadas para avaliar o ponto de controle.

CAPÍTULO VI
ESCOLHA DOS CONTROLES NECESSÁRIOS

Art. 54. A escolha dos controles necessários se constitui na pesquisa e obtenção dos controles que serão utilizados para aferir a conformidade e a efetividade do ponto de controle específico sob auditoria.

Parágrafo único. A escolha depende natureza dos ponto de controle que forma identificados, o que implicará na escolha de um ou mais dos controles relacionados nestas Instruções.

CAPÍTULO VII
PRIORIZAÇÃO DOS PONTOS DE CONTROLE

Art. 55. A priorização de quais pontos de controle devem ser avaliados visa estabelecer quais os pontos de controle que serão objeto dos procedimentos de auditoria e sua precedência.

Art. 56. Cabe à equipe de coordenação decidir quais e com que prioridade os pontos de controle devem ser avaliados.

Art. 57. Caso o número de pontos de controle e as informações disponíveis sobre eles denotem que a decisão sobre a priorização da avaliação seja complexa, deve-se utilizar o instrumento técnico e metodológico adequado para esses casos, que é a análise de riscos. Os pontos de controle que revelarem-se de maior risco deverão ser priorizados.

Parágrafo único. O método de análise de risco a ser empregado deve estar de acordo com as Instruções do Exército sobre este tema.

Art. 58. Se a complexidade das avaliações exigir, um plano específico deve ser elaborado para guiar os procedimentos da equipe de execução.

CAPÍTULO VIII
AVALIAÇÃO DOS PONTOS DE CONTROLE

Art. 59. A avaliação dos pontos de controle visa aplicar as técnicas necessárias para aferir se as medidas de segurança tomadas demonstram efetividade e conformidade com os controles necessários.

Art. 60. De acordo com os pontos de controles escolhidos, deve-se escolher as técnicas e testes mais adequados e os controles a serem considerados. Caso a gerência do sistema possua testes específicos para os pontos de controle considerados, a equipe de coordenação deve levá-los em consideração.

Art. 61. Ao aplicar as técnicas julgadas necessárias para avaliação do ponto de controle, o grupo de execução deve registrar quaisquer inadequações que sejam detectadas tanto nas técnicas empregadas quanto nos controles que servem como referência.

CAPÍTULO IX
CONCLUSÃO E REAVALIAÇÃO DA AUDITORIA

Art. 62. A conclusão do processo de auditoria visa prover informações sobre o estado do sistema auditado em termos de sua efetividade e conformidade. Além dessas informações, visa sugerir as medidas corretivas necessárias a adequação do sistema com os controles e dos próprios controles.

Art. 63. O fecho do processo de auditoria deve ser consolidado em um relatório de auditoria que deve seguir o modelo disponível no ANEXO E.

Art. 64. A documentação produzida durante o processo de auditoria deve ser arquivada pela equipe de coordenação para fins de histórico e aprendizado para auditorias futuras.

Art. 65. Todo o processo de análise de risco deverá ser documentado e comporá um processo, no qual deverá estar registrado o histórico das ações do processo.

Art. 66. O relatório final (ANEXO E) deve ser encaminhado ao Comandante da OM onde a auditoria foi realizada, cabendo a este, se julgar necessário, requerer documentos pertencentes ao processo para maiores informações.

Art. 67. A reavaliação da auditoria visa rever os pontos de controle para os quais foram detectadas inadequações que impliquem em riscos de segurança da informação não aceitáveis e, por essa razão, foram implementadas ações corretivas.

Art. 68. A documentação pertencente ao processo de auditoria será organizada em um ou mais volumes que deverão ser classificados conforme a sensibilidade da informação nele contida e armazenados em conformidade com o prescrito nas Instruções Gerais para Salvaguarda de Assuntos Sigilosos ou instrumento legal que o valha.

TÍTULO VI
DAS RESPONSABILIDADES

CAPÍTULO I
DO DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA

Art. 69. Compete ao Departamento de Ciência e Tecnologia:

I - Implementar o sistema de auditoria de segurança dos sistemas de informação do Exército Brasileiro, definindo:

a) a estrutura funcional necessária a ser empregada no DCT e pelas suas OMDS para realizar os processos de auditoria nas OM do Exército ou apoiar esses processos, quando solicitado;

b) as ferramentas de **software** e o **hardware** necessários para auditar os sistemas corporativos e os demais **softwares** empregados no Exército no processamento de informações corporativas;

c) o detalhamento da aplicação das técnicas de auditoria que se façam necessárias conforme as demandas que ocorrerem em processos específicos.

II - estabelecer os requisitos para especificação, aquisição, distribuição e atualização das ferramentas de **software** necessárias para realizar auditorias nas OM do Exército;

III - estabelecer requisitos básicos para inclusão de controles para auditoria nos sistemas corporativos do Exército;

IV - estabelecer as referências básicas (normas, modelos, orientações) para documentação de sistemas de informação, informatizados ou não , de acordo com a necessidade;

V - definir a sistemática de treinamento e atualização de pessoal para manuseio adequado das ferramentas e **hardware** de auditoria;

VI - manter a atualizada a doutrina relativa a auditoria de segurança da informação definidas nestas IR;

VII - manter o registro dos relatórios sobre as auditorias realizadas nas OM do Exército para fins de aprimoramento da doutrina de auditoria de segurança da informação;

VIII - prever no planejamento orçamentário as necessidades de recursos destinados à auditoria da segurança da informação nas OM do Exército;

IX - planejar, em conjunto com o CITEx, a aplicação de auditorias de segurança da informação nas OM do Exército, estipulando cronograma para aplicação, prioridade, data, duração, tipo de auditoria e responsabilidades;

X - acompanhar o cumprimento das atribuições destas Instruções;

XI - implementar as medidas cabíveis para adequação da doutrina de auditorias da segurança da informação, conforme os resultados da aplicação do processo de auditagem;

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

CAPÍTULO II
DO CENTRO DE DESENVOLVIMENTO DE SISTEMAS

Art. 70. Compete ao Centro de Desenvolvimento de Sistemas:

I - especificar as soluções de **software** e **hardware** para auditoria de segurança da informação conforme os requisitos estabelecidos pelo DCT;

II - desenvolver sistemas corporativos específicos de auditoria de segurança da informação conforme requisitos estabelecidos pelo DCT;

III - incluir nos sistemas corporativos controles de auditoria conforme requisitos estabelecidos pelo DCT;

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

V - 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 advindo do acompanhamento das novidades metodológicas e tecnológicas no setor.

CAPÍTULO III
DO CENTRO INTEGRADO DE TELEMÁTICA DO EXÉRCITO

Art. 71. Compete ao Centro Integrado de Telemática do Exército:

I - apoiar, por meio das suas OMDS, a realização dos processos de auditoria de segurança da informação nas OM do Exército, conforme planejamento, priorização e cronograma estabelecido pelo DCT;

II - informar o DCT as necessidades de especialização e tipos treinamento para o pessoal diretamente envolvido na realização de auditorias de segurança da informação e disseminação da doutrina;

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

IV - manter-se em condições de aplicar as técnicas de auditoria necessárias aos sistemas de informação existentes em sua área de atuação;

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

VI - manter uma base de dados sobre violações de segurança, ameaças e vulnerabilidades encontradas nas auditorias para fins de histórico;

VII - manter atualizada e divulgar, através das páginas eletrônicas do Exército e do CITEx, listas de verificação passíveis de utilização em processos de auditoria de sistemas de informação do Exército;

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

IX - remeter ao DCT os relatórios sobre as auditorias realizadas para fins de acompanhamento por aquele Órgão Setorial;

X - 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 a aplicação de processos de auditoria

XI - periodicamente, selecionar e treinar pessoal externo para receber a auditoria, abrangendo os seguintes aspectos: conceituação de auditoria; controles; processo de implantação das recomendações de auditoria.

CAPÍTULO IV
DO INSTITUTO MILITAR DE ENGENHARIA

Art. 72. 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 auditoria da segurança da informação;

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 no conhecimento adquirido com os resultados dos trabalhos de graduação e pós-graduação realizados sobre o tema.

CAPÍTULO VI
DA DIRETORIA DE SERVIÇO GEOGRÁFICO

Art. 73. Compete à Diretoria de Serviço Geográfico:

I - 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 VIII
DO CENTRO INTEGRADO DE GUERRA ELETRÔNICA

Art. 74. Compete ao Centro Integrado de Guerra Eletrônica:

I - informar o DCT as necessidades de especialização e tipos treinamento para o pessoal diretamente envolvido na realização de auditorias de segurança da informação e disseminação da doutrina no âmbito das atividades de Guerra Eletrônica;

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

III - manter-se em condições de aplicar as técnicas de auditoria necessárias aos sistemas de informação existentes em sua área de atuação;

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

V - 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 a aplicação desta norma.

CAPÍTULO VIII
DO GRUPO FINALÍSTICO DE SEGURANÇA DA INFORMAÇÃO

Art. 75. Compete ao Grupo Finalístico de Segurança da Informação:

I - desenvolver em conjunto com o DCT, CDS e CITEx processos pelos quais possa obter e informações de auditoria que possibilitem diagnosticar o estado da segurança na Força e, em conseqüência, direcionar a escolha ou adequação de linhas de pesquisa no Grupo.

II - propor ao DCT o planejamento relativo à pesquisa e o desenvolvimento de soluções computacionais e metodológicas na área de auditoria.

CAPÍTULO IX
DO CENTRO DE INTELIGÊNCIA DO EXÉRCITO

Art. 76. Compete ao Centro de Inteligência do Exército:

I - realizar os processos de auditoria nos sistemas de informação componentes do Sistema de Inteligência do Exército (SIEx);

II - atuar em parceria com o DCT, para fins de compartilhamento de informações e aprendizado, a respeito de mecanismos utilizados em violações de segurança da informação identificadas no SIEx, as quais potencialmente representem ameaça a outros Sistemas do Exército.

CAPÍTULO X
DAS OM DO EXÉRCITO

Art. 77. 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, estarem em condições adequadas para serem auditados.

ANEXO A
MODELO DE RELATÓRIO DE DESCRIÇÃO DE SISTEMAS DE INFORMAÇÃO

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
OM

RELATÓRIO DE CARACTERIZAÇÃO DE SISTEMAS DE INFORMAÇÃO DA OM XXX

1. APRESENTAÇÃO:

(Resumo informativo sobre as características do sistema de informação, contendo o nome do sistema, sua abrangência de aplicação e sua finalidade)

2. OBJETIVO:

(enunciar os objetivos específicos, se for o caso, em que se desdobra a finalidade do sistema)

3. SERVIÇOS OFERECIDOS:

(descrição dos serviços automatizados oferecidos pelo sistema de informações e suas configurações)

4. SOFTWARES UTILIZADOS:

(lista dos **softwares** utilizados na implementação dos serviços, assim como sua localização, ou seja, equipamentos onde estão instalados e as mídia dos **softwares** originais)

5. HARDWARE UTILIZADO:

(lista dos equipamentos da infra-estrutura computacional e de redes utilizados na implementação do sistema de informação, assim como sua configuração e localização física)

6. INFRA-ESTRUTURA LÓGICA:

(descrição da infra-estrutura lógica de cabeamento de rede, sua configuração lógica e arquitetura física, devendo esta descrição contar com esquemas gráficos, para melhor visualização da descrição)

7. INFRA-ESTRUTURA DE ALIMENTAÇÃO ELÉTRICA:

(descrição da infra-estrutura de alimentação elétrica, devendo constar a distribuição de pontos de alimentação, localização dos quadros de distribuição, tipo e capacidade dos disjuntores principais e esquemas gráficos para melhor visualização da infra-estrutura)

8. PESSOAL:

(descrição do tipo de usuário que utiliza o sistema de informação - gerentes, usuários e manutenção - e o seu grau de privilégio em relação ao uso ou configuração do sistema)

9. NORMAS APLICÁVEIS:

(conjunto de normas de segurança, técnicas ou administrativas aplicáveis ao sistema de informação sob auditoria)

10. PROCEDIMENTOS OPERACIONAIS PADRÃO:

(conjunto de pop relacionados à gestão, uso e manutenção do sistema de informação em uso)

11. RELATÓRIOS DE AUDITORIAS OU ANÁLISES DE RISCO ANTERIORES:

(conjunto de relatórios sobre riscos e auditorias realizadas antes da auditoria em andamento)

Local, data

Assinatura do responsável(eis) pela descrição do sistema de informação sob auditoria

12. PARECER:

(parecer do Comandante contando observações adicionais que sejam necessários)

Assinatura do Comandante da OM onde o sistema de informação está implementado

ANEXO B
MODELO DE NORMA PARA SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
OM

NORMA DE SEGURANÇA DA INFORMAÇÃO PARA O SISTEMAS DE INFORMAÇÃO DA OM XXX

1. APRESENTAÇÃO:

(Resumo informativo sobre as características do sistema de informação, contendo o nome do sistema, sua abrangência de aplicação e sua finalidade. Note-se que o sistema de informação, conforme conceituação feita nestas Instruções pode ter várias configurações, sendo umas das mais comuns, a rede de computadores da OM. Logo, a expressão "sistema de informação", constante no título deste modelo, pode ser substituída conforme o contexto em que for aplicado.)

2. OBJETIVO:

(Enunciar os objetivos específicos, se for o caso, em que se desdobra a finalidade do sistema.)

3. CONCEITOS BÁSICOS

(Conceitos julgados necessários para entendimento das do teor deste documento e que podem ser tanto teóricos, quanto jargão técnico específico do tipo de características do sistema de informação a ser protegido.)

4. REGRAS DE SEGURANÇA:

(Conjunto de regras de segurança a serem obedecidas para proteção do sistema de informação. As regras devem estar distribuídas em diversas categorias conforme a complexidade do sistema de informação, podendo o resultados destas regras se consolidar como uma documentação extensa e com vários capítulos. As categorias variaram conforme as características do sistema de informação, no entanto, um rol mínimo é sugerido a seguir.)

a. SERVIÇOS UTILIZADOS

(Caracterização dos serviços automatizados do sistema de informação, sua finalidade e configurações de segurança necessárias.)

b. **SOFTWARES** UTILIZADOS:

(Descrição das configurações de segurança dos **softwares** utilizados na implementação dos serviços.)

c. **HARDWARE** UTILIZADO:

(Descrição das configurações de segurança do **hardware** utilizado na implementação dos serviços.)

d. INFRA-ESTRUTURA LÓGICA:

(Descrição das configurações de segurança da infra-estrutura lógica de cabeamento de rede e dos equipamentos de interligação de rede.)

e. INFRA-ESTRUTURA DE ALIMENTAÇÃO ELÉTRICA:

(Descrição das configurações de segurança da infra-estrutura da alimentação elétrica que provê energia aos equipamentos que implementam o SI.)

f. PESSOAL:

(Descrição das regras de segurança sobre os procedimentos relacionados ao pessoal que utiliza o SI, seja na gerência, na manutenção ou uso final.)

5. RESPONSABILIDADES:

(Descrição das responsabilidades dos usuários, nas categorias que forem julgadas pertinentes - as categorias "básicas" são previstas Regulamento Interno e dos Serviços Gerais (R-1)).

Local, data

Assinatura do Comandante da OM onde o sistema de informação está implementado

ANEXO C
PLANO DE AUDITORIA

1. FINALIDADE

Transcrição da finalidade do plano. (Exemplo: A finalidade deste plano é descrever os procedimentos necessários para executar uma auditoria de segurança da informação no ambiente de rede local da OM "...".)

2. OBJETIVOS

Transcrição dos objetivos necessários para cumprir a finalidade do plano. (Exemplo: A fim de cumprir a finalidade enunciada, os seguintes objetivos são estipulados: definição dos grupos envolvidos na condução do processo, assim como as respectivas responsabilidades; descrição dos procedimentos para aplicação das técnicas escolhidas para execução da auditoria de segurança da informação.)

3. ESCOPO

Descrição do escopo que a auditoria abrange. Devem ser esclarecidos quais os equipamentos, **softwares**, instalações, processos etc que comporão os pontos de controle a serem verificados.

4. TAREFAS E RECURSOS

Neste item devem constar os procedimentos (tarefas) básicas a serem seguidas no processo de auditoria e os recursos necessários. É recomendável que sejam utilizadas tabelas com subdivisões separadas por objetivos para cada grupo de tarefas.

5. ATRIBUIÇÕES E RESPONSABILIDADES

Identificação das atribuições e responsabilidades no processo de acordo com o estabelecido por estas IR.

6. CRITÉRIOS PARA REGISTRO DE DADOS DE ACOMPANHAMENTO

Descrição do fluxo do documento para fins de acompanhamento.

7. CRONOGRAMA

Descrição das fases do processo em formato de cronograma.

Cidade, ... de .....de .....

Assinatura do responsável pelo planejamento.

DE ACORDO:

Assinatura do Comandante da Unidade que aplicará o processo de auditoria.

ANEXO D
MODELO DE RELATÓRIO DE CARACTERIZAÇÃO DE PONTO DE CONTROLE

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
OM

RELATÓRIO DE CARACTERIZAÇÃO DE PONTOS DE CONTROLE SOB AUDITORIA NO SISTEMAS DE INFORMAÇÃO DA OM XXX

1. APRESENTAÇÃO:

(Resumo informativo sobre as características do ponto de controle, sua finalidade e a delimitação estabelecida no processo de auditoria, sua abrangência de aplicação e)

2. OBJETIVO:

(Enunciar os objetivos específicos, se for o caso, em que se desdobra a finalidade do ponto de controle)

3. CARACTERIZAÇÃO DO PONTO DE CONTROLE

(Descrição do ponto de controle, destacando as categorias do sistema a serem verificadas. As categorias espelham as descritas no relatório de caracterização do sistema de informação, sendo que não necessariamente deverão constar todas)

a. SERVIÇOS OFERECIDOS:

(descrição dos serviços automatizados oferecidos pelo sistema de informações e suas configurações)

b. **SOFTWARES** UTILIZADOS:

(lista dos **softwares** utilizados na implementação dos serviços, assim como sua localização, ou seja, equipamentos onde estão instalados e as mídia dos **softwares** originais)

c. **HARDWARE** UTILIZADO:

(lista dos equipamentos da infra-estrutura computacional e de redes utilizados na implementação do sistema de informação, assim como sua configuração e localização física)

d. INFRA-ESTRUTURA LÓGICA:

(descrição da infra-estrutura lógica de cabeamento de rede, sua configuração lógica e arquitetura física, devendo esta descrição contar com esquemas gráficos, para melhor visualização da descrição)

e. INFRA-ESTRUTURA DE ALIMENTAÇÃO ELÉTRICA:

(descrição da infra-estrutura de alimentação elétrica, devendo constar a distribuição de pontos de alimentação, localização dos quadros de distribuição, tipo e capacidade dos disjuntores principais e esquemas gráficos para melhor visualização da infra-estrutura)

f. PESSOAL:

(descrição do tipo de usuário que utiliza o sistema de informação - gerentes, usuários e manutenção - e o seu grau de privilégio em relação ao uso ou configuração do sistema)

g. NORMAS APLICÁVEIS:

(conjunto de normas de segurança, técnicas ou administrativas aplicáveis ao sistema de informação sob auditoria)

h. PROCEDIMENTOS OPERACIONAIS PADRÃO:
(conjunto de pop relacionados à gestão, uso e manutenção do sistema de informação em uso)

Local, data

Assinatura do responsável(eis) pela descrição do ponto de controle sob auditoria

ANEXO E
MODELO DE RELATÓRIO DE AUDITORIA

MINISTÉRIO DA DEFESA
EXÉRCITO BRASILEIRO
OM

RELATÓRIO DE AUDITORIA DA SEGURANÇA DA INFORMAÇÃO SOBRE OS SERVIÇOS DE REDES DA OM XXX

RELATÓRIO NR____

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. DOCUMENTAÇÃO NORMATIVA DE REFERÊNCIA:
(Normas que servirão como controles normativos para realização da auditoria)

4. PERÍODO DA FISCALIZAÇÃO:
(período em que a auditoria foi realizada)

5. EQUIPE RESPONSÁVEL:
(lista do pessoal que executou a auditoria e as respectivas atribuições)

6. METODOLOGIA ADOTADA:
(Método adotado para executar a auditora. 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)

7. OBJETO:
(Elemento(s) sobre o(s) qual(is) a auditoria será focada)

8. CONTEXTO:

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

9. FATOS RELEVANTES:

(descrição detalhada dos fatos relevantes no que diz respeito a 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)

10. 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 auditoria

11. PARECER:

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

OFÍCIO Nº 120-A1.3-DCT, DE 22 DE FEVEREIRO DE 2007.

Estágio de Proteção Radiológica.

De acordo com o que estabelece a Portaria nº 036-SCT, de 2 de julho de 2002, que aprova as Instruções Reguladoras da Inscrição, da Seleção e da Matrícula nos Estágios de Proteção Radiológica (EPR), foram fixadas as datas de início e término de Estágios Básico e Avançado de Proteção Radiológica, conforme quadro abaixo:

ESTÁGIO	INÍCIO	TÉRMINO
BÁSICO	14 Maio 07	25 Maio 07
AVANÇADO	01 Out 07	23 Nov 07

3ª PARTE
ATOS DE PESSOAL

ATOS DO PODER EXECUTIVO

MINISTÉRIO DA DEFESA

DECRETO DE 22 DE FEVEREIRO DE 2007.

Exoneração do cargo de Chefe do Departamento de Engenharia e Construção

O **PRESIDENTE DA REPÚBLICA**, no uso da atribuição que lhe confere o art. 84, inciso XIII, da Constituição, resolve

E X O N E R A R

no âmbito do Comando do Exército, o General-de-Exército ENZO MARTINS PERI, do cargo de Chefe do Departamento de Engenharia e Construção, a partir de 22 de fevereiro de 2007.

(Decreto publicado no Diário Oficial da União nº 37, de 23 de fevereiro de 2007 – Seção 2).

SECRETARIA DE ORGANIZAÇÃO INSTITUCIONAL

PORTARIA Nº 181-SEORI/MD, DE 16 DE FEVEREIRO DE 2007.

Dispensa militar de ficar à disposição do Ministério da Defesa

O **SECRETÁRIO DE ORGANIZAÇÃO INSTITUCIONAL DO MINISTÉRIO DA DEFESA**, no uso da competência que lhe foi subdelegada pelo contido no art. 4º da Portaria Normativa nº 852/MD, de 1º de julho de 2005, publicada no Diário Oficial da União nº 127, Seção 1, de 5 de julho de 2005, resolve

DISPENSAR

o CB QM 10-55 ANDRÉ LUIZ MENDES de ficar à disposição do Ministério da Defesa, a contar de 16 de fevereiro de 2007.

PORTARIA Nº 182-SEORI/MD, DE 16 DE FEVEREIRO DE 2007

Dispensa militares de ficarem à disposição do Ministério da Defesa

O **SECRETÁRIO DE ORGANIZAÇÃO INSTITUCIONAL DO MINISTÉRIO DA DEFESA**, no uso da competência que lhe foi subdelegada pelo contido no art. 4º da Portaria Normativa nº 852/MD, de 1º de julho de 2005, publicada no Diário Oficial da União nº 127, Seção 1, de 5 de julho de 2005, resolve

DISPENSAR

os militares abaixo relacionados de ficarem à disposição do Ministério da Defesa, a contar de 15 de fevereiro de 2007:

- 1º Ten QAO Adm G LAÉDIO KUMM; e
- 1º Sgt Art ROBERTO CARLOS CRISPIM DOS SANTOS.

(As Portarias nºs 181 e 182 encontram-se publicadas no Diário Oficial da União nº 38, de 26 de fevereiro de 2007 – Seção 2).

COMANDANTE DO EXÉRCITO

PORTARIA Nº 068, DE 22 DE FEVEREIRO DE 2007.

Designação para participação em viagem de serviço.

O **COMANDANTE DO EXÉRCITO,** no uso da atribuição que lhe confere o inciso VII do art. 1º do Decreto nº 2.790, de 29 de setembro de 1998, combinado com o art. 19 da Lei Complementar nº 97, de 9 de junho de 1999, e de acordo com o Plano de Visitas e outras Atividades em Nações Amigas (PVANA), relativo ao ano de 2007, resolve

DESIGNAR

os militares a seguir nominados, todos do B DOMPSA, para visita ao **U. S. Army Quartermaster Center and School – Fort Lee** (Atv X 07/002), em **Fort Lee**, no estado de Virgínia, nos Estados Unidos da América, prevista para ser realizada no mês de março de 2007:

- Cap Int EUDSON BEZERRIL DE MELO SOARES;
- 1º Ten Int JOSE JOÃO DE AZEVEDO JUNIOR;
- 2º Sgt Int JUAN CARLOS AIZCORBE AYERRA; e
- 2º Sgt Int ALEXANDRE BANDEIRA MENEZES.

Para fim de aplicação da Lei nº 5.809, de 10 de outubro de 1972, regulamentada pelo Decreto nº 71.733, de 18 de janeiro de 1973, com as alterações constantes dos Decretos nº 3.643, de 26 de outubro de 2000, e nº 3.790, de 18 de abril de 2001, a missão está enquadrada como eventual, militar, sem mudança de sede, sem dependentes e será realizada com ônus para o Exército Brasileiro, parcial no tocante a diárias no exterior e total com referência ao deslocamento.

PORTARIA Nº 069, DE 22 DE FEVEREIRO DE 2007.

Designação para participação em viagem de serviço.

O **COMANDANTE DO EXÉRCITO**, no uso da atribuição que lhe confere o inciso VII do art. 1º do Decreto nº 2.790, de 29 de setembro de 1998, combinado com o art. 19 da Lei Complementar nº 97, de 9 de junho de 1999, resolve

DESIGNAR

os militares a seguir nominados, para realizar a viagem de Reconhecimento à Missão das Nações Unidas para Estabilização no Haiti (MINUSTAH), na cidade de Porto Príncipe, no Haiti, com início previsto na 2ª quinzena de fevereiro:

- Gen Div RENATO INDIO DA COSTA LEMOS, do DGP;
- Cel Inf JULIO CESAR DE SALES, do Cmdo CML;
- Cel Inf TOMÁS MIGUEL MINÉ RIBEIRO PAIVA, do COTER;
- Cel Cav CARLOS JORGE JORGE DA COSTA; do CCOMSEX;
- Ten Cel Eng ANTONIO CÉSAR ALVES ROCHA; do DEC;
- Ten Cel Eng DOUGLAS BASSOLI, do CIE;
- Ten Cel Cav ÁTILA GONÇALVES TORRES JUNIOR, do EME;
- Ten Cel Inf EDISON NADAL PIMENTA, do EME;
- Ten Cel Art PAULO LIZARDO VALENTIM DE MATTOS, da Cmdo 4ª Bda C Mec;
- Maj Int MARCIO CORDEIRO FREIRE; do EME;
- Maj Com JOÃO MARINONIO ENKE CARNEIRO, do COTER;

- Maj Art CESAR AUGUSTO ROSA DE ARAUJO, do Cmdo 3ª DE;
- Maj Inf CARLOS HENRIQUE FERREIRA DE MELLO, do 63º BI;
- Maj Eng MAURI MARCELO FELIX FREITAS, do 9º B E Cmb;
- Cap Art DAVIDSON PAIXÃO DE OLIVEIRA ALVES; do 3º GAC / Ap;
- Cap Inf MARCOS AURÉLIO DE LIMA OLIVEIRA, do 7º BIB;
- Cap Int LUIZ HENRIQUE GONÇALVES PLUM, do CAEx;
- Cap QEM RODRIGO PEREIRA LOPES, da CRO / 9ª RM;
- Cap Eng ANDREOS SOUZA, do 2º B E Cnst; e
- 1º Ten Com ALAN DIEGO FLACH, da 3ª Cia Com Bld.

Para fim de aplicação da Lei nº 5.809, de 10 de outubro de 1972, regulamentada pelo Decreto nº 71.733, de 18 de janeiro de 1973, a missão está enquadrada como eventual, militar, sem mudança de sede, sem dependentes e será realizada com ônus total para o Exército Brasileiro no tocante a diárias no exterior e sem qualquer ônus com referência ao deslocamento.

PORTARIA Nº 070, DE 22 DE FEVEREIRO DE 2007.

Designação para participação em viagem de serviço.

O **COMANDANTE DO EXÉRCITO,** no uso da atribuição que lhe confere o inciso VII do art. 1º do Decreto nº 2.790, de 29 de setembro de 1998, combinado com o art. 19 da Lei Complementar nº 97, de 9 de junho de 1999, e de acordo com o Plano de Visitas e outras Atividades em Nações Amigas (PVANA), relativo ao ano de 2007, resolve

DESIGNAR

o Cel QEM AMIR ELIAS ABDALLA KURBAN e o Maj QEM MARCELO DE CARVALHO PRATES, ambos do DEC, para participar da Visita ao Centro de Meio Ambiente do Exército Americano (Atv X 07/014), a realizar-se na cidade de **Maryland**, nos Estados Unidos da América, com início previsto para a 2ª quinzena de março de 2007.

Para fim de aplicação da Lei nº 5.809, de 10 de outubro de 1972, regulamentada pelo Decreto nº 71.733, de 18 de janeiro de 1973, a missão está enquadrada como eventual, militar, sem mudança de sede, sem dependentes e será realizada com ônus para o Exército Brasileiro, parcial no tocante a diárias no exterior e total com referência ao deslocamento.

PORTARIA Nº 071, DE 22 DE FEVEREIRO DE 2007.

Designação para participação no vôo de apoio à Operação Antártica.

O **COMANDANTE DO EXÉRCITO**, no uso da atribuição que lhe confere o inciso VII do art. 1º do Decreto nº 2.790, de 29 de setembro de 1998, combinado com o art. 19 da Lei Complementar nº 97, de 9 de junho de 1999, resolve

DESIGNAR

o Gen Div JEANNOT JANSEN DA SILVA FILHO, do Cmdo 8ª RM / 8ª DE, para participar do 6º Vôo de Apoio à Operação Antártica XXV, a realizar-se na 1ª quinzena de março de 2007.

Para fim de aplicação da Lei nº 5.809, de 10 de outubro de 1972, regulamentada pelo Decreto nº 71.733, de 18 de janeiro de 1973, a missão está enquadrada como eventual, militar, sem mudança de sede, sem dependentes e será realizada com ônus parcial para o Exército Brasileiro no tocante a diárias no exterior e sem qualquer ônus com referência ao deslocamento.

PORTARIA Nº 072, DE 23 DE FEVEREIRO DE 2007.

Designação para participação em viagem de serviço.

O **COMANDANTE DO EXÉRCITO,** no uso da atribuição que lhe confere o inciso VII do art. 1º do Decreto nº 2.790, de 29 de setembro de 1998, combinado com o art. 19 da Lei Complementar nº 97, de 9 de junho de 1999, e de acordo com o Plano de Visitas e outras Atividades em Nações Amigas (PVANA), relativo ao ano de 2007, resolve

DESIGNAR

os militares a seguir nominados, para a visita ao Centro Alemão de Operações de Paz (Atv X 07/038), na cidade de **Hammelburg**, na Alemanha, com início previsto para a 2ª quinzena de março de 2007:

- Cel Inf EDIVALDO BARBOSA RODRIGUES DE SOUSA, do COTER;
- Ten Cel Inf ROLANT VIEIRA JÚNIOR, do EME; e
- Maj Inf NELSON RICARDO FERNANDES DA SILVA, do C I Op Paz.

Para fim de aplicação da Lei nº 5.809, de 10 de outubro de 1972, regulamentada pelo Decreto nº 71.733, de 18 de janeiro de 1973, a missão está enquadrada como eventual, militar, sem mudança de sede, sem dependentes e será realizada com ônus para o Exército Brasileiro, parcial no tocante a diárias no exterior e total com referência ao deslocamento.

PORTARIA Nº 073, DE 23 DE FEVEREIRO DE 2007.

Designação para participação em conferência internacional.

O **COMANDANTE DO EXÉRCITO,** no uso da atribuição que lhe confere o inciso VII do art. 1º do Decreto nº 2.790, de 29 de setembro de 1998, combinado com o art. 19 da Lei Complementar nº 97, de 9 de junho de 1999, e de acordo com o Plano de Visitas e outras Atividades em Nações Amigas (PVANA), relativo ao ano de 2007, resolve

DESIGNAR

os militares a seguir nominados, todos do EME, para participar do Apoio da Secretaria Executiva Permanente da Conferência dos Exércitos Americanos à Conferência Especializada e Exercício de Assistência em Casos de Desastre (Atv X 07/039), a realizar-se na cidade de Caracas, na Venezuela, com início previsto para a 2ª quinzena de março de 2007:

- Cel Inf PAULO SERGIO AUGUSTO DO AMARAL;
- Cel Inf LUIZ CARLOS PEREIRA GOMES; e
- ST Inf LUSALEM DA SILVA MATTOS.

Para fim de aplicação da Lei nº 5.809, de 10 de outubro de 1972, regulamentada pelo Decreto nº 71.733, de 18 de janeiro de 1973, a missão está enquadrada como eventual, militar, sem mudança de sede, sem dependentes e será realizada com ônus para o Exército Brasileiro, parcial no tocante a diárias no exterior e total com referência ao deslocamento.

PORTARIA Nº 075, DE 26 DE FEVEREIRO DE 2007

Nomeação de comandante, chefe ou diretor de organização militar

O **COMANDANTE DO EXÉRCITO**, considerando o disposto no art. 19 da Lei Complementar nº 97, de 9 de junho de 1999, e de acordo com o art. 9º, inciso II, alínea a), do Regulamento de Movimentação para Oficiais e Praças do Exército, aprovado pelo Decreto nº 2.040, de 21 de outubro de 1996, resolve

NOMEAR

por necessidade do serviço, **ex officio**, para o cargo de Chefe do C Doc Ex (Brasília - DF), o Cel Cav JORGE ALBERTO FORRER GARCIA.

PORTARIA Nº 076, DE 26 DE FEVEREIRO DE 2007.

Designação para participação no vôo de apoio à Operação Antártica.

O **COMANDANTE DO EXÉRCITO**, no uso da atribuição que lhe confere o inciso VII do art. 1º do Decreto nº 2.790, de 29 de setembro de 1998, combinado com o art. 19 da Lei Complementar nº 97, de 9 de junho de 1999, resolve

TORNAR SEM EFEITO

a designação do Gen Div LUIZ GUILHERME TERRA AMARAL, do CIE, para participar do 6º Vôo de Apoio à Operação Antártica XXV, a realizar-se na 1ª quinzena de março de 2007, conforme a Portaria nº 064, de 14 de fevereiro de 2007, publicada no Boletim do Exército nº 08, de 23 de fevereiro de 2007.

SECRETARIA-GERAL DO EXÉRCITO

PORTARIA Nº 052-SGEx, DE 22 DE FEVEREIRO DE 2007.

Retificação de data de término de decênio da Medalha Militar

O **SECRETÁRIO-GERAL DO EXÉRCITO**, no uso da competência que lhe é conferida pelo art. 1º, Inciso XVII, da Portaria do Comandante do Exército nº 761, de 2 de dezembro de 2003, resolve

RETIFICAR

a data de término de decênio do 1º Sgt Com (041962194-1) EDILSON COSTA CUSTÓDIO, de 2 de fevereiro de 2000 para 29 de janeiro de 1997, constante da Portaria nº 027-DGP/DCA, de 23 de maio de 2000, publicada no BE nº 022, de 2 de junho de 2000.

PORTARIA Nº 053-SGEx, DE 28 DE FEVEREIRO DE 2007.

Concessão de Medalha Militar

O **SECRETÁRIO-GERAL DO EXÉRCITO,** no uso da competência que lhe é conferida pelo art. 1º, inciso XVII, da Portaria do Comandante do Exército nº 761, de 2 de dezembro de 2003, resolve

CONCEDER

a Medalha Militar e Passador de Bronze, nos termos do Decreto nº 4.238, de 15 de novembro de 1901, regulamentado pelo Decreto nº 39.207, de 22 de maio de 1956 e com a redação dada pelo Decreto nº 70.751, de 23 de junho de 1972, aos militares abaixo relacionados, por terem completado dez anos de bons serviços nas condições exigidas pela Portaria do Comandante do Exército nº 322, de 18 de maio de 2005.

Posto/Grad Arma/Q/Sv	Identidade	Nome	Término do decênio	OM
Cap Inf	011480134-3	ANGELO ANTONIO ASSUNÇÃO SANTANA	06 Fev 06	2º B Av Ex
Cap Dent	036727223-4	EDUARDO DE OLIVEIRA	17 Jan 06	H Gu Santa Maria

Posto/Grad Arma/Q/Sv	Identidade	Nome	Término do decênio	OM
Cap Eng	101071314-5	WAGNER FERNANDES DOS SANTOS	07 Fev 05	9º BE Cnst
1º Ten QCO	019266233-6	ABÍLIO DE SOUSA PAIVA	02 Fev 01	H Gu Tabatinga
1º Ten Cav	013054454-7	EDUARDO NOBRE BUENO BRANDÃO	19 Fev 07	1ª Cia Intlg
1º Ten Com	041964564-3	ELBER FÁBIO DOS SANTOS	19 Fev 07	CI Av Ex
1º Ten Eng	013054084-2	ERIC MONIOS	19 Fev 07	5º BE Cnst
1º Ten Inf	101092774-5	FRANCISCO ALFREDO PESSOA MOTA JÚNIOR	19 Fev 07	10ª Cia Gd
1º Ten Int	019470253-6	FREDERICO SANTOS DE AMORIM	19 Fev 07	CMB
1º Ten Inf	013029784-9	FREDERICO VIEIRA CABRAL MENDES	19 Fev 07	71º BI Mtz
1º Ten Inf	013028334-4	GLÊDSON CÉSAR FERREIRA DE AZEVÊDO	19 Fev 07	71º BI Mtz
1º Ten Com	013028344-3	GUSTAVO LYRIO DE OLIVEIRA	19 Fev 07	CI Av Ex
1º Ten Eng	013054554-4	IRAPUAN IGOR MORAES MEDEIROS	19 Fev 07	7º BE Cnst
1º Ten Eng	101080794-7	JOSÉ ADILSON ANDRADE SILVA	19 Fev 07	5º BE Cnst
1º Ten Inf	101042794-4	LUIZ JUVENAL GOMES VIEIRA JÚNIOR	19 Fev 07	71º BI Mtz
1º Ten Cav	030874884-7	LUIZ ROBERTO GONÇALVES	19 Fev 07	16º Esqd C Mec
1º Ten Inf	031782354-0	MARCELO RODRIGUES	19 Fev 07	1ª Cia Intlg
1º Ten Art	020499304-2	UBIRAJARA OLIVEIRA VIEIRA DAS NEVES	19 Fev 07	CI Av Ex
1º Ten QCO	019546773-3	VLADIMIR REIS JOAQUIM LOPES	25 Out 06	DGP
2º Sgt Com	033295494-0	ALMIR MARCOS MENDES DE SOUZA	28 Jan 07	4º B Com
2º Sgt Mnt Com	011356784-6	ANDERSON ARGOLO DA SILVA	25 Jan 06	EsAEx
2º Sgt Inf	030871594-5	ANDRÉ LUIZ DA SILVA	09 Mar 05	9º BI Mtz
2º Sgt Int	011462874-6	ANTONIO JUNIOR LEITE MINERVINO	31 Jan 07	31º BI Mtz
2º Sgt Art	043461194-3	EDER DE PAULA SOUZA TELES	03 Fev 06	12º GAC
2º Sgt Com	043462064-7	EDÍLIO NERES DA SILVA	31 Jan 07	Cia Cmdo 13ª Bda Inf Mtz
2º Sgt Cav	018767283-7	EVERALDO ALVES BOA SORTE	31 Jan 07	B Adm Ap/1ª RM
2º Sgt Inf	043443104-5	FABIO PEREIRA SOUZA	25 Jan 06	9º BI Mtz
2º Sgt Inf	030695104-7	GLAUDIO MONTE DE ÁVILA	31 Jan 07	9º BI Mtz
2º Sgt Eng	043439894-7	JOÃO DA SILVA CERQUEIRA	25 Jan 06	EsAEx
2º Sgt Inf	043459964-3	MARCOS WAGNER SANTOS DE ALBUQUERQUE	31 Jan 07	3º BPE
2º Sgt Inf	043455524-9	TACÍLIO LEONARDO FERREIRA DE OLIVEIRA	31 Jan 07	11º BI Mth
3º Sgt Com	093782894-5	ALMIR DE JESUS VASCONCELOS FILHO	22 Mar 06	18º GAC
3º Sgt Eng	043508004-9	ARMANDO DA SILVA MOURA	12 Ago 06	9º BEC
3º Sgt Inf	043463874-8	CIDINES PEREIRA DE SOUZA	22 Mar 06	9º BI Mtz
3º Sgt Int	013185164-4	ISMAEL BENTANCOURT GOMES	29 Jan 07	21ª Bia AAAe Pqdt
3º Sgt Sau	033210374-6	JOÃO NELIO DOS SANTOS TEODORO	09 Mar 05	5º BEC Bld
3º Sgt Mus	052153164-0	NORBERTO DUARTE FERNANDES	30 Jan 02	Cia Cmdo 15ª Bda Inf Mtz
3º Sgt Int	093865394-6	WAGNER GOMES DA SILVA	16 Mar 05	9º BE Cnst
Cb	072507944-6	JOÃO MANOEL MONTEIRO DA ROCHA	31 Jan 01	71º BI Mtz

PORTARIA Nº 054-SGEx, DE 28 DE FEVEREIRO DE 2007.

Concessão de Medalha Militar

O **SECRETÁRIO-GERAL DO EXÉRCITO,** no uso da competência que lhe é conferida pelo art. 1º, inciso XVII, da Portaria do Comandante do Exército nº 761, de 2 de dezembro de 2003, resolve

CONCEDER

a Medalha Militar e Passador de Prata, nos termos do Decreto nº 4.238, de 15 de novembro de 1901, regulamentado pelo Decreto nº 39.207, de 22 de maio de 1956 e com a redação dada pelo Decreto nº 70.751, de 23 de junho de 1972, aos militares abaixo relacionados, por terem completado vinte anos de bons serviços nas condições exigidas pela Portaria do Comandante do Exército nº 322, de 18 de maio de 2005.

Posto/Grad Arma/Q/Sv	Identidade	Nome	Término do decênio	OM
Maj Art	011534533-2	ALFREDO FERREIRA NUNES	17 Fev 07	Cmdo 11ª Bda Inf L
Maj Cav	030777904-1	CARLOS CESAR HICKMANN	27 Jan 07	C Doc Ex
Maj Int	019315783-1	FABIO RICARDO DA ROSA	17 Fev 07	3ª ICFEx
Cap Com	020288374-0	ANDRE LUIZ DOS SANTOS FRANCO	10 Fev 07	CIGE
Cap Int	020289694-0	EDSON TERRA PIMENTA	21 Fev 07	9º BE Cnst
Cap QCO	019251913-0	EDWARD DOS SANTOS DANTAS	01 Fev 07	AMAN
Cap Art	056403523-6	FABRICIO RAMIRES PINTO	10 Fev 07	14ª Bia AAAe
Cap QCO	049792293-0	FRANCISCO CARLOS DOS SANTOS	27 Jan 07	H Gu São Gabriel da Cachoeira
Cap QCO	019251163-2	JOÃO SILVEIRA DE ANDRADE	27 Jan 07	5ª ICFEx
Cap Int	020291034-5	MARCELO ALMEIDA	15 Fev 07	11ª ICFEx
Cap Cav	097059823-1	RODRIGO TEIXEIRA MONTEIRO DE CASTRO	10 Fev 07	CMB
1º Ten QCO	019304273-6	WALISSON D 'ARC MOIZÉS	27 Jan 07	EME
1º Sgt Eng	011608613-3	ADELSON DA CONCEIÇÃO PEIXOTO	31 Jan 07	B Es Eng
1º Sgt Inf	067392373-6	ADENILTON DA PAIXÃO FRANÇA	27 Jan 07	Cmdo Fron Rondônia/6º BIS
1º Sgt Inf	049791273-3	ADMARDO DIAS DE LIMA	25 Fev 07	DSG
1º Sgt Inf	101029484-9	ALBERTO NASCIMENTO	31 Jan 07	COTER
1º Sgt Inf	059156933-0	ANDRE ROBERTO EYNG	27 Jan 07	51º BIS
1º Sgt Art	020099994-4	AURÉLIO PICCIANO	27 Jan 07	12º GAC
1º Sgt Sau	019251633-4	BISMARCK DA SILVA ASSIS	26 Fev 07	H Gu Santa Maria
1º Sgt Art	010368763-8	CARLOS ALBERTO LEAL DA CUNHA	03 Jan 06	EsACosAAe
1º Sgt Inf	030849974-8	CARLOS CEZAR BUTZGE	27 Jan 07	62º BI
1º Sgt Art	020193374-4	CLAUDIONOR DAS DORES	01 Fev 07	12º GAC
1º Sgt Com	062251304-2	ELIAS GOMES DE SOUZA JUNIOR	27 Fev 07	7º CTA
1º Sgt Int	030833394-7	EURICO DOS SANTOS MACIEL	02 Fev 07	Esqd Cmdo 1ª Bda C Mec
1º Sgt Eng	118184973-6	FLAVIO GOMES BORGES	28 Jan 07	CMB
1º Sgt Art	019225223-7	FRANCISCO ALVES DA SILVA	31 Jan 07	21ª Bia AAAe Pqdt
1º Sgt Mnt Com	019251953-6	FRANCISCO LEONARDO DOS SANTOS CAVALCANTE	27 Fev 07	DCEM
1º Sgt Inf	017927452-7	GERALDO HENRIQUE SANTOS DE LIMA	01 Fev 07	71º BI Mtz
1º Sgt Av Ap	014912993-4	GILBERTO DE MENDONÇA LIRA	15 Maio 04	B Mnt Sup Av Ex
1º Sgt Eng	032992472-4	GILBERTO SOUZA GOULART	26 Fev 07	SGEx
1º Sgt Com	047653823-6	HELIO BERG PINTO	29 Jan 07	14º GAC

Posto/Grad Arma/Q/Sv	Identidade	Nome	Término do decênio	OM
1º Sgt Inf	105197643-7	HERMES NONATO DA SILVA	27 Jan 07	72º BI Mtz
1º Sgt Cav	030742034-9	JANIR ANTONIO MOURA NIMITT	26 Jan 07	DCEM
1º Sgt Eng	030690044-0	JOACIR DE OLIVEIRA REZENDE	27 Jan 07	CPOR/PA
1º Sgt Inf	018585263-9	JOELSON SILVA FERREIRA VERRI	28 Jan 06	H Gu Vila Militar
1º Sgt Cav	030806514-3	JONI BÜRKLE	27 Jan 07	EsSA
1º Sgt Eng	075961233-6	JOSÉ HÉLIO DA SILVA	27 Jan 06	7ª ICFEx
1º Sgt Int	011535193-4	JOSÉ PORFÍRIO DA SILVA JUNIOR	27 Jan 07	18º B Log
1º Sgt Com	075999203-5	LAÉRCIO ALVES DA SILVA	25 Jan 07	72º BI Mtz
1º Sgt Inf	118185763-0	LINDOMAR GOMES	26 Jan 07	DGP
1º Sgt Cav	020137484-0	LUIS AMARO VETRANO DE QUEIROZ	02 Fev 07	5ª CSM
1º Sgt MB Mec Auto	020138034-2	LUIS CARLOS CORREA	27 Jan 07	Cia Cmdo 11ª Bda Inf L
1º Sgt Com	049790923-4	MARCELO LINO DOS SANTOS SILVA	13 Ago 06	Cia Cmdo 6ª RM
1º Sgt Art	020103444-4	MARCELLO RODRIGUES DA SILVA	27 Jan 07	12º GAC
1º Sgt Art	030702384-6	MARLON ROIS DE MORAES RIBAS	28 Jan 07	CCOMSEx
1º Sgt Art	056306583-8	MARCO TÚLIO SOARES SANTOS	27 Jan 07	12º GAC
1º Sgt Cav	030722134-1	MAURICIO TEIXEIRA DOS SANTOS	27 Jan 07	6º GAC
1º Sgt Inf	049791053-9	NÉDSON LUIZ DOS SANTOS CAMPOS	27 Jan 07	DCEM
1º Sgt MB Mec Auto	049756933-5	NELSON ANTONIO DA SILVA	26 Fev 07	6º BE Cnst
1º Sgt Cav	019321313-9	NELSON JOSÉ FELISBERTO	27 Jan 07	DS
1º Sgt Mnt Com	018545843-7	ORLANDO LIMA SANTOS	27 Jan 07	CCOMSEx
1º Sgt Inf	049780393-2	VALTER QUARESMA GONÇALVES	27 Jan 07	34º BI Mtz
1º Sgt Com	030503164-3	VOLMIR EMILIO SCHIEFELBEIN	28 Jan 06	DSM
2º Sgt Com	030771644-9	ANTONIO AUGUSTO DUARDES DORNELES	27 Jan 07	1ª Cia GE
2º Sgt Cav	059146583-6	EGON DALINGHAUS	29 Jan 07	CMB
2º Sgt Mus	076200463-8	FRANCIMAR LOPES DO CARMO	27 Jan 07	DCEM
2º Sgt Cav	059146873-1	LUIS ALBERTO LOEWENSTEIN	27 Jan 07	16º Esqd C Mec
2º Sgt Inf	059165553-5	MARCIO MACEDO DE CARVALHO	19 Fev 07	Gab Cmt Ex
2º Sgt Art	030812124-3	MARCO AURELIO SANTOS DA SILVA	04 Fev 07	DSM
2º Sgt Cav	030813704-1	MARCOS JUAREZ FERNANDES GOMES	27 Jan 07	EsSA
2º Sgt Com	127509473-6	MARIO DE SOUZA MOREIRA	27 Jan 07	CMB
2º Sgt Inf	030753904-9	VILSON FERNANDO MARQUES DA COSTA	27 Jan 07	CPOR/PA
3º Sgt QE	036865053-7	DANIEL LUIZ DALLAGNOL	29 Jan 05	3º B Sup
3º Sgt QE	118175593-3	DIVINO DE SENA LOPES	28 Jan 07	CCOMSEx
3º Sgt QE	030696294-5	ÉDISON ANTÔNIO NICH FERRAZ	27 Jan 07	9º B Log
3º Sgt QE	049761113-7	IDELBARAN DOS SANTOS FRANCO	27 Jan 07	4º D Sup
3º Sgt QE	019233143-7	JORGE LUIS ALVES ROSA	27 Jan 07	DEP
3º Sgt QE	118179793-5	JUAREZ DIAS DE OLIVEIRA	27 Jan 07	6º GLMF/CIF
3º Sgt QE	018542703-6	LUIZ CLAUDIO GHATY BRITTO	29 Jan 06	BIBLIEx
3º Sgt QE	049766563-8	ROBERTO APARECIDO DA SILVA	26 Fev 07	14º GAC
3º Sgt QE	020103664-7	SÉRGIO APARECIDO DE ARAÚJO	27 Jan 07	12º GAC
3º Sgt QE	118223363-3	WANDERLEY AUGUSTO PIRES DE BARROS	27 Jan 07	6º GLMF/CIF
Cb	030521384-5	GERSON LUIZ LEMOS DOS SANTOS	06 Fev 06	6º BE Cnst
Cb	019286033-6	JAIRO ALBERTINO	27 Jan 07	27º BI Pqdt
Cb	036922453-0	JOSÉ DE ANDRADE	29 Jan 05	H Gu Cruz Alta
Cb	076244073-3	VALDEMIR FERNANDES COSTA	27 Jan 07	71º BI Mtz

PORTARIA Nº 055-SGEx, DE 28 DE FEVEREIRO DE 2007.

Concessão de Medalha Militar

O **SECRETÁRIO-GERAL DO EXÉRCITO,** no uso da competência que lhe é conferida pelo art. 1º, inciso XVII, da Portaria do Comandante do Exército nº 761, de 2 de dezembro de 2003, resolve

CONCEDER

a Medalha Militar e Passador de Ouro, nos termos do Decreto nº 4.238, de 15 de novembro de 1901, regulamentado pelo Decreto nº 39.207, de 22 de maio de 1956 e com a redação dada pelo Decreto nº 70.751, de 23 de junho de 1972, aos militares abaixo relacionados, por terem completado trinta anos de bons serviços nas condições exigidas pela Portaria do Comandante do Exército nº 322, de 18 de maio de 2005.

Posto/Grad Arma/Q/Sv	Identidade	Nome	Término do decênio	OM
Cel Com	061999212-6	CLAUDEMIR RANGEL DOS SANTOS	07 Fev 06	EME
Ten Cel Cav	026806092-8	LUIZ EUCLIDES PALMEIRA LEITE	18 Fev 07	EsAEx
2º Ten QAO	034654072-7	ADÃO ROBERTO XAVIER LIMA	15 Fev 07	H Gu Cruz Alta
2º Ten QAO	045600802-8	ADEMAR CELSO PEREIRA	06 Jan 07	Gab Cmt Ex
2º Ten QAO	036142462-5	DANIEL GOULART DA SILVA	30 Jan 07	62º BI
2º Ten QAO	036089482-8	ELISEU SILVA DOS SANTOS	13 Fev 07	52º CT
2º Ten QAO	036137522-3	ERNO BELING	12 Jan 07	D A Prom
2º Ten QAO	024102932-1	JOSÉ APARECIDO MAINETTI	30 Out 06	D A Prom
2º Ten QAO	036132132-6	SEVERO VERA GONÇALVES	07 Jan 07	C Doc Ex
Subten Eng	016588692-0	MAURO LEANDRO DA SILVA	06 Jan 07	EsAEx
Cb	075793872-5	ANTONIO GOMES DA SILVA	12 Jan 07	2ª Cia Gd

PORTARIA Nº 056-SGEx, DE 28 DE FEVEREIRO DE 2007.

Concessão de Medalha Corpo de Tropa

O **SECRETÁRIO-GERAL DO EXÉRCITO**, no uso da atribuição que lhe é conferida pelo art. 16, inciso I, das Normas para Concessão da Medalha Corpo de Tropa, aprovadas pela Portaria do Comandante do Exército nº 715, de 21 de outubro de 2004, resolve

CONCEDER

a Medalha Corpo de Tropa com Passador de Bronze, nos termos do Decreto nº 5.166, de 3 de agosto de 2004, aos militares abaixo relacionados, pelos bons serviços prestados em organizações militares de corpo de tropa do Exército Brasileiro, durante mais de dez anos.

Posto/Grad Arma/Q/Sv	Identidade	Nome	OM
Ten Cel Art	027581872-2	EDSON DIEHL RIPOLI	Gab Cmt Ex
Maj QMB	019315413-5	JOSÉ GERALDO DE SOUZA TANKO	Pq R Mnt/3
Maj Art	020137003-8	MARCOS SIMÕES COSSO	29º GAC AP
Cap Cav	020390064-2	ANGELO MOREIRA CARNAVAL	16º Esqd C Mec
Cap Inf	020369314-8	FRANCISCO MARCELO MATOS SEREJO	13º BIB
Cap Int	020391134-2	GUSTAVO PEREIRA MASSANEIRO CERCAL	5º B Sup
Cap Inf	020391334-8	JEAN MAX OLIVEIRA SANTOS	3º BI
Cap Eng	020391544-2	JORGE CLAUDIO GOMES	6º BE Cnst
Cap Art	030953824-7	PAULO ROBERTO PINHEIRO JACOBSEN	18º GAC

Posto/Grad Arma/Q/Sv	Identidade	Nome	OM
Cap Inf	118077673-2	RENATO DA SILVA RODGERS	5º BIL
Subten Inf	047592222-5	SALALINO DE ASSUNÇÃO E SILVA	28º BIL
1º Sgt Eng	114256093-5	ALBERTO DONIZETTI RODRIGUES	11º BE Cnst
1º Sgt Mnt Com	019426513-8	LUIS CARLOS DE SOUZA BARCELLOS	AMAN
1º Sgt Inf	049790973-9	MARCELO DOS SANTOS ESCOBAR	B Adm Ap/3ª RM
2º Sgt Inf	102858494-2	ALESSANDRO DE ALBUQUERQUE SOARES	BGP
2º Sgt Com	031842744-0	ALOIR DE OLIVEIRA REGO	1º BG
2º Sgt Inf	042039304-3	ANDRÉ GONDIM MONTEIRO	1º BG
2º Sgt Com	042039524-6	EDUARDO BERGAMI	11º BI Mth
2º Sgt Inf	043408774-8	EMERSON FERREIRA CASTELO	1º BG
2º Sgt Art	042026704-9	GERSON ALEXANDRE ROCHA DA SILVA	Cia Cmdo CML
2º Sgt Eng	043443184-7	ITAMAR GONÇALVES MAGALHÃES	Pq R Mnt/8
2º Sgt Sau	031902844-5	JAIR ROBERTO JOHAN	27º B Log
2º Sgt Inf	041996934-0	MARCELO DE LIMA PEREIRA	1º BG
2º Sgt MB Mnt Armt	011288284-0	MARCELO MARIANO DA SILVA	5º B Sup
2º Sgt Art	042041624-0	MARCIEL MARCELO FRANCISCO	DSM
2º Sgt MB Mec Op	019681113-7	MARCILON SANTANA RIBEIRO	Cia Cmdo 2ª Bda Inf Sl
2º Sgt Eng	043414114-9	MARCOS ROBERTO DE ALENCAR	9º BE Cnst
2º Sgt Inf	042018794-0	SANDRO LOPES MIGUEL	4º Pel PE
2º Sgt MB Mnt Auto	011466324-8	VALDECI PEREIRA ELIAS	16º R C Mec
2º Sgt Inf	043442774-6	WILLIAM SILVA FERNANDES	Cia Cmdo 3ª Bda Inf Mtz
3º Sgt Mus	031835454-5	CARLOS ALBERTO BOTELHO DE OLIVEIRA	Cia Cmdo 2ª Bda Inf Sl
3º Sgt Sau	033209934-0	GLAUCIO PEREIRA DOMINGUES	3º B Sup
3º Sgt Mus	101083404-0	MÁRCIO REGINO DA SILVA	71º BI Mtz
3º Sgt Int	093865394-6	WAGNER GOMES DA SILVA	9º BE Cnst
Cb	067393983-1	EPAMINONDAS VIEIRA MACHADO	19ª CSM
Cb	019634853-6	JORGE LUÍS CARDOSO DA SILVA	1º BG
Cb	072521314-4	ROBERTO ARRUDA DA SILVA	10º Pel PE

PORTARIA Nº 057-SGEx, DE 28 DE FEVEREIRO DE 2007.

Concessão de Medalha Corpo de Tropa

O **SECRETÁRIO-GERAL DO EXÉRCITO**, no uso da atribuição que lhe é conferida pelo art. 16, inciso I, das Normas para Concessão da Medalha Corpo de Tropa, aprovadas pela Portaria do Comandante do Exército nº 715, de 21 de outubro de 2004, resolve

CONCEDER

a Medalha Corpo de Tropa com Passador de Prata, nos termos do Decreto nº 5.166, de 3 de agosto de 2004, aos militares abaixo relacionados, pelos bons serviços prestados em organizações militares de corpo de tropa do Exército Brasileiro, durante mais de quinze anos.

Posto/Grad Arma/Q/Sv	Identidade	Nome	OM
Maj Inf	105081653-5	OTÁVIO ROBERTO MARTINS DANTAS	71º BI Mtz
Cap QAO	070687181-1	CONSTÂNCIO DE ANDRADE MELO	21ª CSM
Subten Inf	018994882-1	ABELARDO JORGE BACELLAR FERNANDES	Cia Cmdo 11ª RM
Subten Inf	108388712-3	CESAR AUGUSTO MATIAS DE OLIVEIRA	Cia Cmdo 9ª RM
Subten Cav	047624793-7	EDMILSON ANTONIO MENON	Cmdo 11ª Bda Inf L (GLO)
Subten Cav	010517893-3	JORGE LUIZ DA SILVA TEIXEIRA	Pq R Mnt/8
Subten Int	087060582-1	LUIZ GONZAGA RODRIGUES NOGUEIRA	3º B Sup

Posto/Grad Arma/Q/Sv	Identidade	Nome	OM
Subten Art	047624973-5	OLDAIR MEDEIROS DA SILVA	2º GAAAe
1º Sgt Cav	030582724-8	ANDRÉ LUIZ DE BARROS UBERTI	6º Esqd C Mec
1º Sgt MB Mnt Armt	047645603-3	CARLOS ALBERTO SILVA PINTO	2º B Log L
1º Sgt Inf	052596043-1	EDSON SCHIMANSKI	Cia Cmdo 5ª RM/5ª DE
1º Sgt Int	018785793-3	FLORINDO FREITAS DOS ANJOS	9º B Log
1º Sgt MB Mnt Auto	020364354-9	FRANCISCO CHAGAS DE SOUZA CAVALCANTE	31º BI Mtz
1º Sgt Inf	105098613-0	FRANCISCO EVALDO FÉLIX DE OLIVEIRA	BGP
1º Sgt Inf	018490343-3	GILSIMAR ANTONIO PENA	1º BG
1º Sgt Inf	101044704-1	SÉRGIO ROCHA DA SILVA	71º BI Mtz
2º Sgt Inf	030918024-8	JOÃO BATISTA LOUZADA DE LOUZADA	CPOR/PA
2º Sgt Cav	030975444-8	PAULO ROSANETE BALHEJO MAGALHÃES	16º R C Mec
3º Sgt QE	031753684-5	ANDRELINO ALBINO SANTOS HOCH	3º D Sup
3º Sgt Mus	019491303-4	ELIAS FIGUEIREDO DO NASCIMENTO	1º BG
3º Sgt QE	020113374-1	JOSÉ ANTÔNIO DA SILVA	2º B Av Ex
3º Sgt QE	019347953-2	WILSON DE PAULA NUNES	1º BG
Cb	073628664-2	ADRIANO SANTOS DE LIRA	31º BI Mtz
Cb	019637363-3	ANDRÉ LUIZ DOS SANTOS VIANA	1º BG
Cb	052151394-5	ASTÉRIO NICKNIG	14º R C Mec
Cb	033327894-3	CESAR AUGUSTO ROSA FAGUNDES	12º BEC Bld
Cb	011142864-5	CRISTIANO CÉSAR DOS SANTOS	1º BG
Cb	011136554-0	DARLAN EMANOEL DA COSTA CURVELO	1ª Cia PE
Cb	011174934-7	EDSON NASCIMENTO RODRIGUES	21ª Bia AAAe Pqdt
Cb	031827054-3	JOSÉ AMARÍLIO CÁCERES DUTRA	4º B Log
Cb	019474623-6	JOSUÉ DE SOUSA AMARAL	AMAN
Cb	011123634-5	LUCIANO DELGADO DA SILVA	1º D Sup
Cb	020448944-7	MARCELO HENRIQUE TEODORO	2º B Log L
Cb	011128184-6	MARCIO CAMPOS DA CRUZ	21ª Bia AAAe Pqdt
Cb	018788953-0	MARCOS ANTÔNIO PEREIRA	1ª Cia PE
Cb	019453043-2	MARCOS DA FONSECA SOUZA	27º BI Pqdt
Sd	092609554-8	ALMIRO MESSIAS DE ALMEIDA	17º R C Mec
Sd	123939024-6	RAIMUNDO ANTONIO LIMA	6º BE Cnst

PORTARIA Nº 058-SGEx, DE 28 DE FEVEREIRO DE 2007.

Concessão de Medalha Corpo de Tropa

O **SECRETÁRIO-GERAL DO EXÉRCITO**, no uso da atribuição que lhe é conferida pelo art. 16, inciso I, das Normas para Concessão da Medalha Corpo de Tropa, aprovadas pela Portaria do Comandante do Exército nº 715, de 21 de outubro de 2004, resolve

CONCEDER

a Medalha Corpo de Tropa com Passador de Ouro, nos termos do Decreto nº 5.166, de 3 de agosto de 2004, aos militares abaixo relacionados, pelos bons serviços prestados em organizações militares de corpo de tropa do Exército Brasileiro, durante mais de vinte anos.

Posto/Grad Arma/Q/Sv	Identidade	Nome	OM
Subten Mus	013152072-8	CARLOS RAMOS PEREIRA	1º BG
Subten Eng	047622033-0	CLAUDIO EMÍLIO SOUZA SANTOS	CPOR/PA
Subten Com	031253043-9	IVANOR JOSÉ CANABARRO	9º B Log
1º Sgt Cav	036877423-8	ALFREDO BAZILIO DA ROSA OLIVEIRA	16º R C Mec
1º Sgt Com	031797933-4	CARLOS AUGUSTO MACHADO CHEVARRIA	Cia Cmdo 9ª RM

1º Sgt Mus	011633653-8	FRANCISCO JOSÉ FERREIRA	1º BG
1º Sgt Art	036728813-1	PAULO FERREIRA SEVERO	19º GAC
1º Sgt Com	030554164-1	RONALDO GOMES DE GÓES	25º GAC
1º Sgt Inf	047835273-5	WALTENCIR ALVES DE OLIVEIRA	5º BIL
2º Sgt Mus	067272043-0	AMÉRICO MIRANDA DOS SANTOS	AMAN
2º Sgt Mus	014626533-5	ISAEL DOS SANTOS PEREIRA	1º BG
2º Sgt Mus	030761814-0	JANDIR REIS	Cia Cmdo 2ª Bda Inf Sl
3º Sgt QE	036865053-7	DANIEL LUIZ DALL'AGNOL	3º D Sup
3º Sgt QE	030629294-5	EDISON ANTONIO NICH FERRAZ	9º B Log
3º Sgt QE	049761113-7	IDELBARAN DOS SANTOS FRANCO	4º D Sup
3º Sgt QE	030705934-5	JOÃO MATEUS DOS SANTOS CAETANO	19º GAC
3º Sgt QE	099914823-2	JOSÉ PAULINO RODRIGUES	5º BE Cnst
Cb	030521384-5	GERSON LUIZ LEMOS DOS SANTOS	6º BE Cnst
Cb	019286033-6	JAIRO ALBERTINO	27º BI Pqdt

4ª PARTE
JUSTIÇA E DISCIPLINA

Sem alteração.

Gen Bda LUIZ EDUARDO ROCHA PAIVA
Secretário-Geral do Exército