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

Art.

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 repercurssões 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 ambrandamento 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 estabelecidadas 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.

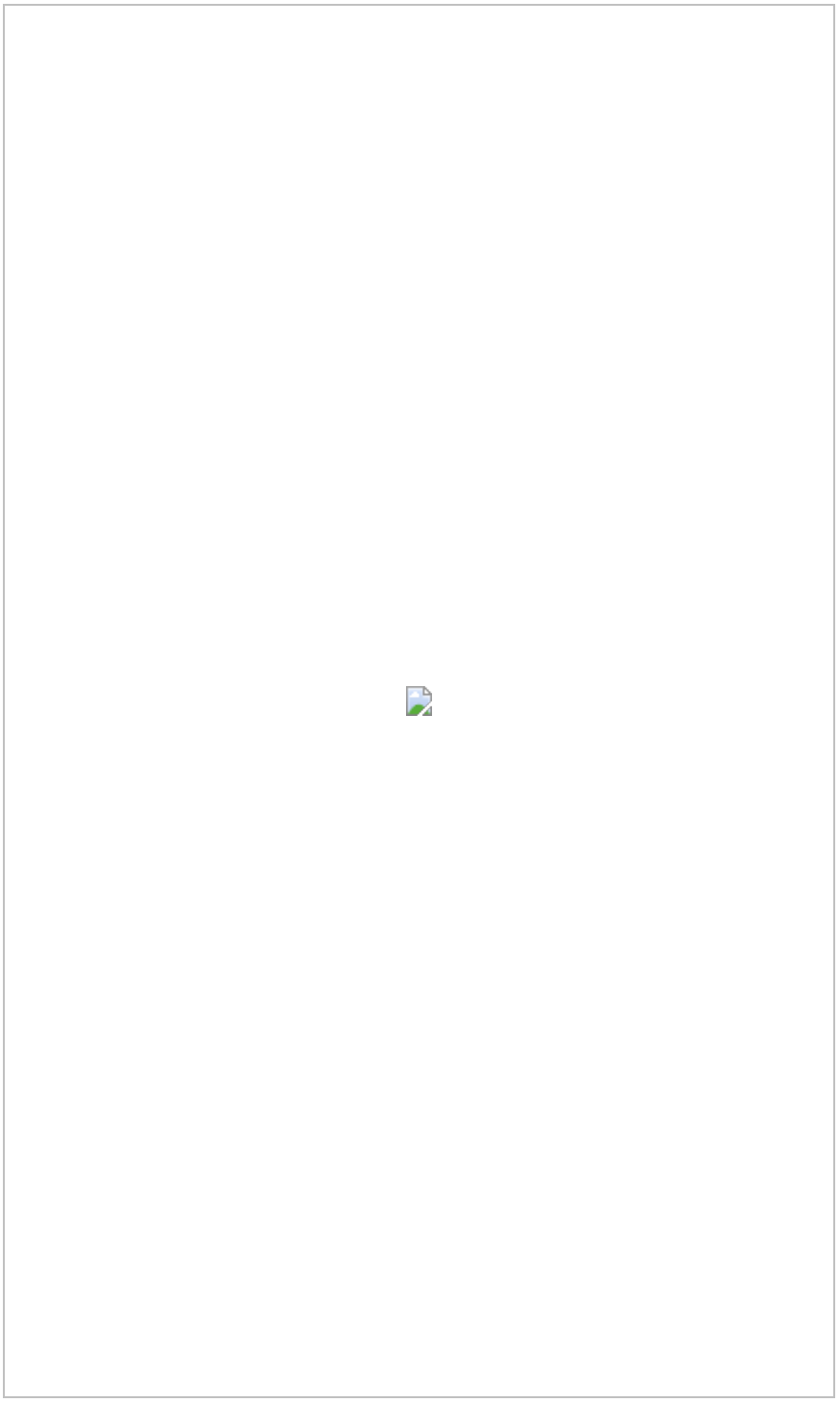

Fig nº 1 - Processo de Analise de Riscos

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 - softw are;

V - hardw are;

VI - hardw are 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 - softw ares;

IV - serviços de rede;

V - hardw are computacional;

VI - hardw are de interligação entre redes;

VII - hardw are 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 implementanção.

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 decobrir 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 contante 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 vulnerabilidadess constante do ANEXO C.

VII - PESQUISA DE VULNERABILIDADES NOTIFICADAS. Pesquisa nas bases de dados de entidades especilizadas 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.

4

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.
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.
		- Destruição ou dano aos dados ou informações, ou, ainda, aos recursos informacionais (hardware e software), porém, com

3	**Mediano**	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	Nunca	Extremamente Improvável	Improvável	Remoto	Ocasional	Provável	Freqüente	Sempre
Impacto								
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 softw are e hardw are 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 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 realcionados 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 apiliquem 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 gradução 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 FINALISTICO 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. Os registros do sistema operacional podem ser editados por quem tiver o privilégio de administrador e modificados para permitir controle externo. 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:

1. Probabilidades possíveis (p) do exemplo:

1. 1, baixa probabilidade;
2. 2, média probabilidade;
3. 3, probabilidade.

2. 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. A senha do administrador foi descoberta e os registros foram trocados pelo uso ilícito dos privilégios do administrador. 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 DEINIÇÃO 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.