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.

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 audiotoria. 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

§ 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 DOCUMETAÇÃO 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 (**logs**) 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 softw are e o hardw are necessários para auditar os sistemas corporativos e os demais softw ares 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 softw are 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 hardw are 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 softw are e hardw are 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 segurançada 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. OFTWARES UTILIZADOS:

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

c. **HARDWARE** UTILIZADO:

(Descrição das configurações de segurança do hardw are 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.)

Descrição do escopo que a auditoria abrange. Devem ser esclarecidos quais os equipamentos, softw ares, 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 softw ares utilizados na implementação dos serviços, assim como sua localização, ou seja, equipamentos onde estão instalados e as mídia dos softw ares 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