DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA

PORTARIA Nº 25-DCT, DE 7 DE JULHO DE 2009.

Aprova as Instruções Reguladoras sobre Segurança da Infraestrutura de Chaves Públicas do Exército Brasileiro - IRESICP (IR 80-05).

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 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 fevereiro de 2002, (resolve:

Art. 1º Aprovar as Instruções Reguladoras sobre Segurança da Infraestrutura de Chaves Públicas do Exército Brasileiro – IRESICP (IR 80-05).

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

INSTRUÇÕES REGULADORAS SOBRE SEGURANÇA DA INFRA-ESTRUTURA DE CHAVES PÚBLICAS DO EXÉRCITO BRASILEIRO - IRESICP (IR 80 - 05)

ÍNDICE DE ASSUNTOS

Art.

TÍTULO I

DAS GENERALIDADES

Art. 1º As presentes Instruções têm por finalidade orientar o planejamento e a execução das ações relacionadas à Segurança da Informação no âmbito da Infra-Estrutura de Chaves Públicas do Exército Brasileiro (ICP-EB) e em conjunto com as Instruções Reguladoras para Práticas de Certificação da Autoridade Certificadora Raiz do Exército Brasileiro (IRERAIZ) e as Instruções Reguladoras para Práticas de Certificação da Autoridade Certificadora do Exército Brasileiro (IREPCAC) foram elaboradas em observância ao art. 18 das Instruções Gerais de Segurança da Informação para o Exército Brasileiro (IG 20-19).

Parágrafo Único. Constituem a ICP-EB a Autoridade Certificadora Raiz do Exército Brasileiro (AC-Raiz EB), a Autoridade Certificadora do Exército Brasileiro no Centro Integrado de Telemática do Exército (AC-EB CITEx) e outras Autoridades Certificadoras (AC) subordinadas à AC-Raiz EB que venham a ser instituídas, a Autoridade de Registro do Exército Brasileiro no CITEx (AR-EB CITEx), os Agentes Validadores e os usuários de certificados digitais e a documentação normativa que define as regras e processos inerentes ao funcionamento da ICP-EB.

Art. 2º Constituem objetivos destas Instruções:

I – definir o escopo da segurança na ICP-EB;

II – orientar as ações de segurança a serem implementadas na ICP-EB, com vistas a reduzir riscos e assegurar a integridade, o sigilo e a disponibilidade de suas informações e recursos;

III – permitir a adoção de soluções de segurança integradas;

IV – servir de referência para auditoria, apuração e avaliação de responsabilidades; e

V – servir de referência às demais documentações normativas da ICP-EB.

Art. 3º As presentes Instruções abrangem aspectos relacionados aos seguintes Requisitos de Segurança:

I – de Pessoal;

II – Física;

III – Lógica;

IV – de Recursos Criptográficos.

Art. 4º Referências:

I – Lei nº 8.159, de 08 de janeiro de 1991 – dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências;

II - Medida Provisória nº 2.200-2, de 24 de agosto de 2001 – institui a Infra-Estrutura de Chaves Públicas Brasileira – ICP-Brasil, e dá outras providências;

III – Decreto nº 3.505, de 13 de junho de 2000 – institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

IV – Decreto nº 2.134, de 24 de janeiro de 1997 – regulamenta o Art. 23 da Lei nº 8.159/91;

V – Decreto nº 4.553, de 27 de dezembro de 2002 – dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências;

VI – Instruções Provisórias IP 30-3 – Ramo Contra-Inteligência ou o documento que a substituir;

VII – Instruções Gerais para a Salvaguarda de Assuntos Sigilosos no Exército Brasileiro - IGSAS (Portaria do Comandante do Exército nº 11, de 10 de janeiro de 2001);

VIII – Instruções Gerais de Segurança da Informação para o Exército Brasileiro (IG 20-19 – Portaria do Comandante do Exército Nr 483, de 20 de setembro de 2001);

IX – Instruções Reguladoras de Auditoria de Segurança de Sistemas de Informação do Exército Brasileiro – IRASEG (IR 13-09);

X – Instruções Reguladoras sobre Análise de Riscos para Ambientes de Tecnologia da Informação do Exército Brasileiro – IRISC (IR 13-10);

XI – Instruções Reguladoras sobre Segurança da Informação nas Redes de Comunicação e de Computadores do Exército Brasileiro – IRESER (IR 13-15);

XII – Normas para o Controle da Utilização dos Meios de Tecnologia da Informação no Exército – NORTI;

XIII – Constituição da República Federativa do Brasil – 1988;

XIV – Lei Nr 8.112, de 11 de dezembro de 1990 – dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais;

XV – Lei Nr 9.296, de 24 de julho de 1996 – regulamenta o inciso XII, parte final, do art. 15 da Constituição Federal;

XVI – Lei Nr 10.406, de 10 de janeiro de 2002 – Código Civil;

XVII – Decreto-Lei Nr 1.001, de 21 de outubro de 1969 – Código Penal Militar;

XVIII – Decreto Nr 4.346, de 26 de agosto de 2002 – Regulamento Disciplinar do Exército (R-4); e

XIX – Instruções Reguladoras sobre Segurança da Infra-Estrutura de Chaves Públicas do Exército Brasileiro – IRESICP ;

XX – Instruções Reguladoras para Práticas de Certificação da Autoridade Certificadora do Exército Brasileiro no CITEx – IREPCAC ;

XXI – **Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework – Internet Engineering Task Force Request For Comments 3647** (IETF RFC 3647);

XXII – **Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP) - Internet Engineering Task Force Request For Comments 4210** (IETF RFC 4210).

XXIII – **Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile – Internet Engineering Task Force Request For Comments 3280** (IETF RFC 3280);

TÍTULO II

DOS CONCEITOS BÁSICOS

Art. 5º Para aplicação destas Instruções, deve-se adotar a seguinte conceituação:

I – ATIVO DE INFORMAÇÃO – patrimônio composto por todos os dados e informações geradas e manipuladas durante a execução dos sistemas e processos da ICP-EB;

II – ATIVO DE PROCESSAMENTO – patrimônio composto por todos os elementos de hardware e software necessários à execução dos sistemas e processos da ICP-EB, tanto os produzidos internamente quanto os adquiridos;

III – CONTROLE DE ACESSO – restringe o acesso às informações da ICP-EB;

IV – CUSTÓDIA – guarda de um ativo para terceiros. A custódia não permite acesso ao ativo, nem o direito de conceder acesso a outros;

V – DIREITO DE ACESSO – privilégio de acessar um ativo associado a um cargo, uma pessoa ou um processo;

VI – FERRAMENTAS – conjunto de equipamentos, programas, procedimentos, normas e demais recursos por intermédio dos quais é aplicada a documentação normativa de segurança da ICP-EB;

VII – INCIDENTE DE SEGURANÇA – qualquer evento ou ocorrência que promova uma ou mais ações que comprometa, ou ameace a integridade, a autenticidade, ou a disponibilidade de qualquer ativo da ICP-EB;

VIII – DOCUMENTAÇÃO NORMATIVA DE SEGURANÇA – conjunto de regras que definem a proteção desejada nos ativos e os riscos aceitáveis, no âmbito da ICP-EB;

IX – PROTEÇÃO DE ATIVOS – processo pelo qual os ativos devem receber classificação quanto ao grau de sensibilidade; o meio de registro de um ativo de informação deve receber a mesma classificação de proteção dada ao ativo que o contém;

X – RESPONSABILIDADE – obrigações e deveres da pessoa que ocupa determinada função quanto ao acervo de informações que lhe é delegado;

XI – SENHA FRACA OU ÓBVIA – utiliza caracteres de fácil associação com o dono da senha, ou que seja muito simples ou pequena, como, por exemplo: data de aniversário, de casamento, de nascimento, o próprio nome, o nome de familiares, seqüências numéricas simples, palavras e unidades léxicas que constem de dicionários de qualquer língua, dentre outras;

XII – CERTIFICADO DIGITAL – Arquivo digital que contém um conjunto de informações referentes à entidade para o qual o certificado foi emitido e sua chave pública;

XIII – CICLO DE VIDA DO CERTIFICADO DIGITAL – O ciclo de vida de um certificado digital compreende as seguintes etapas: requisição do certificado; aprovação da requisição; recuperação do certificado; publicação de certificados; e revogação de certificados;

XIV – SISTEMA DE INFORMAÇÃO – descreve um sistema automatizado, ou manual, que envolve pessoas, máquinas ou métodos organizados para coletar, processar, transmitir e disseminar dados que produzam informação.

XV – AUTORIDADE CERTIFICADORA (AC) – Entidade responsável por emitir certificados digitais.

XVI – INFRA-ESTRUTURA DE CHAVES PÚBLICAS (ICP) – Conjunto de entidades, padrões, técnicas e regulamentos, elaborados para suportar um sistema criptográfico com base em certificados digitais que visa assegurar transações entre seus titulares.

TÍTULO III

DAS REGRAS GERAIS

CAPÍTULO I

DA GESTÃO DE SEGURANÇA

Art. 6º Estas Instruções se aplicam a todos os recursos humanos, administrativos e tecnológicos pertencentes à ICP-EB.

Parágrafo Único. A abrangência dos recursos citados refere-se tanto àqueles ligados à ICP-EB em caráter permanente quanto temporário.

Art. 7º As presentes Instruções Reguladoras devem ser de conhecimento de todo o pessoal envolvido na ICP-EB.

§1º Um programa de conscientização sobre Certificação Digital, e suas implicacões na Segurança da Informação, deve ser implementado para assegurar que todo o pessoal envolvido na ICP-EB seja informado sobre os potenciais riscos de segurança e exposição a que está submetida a ICP-EB.

§2º Todo pessoal integrante da ICP-EB, ou que se relacione diretamente com os usuários, deve estar treinado e atualizado em relação aos ataques mais recentes, como se proteger deles e como proceder quando um deles se concretiza.

§3º Estas Instruções devem ser amplamente divulgadas assegurando que o público interno as conheça e as aplique.

Art. 8º Todos os procedimentos afetos ao ciclo de vida dos certificados digitais devem ser documentados.

Art. 9º Devem ser implementadas salvaguardas para garantir que, quando o pessoal integrante da ICP-EB for afastado de suas funções, todos os seus privilégios de acesso sejam revogados.

Art. 10. Deve ser implementado mecanismo, preferencialmente com repositório centralizado, para ativação e manutenção de registros de eventos (**logs**).

§1º Os **logs** devem ser integrados às medidas para tratamento de incidentes de segurança.

§2º Os **logs** devem conter, pelo menos, a data e a hora das atividades, a identificação do usuário, os comandos executados e seus argumentos, a identificação da estação local ou da remota que iniciou a conexão.

Art. 11. Os processos de aquisição de bens e serviços para a ICP-EB devem estar em conformidade com estas Instruções.

Art. 12. No que se refere à seguranca da informação, deve ser considerado proibido tudo aquilo que não estiver previamente autorizado pelo Chefe da Seção de Certificação Digital da Divisão de Segurança do CITEx.

CAPÍTULO II

DO GERENCIAMENTO DE RISCOS

Art. 13. O processo de gerenciamento de riscos deve seguir o preconizado nas Instruções Reguladoras Sobre Análise de Riscos para Ambientes de Tecnologia da Informação do Exército Brasileiro - IR 13-10 (IRRISC).

Parágrafo Único. Esse processo deve ser revisto, no máximo, a cada 18 (dezoito) meses.

CAPÍTULO III

DO INVENTÁRIO DE ATIVOS

Art. 14. Todos os ativos da ICP-EB devem ser inventariados por gestor formalmente designado.

§1º Os relatórios de inventários devem ser permanentemente atualizados.

§2º Devem ser utilizadas ferramentas automáticas de inventário de ativos desde que os relatórios gerados, afetos aos ativos da ICP-EB, sejam mantidos impressos, arquivados na Seção de Certificação Digital, e conferidos pelo gestor.

CAPÍTULO IV

DO PLANO DE CONTINUIDADE DO NEGÓCIO

Art. 15. O Plano de Continuidade do Negócio (PCN) da ICP-EB deve ser elaborado, implementado e testado ao menos duas vezes por ano, definindo regras, no mínimo, nos seguintes assuntos:

I – local alternativo para salvaguarda e processamento dos dados em caso de necessidade (**site backup**);

II – serviços de cópia de segurança (**backup**) e recuperação;

III – infra-estrutura redundante;

IV – disponibilidade;

V – recuperação de desastres;

VI – revogação dos certificados afetados, quando for o caso;

VII – documentação de usuários;

VIII – relacionamento com o público e com os meios de comunicação, se for o caso.

Art. 16. O certificado da Autoridade Certificadora Raiz do Exército Brasileiro (AC Raiz EB) deve ser imediatamente revogado se um evento provocar perda ou comprometimento de sua chave privada ou do seu meio de armazenamento, bem como, todos os certificados por ela emitidos para outras Autoridades Certificadoras (AC), quando for o caso, e para usuários.

Parágrafo Único. Nesta situação, a AC Raiz EB deverá seguir os procedimentos detalhados em nas Instruções Reguladoras para Práticas de Certificação da Autoridade Certificadora Raiz do Exército Brasileiro (IRERAIZ).

TÍTULO IV

DOS REQUISITOS DE SEGURANÇA

CAPÍTULO I

DA SEGURANÇA DE PESSOAL

SEÇÃO I

DA DEFINIÇÃO

Art. 17. Trata-se de um conjunto de medidas e procedimentos de segurança necessários à proteção dos ativos da ICP-EB, visando redução dos riscos que tenham como origem o fator humano, por meio de seus próprios integrantes.

SEÇÃO II

DOS OBJETIVOS

Art. 18. A Segurança de Pessoal tem como objetivos:

I – reduzir os riscos de erros humanos, furto, roubo, apropriação indébita, fraude ou uso inapropriado dos ativos da ICP-EB;

II – prevenir e neutralizar ações sobre pessoas que possam comprometer a segurança das entidades participantes da ICP-EB;

III – orientar e capacitar todo o pessoal envolvido nos trabalhos relacionados à ICP-EB quanto à adoção de medidas de proteção compatíveis com a natureza da função que desempenham;

IV – orientar todo o pessoal envolvido em atividades de apoio, tais como limpeza e manutenção das instalações físicas quanto à adoção de medidas de proteção compatíveis com a natureza da função que desempenham.

SEÇÃO III

DAS DIRETRIZES

SUBSEÇÃO I

DO PROCESSO DE DESIGNAÇÃO

Art. 19. Os militares que vierem a ser designados para atuar na ICP-EB devem ser pessoas reconhecidamente idôneas, sem antecedentes criminais.

Parágrafo Único. Para levantamento das informações necessárias, far-se-á uso do SIEx.

Art. 20. Apenas militares de carreira podem exercer funções na ICP-EB.

Parágrafo Único. Para função de validação, como especificada nas IREPCAC , não há necessidade de serem levantadas informações são admitidos quaisquer militares.

Art. 21. Os integrantes da ICP-EB, para exercerem suas funções, devem assinar previamente Termo de Compromisso de Manutenção de Sigilo.

SUBSEÇÃO II

DA CREDENCIAL DE SEGURANÇA

Art. 22. A Credencial de Segurança identifica o nível de acesso a informações sigilosas por integrante da ICP-EB.

Art. 23. A Credencial de Segurança somente será concedida por meio da 2ª Seção, ou equivalente, da OM do militar, em conformidade com as Instruções Gerais para Salvaguarda de Assuntos Sigilosos - IG 10-51 (IGSAS).

§1º Para integrantes com necessidade de acesso a ativos da ICP-EB, deve ser concedida Credencial de Segurança com grau de sigilo "Secreto".

§2º Aos demais integrantes da ICP-EB com função apenas de validação, deve ser concedida Credencial de Segurança com grau de sigilo "Reservado".

SUBSEÇÃO III

DO TREINAMENTO

Art. 24. Uma agenda de treinamento do público interno ao EB, no qual serão apresentadas, estas Instruções e outras a ela vinculadas, as funcionalidades e os procedimentos relativos à ICP-EB, deve ser definida pelo DCT e sugerida aos demais órgãos setoriais.

SUBSEÇÃO IV

DO AFASTAMENTO

Art. 25. O acesso de ex-integrantes da ICP-EB, quando necessário, será restrito a suas áreas de acesso público.

Art. 26. Ao afastar-se de suas funções da ICP-EB, todo e qualquer dispositivo de identificação e controle de acesso de posse do militar deve ser recolhido, assim como todos os seus privilégios de acesso aos ativos da ICP-EB devem ser revogados.

Art. 27. Por ocasião de seu afastamento deve ser realizada uma entrevista com o militar, orientando-o sobre sua responsabilidade na manutenção do sigilo das informações da ICP-EB e de seus usuários às quais teve acesso, lembrando-lhe do Termo de Compromisso de Manutenção do Sigilo assinado anteriormente.

CAPÍTULO II

DA SEGURANÇA FÍSICA

SEÇÃO I

DA DEFINIÇÃO

Art. 28. Ambiente físico é aquele composto por todo o ativo permanente da ICP-EB.

SEÇÃO II

DAS DIRETRIZES GERAIS

Art. 29. As responsabilidades pela segurança física da ICP-EB deverão ser formalmente definidas e atribuídas aos seus integrantes.

Art. 30. Controles de acesso físico deverão ser instalados no ambiente da ICP-EB.

Art. 31. Perdas de cartões/chaves de acesso deverão ser imediatamente comunicadas à Chefia da Seção de Certificação Digital, da Divisão de Segurança do CITEx, que deverá tomar as medidas apropriadas.

Parágrafo Único. A comunicação de uma perda de cartão ou chave será realizada de modo tão rápido quanto os meios de fortuna permitirem, porém essa comunicação deverá ser formalizada tão logo seja possível.

Art. 32. Chaves criptográficas sob custódia de seus responsáveis devem ser protegidas contra acesso físico e lógico, uso ou duplicação não autorizados.

Art. 33. A localização das instalações e o sistema de certificação da ICP-EB não deverão ser publicamente identificados.

Art. 34. As máquinas da ICP-EB deverão ser preferencialmente instaladas em área protegida ou afastada de fontes de magnetismo e interferência de eletromagnética.

Art. 35. Os ativos da ICP-EB devem ser mantidos em área segura, protegida por perímetro de segurança explicitamente definido e com controle de acesso.

§ 1º A área segura deve ser fisicamente protegida de acesso não autorizado e danos.

§ 2º A proteção fornecida deve ser proporcional aos riscos identificados.

Art. 36. O acesso físico à área da ICP-EB, deve ser monitorado e registrado através de um sistema de controle de acesso.

§1º Os registros devem ser analisados pelo menos uma vez por semana e verificadas possíveis inconsistências entre os horários de entrada e de saída.

§2º Os registros devem ser mantidos em local protegido por, pelo menos, 5 (cinco) anos.

§3º O sistema de controle de acesso deve ser testado regularmente.

Art. 37. O acesso aos componentes da infra-estrutura, tais como painéis de controle de energia, comunicações e cabeamento, etc, deve ser restrito somente àquelas pessoas que foram formalmente autorizadas.

Art. 38. Nas instalações da ICP-EB, quaisquer equipamentos de gravação, fotografia, vídeo, som ou similares, somente devem ser utilizados mediante autorização formal e sob supervisão.

Art. 39. Visitantes nas áreas da ICP-EB devem ser permanentemente supervisionados.

Parágrafo Único. Os visitantes devem obter acesso apenas às áreas específicas, com propósitos autorizados, e esses acessos devem seguir instruções baseadas nos requisitos de segurança da área visitada.

Art. 40. As instalações da ICP-EB ou, pelo menos, o acesso às suas máquinas devem ser monitorados por vídeo em tempo real.

§1º As imagens devem registrar a data e a hora da cena.

§2º As imagens devem ser mantidas em local protegido por, pelo menos, 1 (um) ano.

§3º As imagens devem ser conferidas com as informações de entrada e saída do sistema de controle de acesso, pelo menos, uma vez por semana, de forma aleatória e verificando possíveis inconsistências.

§4º Os sistemas de monitoramento de vídeo devem ser testados regularmente.

CAPÍTULO III

DA SEGURANÇA LÓGICA

SEÇÃO I

DA DEFINIÇÃO

Art. 41. Ambiente lógico é composto por todos os ativos de informação da ICP-EB.

SEÇÃO II

DAS DIRETRIZES GERAIS

Art. 42. A informação deve ser protegida de acordo com seu valor, sua criticidade e seu grau de sigilo.

Parágrafo Único. Para grau de sigilo devem ser empregadas as IG 10-51 (IGSAS).

Art. 43. Os ativos de informação da ICP-EB devem ser protegidos contra ameaças, acidentais ou não, de modo a assegurar suas integridade, confidencialidade, disponibilidade e autenticidade em níveis aceitáveis.

Art. 44. As violações de segurança devem ser registradas e esses registros devem ser analisados periodicamente com propósito corretivo, legal ou de auditoria.

Parágrafo Único. Os registros devem ser protegidos e armazenados de acordo com a sua classificação de sigilo.

SEÇÃO III

DAS DIRETRIZES ESPECÍFICAS

SUBSEÇÃO I

DOS SISTEMAS DE INFORMAÇÃO

Art. 45. A documentação dos sistemas de informação da ICP-EB deve ser mantida atualizada.

Art. 46. Os sistemas de informação devem possuir controle de acesso de modo a assegurar o uso apenas por usuários ou processos autorizados.

§1º O responsável pela autorização de acesso deve ser formalmente designado.

§2º Toda autorização de acesso deve ser formalmente registrada.

Art. 47. Os registros de eventos (**logs**) devem ser criteriosamente definidos para auxiliar na recuperação em situações de falha e no tratamento de incidentes de segurança, na auditoria e na contabilização do uso de recursos.

§1º Os **logs** devem ser periodicamente analisados, conforme preconizado nas Instruções Reguladoras Sobre Segurança da Informação nas Redes de Comunicação e de Computadores do Exército Brasileiro (IR 13-15) - IRESER , para identificar tendências,

§2º Os **logs** devem ser protegidos e armazenados de acordo com sua classificação de sigilo.

§3º Os **logs** devem ser armazenados por um período mínimo de 5 (cinco) anos.

Art. 48. Os sistemas de informação da ICP-EB devem ser avaliados com relação aos aspectos de seguranç;a antes de serem disponibilizados para produção.

SUBSEÇÃO II

DAS MÁQUINAS SERVIDORAS

Art. 49. O acesso lógico, ao ambiente ou aos serviços disponíveis em servidores, deve ser controlado e protegido.

§1º O responsável pela autorização de acesso deve ser formalmente designado.

§2º Toda autorização de acesso deve ser formalmente registrada.

Art. 50. Devem ser adotados procedimentos sistematizados para monitorar a segurança do ambiente operacional, principalmente no que diz respeito à integridade dos arquivos de configuração do Sistema Operacional e de outros considerados críticos.

Art. 51. Todo acesso e qualquer outro evento considerado necessário ao adequado monitoramento de segurança deve ser registrado.

§1º Os **logs** devem ser periodicamente analisados, conforme preconizado nas IR 13-15 (IRESER), para identificar tendências, falhas e usos indevidos.

§2º Os **logs** devem ser protegidos e armazenados de acordo com sua classificação de sigilo.

§3º Os **logs** devem ser armazenados por um período mínimo de 5 (cinco) anos.

Art. 52. As máquinas da ICP-EB devem possuir sistema de sincronismo de tempo.

Parágrafo Único. O UTC (**Universal Coordinated Time**) deve ser adotado como referência de tempo.

Art. 53. Ao Sistema Operacional, assim como em qualquer outro *software* instalado em máquinas servidoras, devem ser aplicadas as atualizações de segurança recomendadas de seus desenvolvedores.

Parágrafo Único. Antes de serem aplicadas nas máquinas de produção, as atualizações devem ser testadas em ambiente de homologação.

Art. 54. Somente **software** devidamente licenciado pode ser empregado nas máquinas da ICP-EB.

Art. 55. Não é permitido acesso remoto às máquinas servidoras das AC da ICP-EB.

§1º O acesso remoto às máquinas servidoras das Autoridades de Registro (AR) da ICP-EB é realizado por todos os seus usuários, por meio de interface **web** pública.

§2º Outras interfaces das AR da ICP-EB devem ser acessadas remotamente apenas por máquinas prévia e formalmente cadastradas e operadas por integrantes da ICP-EB.

Art. 56. Os procedimentos de cópia de segurança (**backup**) e de recuperação devem ser documentados, mantidos atualizados e regularmente testados, de modo a assegurar disponibilidade e integridade das informações.

Art. 57. Os sistemas em uso devem solicitar nova autenticação após tempo predefinido de inatividade da sessão (**timeout**), o qual não deverá exceder 15 (quinze) minutos.

Parágrafo Único. No Hardware Secure Module (HSM) as operações são validadas somente com a inserção de **smart card** válido dispensando, assim, a restrição de **timeout.**

Art. 58. Toda mídia utilizada para armazenamento de dados referentes à ICP-EB deve ser eliminada de forma segura, conforme legislação em vigor, quando não for mais necessária.

Parágrafo Único. Procedimentos formais para a eliminação segura de mídia devem ser executados conforme legislação em vigor.

SUBSEÇÃO III

DAS ESTAÇÕES DE TRABALHO

Art. 59. As estações de trabalho, incluindo equipamentos portáteis ou **stand alone**, e as informações nelas contidas devem ser protegidas contra danos ou perdas, bem como acesso, uso ou exposição indevidos.

Art. 60. Devem ser adotadas medidas de segurança referentes a combate ao uso de **software** não autorizado ou sem licença de uso.

Art. 61. Os procedimentos de cópia de segurança (**backup**) e de recuperação devem ser documentados, mantidos atualizados e regularmente testados, de modo a assegurar disponibilidade e integridade das informações.

Art. 62. As informações armazenadas ou processadas na ICP-EB somente devem ser utilizadas em equipamentos das entidades onde foram geradas ou naqueles por elas autorizadas, com controles adequados.

Art. 63. A impressão de documentos sigilosos deve ser feita sob supervisão de seu responsável.

Parágrafo Único. A manipulação de documentos sigilosos deve ser feita como preconizado pelas IG 10-51 (IGSAS).

Art. 64. Toda mídia utilizada para armazenamento de dados referentes à ICP-EB deve ser eliminada de forma segura, de acordo com a legislação em vigor, quando não for mais necessária.

Parágrafo Único. Procedimentos formais para a eliminação segura de mídia devem ser executados conforme legislação em vigor.

SUBSEÇÃO IV

DAS REDES

Art. 65. O tráfego das informações no ambiente de rede da ICP-EB deve ser protegido contra perdas e danos, bem como acesso, uso ou exposição indevidos.

Art. 66. Componentes críticos da rede da ICP-EB devem ser mantidos em locais protegidos por controles de acesso.

Art. 67. Devem ser habilitadas as facilidades de segurança disponíveis de forma inata nos ativos de processamento da rede como, por exemplo, ativação da senha de BIOS, travamento do acesso local ao computador por tempo de inatividade e configuração adequada de diretivas de segurança.

Art. 68. A configuração de todos os ativos de processamento deve ser averiguada quando da sua instalação inicial, para que sejam detectadas e corrigidas as vulnerabilidades inerentes a suas configurações originais.

Art. 69. Serviços de rede considerados vulneráveis devem receber nível de proteção adicional.

Art. 70. O uso de senhas deve obedecer norma interna específica.

Art. 71. O acesso lógico aos recursos da rede ICP-EB deve ser verificado por meio de um sistema de controle de acesso.

Parágrafo Único. O critério para concessão de acesso deve se basear nas responsabilidades do solicitante, nas suas atribuições e na sua necessidade de conhecimento.

Art. 72. Qualquer mecanismo capaz de realizar testes de qualquer natureza na rede só deve ser utilizado após obtenção de autorização formal e mediante supervisão.

Art. 73. A conexão com outras redes e alterações nas topologia ou configuração de rede somente podem ser levadas a efeito mediante autorização formal e devem ser documentadas.

Parágrafo Único. O diagrama topológico, a configuração e o inventário dos ativos devem ser mantidos atualizados e sob sigilo.

Art. 74. O tráfego de informações deve ser monitorado, a fim de verificar sua normalidade, assim como detectar situações anômalas do

ponto de vista da segurança.

Parágrafo Único. O monitoramento da rede somente é permitido ao pessoal de segurança formalmente autorizado, desde que os procedimentos e mecanismos empregados não prejudiquem o funcionamento da ICP-EB.

Art. 75. Informações sigilosas ou que possam causar prejuízo à ICP-EB devem ser protegidas e não devem ser enviadas para outras redes, sem proteção adequada.

Art. 76. Nas máquinas da ICP-EB somente os serviços de certificação e aqueles necessários à sua execução devem estar ativos.

Parágrafo Único. Todos os demais serviços devem ser bloqueados ou desabilitados.

Art. 77. Uma estrutura de segurança baseada em camadas que inclua **firewalls,** Sistemas de Prevenção de Intrusão (**Intrusion Prevention System** - IPS) e **proxies** deve ser utilizada para proteger o acesso às máquinas da ICP-EB e o tráfego de dados.

Art. 78. Ambientes de rede considerados críticos devem ser isolados.

Art. 79. Conexões entre as redes da ICP-EB e redes externas devem ficar restritas somente àquelas que visem efetivar os processos necessários ao ciclo de vida de seus certificados.

Art. 80. As chaves privadas das AC da ICP-EB deverão receber proteção para assegurar seu sigilo, sua integridade e sua disponibilidade.

Art. 81. Todo e qualquer incidente de segurança deverá ser reportado imediata e sigilosamente à área de Tratamento de Incidentes à qual a ICP-EB estiver vinculada, assim que for verificada a ocorrência.

SUBSEÇÃO V

DO CONTROLE DE ACESSO LÓGICO

Art. 82. Não deve ser permitido a nenhum usuário obter os direitos de acesso de outro usuário da ICP-EB.

Art. 83. A informação que especifica os direitos de acesso de cada usuário ou aplicação deve ser protegida contra modificações indevidas.

Art. 84. Os arquivos de senhas devem ser criptografados e ter acesso restrito e controlado.

Art. 85. As autorizações de acesso devem ser definidas de acordo com a necessidade de desempenho das funções e considerando o princípio dos privilégios mínimos, ou seja, ter acesso apenas aos ativos necessários à execução dessas funções.

Art. 86. As senhas devem ser individuais, sigilosas, intransferíveis e protegidas.

§1º O sistema de controle de acesso deve possuir mecanismos que impeçam a geração de senhas fracas, ou óbvias, e sua visualização.

§2º O sistema de controle de acesso deve permitir ao usuário alterar sua senha sempre que desejar.

Art. 87. Devem ser adotados critérios para bloquear ou desativar usuários.

§1º Um usuário que não acessar o sistema por mais de 20 (vinte) dias úteis consecutivos deve ser bloqueado.

§2º Um mesmo usuário que realize 3 (três) tentativas consecutivas de acesso sem sucesso deve ser bloqueado.

§3º O desbloqueio de usuário só pode ser executado após a sua identificação positiva.

SUBSEÇÃO VI

DOS CÓDIGOS MALICIOSOS

Art. 88. Os procedimentos de combate a processos não desejados e maliciosos, tais como vírus, cavalos-de-tróia, **worms, spyware** etc., devem ser sistematizados e abranger máquinas servidoras, estações de trabalho, equipamentos portáteis, computadores **stand alone**, mídias e dispositivos removíveis.

Parágrafo Único. Todo **software** anti-vírus, **anti-spyware** etc. deve ser devidamente licenciado.

SUBSEÇÃO VII

DA MÍDIA E DOS DISPOSITIVOS REMOVÍVEIS

Art. 89. Deve ser levado a efeito um rigoroso controle de gravação de dados em qualquer tipo de mídia removível visando minimizar possíveis vazamentos de informação.

Parágrafo Único. Deve ser proibido o uso de todo e qualquer dispositivo removível de armazenamento ou transferência de dados, tais como dispositivos USB de armazenamento (**pen drives**), interfaces **Bluetooth e WiFi,** dentre outros, tanto para leitura, quanto para gravação de dados.

Art. 90. Gravações em mídia removível devem ser realizadas apenas para cópias de segurança (**backup**).

Parágrafo Único. Se houver necessidade de gravação para outro fim, esta deve ser formalmente autorizada e o processo deve ser supervisionado.

Art. 91. Portas e interfaces não utilizadas em computadores, servidores e qualquer outro ativo de processamento da informação devem ser desabilitadas.

Parágrafo Único. Caso seja imprescindível, essas portas e interfaces devem ser habilitadas temporariamente e utilizadas sob supervisão, após autorização formal.

CAPÍTULO IV

DA SEGURANÇA DOS RECURSOS CRIPTOGRÁFICOS

SEÇÃO I

DAS DIRETRIZES GERAIS

Art. 92. Toda a documentação, referente a definição, descrição e especificação dos componentes dos sistemas criptográficos utilizados na ICP-EB, deve ser formalmente aprovada por comissão constituída de integrantes do DCT, do CITEx e do CDS.

SEÇÃO II

DAS CHAVES CRIPTOGRÁFICAS

Art. 93. Todos processos que envolvem as chaves criptográficas utilizadas nos sistemas criptográficos da ICP-EB devem ser executados por dois militares, no mínimo.

Parágrafo Único. Os militares que atuam em processos criptográficos da ICP-EB devem ser formalmente designados, atendendo ao preconizado no Título IV destas Instruções e, conforme as funções que vierem a desempenhar, receber a credencial de segurança necessária e ter suas responsabilidades definidas explicitamente.

Art. 94. Os diferentes tipos de chaves criptográficas e suas funções no sistema criptográfico das AC da ICP-EB devem ser explicitados em Normas de Certificado específicas.

SEÇÃO III

DO TRANSPORTE DAS INFORMAÇÕES

Art. 95. O processo de transporte de chaves criptográficas e demais parâmetros dos sistemas de criptografia das AC da ICP-EB deve ter assegurados sua integridade e o seu sigilo.

TÍTULO V

DA AUDITORIA

Art. 96. Auditorias periódicas do tipo II na ICP-EB devem ser realizadas por equipe designada pelo DCT, em conformidade com as IR 13-09 (IRASEG).

Art. 97. Auditorias periódicas do tipo I na ICP-EB podem ser realizadas por equipe própria da entidade na qual o ativo encontra-se instalado ou por equipe designada pelo Chefe do CITEx, ou pelo DCT, em conformidade com as IR 13-09 (IRASEG).

Art. 98. Os processos de auditoria devem ser realizados mediante assinatura de Termo de Compromisso de Manutenção de Sigilo, bem como o cumprimento de todos os procedimentos de segurança aplicáveis, pela equipe auditora.

TÍTULO VI

DAS RESPONSABILIDADES

CAPÍTULO I

DO DEPARTAMENTO DE CIÊNCIA E TECNOLOGIA

Art. 99. É de responsabilidade do DCT:

I – prover os recursos e os meios necessários para que as entidades pertencentes à ICP-EB cumpram estas Instruções;

II – aprovar e publicar as Normas e as Instruções necessárias ao funcionamento da ICP-EB;

III – Realizar auditorias periódicas do tipo II na ICP-EB;

IV – Coordenar a Comissão Conjunta com o CITEx e o CDS para definir, especificar e/ou aprovar componentes dos sistemas criptográficos utilizados na ICP-EB.

CAPÍTULO II

DO CENTRO INTEGRADO DE TELEMÁTICA DO EXÉRCITO

Art. 100. São responsabilidades do CITEx:

I – zelar pelo cumprimento destas Instruções e de todas as outras a ela vinculadas;

II – identificar possíveis desvios e adotar medidas corretivas apropriadas;

III – proteger os ativos de informação e de processamento da ICP-EB;

IV – estabelecer as regras de proteção dos ativos da ICP-EB;

V – decidir quais medidas devem tomadas no caso de violação das regras estabelecidas;

VI – revisar, ao menos a cada 18 (dezoito) meses, as regras de proteção estabelecidas;

VII – restringir e controlar o acesso aos ativos da ICP-EB;

VIII – especificar os privilégios de todos os militares que tenham necessidade de manipular informações na ICP-EB e conceder acesso segundo os critérios estabelecidos nestas Instruções;

IX – elaborar e manter atualizado o PCN;

X – detectar, identificar, registrar as violações ou tentativas de acesso não autorizadas;

XI – manter os registros de atividades (**logs**) da forma e pelos prazos especificados nestas Instruções; e,

XII – prestar suporte de certificação digital, no âmbito da ICP-EB, a usuários, podendo empregar os CTA e CT quando necessário; e

XIII – propor ao DCT melhorias nos processos de certificação digital no âmbito do EB;

XIV – Realizar auditorias periódicas do tipo I na ICP-EB.

CAPÍTULO III

DO CENTRO DE DESENVOLVIMENTO DE SISTEMAS

Art. 101. São responsabilidades do CDS:

I – propor ao DCT melhorias nos processos de certificação digital no âmbito do EB; e

II – assessorar o DCT e o CITEx em assuntos relacionados a projetos que envolvam certificação digital.

CAPÍTULO IV

DOS INTEGRANTES DA INFRA-ESTRUTURA DE CERTIFICAÇÃO DIGITAL DO EXÉRCITO BRASILEIRO

Art. 102. É de responsabilidade de todos integrantes da ICP-EB:

I – preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos ativos de processamento e informações;

II – cumprir as regras contidas na documentação normativa de segurança da ICP-EB e outras a elas vinculadas, sob pena de incorrer nas sanções disciplinares e legais cabíveis;

III – utilizar os Sistemas de Informações da ICP-EB e os ativos a ela relacionados somente para os fins previstos;

IV – cumprir as regras de proteção estabelecidas aos ativos de informação;

V – manter o caráter sigiloso de suas senhas de acesso;

VI – somente compartilhar informações com pessoas que tenham a devida credencial de segurança e a necessidade de conhecimento;

VII – responder por todo e qualquer acesso aos ativos da ICP-EB, bem como pelos efeitos desses acessos efetivados por meio do seu código de identificação, ou outro atributo para este fim;

VIII – respeitar a proibição de não usar, inspecionar, copiar ou armazenar programas de computador ou qualquer outro material, em violação da legislação de propriedade intelectual pertinente;

IX – comunicar ao seu superior imediato o conhecimento de qualquer irregularidade ou desvio; e

X – propor ao DCT melhorias nos processos de certificação digital no âmbito do EB.

Art. 103. É responsabilidade do Chefe da Seção de Certificação Digital da Divisão de Segurança do CITEx:

I – definir e aplicar, para cada integrante da ICP-EB, restrições de acesso aos ativos, como horário autorizado, dias autorizados, dentre outras;

II - fornecer senhas e outros mecanismos de autenticação, quando for o caso, somente aos integrantes da ICP-EB que necessitem efetivamente desses privilégios, mantendo os devidos registro e controle;

III – excluir as contas inativas;

IV – coordenar e supervisionar as atividades da ICP-EB; e

V – propor a seu superior imediato melhorias nos processos da ICP-EB.

CAPÍTULO VI

DOS USUÁRIOS DA INFRA-ESTRUTURA DE CERTIFICAÇÃO DIGITAL DO EXÉRCITO BRASILEIRO

Art. 104. Os usuários da ICP-EB deverão proceder conforme previsto nas Instruções Reguladoras para Práticas de Certificação da Autoridade Certificadora do Exército Brasileiro.

TÍTULO VII

DAS SANÇÕES

Art. 105. O descumprimento destas Instruções de Segurança e dos outros documentos a elas subordinados incorrerá nas sanções previstas pela legislação vigente.