PORTARIA Nº 27-DCT, DE 7 DE JULHO DE 2009.

Aprova as Instruções Reguladoras para Práticas de Certificação da Autoridade Certificadora do Exército Brasileiro – IREPCAC (IR 80-07).

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 para Práticas de Certificação da Autoridade Certificadora do Exército Brasileiro – IREPCAC (IR 80-07).

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

INSTRUÇÕES REGULADORAS PARA PRÁTICAS DE CERTIFICAÇÃO DA AUTORIDADE CERTIFICADORA DO EXÉRCITO BRASILEIRO – IREPCAC (IR 80-07)

ÍNDICE DE ASSUNTOS

Art.

TÍTULO I

DAS GENERALIDADES

CAPÍTULO I

DA FINALIDADE

Art. 1º As presentes Instruções têm por finalidade descrever as práticas e os procedimentos empregados pelo Centro Integrado de Telemática de Área (CITEx) na execução de seus serviços de Autoridade Certificadora do Exército Brasileiro no CITEx (AC-EB CITEx) e em conjunto com as Instruções Reguladoras para Práticas de Certificação da Autoridade Certificadora Raiz do Exército Brasileiro (IRERAIZ) e as Instruções Reguladoras sobre Segurança da Infraestrutura de Chaves Públicas do Exército Brasileiro (IRESICP) foram elaboradas em observância ao art. 18 das Instruções Gerais de Segurança da Informação para o Exército Brasileiro (IG 20-19).

Art. 2º A AC-EB CITEx gerencia o ciclo de vida dos certificados por ela emitidos e suas Listas de Certificados Revogados (LCR).

CAPÍTULO II

DAS DEFINIÇÕES

Art. 3º A AC-EB CITEx é diretamente subordinada à AC-Raiz EB, devendo ter, por esta última, assinado seu certificado digital de AC.

Art. 4º Constituem a AC-EB CITEx suas máquinas servidoras, a infra-estrutura necessária ao seu funcionamento, a Autoridade de Registro do Exército Brasileiro no CITEx (AR-EB CITEx) que, por sua vez, é constituída de suas máquinas servidoras e dos agentes validadores.

CAPÍTULO III

DA INTERPRETAÇÃO E DA EXECUÇÃO

Art. 5º Estas Normas são regidas pelo § 2º, do art. 10 da Medida Provisória Nr 2.200-2, de 24 de agosto de 2001, bem como pelas demais leis pertinentes em vigor no Brasil.

Parágrafo Único. Na hipótese de uma ou mais das disposições destas Instruções ser, por qualquer razão, considerada inválida, ilegal, ou inaplicável por lei, tal inaplicabilidade não afetará as demais disposições, sendo estas Instruções interpretadas então como se não contivessem tal disposição e, na medida do possível, interpretadas para manter a intenção original das IREPCAC.

Art. 6º A regulamentação dos tipos específicos de certificados emitidos pela AC-EB CITEx deve ser publicada nas Normas de Certificados Tipo X da Autoridade Certificadora do Exército Brasileiro (NORCERT-X), onde X deve ser o tipo do certificado, na página http://icpeb.citex.eb.mil.br.

CAPÍTULO IV

DAS REFERÊNCIAS

Art. 7º São empregadas como referências a legislação e as normas abaixo relacionadas:

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);

CAPÍTULO V

DA IDENTIFICAÇÃO

Art. 8º O Identificador de Objeto (*Object Identifier* – OID) destas Normas é 4.19.67.1.1.1.

CAPÍTULO VI

DA APLICABILIDADE

SEÇÃO I

DA AUTORIDADE CERTIFICADORA

Art. 9º Estas Normas referem-se unicamente à Autoridade Certificadora do Exército Brasileiro (AC-EB CITEx), gerenciada e operada pelo

Centro Integrado de Telemática do Exército (CITEx).

SEÇÃO II

DA AUTORIDADE DE REGISTRO

Art. 10. Os processos de recebimento, validação e encaminhamento de requisições de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes, são de competência da Autoridade de Registro do Exército Brasileiro no CITEx (AR-EB CITEx), vinculada diretamente à AC-EB CITEx.

SEÇÃO III

DOS TITULARES DE CERTIFICADO

Art. 11. Os certificados emitidos pela AC-EB CITEx devem ter como titulares militares e/ou servidores civis do EB ou qualquer outra pessoa que necessite acessar sistemas corporativos.

Parágrafo Único. Para fazer uso de certificado digital da ICP-EB, o titular deve cumprir toda a legislação listada no art. 5º e todo o arcabouço normativo pertinentes.

Art. 12. Quando o certificado digital for para uso especifico em máquina, o titular deverá ser a pessoa responsável pela operação desse equipamento, formalmente designada pelo Cmt/Ch/Dir da OM.

Parágrafo Único. O responsável deve digitar a senha de ativação da chave privada correspondente ao certificado sempre que for ativado o serviço da máquina que o utiliza.

SEÇÃO IV

DAS NORMAS DE CERTIFICADO

Art. 13. A AC-EB CITEx deve implementar as seguintes Normas de Certificado:

Normas de Certificado	Abreviatura	OID
Normas de Certificado de Assinatura Digital tipo A1 da Autoridade Certificadora do Exército Brasileiro	NORCERT-A1	4.19.67.1.2.1.1
Normas de Certificado de Assinatura Digital tipo A4 da Autoridade Certificadora do Exército Brasileiro	NORCERT-A4	4.19.67.1.2.4.1
Normas de Certificado de Sigilo tipo S1 da Autoridade Certificadora do Exército Brasileiro	NORCERT-S1	4.19.67.1.2.101.1
Normas de Certificado de Sigilo tipo S4 da Autoridade Certificadora do Exército Brasileiro	NORCERT-S4	4.19.67.1.2.104.1

Art. 14. Nas NORCERT correspondentes devem ser relacionadas as finalidades para as quais são adequados os certificados emitidos pela AC-EB CITEx e, quando cabíveis, as finalidades para as quais existam restrições ou proibições para o uso desses certificados.

CAPÍTULO V

DOS DADOS DE CONTATO

Art. 15. Os dados de contato da AC-EB CITEx são os seguintes:

I – Nome da OM: Centro Integrado de Telemática do Exército (CITEx);

II – Endereço: Avenida Duque de Caxias, S/Nr – Setor Militar Urbano – Brasília, DF;

III – Telefones: (61) 3415-7078 e RITEx 866-7078;

V – Fac-símile: (61)3415-7050 e RITEx 866-7050;

VI – Página *web*: https://icpeb.citex.eb.mil.br/pub; e

VII – E-mail: icpeb@citex.eb.mil.br.

CAPÍTULO VI

DAS OBRIGAÇÕES

SEÇÃO I

DAS OBRIGAÇÕES DA AC-EB CITEx

Art. 16. Constituem-se obrigações da AC-EB CITEx:

I – operar de acordo com as IRESICP, estas Instruções e as NORCERT que implementar;

II – gerar e gerenciar os seus pares de chaves criptográficas;

III – assegurar a proteção de suas chaves privadas;

IV – quando ocorrer suspeita de comprometimento de sua chave privada, providenciar a imediata revogação do certificado correspondente;

V – notificar os seus usuários quando ocorrer:

a) suspeita de comprometimento da chave privada da AC-EB CITEx;

c) encerramento de suas atividades;

VI – publicar seu próprio certificado;

VII – emitir, expedir e distribuir os certificados de usuários;

VIII – informar a emissão do certificado ao respectivo solicitante;

IX – revogar os certificados por ela emitidos;

X – emitir, gerenciar e publicar suas Listas de Certificados Revogados (LCR);

XI – publicar em sua página as IREPCAC e as NORCERT que implementar;

XII – publicar, em sua página, as informações definidas nos art. 22º e 25º destas Instruções;

XIII – utilizar protocolo de comunicação seguro ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via *web*;

XIV – identificar e registrar todas as ações executadas, conforme as Normas pertinentes;

XV – adotar as medidas de segurança e controle previstas nas IRESICP, nestas Normas e nas NORCERT implementadas;

XVI – manter a conformidade dos seus processos, procedimentos e atividades com as Normas pertinentes e com a legislação vigente;

XVII – manter a segurança da informação e dos dados por ela tratados;

XVIII – manter e testar regularmente seu Plano de Continuidade do Negócio (PCN); e

XIX – não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado.

SEÇÃO II

DAS OBRIGAÇÕES DA AR-EB CITEx

Art. 17. São obrigações da AR-EB CITEx:

I – receber requisições de emissão e de revogação de certificados;

II – confere a documentação recebida do requisitante com a identidade do solicitante e a validade da solicitação;

III – encaminhar a requisição de emissão ou de revogação de certificado à AC-EB CITEx, utilizando protocolo de comunicação seguro, conforme padrão definido na documentação normativa que define os Padrões e Algoritmos Criptográficos da ICP-EB;

IV – disponibilizar os certificados emitidos pela AC-EB CITEx a seus respectivos titulares;

V – identificar e registrar todas as ações executadas, conforme as normas vigentes;

VI – manter a conformidade dos seus processos, procedimentos e atividades em conformidade com as normas, os critérios, as práticas, as regras estabelecidas e a legislação pertinente à ICP-EB.

VII – manter a segurança da informação por ela tratada, de acordo com o estabelecido as normas, os critérios, as práticas, as regras estabelecidas e a legislação pertinente à ICP-EB.

VIII – proceder o reconhecimento das assinaturas e da validade dos documentos apresentados na forma dos art. 50º e 51º;

IX – garantir que todas as aprovações de requisição de certificados sejam realizadas em instalações técnicas formalmente destinadas a tal fim; e

X – operar de acordo com as IRESICP, estas Normas e as NORCERT que devem ser implementadas pela AC-EB CITEx.

SEÇÃO III

DAS OBRIGAÇÕES DO TITULAR DO CERTIFICADO

Art. 18. Cabe ao titular do certificado:

I – fornecer, de forma completa e precisa, todas as informações necessárias à sua identificação;

II – proteger e manter o sigilo de suas chaves privadas, senhas e dispositivos criptográficos;

III – gerar seu par de chaves criptográficas em conformidade com as NORCERT correspondentes;

IV – verificar se o tamanho das chaves criptográficas geradas está em conformidade com as NORCERT correspondentes;

V – assegurar que as chaves criptográficas foram geradas no dispositivo adequado em conformidade com as NORCERT correspondentes;

VI – utilizar seus certificados e chaves privadas de forma apropriada, conforme previsto nas NORCERT correspondentes;

VII – informar à AC-EB CITEx, por intermédio da AR-EB CITEx, qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente;

VIII – verificar, no momento da aceitação do certificado, a veracidade e exatidão das informações contidas no seu certificado e solicitar à AC-EB CITEx, por intermédio da AR-EB CITEx, a imediata revogação do certificado que contiver inexatidões ou erros;

IX – seguir o que preceituam estas Normas e as NORCERT aplicáveis, no que lhe for pertinente.

SEÇÃO IV

DA OBRIGAÇÃO DO COMANDANTE/CHEFE/DIRETOR

Art. 19. Cabe ao Cmt/Ch/Dir do titular, ou por ele responsável, assinar a requisição de certificado assumindo o papel de co-responsável pelas informações contidas no documento.

SEÇÃO V

DAS OBRIGAÇÕES DA TERCEIRA PARTE

Art. 20. Constituem-se obrigações da terceira parte:

I – recusar a utilização do certificado para fins diversos dos previstos nas NORCERT correspondentes;

II – verificar, sempre que necessário, a validade do certificado.

SEÇÃO VI

DAS OBRIGAÇÕES DO REPOSITÓRIO

Art. 21. São obrigações do repositório:

I – disponibilizar, logo após a sua emissão, os certificados emitidos pela AC-EB CITEx e suas LCR;

II – possuir a disponibilidade prevista no art. 23 destas Normas; e

III – implementar os recursos necessários para a segurança dos dados nele armazenados.

CAPÍTULO VII

DA PUBLICAÇÃO EM REPOSITÓRIO

Art. 22. Os certificados da AC-EB CITEx e os por ela emitidos, além de suas Listas de Certificados Revogados (LCR), devem ser publicados na página de endereço http://ipceb.citex.eb.mil.br/pub/crl/cacrl.crl.

Art. 23. A disponibilidade mínima do repositório da AC-EB CITEx deve ser de 98,5% (noventa e oito e meio por cento) do tempo.

Art. 24. Os certificados devem ser publicados em até 1 (um) dia útil após sua emissão.

Art. 25. As seguintes informações devem ser publicadas na página da AC-EB CITEx:

I – seu próprio certificado;

II – os certificados por ela emitidos;

III – suas LCR;

IV – as IREPCAC;

V – as NORCERT que implementa.

Art. 26. A LCR da AC-EB CITEx deve ser emitida e publicada com a freqüência indicada no art. 74.

Art. 27. Não deve haver restrição ao acesso, no âmbito do EB, para consulta a estas Normas, aos certificados emitidos e às LCR da AC-EB CITEx.

CAPÍTULO VIII

DA AUDITORIA

Art. 28. As auditorias realizadas na AC-EB CITEx têm por objetivo verificar se os processos, procedimentos e atividades estão em conformidade com suas IRESICP, IREPCAC, NORCERT e demais Normas e Procedimentos estabelecidos pelo DCT.

Art. 29. As auditorias devem ser realizadas de acordo com as IR 13-09.

§ 1º As auditorias do tipo 2 destinam-se à verificação geral de conformidade da AC-EB CITEx, devem ser realizadas por equipe designada pelo DCT num prazo máximo de 1 (um) ano.

§ 2º As auditorias do tipo 1, que destinam-se a verificar processos, procedimentos ou atividades específicos, conforme demanda estabelecida pelo DCT ou pelo CITEx, devem ser realizadas por equipe designada pelo órgão solicitante sempre que houver necessidade.

Art. 30. Para ativação da AC-EB CITEx, deve haver uma auditoria prévia realizada por equipe designada pelo DCT.

CAPÍTULO IX

DO SIGILO

Art. 31. A chave privada da AC-EB CITEx deve ser gerada e mantida pela própria AC, que deve assegurar seu sigilo.

Art. 32. Os documentos, informações e registros da AC-EB CITEx abaixo discriminados devem ser considerados ostensivos:

I – certificados digitais;

II – LCR, contendo número de série e data/hora de revogação de cada certificado revogado;

III – Informações corporativas ou pessoais, que necessariamente façam parte dos Incisos I e II deste Art.

IV – as NORCERT aplicáveis;

V – estas Instruções; e

VI – as IRESICP.

Art. 33. Mediante ordem judicial, serão fornecidos quaisquer documentos, informações ou registros sob a guarda da AC-EB CITEx.

Art. 34. O titular de certificado e seu representante legal devem ter amplo acesso a seus próprios dados, desde que os requeiram formalmente, em conformidade com a legislação pertinente.

TÍTULO II

DOS CONCEITOS BÁSICOS

Art. 35. Para aplicação destas Normas, deve-se adotar as seguintes conceituação:

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

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

III – CONTROLE DE ACESSO – restrições ao acesso às informações de um sistema exercido pela gerência de Segurança da Informação da AC-EB CITEx;

IV – CUSTÓDIA – responsabilidade de se guardar um ativo para terceiros. Entretanto, a custódia não permite automaticamente o acesso ao ativo, nem o direito de conceder acesso a outros;

V – DIREITO DE ACESSO – privilégio associado a cargo, pessoa ou processo para ter acesso a um ativo;

VI – FERRAMENTAS – conjunto de equipamentos, programas, procedimentos, normas e demais recursos por meio dos quais se aplicam as Normas de Segurança da AC-EB CITEx;

VII – INCIDENTE DE SEGURANÇA – qualquer evento ou ocorrência que promova uma ou mais ações que comprometa ou que seja uma ameaça à integridade, autenticidade, ou disponibilidade de qualquer ativo da AC-EB CITEx;

VIII – NORMAS DE SEGURANÇA – conjunto de regras destinadas a definir a proteção adequada dos ativos produzidos pelos Sistemas de Informação da AC-EB CITEx;

IX – PROTEÇÃO DE ATIVOS – processo pelo qual os ativos devem receber classificação quanto ao grau de sensibilidade;

X – RESPONSABILIDADE – obrigações e deveres da pessoa que ocupa determinada função em relação ao acervo de informações;

XI – SENHA FRACA OU ÓBVIA – aquela onde se utilizam 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 – TERCEIRA PARTE – parte que confia no teor, na validade e na aplicabilidade do certificado digital.

XIII – CERTIFICADO VÁLIDO - Um certificado emitido pela AC-EB CITEx é considerado válido quando:

a) não constar da LCR da AC-EB CITEx;

b) não estiver expirado; e

c) puder ser verificado com o uso do certificado válido da AC-EB CITEx;

XIV – PROVEDOR CRIPTOGRÁFICO – software destinado à comunicação entre os programas de computador e os **drivers** de um dispositivo criptográfico;

XV – DISPOSITIVO CRIPTOGRÁFICO – dispositivo destinado à geração de pares de chaves criptográficas, armazenamento de certificados digitais e operações criptográficas, como autenticação, assinatura digital e sigilo de documentos eletrônicos;

XVI – TERMO DE TITULARIDADE – Termo assinado por quem requisita um certificado digital, firmando seu comprometimento com a legislação e as normas aplicáveis, no que se refere à guarda de sua chave privada e ao uso de seu certificado digital;

XVII – COMPROVAÇÃO DA IDENTIDADE DE UM INDIVÍDUO – comprovação de que a pessoa que se apresenta como titular ou responsável pelo certificado é realmente aquela cujos dados constam na documentação apresentada.

TÍTULO III

DA IDENTIFICAÇÃO E DA AUTENTICAÇÃO

CAPÍTULO I

DO DISPOSITIVO DE AUTENTICAÇÃO

Art. 36. O Cmt/Ch/Dir do titular, ou por ele responsável, pode solicitar, por ofício direto ao Comandante do CITEx, a quantidade de dispositivos de autenticação (**smartcards** ou **tokens** USB) necessários, os nomes e os CPF dos titulares aos quais serão distribuídos os dispositivos.

§ 1º A concessão do dispositivo de autenticação para titulares, pelo CITEx, é dependente da existência de um projeto onde este titular fará uso de certificação digital;

§ 2º O titular poderá adquirir um dispositivo de autenticação por sua conta, desde que compatível com os certificados emitidos pela AC-EB CITEx.

Art. 37. O fornecimento do dispositivo será feito, por ofício, do Chefe do CITEx diretamente ao Cmt/Ch/Dir do titular ou por ele responsável.

§ 1º O fornecimento deve ser realizado somente após o **smartcard** ou **token** USB ser testado e estar devidamente formatado;

§ 2º Se o titular adquirir um **smartcard** ou **token** USB é de sua inteira responsabilidade testá-lo e formatá-lo.

CAPÍTULO II

DO REGISTRO INICIAL

SEÇÃO I

DA REQUISIÇÃO DE CERTIFICADO

Art. 38. A Requisição de Certificado deve ser efetuada por seu futuro titular, por meio de preenchimento de formulário **online** na página da AC-EB CITEx, no endereço https://icpeb.citex.eb.mil.br/pub.

§ 1º Para certificados com chaves criptográficas geradas em dispositivos criptográficos, tais como **smartcards** e **tokens** USB, todos os **drivers** e qualquer outro software necessário à sua operação devem ser instalados na máquina do futuro titular antes deste efetuar a Requisição de Certificado.

§ 2º Todos os **drivers** necessários aos **smartcards** e/ou **tokens** fornecidos pelo CITEx devem estar disponíveis no endereço http://icpeb.citex.eb.mil.br.

Art. 39. Após o preenchimento do formulário **online** citado no **caput** do Artigo anterior deve ser gerado o par de chaves criptográficas, no próprio **browser** do titular ou em dispositivo criptográfico.

Art. 40. Após a geração do par de chaves criptográficas, uma Requisição deve ser enviada à máquina servidora da AR-EB CITEx e o Termo de Titularidade, mostrado na tela, deve ser impresso pelo futuro titular, rubricado em todas as páginas e assinado na última.

Art. 41. O futuro titular deve juntar a documentação de identificação constante dos Artigos 51 ou 53, necessária à validação de sua Requisição de Certificado, ao Termo de Titularidade e encaminhá-lo a seu Cmt/Ch/Dir ou à pessoa responsável.

Art. 42. O Cmt/Ch/Dir do futuro titular, ou por ele responsável, deve enviar Ofício diretamente ao Chefe do CITEx, com as cópias da documentação de identificação do futuro titular, devidamente autenticadas, e seu Termo de Titularidade original, com as informações neles contidas previamente verificadas por seu Chefe de 1ª Seção, ou correspondente, para que a identidade do futuro titular seja comprovada.

Parágrafo Único. Todas as páginas anexas a esse Ofício devem também ser rubricadas pelo Chefe da 1ª Seção e pelo Cmt/Ch/Dir da OM à qual pertence o futuro titular.

SEÇÃO II

DA VALIDAÇÃO DA REQUISIÇÃO DE CERTIFICADO

Art. 43. O Agente Validador da AR-EB CITEx efetua a validação da Requisição de Certificado conferindo a documentação recebida via Ofício.

Art. 44. Caso as informações estejam todas corretas e a documentação esteja regular, o Agente Validador, na máquina servidora da AR-EB CITEx valida a Requisição, autorizando a máquina servidora da AC-EB CITEx a emitir o certificado requisitado.

Parágrafo Único. Qualquer irregularidade ou incorreção constatada devem provocar a rejeição da Requisição, com a comunicação do motivo ao futuro titular, via ofício ao seu Cmt/Ch/Dir, ou responsável.

Art. 45. Após finalizar o processo de validação, o Agente Validador da AR-EB CITEx deve encaminhar a documentação do requerente ao Operador da AC-EB CITEx, para nova conferência e emissão do certificado.

Art. 46. Todas as etapas do processo de Validação da Requisição de Certificado devem ser registradas e assinadas digitalmente pelos executantes com a utilização de certificado digital de Tipo A4.

Parágrafo Único. Tais registros devem feitos de forma a permitir a reconstituição completa dos processos executados, para fins de auditoria.

Art. 47. Deve ser mantido arquivo com as cópias dos documentos utilizados para confirmação da identidade do requisitante, em papel, seguindo-se os procedimentos preconizados pela legislação e normas aplicáveis.

CAPÍTULO III

DAS COMPROVAÇÕES E DOS NOMES

SEÇÃO I

DOS TIPOS DE NOMES

Art. 48. A AC-EB CITEx deve emitir certificados com nomes que permitam a identificação unívoca de seu titular, utilizando o **Distinguished Name** (DN).

Parágrafo Único. O número do CPF do titular deve ser inserido no campo **Common Name** (CN) logo após o nome completo e antecedido por dois pontos (:), sem espaços nem caracteres separadores;

SEÇÃO II

DA COMPROVAÇÃO DE POSSE DA CHAVE PRIVADA

Art. 49. A AC-EB CITEx deve confirmar que o futuro titular possui a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital, conforme o padrão RFC 4210.

SEÇÃO III

DA COMPROVAÇÃO DA IDENTIDADE DE UM INDIVÍDUO

Art. 50. A comprovação da identidade do indivíduo, que requisita um certificado digital, deve ser realizada mediante sua presença física junto ao Chefe da 1ª Seção na OM da qual for integrante ou à qual estiver vinculado, com base em documentos de identificação legalmente aceitos e com a ratificação do Cmt/Dir/Ch dessa OM.

Parágrafo Único. No caso de usuários externos à Força a documentação deve ser providenciada pelo usuário que deverá comparecer à 1ª Seção, ou equivalente, da OM que está se responsabilizando pela requisição do certificado. O Cmt/Ch/Dir deve ratificar a identificação.

Art. 51. Para comprovar sua identidade, o futuro titular deve apresentar a seguinte documentação, em sua versão original com uma cópia simples de cada, a ser autenticada pela 1ª Seção:

I – Cédula de Identidade Militar, se militar;

II – Se civil, Cédula de Identidade, emitida por Secretaria de Segurança Pública, ou equivalente por força de lei, desde que contenha foto e seja válida em todo o território nacional;

III – Cadastro de Pessoa Física (CPF), caso seu número não conste da Cédula de Identidade;

SEÇÃO IV

DA COMPROVAÇÃO DA IDENTIDADE DE EQUIPAMENTO

Art. 52. A comprovação da identidade de equipamento, para uso de certificado digital, deve ser realizada mediante a presença física do responsável por esse equipamento ou aplicação junto ao Chefe da 1ª Seção na OM da qual for integrante ou à qual estiver vinculado, com base em documentos de identificação legalmente aceitos e com a ratificação do Cmt/Dir/Ch dessa OM.

Art. 53. Para comprovar a identidade do responsável pelo equipamento ou aplicação, deve ser apresentada a seguinte documentação, em sua versão original com uma cópia simples de cada, a ser autenticada pela 1ª Seção:

I – Cédula de Identidade Militar, se militar;

II – Se civil, Cédula de Identidade, emitida por Secretaria de Segurança Pública, ou equivalente por força de lei, desde que contenha foto e seja válida em todo o território nacional;

III – Cadastro de Pessoa Física (CPF), caso seu número não conste da Cédula de Identidade;

IV – Termo de Autorização de Uso de Domínio ou documento similar, para o caso de uso do certificado em equipamento ou aplicação que utilize URL no campo **Common Name**, emitido por órgão competente.

TÍTULO IV

DOS REQUISITOS OPERACIONAIS

CAPÍTULO I

DA REQUISIÇÃO DE CERTIFICADO

Art. 54. Para atender à requisição de emissão de certificados a AC-EB CITEx deve exigir que a AR-EB CITEx tenha provido:

I – a comprovação de atributos de identificação constantes do certificado e o recebimento dos documentos obrigatórios exigidos para identificação dos titulares e o Termo de Titularidade;

II – a autenticação do Agente Validador da AR-EB CITEx deve ser efetuada mediante o uso de certificado digital do tipo A4;

CAPÍTULO II

DA EMISSÃO DE CERTIFICADO

Art. 55. A emissão de certificado digital deve ser efetuada somente após a segunda conferência bem-sucedida das informações constantes da requisição de certificado, conforme o art. 46 destas Instruções.

Art. 56. Devem ser obrigatoriamente preenchidos os seguintes campos do certificado de um indivíduo com as informações constantes dos documentos apresentados:

I – nome completo, sem abreviações;

II – data de nascimento;

III – Cadastro de Pessoa Física (CPF);

IV – número da Cédula de Identidade do titular e órgão expedidor;

Art. 57. Devem ser obrigatoriamente preenchidos os seguintes campos do certificado de equipamento com as informações constantes dos documentos apresentados:

I – URL ou nome da aplicação;

II – nome completo do responsável pelo certificado, sem abreviações;

III – data de nascimento do responsável pelo certificado;

IV – nome da OM.

Art. 58. Logo após emitido o certificado, seu titular deve ser notificado, por mensagem de correio eletrônico e via Ofício Urgente, da emissão do certificado.

Art. 59. O certificado deve ser considerado válido após sua emissão, em conformidade com as informações de data e hora de início e fim de validade, constantes de campo específico desse certificado.

CAPÍTULO III

DA ACEITAÇÃO DE CERTIFICADO

Art. 60. O titular do certificado deve verificar as informações contidas no certificado e aceitá-lo se as informações forem corretas e verdadeiras.

Parágrafo Único. Se constatar qualquer incorreção ou irregularidade, o titular do certificado não deve utilizar o certificado, sob pena de ser enquadrado por falsidade ideológica, e deve solicitar imediatamente sua revogação.

Art. 61. Ao aceitar o certificado, o titular do certificado:

I – concorda com as responsabilidades, obrigações e deveres constantes da IRESICP, destas Normas, e da NORCERT correspondente;

II – garante que, com seu conhecimento, nenhuma pessoa sem autorização teve acesso à chave privada associada ao certificado;

III – afirma que as informações contidas no certificado, fornecidas na requisição, são verdadeiras e estão corretas e completas.

Art. 62. A aceitação do certificado e do seu conteúdo é dada quando da primeira utilização da chave privada correspondente.

Art. 63. O prazo máximo para aceitação do certificado pelo titular deve ser de 15 (quinze) dias úteis, a contar da data de emissão do certificado, findo o qual o certificado será revogado.

CAPÍTULO IV

DA REVOGAÇÃO DE CERTIFICADO

SEÇÃO I

DAS CIRCUNSTÂNCIAS PARA REVOGAÇÃO

Art. 64. Um certificado pode ser revogado a qualquer instante por solicitação de seu titular.

Art. 65. Um certificado deve ser revogado, obrigatoriamente:

I – quando constatada emissão imprópria ou defeituosa;

II – quando for necessária a alteração de qualquer informação nele constante;

III – no caso de desativação da AC-EB CITEx;

IV – no caso de perda, roubo, acesso indevido, comprometimento ou suspeita de comprometimento da chave privada correspondente à chave pública contida no certificado ou de sua mídia armazenadora;

V – no caso de falecimento do titular;

VI – quando houver mudança na denominação de equipamento ao qual o certificado estiver vinculado;

VII – quando da desativação de equipamento ao qual o certificado estiver vinculado; ou

VIII – quando o titular for para a reserva, aposentado ou reformado, sendo neste caso obrigatória a devolução do dispositivo de autenticação.

Art. 66. A AC-EB CITEx deve revogar, no prazo definido no art. 72 destas Normas, o certificado do titular que descumprir a legislação vigente ou as normas pertinentes.

Art. 67. O DCT deve determinar a revogação do certificado da AC-EB CITEx quando essa deixar de cumprir a legislação vigente ou as normas pertinentes.

SEÇÃO II

DAS PRERROGATIVAS PARA SOLICITAR REVOGAÇÃO

Art. 68. A revogação de um certificado emitido pela AC-EB CITEx somente pode ser feita:

I – por solicitação do titular;

II – por determinação do CITEx;

III – por determinação do DCT;

IV – por determinação judicial.

SEÇÃO III

DO PROCEDIMENTO PARA SOLICITAÇÃO DE REVOGAÇÃO

Art. 69. O processo de revogação deve ser iniciado por meio de uma solicitação de revogação à AR-EB CITEx, que pode ser efetuada:

I – em formulário **online** próprio, disponível na página da AR-EB CITEx, com autenticação por frase-senha fornecida na ocasião da requisição do certificado e fornecimento do motivo da solicitação;

II – via Ofício "Urgentíssimo" enviado diretamente ao CITEx, contendo os dados de seu titular, o número de série do certificado e o motivo da solicitação;

III – pelo sistema de gerenciamento de certificados digitais, nos casos previstos nos Incisos II a IV do art. 68 destas Normas.

Art. 70. Instruções para a solicitação de revogação do certificado devem ser divulgadas na página da AR-EB CITEx.

Art. 71. Como diretrizes gerais:

I – o Solicitante da revogação de um certificado deve ser identificado;

II – as solicitações de revogação, bem como as ações delas decorrentes devem ser registradas e armazenadas pela AC-EB CITEx;

III – as justificativas para a revogação de um certificado devem registradas;

IV – o processo de revogação de um certificado deve ser encerrado com a geração e a publicação de uma LCR que contenha os dados do certificado revogado.

Art. 72. O prazo máximo admitido para a conclusão do processo de revogação dos certificados emitidos pela AC-EB CITEx, após o recebimento da respectiva solicitação deve ser de 24 (vinte e quatro) horas, se em dia de expediente, ou no primeiro dia útil após o recebimento da solicitação caso esta chegue em dia sem expediente.

SEÇÃO IV

DO PRAZO PARA SOLICITAÇÃO DE REVOGAÇÃO

Art. 73. A solicitação de revogação deve ser imediata quando configuradas as circunstâncias definidas no art. 65 destas Normas.

SEÇÃO V

DA FREQÜÊNCIA DE EMISSÃO DE LISTAS DE CERTIFICADOS REVOGADOS (LCR)

Art. 74. As LCR da AC-EB CITEx devem ser emitidas a cada 24 (vinte e quatro) horas em dias úteis.

Parágrafo Único. Em sextas-feiras ou vésperas de feriados, as LCR emitidas devem ser válidas até o próximo dia útil.

SEÇÃO VI

DOS REQUISITOS PARA VERIFICAÇÃO DE LCR

Art. 75. Todos os certificados emitidos pela AC-EB CITEx devem ter a validade verificada nas suas LCR antes de serem utilizados.

Parágrafo Único. Também deve ser verificada a autenticidade das LCR da AC-EB CITEx, por meio da verificação da assinatura da AC-EB CITEx e do período de validade da LCR.

SEÇÃO VII

DA VERIFICAÇÃO DE STATUS

Art. 76. A única forma de verificação de status de certificado deve ser por meio de consulta a LCR.

CAPÍTULO V

DOS PROCEDIMENTOS DE VERIFICAÇÃO DE REGISTROS DE EVENTOS (LOGS) DE SEGURANÇA

SEÇÃO I

DOS TIPOS DE EVENTOS REGISTRADOS

Art. 77. Todas as ações executadas pelos integrantes da AC-EB CITEx, no desempenho de suas atribuições, devem ser registradas de

modo que cada ação esteja associada a quem a realizou.

Art. 78. A AC-EB CITEx deve registrar em arquivos os eventos relacionados à segurança do sistema de certificação, dentre outros porventura necessários, obrigatoriamente os seguintes:

I – início de funcionamento e desligamento do sistema de certificação;

II – tentativas de criar, remover, definir senhas ou mudar os privilégios dos operadores;

III – mudanças na configuração da AC-EB CITEx e nas suas chaves criptográficas;

IV – mudanças nas políticas de criação de certificados;

V – tentativas de acesso (**login**) e de saída do sistema (**logoff**);

VI – tentativas não-autorizadas de acesso aos arquivos de sistema;

VII – geração de chaves próprias da AC-EB CITEx;

VIII – emissão e revogação de certificados;

IX – geração de LCR;

X – tentativas de iniciar, remover, habilitar e desabilitar usuários, de atualizar e de recuperar suas chaves; e

XI – operações falhas de escrita e leitura no repositório de certificados e da LCR.

Art. 79. Todos os registros de eventos, eletrônicos ou manuais, devem conter a data e a hora do evento e a identificação do usuário que o causou, incluindo obrigatoriamente os seguintes eventos:

I – registros de acessos físicos;

II – manutenção e mudanças na configuração dos seus sistemas;

III – mudanças de pessoal;

IV – relatórios de discrepância e comprometimento; e

V – registros de destruição de mídia contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuário.

Art. 80. Para facilitar os processos de auditoria, toda a documentação relacionada aos serviços da AC-EB CITEx deve ser armazenada, eletrônica ou manualmente, em local único e em conforme com as IRESICP.

Art. 81. A AC-EB CITEx e a AR-EB CITEx devem registrar eletronicamente, em arquivos de auditoria, todos os eventos relacionados à validação de certificados e sua revogação, sendo obrigatórias as informações abaixo relacionadas:

I – os Operadores de AC e Agente Validadores responsáveis;

II – data e hora das operações;

III – a associação entre os Operadores de AC e Agente Validadores que realizaram a validação e o certificado emitido; e

IV – a assinatura digital do executante.

SEÇÃO II

DA FREQÜÊNCIA DE VERIFICAÇÃO DE REGISTROS

Art. 82. Os registros de eventos (**logs**) de segurança da AC-EB CITEx devem ser analisados:

I – semanalmente se a análise for manual; diária ou em tempo quase real se assistido por sistema específico de análise e correlação de registros; ou

II – em caso de suspeita de comprometimento da segurança.

Art. 83. Todos os eventos significativos devem ser analisados e reportados em relatório de verificação de registros.

§1º Tal análise deve envolver uma inspeção breve de todos os registros, verificando se não indicam alterações, seguida de uma investigação mais detalhada de quaisquer alertas ou irregularidades encontrados.

§2º Todas as ações tomadas em decorrência dessa análise devem ser documentadas.

SEÇÃO III

DO PERÍODO DE RETENÇÃO DE REGISTROS

Art. 84. A AC-EB CITEx deve manter em suas próprias máquinas os seus registros de eventos de segurança por pelo menos 2 (dois) meses e, subseqüentemente, armazená-los pelo tempo indicado no Inciso III do art. 90 destas Normas.

SEÇÃO IV

DA PROTEÇÃO DOS REGISTROS

Art. 85. O sistema de registro de eventos deve incluir mecanismos para proteger esses registros contra leitura não autorizada, modificação e remoção.

SEÇÃO V

DOS PROCEDIMENTOS PARA CÓPIA DE SEGURANÇA (BACKUP) DE REGISTROS DE EVENTOS

Art. 86. Devem-se realizar cópias de segurança (*backup*) dos registros de eventos (*logs*) de segurança das máquinas da AC-EB CITEx e da AR-EB CITEx mensalmente.

Art. 87. A integridade das cópias de segurança deve ser verificada a cada 6 (seis) meses.

SEÇÃO VI

DA NOTIFICAÇÃO DE AGENTES CAUSADORES DE EVENTOS

Art. 88. Quando um evento é registrado nenhuma notificação deve ser enviada à pessoa, organização, dispositivo ou aplicação que causou o evento.

SEÇÃO VII

DAS AVALIAÇÕES DE VULNERABILIDADE

Art. 89. Eventos que representem uma possível vulnerabilidade devem ser analisados detalhadamente e, dependendo de sua gravidade, devem ser registrados em separado.

Parágrafo Único. Como decorrência, ações corretivas devem ser implementadas e registradas para fins de auditoria.

CAPÍTULO VI

DO ARQUIVAMENTO DE REGISTROS

SEÇÃO I

DO PERÍODO DE ARMAZENAMENTO DOS REGISTROS

Art. 90. A documentação relativa aos eventos relacionados nos art. 78 e 79 destas Normas deve ser armazenada pelos seguintes períodos:

I – certificados emitidos pela AC-EB CITEx e respectivas LCR – permanentemente, para fins de consulta histórica;

II – informações sobre os processos de emissão e revogação de certificados de AC – no mínimo 30 (trinta) anos, a contar da data de expiração ou revogação do certificado;

III – demais informações, inclusive arquivos de registros de eventos – 5 (cinco) anos.

SEÇÃO II

DA PROTEÇÃO DOS ARQUIVOS

Art. 91. Os arquivos de registros de eventos devem receber proteção adequada proporcional a seu tempo de armazenamento.

SEÇÃO III

DAS CÓPIAS DE SEGURANÇA DOS ARQUIVOS DE REGISTROS

Art. 92. Uma segunda cópia de todas as informações citadas nos art. 78 e 79 deve ser armazenada no local de contingência, recebendo o mesmo tipo de proteção das informações originais, devendo também ser armazenada pelo mesmo tempo.

SEÇÃO IV

DOS REQUISITOS PARA DATAÇÃO DE REGISTROS

Art. 93. Informações de data e hora nos registros devem utilizar o horário oficial internacional, Coordinated Universal Time – UTC.

CAPÍTULO VII

DA TROCA DE CHAVE

Art. 94. O titular do certificado pode requisitar novo certificado antes da data de expiração do seu certificado ainda válido, por meio de formulário **online** na página da AR-EB CITEx.

Parágrafo Único. Na reemissão de certificado devem ser exigidos novamente os documentos de identificação do titular.

CAPÍTULO VIII

DO COMPROMETIMENTO E DA RECUPERAÇÃO DE DESASTRES

SEÇÃO I

DAS ATIVIDADES DA AC-EB CITEX

Art. 95. A AC-EB CITEx deve possuir um Plano de Continuidade de Negócios (PCN) em conformidade com as IRESICP e contendo as seguintes informações:

I – identificação dos eventos que podem causar interrupções nos processos do negócio;

II – identificação e concordância de todas as responsabilidades e procedimentos de emergência;

III – os procedimentos de emergência para a recuperação e restauração, nos prazos necessários, com especial atenção à recuperação da documentação armazenada nas instalações técnicas atingidas pelo desastre;

IV – documentação dos processos e procedimentos acordados;

V – plano de treinamento do pessoal nos procedimentos e processos de emergência definidos, incluindo o gerenciamento de crise; e

VI – plano de testes; e,

VII – procedimento de atualização dos planos.

SUBSEÇÃO I

DOS RECURSOS COMPUTACIONAIS, DO SOFTWARE E DOS DADOS CORROMPIDOS

Art. 96. Em caso de suspeita de corrupção de dados, **software** ou recursos computacionais, o fato deve ser comunicado ao Chefe da Divisão de Segurança da Informação do CITEx, que decreta o início da fase de resposta.

§ 1º Na fase de resposta, uma rigorosa inspeção deve ser realizada para verificar a veracidade do fato e as conseqüências que ele pode gerar.

§ 2º Esse procedimento deve ser realizado pelos integrantes da Seção de Certificação Digital do CITEx.

§ 3º Caso haja necessidade, o chefe da Divisão de Segurança da Informação do CITEx deverá decretar a situação de contingência.

SUBSEÇÃO II

DA REVOGAÇÃO DO CERTIFICADO DA AC-EB CITEx

Art. 97. Em caso de revogação do certificado da AC-EB CITEx o Chefe da Seção de Certificação Digital deverá providenciar a revogação dos certificados por ela emitidos.

§ 1º Os titulares dos certificados revogados deverão ser informados.

§ 2º A AC-EB CITEx deverá emitir novos certificados em substituição aos revogados com data de expiração coincidente com a dos certificados revogados.

SUBSEÇÃO III

DO COMPROMETIMENTO DA CHAVE DA AC-EB CITEx

Art. 98. Em caso de suspeita de comprometimento de chave da AC-EB CITEx, o fato deve ser imediatamente comunicado ao Chefe da Divisão de Segurança da Informação do CITEx, que deve decretar o início da fase resposta e seguir um plano de ação para analisar a veracidade e a dimensão do fato.

Art. 99. Após confirmado o comprometimento, se houver necessidade, deve ser declarada a situação de contingência e as seguintes providências devem ser tomadas:

I – todos os certificados afetados devem ser revogados e as partes devem ser notificadas;

II – cerimônias específicas devem ser realizadas para geração de novos pares de chaves, exceto em caso de extinção das atividades da AC-EB CITEx.

SUBSEÇÃO IV

DA SEGURANÇA DOS RECURSOS APÓS DESASTRE NATURAL OU DE OUTRA ORIGEM

Art. 100. Em caso de desastre natural ou de outra origem, como por exemplo, inundação ou incêndio ou em caso de impossibilidade de acesso às instalações da AC-EB CITEx deve-se notificar Chefe da Seção de Segurança Orgânica e seguir procedimentos para:

I – garantir a integridade física das pessoas que se encontram nas instalações da AC-EB CITEx;

II – monitorar e controlar o foco da contingência;

III – minimizar os danos aos ativos de processamento da AC-EB CITEx, de forma a evitar a descontinuidade dos serviços.

SEÇÃO II

DAS ATIVIDADES DA AUTORIDADE DE REGISTRO

Art. 101. A AR-EB CITEx deve possuir um Plano de Continuidade de Negócios (PCN) em conformidade com as IRESICP e contendo as seguintes informações:

I – identificação dos eventos que podem causar interrupções nos processos do negócio;

II – identificação e concordância de todas as responsabilidades e procedimentos de emergência;

III – os procedimentos de emergência para a recuperação e restauração, nos prazos necessários, com especial atenção à recuperação da documentação armazenada nas instalações técnicas atingidas pelo desastre;

IV – documentação dos processos e procedimentos acordados;

V – plano de treinamento do pessoal nos procedimentos e processos de emergência definidos, incluindo o gerenciamento de crise; e

VI – plano de testes; e,

VII – procedimento de atualização dos planos.

CAPÍTULO IX

DA EXTINÇÃO DA AC-EB CITEx

Art. 102. No caso de encerramento de suas atividades, a AC-EB CITEx deve cumprir os procedimentos a seguir:

I – comunicar publicamente a extinção dos serviços da AC-EB CITEx, por meio de publicação em Boletim do Exército e outros meios de comunicação julgados relevantes;

II – revogar todos os certificados gerados pela AC-EB CITEx nos prazos estipulados nas NORCERT implementadas após a publicação e comunicar às partes afetadas por meio de de mensagem eletrônica e ofício;

III – extinguir os serviços de emissão de certificados;

IV – extinguir os serviços de revogação, como emissão da LCR, após a revogação completa de todos os certificados;

V – destruir a chave privada da AC-EB CITEx extinta seguindo o procedimento descrito no art. 177;

VI – transferir os dados e gravações da AC-EB CITEx para a Autoridade Certificadora sucessora, se for o caso, que deverá armazená-los conforme o que preconizam estas Normas;

VII – transferir as chaves públicas dos certificados emitidos pela AC-EB CITEx para serem armazenadas por outra AC ou, caso as chaves públicas não sejam assumidas por outra AC, repassar os documentos referentes aos certificados digitais e as respectivas chaves públicas à AC-Raiz EB;

VIII – ficar o Chefe da Divisão de Segurança da Informação do CITEx responsável por verificar se a guarda desses dados e registros atendem os mesmos requisitos de segurança exigidos para a AC-EB CITEx;

IX – transferir, quando aplicável, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas.

TÍTULO V

DOS CONTROLES DE SEGURANÇA

CAPÍTULO I

DA SEGURANÇA FÍSICA

SEÇÃO I

DA CONSTRUÇÃO E DA LOCALIZAÇÃO DAS INSTALAÇÕES

Art. 103. A AC-EB CITEx deve operar em instalações homologadas por auditoria prévia.

Art. 104. A localização e o sistema de certificação da AC-EB CITEx não devem ser publicamente identificados.

Art. 105. Não devem ser admitidos ambientes compartilhados que permitam visibilidade das operações de emissão e revogação de certificados.

Parágrafo Único. As operações de emissão e de revogação devem ser segregadas dos demais serviços sendo executadas em em compartimentos fechados e fisicamente protegidos.

Art. 106. As instalações da AC-EB CITEx devem possuir os seguintes as seguintes características de segurança física:

I – instalações para equipamentos de apoio, tais como:

a) máquinas de ar condicionado;

b) grupos geradores;

c) **no-breaks**;

d) baterias;

e) quadros de distribuição de energia e de telefonia;

f) subestações;

g) retificadores, estabilizadores e similares;

II – instalações para sistemas telecomunicações;

III – sistemas de aterramento e de proteção contra descargas atmosféricas; e

IV – iluminação de emergência.

SEÇÃO II

DO ACESSO FÍSICO

SUBSEÇÃO I

DOS NÍVEIS DE ACESSO

Art. 107. A AC-EB CITEx deve possuir 4 (quatro) níveis de acesso físico aos diversos ambientes e mais 2 (dois) níveis de proteção da chave privada da AC-EB CITEx;

Art. 108. O primeiro nível, ou NÍVEL 1, deve ser a primeira barreira de acesso às instalações da AC-EB CITEx.

§ 1º Para entrar em uma área de NÍVEL 1, cada indivíduo deve ser identificado e registrado.

§ 2º A partir deste nível, estranhos ao serviço no CITEx somente devem transitar devidamente identificados e acompanhados.

§ 3º Nenhum tipo de processo operacional ou administrativo da AC-EB CITEx, a menos do monitoramento por vídeo, deve ser executado nesse nível.

Art. 109. O segundo nível, ou NÍVEL 2, deve ser interno ao primeiro e requerer, controle de acesso com registro de entrada e saída.

§ 1º A passagem do primeiro para o segundo nível deve exigir autorização de acesso por meio eletrônico e uso de crachá.

§ 2º Neste nível de acesso, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, têm sua entrada controlada e somente são utilizados mediante autorização formal e supervisão.

Art. 110. O terceiro nível, NÍVEL 3, deve situar-se dentro do segundo, devendo ser o primeiro nível a abrigar material e atividades da operação da AC-EB CITEx.

§ 1º Este deve ser o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da AC-EB CITEx.

§ 2º Qualquer atividade relativa ao ciclo de vida dos certificados digitais deve ser executada a partir deste nível.

§ 3º Indivíduos não envolvidos nessas atividades somente deverão ter permissão de acesso a este nível mediante necessidade do serviço e credencial de segurança com grau de sigilo Reservado, acompanhadas de integrante da ICP-EB.

§ 4º No NÍVEL 3 devem ser controladas tanto as entradas quanto as saídas de cada pessoa autorizada.

§ 5º Dois mecanismos de controle de acesso devem ser exigidos para a entrada nesse nível, para autenticação individual por dois de três fatores, cartão de acesso, senha ou biometria.

Art. 111. No quarto nível, ou NÍVEL 4, interior ao terceiro, deve ser onde ocorrem atividades especialmente sensíveis da operação da AC-EB CITEx, tais como emissão e revogação de certificados e emissão de LCR.

§ 1º Todos os sistemas e equipamentos necessários a estas atividades devem localizar-se a partir deste nível.

§ 2º O NÍVEL 4 deve possuir os mesmos controles de acesso do NÍVEL 3 e, adicionalmente, deve ser exigida em cada acesso ao seu ambiente a identificação de, no mínimo, 2 (dois) indivíduos formalmente autorizados.

§ 3º Neste nível, a permanência de 2 (dois) desses indivíduos deve ser exigida enquanto o ambiente estiver sendo ocupado.

§ 4º No NÍVEL 4, todas as paredes, o piso e o teto devem ser de alvenaria.

§ 5º As paredes, o piso e o teto, devem ser inteiriços, constituindo célula estanque contra ameaças de acesso indevido.

§ 6º Os dutos de refrigeração e de energia, bem como os dutos de comunicação, não devem permitir invasão física das áreas de quarto nível.

§ 7º Telefones celulares, bem como quaisquer outros tipos de dispositivos portáteis de comunicação ou armazenamento de dados, exceto aqueles exigidos para a operação da AC-EB CITEx, devem ser proibidos a partir deste nível.

§ 8º Na AC-EB CITEx, deve haver ambientes de quarto nível para abrigar e segregar equipamentos de produção e cofre ou gabinete reforçado para armazenamento.

Art. 112. O quinto nível, ou NÍVEL 5, interior ao ambiente de NÍVEL 4, deve compreender um cofre ou gabinete reforçado trancado.

§ 1º Materiais criptográficos tais como chaves, dados de ativação, suas cópias e equipamentos criptográficos devem ser armazenados em ambiente de NÍVEL 5 ou superior.

§ 2º Para garantir a segurança do material o cofre e o gabinete devem possuir tranca com chave ou tranca eletrônica e serem adequados para o armazenamento seguro de mídia.

Art. 113. O sexto nível, ou NÍVEL 6, deve ser constituído de recipientes armazenados no interior do NÍVEL 5.

§ 1º Cada um desses depósitos deve dispor de fechadura.

§ 2º Os dados de ativação da chave privada da AC-EB CITEx devem ser armazenados nesses depósitos.

SUBSEÇÃO II

DOS SISTEMAS FÍSICOS DE DETECÇÃO

Art. 114. Todas as passagens entre os níveis de acesso, bem como as salas de operação de NÍVEL 4, devem ser monitoradas por câmeras de vídeo ligadas a um sistema de gravação 24x7 (vinte e quatro horas por dia, sete dias por semana).

§ 1º A mídia contendo o vídeo resultante deve ser armazenada em ambiente de NÍVEL 3 por, no mínimo, 1 (um) ano.

§ 2º Essa mídia deve ser testada, por meio de verificação de trechos aleatórios no início, no meio e no final da mídia) trimestralmente, com a escolha de, no mínimo, uma referente a cada semana.

Art. 115. O sistema de monitoramento das câmeras de vídeo deve localizar-se em ambiente de NÍVEL 3 e ser permanentemente monitorado.

Parágrafo Único. As instalações do sistema de monitoramento devem ser monitoradas por câmera de vídeo.

SUBSEÇÃO III

DO SISTEMA DE CONTROLE DE ACESSO

Art. 116. O sistema de controle de acesso deve ser hospedado em ambiente de NÍVEL 3.

SUBSEÇÃO IV

DOS MECANISMOS DE EMERGÊNCIA

Art. 117. Mecanismos específicos devem ser implantados pela AC-EB CITEx para garantir a segurança de seu pessoal e de seus equipamentos em situações de emergência.

Parágrafo Único. Esses mecanismos devem permitir o destravamento de portas por meio de acionamento mecânico, para a saída de emergência de todos os ambientes com controle de acesso.

Art. 118. Todos os procedimentos referentes aos mecanismos de emergência devem documentados.

Art. 119. Os mecanismos e procedimentos de emergência devem ser verificados, semestralmente, por meio de simulação de situações de emergência.

SEÇÃO III

DA ENERGIA ELÉTRICA E DO SISTEMA DE AR-CONDICIONADO

Art. 120. As instalações da AC-EB CITEx, além de conectadas à rede elétrica, devem dispor dos seguintes recursos, que permitam sua operação contínua, mesmo em caso de interrupção no fornecimento de energia elétrica:

I – gerador de porte compatível;

II – sistema de **no-breaks**;

III – sistema eficiente de aterramento e proteção a descargas atmosféricas, com instalação e manutenção em conformidade com as normas vigentes;

IV – iluminação de emergência.

Art. 121. As condições de fornecimento de energia devem ser mantidas de forma a atender os requisitos de disponibilidade dos sistemas da AC-EB CITEx e seus respectivos serviços.

Art. 122. Todos os cabos elétricos devem ser protegidos por tubulações, dutos ou calhas apropriados.

Art. 123. Deve haver tubulações, dutos, calhas, quadros e caixas – de passagem, distribuição e terminação – projetados e construídos de forma a facilitar vistorias e a detecção de tentativas de violação.

Parágrafo Único. Devem ser utilizados dutos e calhas separados para cabos de energia elétrica, telefonia e dados.

Art. 124. Não devem ser admitidas instalações provisórias, fiações expostas ou diretamente conectadas às tomadas sem a utilização de conectores adequados.

Art. 125. O sistema de climatização deve atender os requisitos de temperatura exigidos pelos equipamentos utilizados no ambiente e dispor de filtros de poeira.

SEÇÃO IV

DA PREVENÇÃO E DA PROTEÇÃO CONTRA INCÊNDIO

Art. 126. As instalações da AC-EB CITEx devem possuir sistemas para detecção de fumaça e de extinção de incêndio.

Art. 127. Todos os integrantes da AC-EB CITEx devem ser treinados, com freqüência mínima semestral, para operações de combate a incêndio nas instalações sob sua responsabilidade, sob coordenação do Oficial de Combate a Incêndio do CITEx.

Art. 128. Deve-se evitar ao máximo o emprego de materiais inflamáveis no ambiente da AC-EB CITEx.

SEÇÃO V

DO ARMAZENAMENTO DE MÍDIA

Art. 129. Para assegurar que a mídia armazenada não sofra nenhum tipo de dano gerado por fatores externos, a AC-EB CITEx deve dispor de ambiente específico de proteção de armazenamento.

SEÇÃO VI

DA DESTRUIÇÃO DO LIXO

Art. 130. Todos os documentos em papel com informações sensíveis devem destruídos, conforme as IG 10-51 e a legislação vigente.

Art. 131. Todos os dispositivos eletrônicos e outros tipos de mídia não mais utilizáveis, que tenham sido anteriormente utilizados no armazenamento de informações sensíveis, devem ser fisicamente destruídos, também conforme as IG 10-51 e a legislação vigente.

SEÇÃO VII

DAS INSTALAÇÕES DE CONTINGÊNCIA EXTERNAS À AC-EB CITEx

Art. 132. A AC-EB CITEx deve possuir instalação de contingência que atenda aos mesmos requisitos de segurança da instalação principal.

Parágrafo Único. A contingência deve se tornar totalmente operacional em, no máximo, 24 (vinte e quatro) horas.

CAPÍTULO II

DA SEGURANÇA DE PESSOAL

SEÇÃO I

DOS PERFIS DE ACESSO

Art. 133. A AC-EB CITEx deve assegurar a separação das tarefas de seu pessoal para o exercício de funções críticas, com o intuito de evitar que um integrante de má fé utilize o sistema de certificação sem ser detectado.

Art. 134. As ações de cada integrante devem ser limitadas de acordo com seu perfil de acesso.

Art. 135. Deve ser estabelecido um mínimo de 4 (quatro) perfis distintos para sua operação, a serem ocupados por membros da Divisão de Segurança da Informação do CITEx, separados por divisão de atribuições:

I – Administrador;

II – Gerente de Segurança;

III – Operador de AC; e,

IV – Agente Validador da AR-EB CITEx.

SUBSEÇÃO I

DAS ATRIBUIÇÕES DO ADMINISTRADOR

Art. 136. Ao Administrador da AC-EB CITEx compete:

I – configurar e manter o hardware e do software da AC-EB CITEx;

II – iniciar e terminar os serviços da AC-EB CITEx;

III – realizar e recuperar cópias de segurança (**backup**);

IV – distribuir e controlar dispositivos criptográficos de acesso às funcionalidades do sistema de certificação digital da AC-EB CITEx atribuídas aos Operadores e Gerentes de Segurança.

SUBSEÇÃO II

DAS ATRIBUIÇÕES DO GERENTE DE SEGURANÇA

Art. 137. Ao Gerente de Segurança cabe:

I – monitorar o trabalho dos Administradores e Operadores da AC-EB CITEx;

II – implementar as e fiscalizar a execução das Normas de Segurança da ICP-EB (IRESICP) na AC-EB CITEx;

III – verificar os registros de eventos;

IV – fiscalizar o cumprimento destas Normas.

SUBSEÇÃO III

DAS ATRIBUIÇÕES DO OPERADOR

Art. 138. São atribuições do Operador:

I – gerenciar o uso das chaves privadas da AC-EB CITEx;

II – emitir, distribuir, revogar e gerenciar os certificados digitais.

SUBSEÇÃO IV

DAS ATRIBUIÇÕES DO AGENTE VALIDADOR

Art. 139. São atribuições do Agente Validador:

I – validar as requisições de certificados, conferindo a documentação recebida dos futuros titulares com os dados fornecidos nos formulários online de requisição e nos Termos de Titularidade;

II – autorizar a emissão dos certificados digitais.

SEÇÃO II

DO NÚMERO DE MILITARES NECESSÁRIOS POR TAREFA

Art. 140. Para geração e utilização da chave privada da AC-EB CITEx, deve-se empregar a técnica autenticação por segredo compartilhado “m de n”.

Art. 141. Todas as tarefas executadas no ambiente de NÍVEL 4 necessitam da presença de, no mínimo, 2 (dois) de seus integrantes.

Parágrafo Único. As demais tarefas da AC-EB CITEx podem ser executadas por um único integrante.

SEÇÃO III

DA IDENTIFICAÇÃO E DA AUTENTICAÇÃO PARA CADA PERFIL

Art. 142. Todo integrante da AC-EB CITEx deve ter sua identidade e seu perfil verificados antes de:

I – ser incluído em uma lista de acesso às instalações da AC-EB CITEx;

II – ser incluído em uma lista para acesso físico às dependências da AC-EB CITEx;

III – receber um certificado digital ou lhe ser habilitado qualquer outro meio de autenticação para executar suas atividades operacionais na AC-EB CITEx;

IV – ativar uma conta no sistema de certificação da AC-EB CITEx.

Art. 143. Os certificados, contas, senhas e quaisquer outros meios utilizados para identificação e autenticação dos integrantes da AC-EB CITEx devem:

I – ser diretamente atribuídos a um único integrante;

II – proibir compartilhamento;

III – ser restritos às ações associadas ao perfil para o qual foram criados.

Art. 144. A AC-EB CITEx deve adotar padrão de utilização de "senhas fortes", juntamente com procedimentos de validação dessas senhas.

CAPÍTULO III

DOS CONTROLES DE PESSOAL

SEÇÃO I

DAS CREDENCIAIS DE SEGURANÇA

Art. 145. Todos os integrantes da AC-EB CITEx devem possuir credencial de segurança concedida em conformidade com o que preceitua o art. 23 das IRESICP.

Art. 146. A nomeação para exercício de cada perfil na AC-EB CITEx deve ser feita em Boletim Interno do CITEx.

SEÇÃO II

DOS ANTECEDENTES, DA QUALIFICAÇÃO, DA EXPERIÊNCIA E DOS REQUISITOS DE IDONEIDADE

Art. 147. Todo integrante da AC-EB CITEx em atividades diretamente relacionadas com os processos afetos ao ciclo de vida dos certificados digitais deve ser designado conforme o estabelecido nos art. 19 a 21 das IRESICP.

Art. 148. Para que possa ser designado para exercer função na AC-EB CITEx, o militar deve antes ter:

I – verificados seus antecedentes criminais;

II – assinado os Termos de Sigilo e Responsabilidade específicos de sua função.

SEÇÃO III

DOS REQUISITOS DE TREINAMENTO

Art. 149. Todo integrante da AC-EB CITEx em atividades diretamente relacionadas com os processos afetos ao ciclo de vida dos certificados digitais deve receber treinamento, sob responsabilidade de seu Chefe imediato, nas seguintes áreas:

I – princípios e mecanismos de segurança da AC-EB CITEx;

II – solução de certificação em uso na AC-EB CITEx;

III – atividades sob sua responsabilidade; e

IV – procedimentos de recuperação de desastres e de continuidade do negócio.

Art. 150. Os integrantes da AC-EB CITEx devem ser mantidos atualizados sobre as mudanças no processo de certificação da AC-EB CITEx.

Parágrafo Único. Treinamentos de reciclagem devem ser realizados sempre que houver necessidade.

SEÇÃO IV

DAS SANÇÕES

Art. 151. Na eventualidade de uma ação não autorizada, real ou suspeita, realizada por pessoa responsável em qualquer etapa do ciclo de vida de certificados digitais, a AC-EB CITEx deve suspender o acesso dessa pessoa ao sistema de certificação e tomar as medidas técnicas, administrativas e legais cabíveis.

SEÇÃO V

DA DOCUMENTAÇÃO FORNECIDA AO PESSOAL

Art. 152. A AC-EB CITEx deve disponibilizar a todos os seus integrantes:

I – as IRESICP;

II – as IREPCAC;

III – as NORCERT implementadas;

IV – documentação operacional relativa a suas atividades; e

V – legislação, normas e procedimentos relevantes a suas atividades.

CAPÍTULO IV

DA SEGURANÇA LÓGICA

SEÇÃO I

DA GERAÇÃO E DA INSTALAÇÃO DO PAR DE CHAVES CRIPTOGRÁFICAS

SUBSEÇÃO I

DA GERAÇÃO DO PAR DE CHAVES CRIPTOGRÁFICAS

Art. 153. Os pares de chaves criptográficas vinculados aos certificados da AC-EB CITEx devem ser gerados pela própria AC-EB CITEx, em **hardware** criptográfico específico.

Parágrafo Único. A geração deve seguir procedimento formalizado, controlado e passível de auditoria.

Art. 154. Os pares de chaves criptográficas vinculados aos certificados emitidos pela AC-EB CITEx somente devem ser gerados pelo próprio titular do certificado correspondente, seguindo procedimentos específicos descritos nas NORCERT implementadas.

Art. 155. Os algoritmos a serem utilizados para geração das chaves criptográficas da AC-EB CITEx devem ser definidos nas Normas de Definição de Padrões e Algoritmos Criptográficos da ICP-EB (NORPAC).

SUBSEÇÃO II

DA ENTREGA DA CHAVE PÚBLICA AO EMISSOR DO CERTIFICADO

Art. 156. A AC-EB CITEx deve entregar cópia de sua chave pública para a AC-Raiz EB em formato PKCS #10, em cerimônia especifica, com data e hora previamente estabelecidas.

Art. 157. Os usuários finais devem enviar suas chaves públicas à AC-EB CITEx por meio eletrônico em formato PKCS#10, por meio de sessão segura fixada pelo protocolo **Secure Socket Layer** (SSL) ou **Transport Layer Security** (TLS).

Parágrafo Único. Os procedimentos específicos aplicáveis devem ser detalhados nas NORCERT implementadas.

SUBSEÇÃO III

DA DISPONIBILIZAÇÃO DA CHAVE PÚBLICA DA AC-EB CITEx

Art. 158. A disponibilização dos certificados da AC-EB CITEx ao público deve ser realizada por uma das seguintes formas:

I – em repositório;

II – em página **web**;

III – por outros meios seguros aprovados pelo DCT.

SUBSEÇÃO IV

DOS TAMANHOS DE CHAVES CRIPTOGRÁFICAS

Art. 159. Os tamanhos das chaves criptográficas da AC-EB CITEx devem ser os definidos nas NORPAC.

SUBSEÇÃO V

DOS PARÂMETROS DE GERAÇÃO DE CHAVES CRIPTOGRÁFICAS ASSIMÉTRICAS

Art. 160. Os parâmetros de geração das chaves criptográficas assimétricas da AC-EB CITEx devem ser os definidos nas NORPAC.

SUBSEÇÃO VI

DA VERIFICAÇÃO DA QUALIDADE DOS PARÂMETROS

Art. 161. Os parâmetros de geração das chaves criptográficas assimétricas devem ser verificados de acordo com o que preconizam as NORPAC.

SUBSEÇÃO VII

DA GERAÇÃO DE CHAVES CRIPTOGRÁFICAS POR HARDWARE/SOFTWARE

Art. 162. A AC-EB CITEx deve utilizar componentes seguros de **hardware** para a geração de seus pares de chaves, de seus certificados, e para a geração de suas LCR.

Parágrafo Único. Os componentes seguros de **hardware** devem utilizar mecanismos de prevenção e detecção de violação, em conformidade com as NORPAC.

Art. 163. Cada NORCERT implementada deve caracterizar o processo empregado na geração de chaves criptográficas privativas dos titulares dos certificados, em conformidade com as NORPAC.

SUBSEÇÃO VIII

DOS PROPÓSITOS DE USO DE CHAVES

Art. 164. As chaves privadas da AC-EB CITEx devem ser utilizadas somente para assinatura de certificados e LCR por ela emitidos.

Art. 165. Os propósitos para os quais podem ser utilizadas as chaves privadas dos titulares de certificados emitidos pela AC-EB CITEx, bem como as possíveis restrições, estão especificados em cada NORCERT implementada.

SEÇÃO II

DA PROTEÇÃO DA CHAVE PRIVADA

SUBSEÇÃO I

DO ARMAZENAMENTO DAS CHAVES PRIVADAS

Art. 166. As chaves privadas da AC-EB CITEx devem ser armazenadas de forma cifrada nos mesmos módulos de segurança em hardware utilizados para sua geração.

Parágrafo Único. O acesso a essas chaves deve controlado por meio de chave criptográfica de ativação.

Art. 167. Os titulares dos certificados emitidos pela AC-EB CITEx devem responsabilizar-se pela guarda de sua chave privada correspondente, adotando procedimentos aplicáveis à proteção dessa chave, em conformidade com o que preconizam as NORCERT específicas.

SUBSEÇÃO II

DOS PADRÕES PARA MÓDULO CRIPTOGRÁFICO

Art. 168. Os módulos criptográficos da AC-EB CITEx devem adotar a padronização definida nas NORPAC.

Art. 169. Os Titulares de Certificado emitidos pela AC-EB CITEx devem garantir que o módulo criptográfico empregado na geração e na utilização de suas chaves criptográficas segue os padrões definidos nas NORPAC.

SUBSEÇÃO III

DO CONTROLE "M DE N" PARA A CHAVE PRIVADA

Art. 170. As chaves criptográficas de ativação dos componentes seguros de **hardware** que armazenam as chaves privadas da AC-EB CITEx devem ser divididas em 3 (três) partes e distribuídas entre 3 (três) pessoas designadas pela AC-EB CITEx.

Parágrafo Único. Deve ser necessária a presença de apenas 2 (duas) dessas 3 (três) pessoas para a ativação do componente e a conseqüente utilização da chave privada.

SUBSEÇÃO IV

DA CUSTÓDIA DE CHAVE PRIVADA

Art. 171. Não é permitida a custódia das chaves privadas da AC-EB CITEx nem das chaves privadas dos titulares de certificados por ela emitidos.

SUBSEÇÃO V

DA CÓPIA DE SEGURANÇA DE CHAVE PRIVADA

Art. 172. A AC-EB CITEx deve manter cópia de segurança de suas chaves privadas, que deverão ser armazenadas cifradas e protegidas, com um nível de segurança não inferior àquele definido para a versão original da chave, e mantidas pelo prazo de validade do certificado correspondente.

Parágrafo Único. Uma cópia das chaves privadas da AC-EB CITEx deve ser efetuada em outro módulo de segurança em **hardware**, armazenado nas instalações de contingência, e outra em dispositivo de armazenamento USB, que deverá ser armazenado em NÍVEL 6 e só poderá ser manipulado em cerimônia específica.

Art. 173. A AC-EB CITEx não deve manter cópia de segurança das chaves privadas dos titulares de certificados por ela emitidos.

SUBSEÇÃO VI

DA INSERÇÃO DE CHAVE PRIVADA EM MÓDULO CRIPTOGRÁFICO EM HARDWARE

Art. 174. As chaves privadas da AC-EB CITEx devem ser inseridas no módulo criptográfico em **hardware** de acordo com o estabelecido na RFC 4210.

SUBSEÇÃO VII

DO MÉTODO DE ATIVAÇÃO DE CHAVES PRIVADAS

Art. 175. A ativação das chaves privadas da AC-EB CITEx deve ocorrer no módulo criptográfico, após identificação dos Operadores de AC responsáveis.

Parágrafo Único. Esta identificação deve ser realizada por meio de senha e de dispositivo de controle de acesso em hardware (**token**).

Art. 176. Cada NORCERT implementada deve descrever os requisitos e procedimentos necessários à ativação da chave privada do titular de certificado emitido pela AC-EB CITEx.

SUBSEÇÃO VIII

DO MÉTODO DE DESATIVAÇÃO DE CHAVES PRIVADAS

Art. 177. Quando as chaves privadas da AC-EB CITEx forem desativadas, em decorrência de expiração ou revogação, estas devem ser eliminadas da memória do módulo criptográfico.

Parágrafo Único. Qualquer espaço em disco ou qualquer outro dispositivo, onde as chaves eventualmente estivessem armazenadas, deve ser sobrescrito.

Art. 178. Cada NORCERT implementada deve descrever os requisitos e procedimentos necessários à desativação da chave privada do titular de certificado emitido pela AC-EB CITEx.

SUBSEÇÃO IX

DO MÉTODO DE DESTRUIÇÃO DE CHAVES PRIVADAS

Art. 179. Além do estabelecido no art. 177, todas as cópias de segurança das chaves privadas da AC-EB CITEx devem ser destruídas em conformidade com as IG 10-51 e legislação pertinente, como também todos os discos rígidos, **tokens** e qualquer mídia de armazenamento que as tenham hospedado por algum período.

Art. 180. Cada NORCERT implementada deve descrever os requisitos e procedimentos necessários à destruição da chave privada de titular de certificado emitido pela AC-EB CITEx.

SEÇÃO III

DOS OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES

Art. 181. As chaves públicas da AC-EB CITEx e dos titulares de certificados por ela emitidos devem ser armazenadas permanentemente para verificação de assinaturas geradas durante seu prazo de validade, mesmo após seu vencimento.

Art. 182. As chaves privadas da AC-EB CITEx e dos titulares de certificados por ela emitidos devem ser utilizadas apenas durante o período de validade do certificado correspondente.

Art. 183. Os períodos de uso das chaves correspondentes aos certificados de sigilo emitidos pela AC-EB CITEx devem ser definidos nas respectivas NORCERT.

Art. 184. Cada NORCERT implementada deve definir o período máximo de validade do certificado.

SEÇÃO IV

DOS DADOS DE ATIVAÇÃO

Art. 185. Os dados de ativação das chaves privadas da AC-EB CITEx devem ser únicos e aleatórios, instalados fisicamente em dispositivos de controle de acesso em hardware **(token)**.

Art. 186. Cada NORCERT implementada deve assegurar que os dados de ativação da chave privada do titular do certificado, se utilizados, devem ser únicos e aleatórios.

Art. 187. Os dados de ativação das chaves privadas da AC-EB CITEx devem ser protegidos contra uso não autorizado, por meio de mecanismo de criptografia e de controle de acesso físico.

Art. 188. Cada NORCERT implementada deve assegurar que os dados de ativação da chave privada do titular de certificado, se utilizados, devem ser protegidos contra uso não autorizado, por meio de mecanismo de criptografia e de controle de acesso físico.

SEÇÃO V

DOS CONTROLES DE SEGURANÇA COMPUTACIONAL

Art. 189. A geração dos pares de chaves da AC-EB CITEx deve ser realizada em ambiente **offline,** para impedir acesso remoto não autorizado.

Parágrafo Único. As informações utilizadas nesses procedimentos devem ser mantidas no ambiente **offline**, com acesso restrito.

Art. 190. Os controles de segurança computacional do equipamento onde são gerados os pares de chaves criptográficas dos titulares de certificados emitidos pela AC-EB CITEx devem ser descritos em cada NORCERT implementada.

Art. 191. Cada máquina servidora da AC-EB CITEx diretamente relacionado com processo do ciclo de vida de certificados digitais deve possuir as seguintes características:

I – controle de acesso aos serviços da AC-EB CITEx;

II – clara separação das tarefas e atribuições relacionadas a cada perfil da AC-EB CITEx;

III – preferencialmente, uso de criptografia para segurança de base de dados;

IV – geração e armazenamento de registros de auditoria da AC-EB CITEx;

V – mecanismos internos de segurança para assegurar a integridade de dados e processos críticos; e

VI – mecanismos para cópias de segurança (**backup**).

Art. 192. As máquinas servidoras da AR-EB CITEx devem possuir as seguintes características:

I – controle de acesso aos serviços da AR-EB CITEx;

II – preferencialmente, uso de criptografia para segurança de base de dados;

III – geração e armazenamento de registros de auditoria da AR-EB CITEx;

IV – mecanismos internos de segurança para assegurar a integridade de dados e processos críticos; e

V – mecanismos para cópias de segurança (**backup**).

SEÇÃO VI

DOS CONTROLES TÉCNICOS DO CICLO DE VIDA

Art. 193. Uma metodologia formal de gerenciamento de configuração deve usada para instalação e contínua manutenção dos sistemas de certificação da AC-EB CITEx.

Parágrafo Único. Novas versões de **software** somente deverão ser instaladas após testes em ambiente de homologação da AC-EB CITEx.

SEÇÃO VII

DOS CONTROLES DE SEGURANÇA DE REDE

Art. 194. Nas máquinas servidoras da AC-EB CITEx e da AR-EB CITEx, somente os serviços estritamente necessários para o funcionamento das aplicações devem ser habilitados.

Art. 195. Todas máquinas servidoras e elementos de infra-estrutura e proteção de rede, tais como roteadores, **hubs, switches, firewalls,** e sistemas de detecção de intrusão (IDS) e sistemas de prevenção de intrusão (IPS), localizados no segmento de rede que hospeda o sistema de certificação devem estar localizados e operar em ambiente de NÍVEL 3.

Art. 196. As versões mais recentes dos sistemas operacionais e dos aplicativos servidores, bem como as eventuais correções (**patches**), disponibilizadas pelos respectivos fabricantes devem ser implantadas após testes em ambiente homologação.

Art. 197. O acesso lógico aos elementos de infra-estrutura e proteção de rede deve ser restrito, por meio de sistema de controle de acesso.

Parágrafo Único. Os roteadores conectados a redes externas devem implementar filtros de pacotes de dados e outros mecanismos julgados necessários a permitir somente as conexões aos serviços e servidores previamente definidos como passíveis de acesso externo.

TÍTULO VI

DOS PERFIS DOS CERTIFICADOS E LCR

CAPÍTULO I

DO PERFIL DE CERTIFICADO DA AC-EB CITEx

SEÇÃO I

DAS DIRETRIZES GERAIS

Art. 198. O formato de todos os certificados emitidos pela AC-EB CITEx deve seguir as Recomendações ITU X.509 v3, ou o Padrão ISO/IEC 9594-8, em conformidade com o perfil estabelecido na RFC 3280.

Art. 199. As seguintes NORCERT, implementadas pela AC-EB CITEx, devem especificar o formato dos certificados gerados e LCR correspondentes, incluindo informações sobre os padrões adotados, seus perfis, versões e extensões:

I – NORCERT-A1 da AC-EB CITEx – OID 2.16.76.1.2.1.1;

II – NORCERT-A4 da AC-EB CITEx – OID 2.16.76.1.2.4.1;

III – NORCERT-S1 da AC-EB CITEx – OID 2.16.76.1.2.101.1;

IV – NORCERT-S4 da AC-EB CITEx – OID 2.16.76.1.2.104.1;

SEÇÃO II

DO NÚMERO DE VERSÃO

Art. 200. Os certificados da AC-EB CITEx devem implementar a versão 3 de certificado das Recomendações ITU X.509.

SEÇÃO III

DO OBJECT IDENTIFIER (OID) DAS IREPCAC

Art. 201. O OID destas Normas é 2.16.76.1.1.1, conforme art. 8.

CAPÍTULO II

DO PERFIL DE LISTA DE CERTIFICADOS REVOGADOS (LCR)

SEÇÃO I

DO NÚMERO DE VERSÃO

Art. 202. A AC-EB CITEx deve implementar suas LCR conforme a versão 2 do padrão ITU X.509.

SEÇÃO II

DAS EXTENSÕES DE LCR E DE SUAS ENTRADAS

Art. 203. As LCR emitidas pela AC-EB CITEx devem implementar as seguintes extensões previstas na RFC 3280:

I – **AuthorityKeyIdentifier**: deve conter o mesmo valor do campo **SubjectKeyIdentifier** do certificado da AC-EB CITEx;

II – **cRLNumber**: deve conter um número seqüencial para cada LCR emitida.

TÍTULO VII

DAS PRESCRIÇÕES DIVERSAS

Art. 204. Qualquer alteração nestas Normas deve ser formalmente aprovada pelo DCT.