DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO

DA

AUTORIDADE CERTIFICADORA DE DEFESA

Assinatura Geral e Proteção de E-mail (S/MIME)

Infraestrutura de Chaves Públicas Brasileira
ICP - Brasil

Sumário

CONTROLE DE VERSÃO

VERSÃO	DATA	DESCRIÇÃO
1.0	24/04/2017	Versão inicial, a partir do DOC-ICP-05 versão 4.1.
1.1	15/09/2017	Atualizado de acordo com a DOC-ICP-05 versão 4.2.

TABELA DE SIGLAS E ACRÔNIMOS

SIGLA	DESCRIÇÃO
AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICP-Brasil
AR	Autoridades de Registro
CEI	Cadastro Específico do INSS
CG	Comitê Gestor
CMM-SEI	Capability Maturity Model do Software Engineering Institute
CMVP	Cryptographic Module Validation Program
CN	Common Name
CNE	Carteira Nacional de Estrangeiro
CNPJ	Cadastro Nacional de Pessoas Jurídicas
COBIT	Control Objectives for Information and related Technology
COSO	Comitee of Sponsoring Organizations
CPF	Cadastro de Pessoas Físicas
DMZ	Zona Desmilitarizada
DN	Distinguished Name
DPC	Declaração de Práticas de Certificação
ICP-Brasil	Infraestrutura de Chaves Pública Brasileira
IDS	Sistemas de Detecção de Intrusão
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ITSEC	European Information Technology Security Evaluation Criteria
ITU	International Telecommunications Union
LCR	Lista de Certificados Revogados
NBR	Norma Brasileira
NIS	Número de Identificação Social
NIST	National Institute of Standards and Technology
OCSP	On-line Certificate Status Protocol
OID	Object Identifier
OU	Organization Unit

SIGLA	DESCRIÇÃO
PASEP	Programa de Formação do Patrimônio do Servidor Público
PC	Políticas de Certificado
PCN	Plano de Continuidade de Negócio
PIS	Programa de Integração Social
POP	Proof of Possession
PSS	Prestadores de Serviço de Suporte
RFC	Request for Comments
RG	Registro Geral
SGC	Sistema de Gerenciamento de Certificado
SNMP	Simple Network Management Protocol
TCSEC	Trusted System Evaluation Criteria
TSDM	Trusted Software Development Methodology
UF	Unidade da Federação
URL	Uniform Resource Location

1 INTRODUÇÃO

1.1 VISÃO GERAL

1.1.1 Esta Declaração de Práticas de Certificação (DPC) descreve as práticas e os procedimentos empregados pela Autoridade Certificadora de Defesa (AC DEFESA) na execução dos seus serviços.

1.1.2 Esta DPC adota a estrutura recomendada pelo DOC-ICP-05 do Comitê Gestor da ICP-Brasil.

1.2 IDENTIFICAÇÃO

Esta Declaração de Práticas de Certificação da Autoridade Certificadora de Defesa - DPC AC DEFESA possui Identificador de Objeto (OID) 2.16.76.1.1.92, atribuído pela ICP-Brasil.

1.3 COMUNIDADE E APLICABILIDADE

1.3.1 Autoridades Certificadoras

Esta DPC se refere unicamente à AC DEFESA, integrante da ICP-Brasil.

1.3.2 Autoridades de Registro

Esta DPC se refere unicamente à AC DEFESA, integrante da ICP-Brasil.

1.3.2.1 O endereço da página web (URL) da AC DEFESA é *http://www.acdefesa.mil.br*, onde estão publicados os dados abaixo, referentes às Autoridades de Registro, responsáveis pelos processos de recebimento, validação e encaminhamento de solicitação de emissão ou de revogação de certificados digitais, e de identificação de seus solicitantes:

a) relação de todas as Autoridades de Registro (AR) credenciadas, com informações sobre as PC que implementam;

b) para cada AR credenciada, os endereços de todas as instalações técnicas, autorizadas pela AC Raiz a funcionar;

c) para cada AR credenciada, relação de postos de validação remotos, autorizados pela AC Raiz a funcionar, seus respectivos endereços e dados de seus responsáveis;

d) para cada AR credenciada, relação de eventuais postos provisórios autorizados pela AC Raiz a funcionar, com data de criação e encerramento de atividades;

e) relação de AR que tenham se descredenciado da cadeia da AC, com respectiva data do descredenciamento;

f) relação de instalações técnicas de AR credenciadas que tenham deixado de operar, com respectiva data de encerramento das atividades;

g) acordos operacionais celebrados pelas AR vinculadas com outras AR da ICP-Brasil, se for o caso.

1.3.2.2 A AC DEFESA mantém as informações acima atualizadas.

1.3.3 Prestador de Serviço de Suporte

1.3.3.1 A AC DEFESA publica em sua página *https://www.acdefesa.mil.br*, a relação de prestadores de serviço de suporte (PSS), quando houver.

1.3.3.2 PSS são entidades contratadas pela AC ou pela AR para desempenhar as seguintes atividades:

a) disponibilizar infraestrutura física e lógica;

b) disponibilizar recursos humanos especializados;

c) disponibilizar infraestrutura física e lógica e de recursos humanos especializados.

1.3.3.3 A AC DEFESA mantém as informações acima atualizadas.

1.3.4 Titulares de Certificado

Titulares de Certificados são as entidades - pessoas físicas ou jurídicas autorizadas pela AR responsável a receber um certificado digital, emitido pela AC DEFESA, para sua própria utilização ou para utilização em equipamentos ou aplicações.

1.3.5 Aplicabilidade

A AC DEFESA implementa as seguintes Políticas de Certificados:

- Política de Certificado da AC DEFESA do Tipo A1 para Certificação de Pessoa Física ou Pessoa Jurídica, PC AC DEFESA A1, OID 2.16.76.1.2.1.78;
- Política de Certificado da AC DEFESA do Tipo A3 para Certificação de Pessoa Física ou Pessoa Jurídica, PC AC DEFESA A3, OID 2.16.76.1.2.3.75;
- Política de Certificado da AC DEFESA do Tipo A4 para Certificação de Pessoa Física ou Pessoa Jurídica, PC AC DEFESA A4, OID 2.16.76.1.2.4.44;
- Política de Certificado da AC DEFESA do Tipo S1 para Sigilo de Dados de Pessoa Física ou Pessoa Jurídica , PC AC DEFESA S1, OID 2.16.76.1.2.101.17;
- Política de Certificado da AC DEFESA do Tipo S3 para Sigilo de Dados de Pessoa Física ou Pessoa Jurídica, PC AC DEFESA S3, OID 2.16.76.1.2.103.15;
- Política de Certificado da AC DEFESA do Tipo S4 para Sigilo de Dados de Pessoa Física ou Pessoa Jurídica, PC AC DEFESA S4, OID 2.16.76.1.2.104.12.

1.4 DADOS DE CONTATO

A AC DEFESA, responsável por esta DPC, funciona no seguinte endereço:
Centro Integrado de Telemática do Exército - CITEx
Av. Duque de Caxias, s/n
Setor Militar Urbano
CEP 70630-100 Brasília-DF

Pessoa de contato

Nome: Marcos Elias dos Prazeres Caetano
Telefone: (61) 2035-1076
E-mail: contato@acdefesa.mil.br

2 DISPOSIÇÕES GERAIS

2.1 OBRIGAÇÕES E DIREITOS

Nos itens a seguir estão descritas as obrigações gerais das entidades envolvidas.

2.1.1 Obrigações da AC DEFESA

a) operar de acordo com esta DPC e com as PC que implementa;

b) gerar e gerenciar os seus pares de chaves criptográficas;

c) assegurar a proteção de suas chaves privadas;

d) notificar a AC de nível superior, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação do correspondente certificado;

e) notificar os seus usuários quando ocorrer: suspeita de comprometimento de sua chave privada, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;

f) distribuir o seu próprio certificado;

g) emitir, expedir e distribuir os certificados de AR a ela vinculada e de usuários finais;

h) informar a emissão do certificado ao respectivo solicitante;

i) revogar os certificados por ela emitidos;

j) emitir, gerenciar e publicar suas LCR;

k) publicar em página *web* a DPC e as PC aprovadas que implementa;

l) publicar em página *web* as informações definidas no item 2.6.1.2 deste documento;

m) publicar em página *web* as informações sobre o descredenciamento de AR bem como sobre extinção de instalação técnica;

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

o) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;

p) adotar as medidas de segurança e controle previstas na DPC, PC e Política de Segurança (PS) que implementa, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil;

q) manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;

r) manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;

s) manter e testar anualmente seu Plano de Continuidade do Negócio (PCN);

t) à AC DEFESA, por ser órgão da Administração Direta da União, não cabe a contratação de seguro de responsabilidade civil;

u) informar às terceiras partes e titulares de certificado acerca das garantias, coberturas condicionantes e limitações determinadas pela legislação vigente;

v) informar à AC Raiz, mensalmente, a quantidade de certificados digitais emitidos;

w) não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado.

2.1.2 Obrigações da AR

As obrigações de AR vinculada à AC DEFESA são as abaixo relacionadas:

a) operar de acordo com esta DPC e com as PC que implementa;

b) receber solicitações de emissão ou de revogação de certificados;

c) confirmar a identidade do solicitante e a validade da solicitação;

d) encaminhar a solicitação de emissão ou de revogação de certificado à AC DEFESA utilizando protocolo de comunicação seguro, conforme padrão definido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1];

e) informar aos respectivos titulares a emissão ou a revogação de seus certificados;

f) disponibilizar os certificados emitidos pela AC aos seus respectivos solicitantes;

g) identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;

h) manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC DEFESA e pela ICP-Brasil, em especial com o contido no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1];

i) manter e garantir a segurança da informação por elas tratada, de acordo com o estabelecido nas normas, critérios, práticas e procedimentos da ICP- Brasil;

j) manter e testar anualmente seu PCN;

k) executar o reconhecimento das assinaturas e da validade dos documentos apresentados na forma dos itens 3.1.9, 3.1.10 e 3.1.11;

l) garantir que todas as aprovações de solicitação de certificados sejam realizadas em instalações técnicas autorizadas a funcionar como AR vinculada credenciada.

2.1.3 Obrigações do Titular do Certificado

As obrigações do titular de certificado emitido de acordo com esta DPC são as abaixo relacionadas:

a) fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação;

b) garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos;

c) utilizar os seus certificados e chaves privadas de modo apropriado, conforme o previsto na PC correspondente;

d) conhecer os seus direitos e obrigações, contemplados pela DPC da AC DEFESA e pela PC correspondente e por outros documentos aplicáveis da ICP-Brasil;

e) informar à AC emitente qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente.

NOTA: Em se tratando de certificado emitido para pessoa jurídica, equipamento ou aplicação, estas obrigações se aplicam ao responsável pelo uso do certificado.

2.1.4 Direitos da Terceira Parte (Relying Party)

2.1.4.1 Considera-se terceira parte, a parte que confia no teor, na validade e na aplicabilidade do certificado digital.

2.1.4.2 Constituem direitos da terceira parte:

a) recusar a utilização do certificado para fins diversos dos previstos na PC correspondente;

b) verificar a qualquer tempo a validade do certificado. Um certificado emitido por AC integrante da ICP-Brasil é considerado válido quando:

1) não constar da LCR da AC DEFESA;

2) não estiver espirado;

3) puder ser verificado com o uso de certificado válido da AC DEFESA.

2.1.4.3 O não exercício desses direitos não afasta a responsabilidade da AC DEFESA e do titular do certificado.

2.1.5 Obrigações do Repositório

a) disponibilizar, logo após a sua emissão, a Lista de Certificados Revogados (LCR);

b) estar disponível para consulta durante 24 horas por dia, 7 dias por semana;

c) implementar os recursos necessários para a garantia da segurança dos dados nele armazenados.

2.2 RESPONSABILIDADES

2.2.1 Responsabilidades da AC DEFESA

2.2.1.1 A AC DEFESA responde pelos danos a que der causa.

2.2.1.2 A AC DEFESA responde solidariamente pelos atos das entidades de sua cadeia de certificação: AR e PSS.

2.2.1.3 Não se aplica.

2.2.1.4 Quando da emissão de certificado digital para servidores públicos da ativa e militares da União autorizados pelos responsáveis dos respectivos órgãos competentes, a responsabilidade por qualquer irregularidade na identificação do requerente do certificado incidirá sobre o órgão responsável pela identificação.

2.2.2 Responsabilidades da AR

A AR será responsável pelos danos a que der causa.

2.3 RESPONSABILIDADE FINANCEIRA

2.3.1 Indenizações devidas pela terceira parte usuária (*Relying Party*)

Não existe responsabilidade da Terceira Parte perante a AC DEFESA ou a AR a ela vinculada, que requeira prática de indenização, exceto na hipótese de prática de ato ilícito.

2.3.2 Relações Fiduciárias

Não existe situação específica de utilização do certificado da AC DEFESA que requeira prática de indenização aos Usuários de Certificados. Surgindo qualquer solicitação, será analisada caso a caso.

2.3.3 Processos Administrativos

Os processos administrativos cabíveis, relativos às operações da AC DEFESA e de sua AR, seguirão a legislação específica na qual os procedimentos questionados se enquadrarem.

2.4 INTERPRETAÇÃO E EXECUÇÃO

2.4.1 Legislação

Esta DPC AC DEFESA obedece às leis da República Federativa do Brasil e atende aos requisitos da legislação em vigor, incluindo a Medida Provisória nº 2200-2, de 24 de agosto de 2001, bem como as Resoluções do CG da ICP-Brasil.

2.4.2 Forma de interpretação e notificação

2.4.2.1 Caso uma ou mais disposições desta DPC, por qualquer razão, sejam consideradas inválidas, ilegais, ou não aplicáveis, somente essas disposições serão afetadas. Todas as demais permanecem válidas dentro do escopo de abrangência deste documento. Nesse caso, a AC DEFESA, examinará a disposição inválida e proporá, no prazo máximo de 30 dias, nova redação ou a retirada da disposição afetada.

2.4.2.2 Todas as solicitações, notificações ou quaisquer outras comunicações necessárias sujeitas às práticas descritas nessa DPC serão realizadas por iniciativa da AC DEFESA por intermédio de seus responsáveis, e enviadas formalmente ao CG da ICP-Brasil.

2.4.3 Procedimentos de solução de disputa

2.4.3.1 Em caso de conflito prevalecem as práticas e os procedimentos da ICP-Brasil.

2.4.3.2 No caso de um conflito entre esta DPC e as resoluções do Comitê Gestor da ICP-Brasil, prevalecerão sempre as normas, critérios, práticas e procedimentos estabelecidos pela ICP-Brasil. Nesta situação esta DPC será alterada para a solução da disputa.

2.4.3.3 Os casos omissos serão encaminhados para a apreciação da AC Raiz.

2.5 TARIFAS DE SERVIÇO

Não se aplica.

2.5.1 Tarifas de emissão e renovação de certificados

Não se aplica.

2.5.2 Tarifas de acesso ao certificado

Não há tarifa que incida sobre este serviço.

2.5.3 Tarifas de revogação ou de acesso à informação de status

Não se aplica.

2.5.4 Tarifas para outros serviços

Não há tarifa que incida sobre este serviço.

2.5.5 Política de reembolso

Não há política de reembolso.

2.6 PUBLICAÇÃO E REPOSITÓRIO

2.6.1 Publicação de informação da AC DEFESA

2.6.1.1 A AC DEFESA publica e mantém disponível em sua página *web* as informações descritas no item 2.6.1.2 no endereço *http://www.acdefesa.mil.br*. A disponibilidade da página é de no mínimo 99,5% do mês, 24 horas por dia, 7 dias por semana.

2.6.1.2 As informações publicadas nas páginas da AC DEFESA, são:

a) seu próprio certificado;

b) suas LCR;

c) sua DPC;

d) as PC que implementa;

e) relação atualizada contendo as AR vinculadas e seus respectivos endereços de instalação técnica em funcionamento.

2.6.2 Frequência de publicação

Os certificados e a LCR são publicados imediatamente após sua emissão pela AC DEFESA. As demais informações mencionadas no item 2.6.1 serão publicadas sempre que sofrerem alterações.

2.6.3 Controles de acesso

Não há qualquer restrição ao acesso para consulta a esta DPC, a sua PC, aos certificados emitidos e à LCR da AC DEFESA.

Acessos para escrita nos locais de armazenamento e publicação são permitidos apenas às pessoas responsáveis designadas especificamente para esse fim. Os controles de acesso incluem identificação pessoal para acesso aos equipamentos e utilização de senhas.

2.6.4 Repositórios

2.6.4.1 A AC DEFESA adota como repositório de LCR os seguintes endereços:

-http://repositorio-acp.acdefesa.mil.br/lcr/acdefesa-v0.crl;

-http://repositorio-acr.acdefesa.mil.br/lcr/acdefesa-v0.crl.

O repositório de LCR atende os seguintes requisitos:

a) disponibilidade - aquela definida no item 2.6.1;

b) protocolos de acesso - HTTP e HTTPS;

c) requisitos de segurança - obedece aos requisitos definidos no item 5.

2.7 FISCALIZAÇÃO E AUDITORIA DE CONFORMIDADE

2.7.1 As fiscalizações e auditorias realizadas no âmbito da ICP-Brasil têm por objetivo verificar se os processos, procedimentos e atividades da AC DEFESA estão em conformidade com suas respectivas DPC, PC, PS e demais normas e procedimentos estabelecidos pela ICP-Brasil.

2.7.2 As fiscalizações das entidades integrantes da ICP-Brasil são realizadas pela AC Raiz, por intermédio de servidores de seu quadro próprio, a qualquer tempo, sem aviso prévio, observando o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [2].

2.7.3 Com exceção da auditoria da própria AC Raiz, que é de responsabilidade do CG da ICP-Brasil, as auditorias das entidades integrantes da ICP-Brasil é realizada pela AC Raiz, por intermédio de servidores de seu quadro próprio, ou por terceiros por ela autorizados, observando o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

2.7.4 A AC DEFESA recebeu auditoria prévia da AC Raiz para fins de credenciamento na ICP-Brasil. A AC DEFESA é auditada anualmente, para fins de manutenção do credenciamento, com base no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3]. Esse documento trata do objetivo, frequência e abrangência das auditorias, da identidade e qualificação do auditor e demais temas correlacionados.

2.7.5 A AR vinculada recebeu auditoria prévia, para fins de credenciamento. A AC DEFESA é responsável pela realização de auditorias anuais de conformidade em todas as entidades a ela vinculadas, para fins de manutenção de credenciamento conforme documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL [3].

2.8 SIGILO

2.8.1 Disposições Gerais

2.8.1.1 A chave privada de assinatura digital da AC DEFESA foi gerada e é mantida pela própria AC DEFESA, que é responsável pelo seu sigilo. A divulgação ou utilização indevida de sua chave privada de assinatura é de sua inteira responsabilidade.

2.8.1.2 Os titulares de certificados emitidos pela AC DEFESA ou os responsáveis pelo seu uso terão as atribuições de geração, manutenção e sigilo de suas respectivas chaves privadas. Além, disso, são responsáveis pela divulgação ou utilização indevidas dessas mesmas chaves.

2.8.1.3 No intuito de preservar o sigilo da sua chave privada, o titular pelo certificado deve tomar todas as medidas para a proteção da mesma. O sigilo da chave privada do certificado é garantido através de senha de acesso à chave privada. Esta senha será definida pelo usuário no momento da instalação do certificado. A criação e utilização dessa senha para acesso à aplicação são de responsabilidade do usuário.

O titular do certificado deve observar procedimentos básicos de segurança, tais como:

a) nunca fornecer a senha a terceiros;

b) utilizar senha de, no mínimo, 8 caracteres;

c) não utilizar senha fraca ou óbvia, conforme definido na Política de Segurança da AC DEFESA, item 5;

d) montar senha com caractere numéricos e alfanuméricos;

e) memorizar a senha e não escrevê-la;

f) guardar a mídia principal e cópia de segurança em lugar seguro.

2.8.2 Tipos de informações sigilosas

2.8.2.1 Todas as informações coletadas, geradas, transmitidas e mantidas pela AC DEFESA e a AR vinculada são consideradas sigilosas, exceto aquelas informações citadas no item 2.8.3.

2.8.2.2 Como princípio geral, nenhum documento, informação ou registro fornecido à AC DEFESA ou à AR vinculada deverá ser divulgado.

2.8.3 Tipos de informações não sigilosas

Os seguintes documentos da AC DEFESA e da AR vinculada são considerados documentos não sigilosos:

a) os certificados e as LCR emitidos;

b) informações corporativas ou pessoais que façam parte de certificados ou de diretórios públicos;

c) as PCs implementadas;

d) esta DPC;

e) versões públicas de Políticas de Segurança;

f) a conclusão dos relatórios de auditoria.

2.8.4 Divulgação de informação de revogação/suspensão de certificado

2.8.4.1 A AC DEFESA divulga informações de revogação de certificados por ela emitidos, na sua página *web* descrita no item 2.6.1.1 desta DPC, por intermédio de sua lista de certificados revogados.

2.8.4.2 As razões para revogação do certificado sempre serão informadas ao seu titular.

2.8.4.3 A suspensão de certificados não é admitida no âmbito da ICP-Brasil.

2.8.5 Quebra de sigilo por motivos legais

Como princípio geral, nenhum documento, informação ou registro que pertençam ou estejam sob a guarda da AC DEFESA ou de sua AR vinculada será divulgado a entidades legais ou seus funcionários, exceto quando houver ordem judicial corretamente constituída e o representante da lei que a portar estiver corretamente identificado.

2.8.6 Informações a terceiros

Como diretriz geral, nenhum documento, informação ou registro, sob a guarda da AC DEFESA ou AR vinculada, será fornecido a terceiros, exceto quando o requerente, que o solicite por intermédio de instrumento devidamente constituído, seja autorizado a fazê-lo e esteja corretamente identificado.

2.8.7 Divulgação por solicitação do titular

2.8.7.1 O titular de certificado e seu representante legal terão amplo acesso a quaisquer dos seus próprios dados e identificações, e poderão autorizar a divulgação de seus registros a outras pessoas.

2.8.7.2 Qualquer liberação de informação pela AC DEFESA ou AR vinculada somente será permitida mediante autorização formal do titular do certificado. As formas de autorização são as seguintes:

a) por meio eletrônico, contendo assinatura válida garantida por certificado do titular, reconhecido pela AC DEFESA;

b) por intermédio de documento oficial.

2.8.8 Outras circunstâncias de divulgação de informação

Nenhuma outra liberação de informação, que não as expressamente descritas nesta DPC, é permitida.

2.9 DIREITOS DE PROPRIEDADE INTELECTUAL

2.9.1 Todos os direitos de propriedade intelectual inclusive todos os direitos autorais em todos os certificados e todos os documentos gerados para a AC DEFESA, eletrônico ou não, pertencem e continuarão sendo propriedade do Ministério da Defesa.

2.9.2 O Titular do Certificado concede à AC DEFESA, o direito de publicar e divulgar em página *web*, a chave pública que corresponde à chave privada que está em sua posse. Esta publicação ocorrerá pela incorporação da chave pública em certificado emitido pela AC DEFESA.

3 IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1 REGISTRO INICIAL

3.1.1 Disposições Gerais

3.1.1.1 Neste item e nos seguintes a DPC descreve os requisitos e os procedimentos gerais utilizados pela AR, vinculada à AC DEFESA, responsável para a realização dos seguintes processos:

a) validação da solicitação de certificado: compreende as etapas abaixo, realizadas mediante a presença física do interessado, com base nos documentos de identificação citados nos itens 3.1.9, 3.1.10 e 3.1.11:

1) confirmação da identidade de um individuo: comprovação de que a pessoa que se apresenta como titular do certificado de pessoa física é realmente aquela cujos dados

constam na documentação apresentada, vedada qualquer espécie de procuração para tal fim. No caso de pessoa jurídica, comprovar que a pessoa física que se apresenta como responsável pelo uso do certificado ou como representante legal é realmente aquela cujos dados constam na documentação apresentada, admitida a procuração apenas se o ato constitutivo prever expressamente tal possibilidade, devendo-se, para tanto, revestir-se da forma pública com poderes específicos para atuar perante a ICP-Brasil;

2) confirmação da identidade de uma organização: comprovação de que os documentos apresentados referem-se efetivamente à pessoa jurídica titular do certificado e de que a pessoa que se apresenta como representante legal da pessoa jurídica realmente possui tal atribuição;

3) emissão do certificado: conferência dos dados da solicitação de certificado com os constantes dos documentos apresentados e liberação para o segundo agente de registro efetuar a verificação da solicitação do certificado;

b) verificação da solicitação de certificado: confirmação da validação realizada, executados obrigatoriamente:

1) por agente de registro distinto do que executou a etapa de validação;

2) em uma das instalações técnicas da AR devidamente autorizadas a funcionar pela AC Raiz;

3) somente após o recebimento, na instalação técnica da AR, de cópia da documentação apresentada na etapa de validação;

4) antes do início da validade do certificado, sendo comandada a emissão do certificado no sistema de AC somente após a etapa de a verificação ter ocorrido.

3.1.1.2 O processo de validação pode ser realizado pelo agente de registro fora do ambiente físico da AR, desde que utilize ambiente computacional auditável e devidamente registrado no inventário de *hardware* e *softwares* da AR.

3.1.1.3 Todas as etapas dos processos de validação e verificação da solicitação de certificado são registradas e assinadas digitalmente pelos executantes, na solução de certificação disponibilizada pela AC DEFESA, com a utilização de certificado digital ICP-Brasil, no mínimo, do tipo A3. Tais registros são feitos de forma a permitir a reconstituição completa dos processos executados, para fins de auditoria.

3.1.1.4 São mantidos arquivos com as cópias de todos os documentos utilizados para confirmação da identidade de uma organização ou de um indivíduo. Tais cópias são mantidas em papel ou em forma digitalizada, observadas as condições definidas no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1].

3.1.1.5 Nos casos de certificado digital emitido para Servidores do Serviço Exterior Brasileiro, em missão permanente no exterior, assim caracterizados conforme a Lei nº 11.440, de 29 de dezembro de 2006, se houver impedimentos para a identificação conforme o disposto no subitem 3.1.1.1 deste anexo, é facultada a remessa da documentação pela mala diplomática e a realização da identificação por outros meios seguros, a serem definidos e aprovados pela AC-Raiz da ICP-Brasil.

3.1.1.6 Não se aplica.

3.1.1.7 Não se aplica.

3.1.1.8 Não se aplica.

3.1.1.9 As disposições para a validação de solicitação de certificados para servidores públicos da ativa e militares da União estão contidas no DOC-ICP-05.02.

3.1.2 Tipos de nomes

3.1.2.1 Os tipos de nomes admitidos para os titulares de certificados da AC DEFESA são:

a) certificados de pessoa física, o campo *Common Name* (CN) é preenchido com o nome completo do Titular do Certificado, acrescido do caracter : e, em seguida, seu respectivo CPF;

b) certificados de pessoa jurídica, o campo *Common Name* (CN) é preenchido com o nome completo do órgão responsável pelo certificado, acrescido do caracter : e, em seguida, seu respectivo CNPJ.

3.1.2.2 A AC DEFESA não emite certificados para AC subsequente.

3.1.3 Necessidade de nomes significativos

Para identificação dos titulares dos certificados emitidos, a AC DEFESA faz uso de nomes significativos que possibilitam determinar a identidade da pessoa ou organização a que se referem.

3.1.4 Regras para interpretação de vários tipos de nomes

Identificadores do tipo *Distinguished Name* (DN) devem ser únicos para cada titular de certificado, no âmbito da AC DEFESA.

A AR pode propor e aprovar nomes distintos para candidatos de certificado.

3.1.5 Unicidade de nomes

Distinguished Name (DN) devem ser únicos e não ambíguos. Números ou letras adicionais poderão ser incluídos ao nome de cada entidade para assegurar a unicidade do campo.

3.1.6 Procedimento para resolver disputa de nomes

A AC DEFESA se reserva o direito de tomar todas as decisões na hipótese de haver disputa decorrente da igualdade de nomes entre solicitantes de certificados. Durante o processo de confirmação de identidade, caberá ao solicitante do certificado provar o seu direito de uso de um nome específico.

3.1.7 Reconhecimento, autenticação e papel de marcas registradas

De acordo com a legislação em vigor.

3.1.8 Método para comprovar a posse de chave privada

O Sistema de Gerenciamento de Certificados (SGC) implementado e utilizado pela AC DEFESA no gerenciamento do ciclo de vida de seus certificados, controla e garante, de forma automática, a entrega do certificado somente ao detentor da chave privada correspondente à chave pública constante do certificado.

A mensagem de solicitação de certificado obedece ao formato PKCS#10, que inclui na própria mensagem sua assinatura digital realizada com a chave privada correspondente à chave pública contida na solicitação.

Ao recebê-la, o SGC verifica automaticamente a assinatura digital com uso da chave pública incluída nessa solicitação. Esse teste confirma a posse da chave privada pelo requisitante. A solicitação, com seu número de identificação, é então armazenada no banco de dados do SGC.

Este número é impresso no Termo de Responsabilidade juntamente com os dados da entidade solicitante. Os dados são autenticados pela AR por meio da verificação das informações com base em originais de documentos oficiais, efetivando a vinculação da solicitação e chave privada à entidade autenticada pela AR.

A AC DEFESA segue padrão RFC 4210, relativos a POP (*Proof of Possession*).

3.1.9 Autenticação da identidade de um indivíduo

A confirmação da identidade de um indivíduo é realizada mediante a presença física do interessado, com base em documentos legalmente aceitos.

3.1.9.1 Documentos para efeito de identificação de um indivíduo

Deverá ser apresentada a seguinte documentação, em sua versão original, para fins de identificação de um indivíduo solicitante de certificado:

a) cédula de identidade militar, se militar;

b) cédula de identidade ou Passaporte, se brasileiro;

c) carteira nacional de estrangeiro - CNE, se estrangeiro domiciliado no Brasil;

d) passaporte, se estrangeiro não domiciliado no Brasil;

e) caso os documentos acima tenham sido expedidos há mais de 5 anos, ou não possuam fotografia, uma foto colorida recente ou documento de identidade com foto colorida, emitido há no máximo 5 anos da data de validação presencial;

f) comprovante de residência ou domicílio, emitido há no máximo 3 meses da data de validação presencial.

Nota 1 Entende-se como cédula de identidade os documentos emitidos pelas Secretarias de Segurança Pública bem como os que, por força de lei, equivalem a documento de identidade em todo o território nacional, desde que contenham fotografia, incluindo carteiras de identidades emitidas por órgãos de identificação das Forças Armadas.

Nota 2 Entende-se como comprovante de residência ou de domicílio contas de concessionárias de serviços públicos, extratos bancários ou contrato de aluguel onde conste o nome do titular; na falta desses, declaração emitida pelo titular ou seu empregador.

Nota 3 A emissão de certificados em nome dos absolutamente incapazes e dos relativamente incapazes observará o disposto na lei vigente.

Nota 4 Para a identificação de indivíduo na emissão de certificado que integra o Documento RIC, deverá ser observado o disposto no item 3.1.1.6.

Nota 5 Caso não haja suficiente clareza no documento apresentado, a AR deve solicitar outro documento, preferencialmente a CNH - Carteira Nacional de Habilitação ou o Passaporte Brasileiro.

Nota 6 Deverão ser consultadas as bases de dados dos órgãos emissores da Carteira Nacional de Habilitação, e outras verificações documentais expressas no item 7 do documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1].

Nota 7 Caso haja divergência dos dados constantes do documento de identidade, a emissão do certificado digital deverá ser suspensa e o solicitante orientado a regularizar sua situação junto ao órgão responsável.

3.1.9.2 Informações contidas no certificado emitido para um indivíduo

3.1.9.2.1 É obrigatório o preenchimento dos seguintes campos do certificado de uma pessoa física com as informações constantes nos documentos apresentados:

a) nome completo, sem abreviações e sem acentuação, (:) CPF (*1);

b) data de nascimento (*2);

c) Cadastro de Pessoa Física (CPF).

*1 *No campo Subject, como parte do campo Common Name, que compõe o Distinguish Name.;*

*2 *No campo Subject Alternative Name, nas primeiras 8 (oito) posições do OID 2.16.76.1.3.1*

3.1.9.2.2 A AC DEFESA define também como obrigatório o preenchimento do seguinte campo: *e-mail* do usuário

NOTA: Os campos abaixo são opcionais e serão preenchidos caso o solicitante apresente o documento original de referência:

a) número do Registro Geral - RG do titular e órgão expedidor;

b) número de Identificação Social - NIS (PIS, PASEP ou CI);

c) número do Cadastro Específico do INSS (CEI);

d) número do Título de Eleitor; Zona Eleitoral; Seção; Município e UF do Título de Eleitor;

3.1.9.2.3 A AC DEFESA manterá arquivo com as cópias de todos os documentos utilizados.

Nota 1 É permitida a substituição dos documentos elencados acima por documento único, desde que este seja oficial e contenha as informações constantes daqueles.

Nota 2 O cartão CPF poderá ser substituído por consulta à página da Receita Federal. Cópia dessa consulta deverá ser arquivada junto à documentação, para fim de auditoria.

3.1.10 Autenticação da Identidade de uma organização

3.1.10.1 Disposições Gerais

3.1.10.1.1 Os procedimentos empregados pela AR da AC DEFESA para a confirmação da identidade de uma pessoa jurídica são realizados mediante a presença física do responsável legal, com base em documentos de identificação legalmente aceitos.

3.1.10.1.2 Sendo titular do certificado uma pessoa jurídica, será designada pessoa física responsável pelo certificado, que será a detentora da chave privada.

3.1.10.1.3 Será feita a confirmação da identidade da organização e das pessoas físicas, nos seguintes termos:

a) apresentação do rol de documentos elencados no item 3.1.10.2;

b) apresentação do rol de documentos elencados no item 3.1.9.1 do(s) representante(s) legal(is) da pessoa jurídica e do responsável pelo uso do certificado;

c) presença física do(s) representante(s) legal(is) da pessoa jurídica e do responsável pelo uso do certificado e assinatura do termo de titularidade de que trata o item 4.1.1;

3.1.10.2 Documentos para efeitos de identificação de uma organização

A confirmação da identidade de uma pessoa jurídica deverá ser feita mediante a apresentação de, no mínimo, os seguintes documentos:

a) relativos à sua habilitação jurídica:

1) para pessoa jurídica criada ou autorizada a sua criação por lei, cópia do ato constitutivo e CNPJ;

2) item não se aplica. A AC DEFESA não emite certificados para entidades privadas.

b) relativos à sua habilitação fiscal:

1) prova de inscrição no Cadastro Nacional de Pessoas Jurídicas CNPJ;

2) item prova de inscrição no Cadastro Específico do INSS CEI.

3.1.10.3 Informações contidas no certificado emitido para uma organização

3.1.10.3.1 É obrigatório o preenchimento dos seguintes campos do certificado de uma pessoa jurídica, com as informações constantes nos documentos apresentados:

a) nome empresarial constante do CNPJ (Cadastro Nacional de Pessoa Jurídica), sem abreviações, (:) CNPJ (*1);

b) Cadastro Nacional de Pessoa Jurídica (CNPJ);

c) nome completo do responsável pelo certificado, sem abreviações;

d) data de nascimento do responsável pelo certificado;

e) cadastro de Pessoa Física (CPF) do responsável pelo certificado;

f) *e-mail* do responsável pelo certificado.

*(*1) No campo Subject, como parte do campo Common Name, que compõe o Distinguish Name;*

3.1.10.3.2 Cada PC pode definir como obrigatório o preenchimento de outros campos ou o responsável pelo certificado, a seu critério e mediante declaração expressa no termo de titularidade, poderá solicitar o preenchimento de campos do certificado com suas informações pessoais, conforme item 3.1.9.2.

3.1.11 Autenticação da Identidade de um equipamento ou uma aplicação

3.1.11.1 Disposições Gerais

3.1.11.1.1 Não se aplica.

3.1.11.1.2 Não se aplica.

3.1.11.1.3 Não se aplica.

3.1.11.2 Informações contidas no certificado emitido para um equipamento ou uma aplicação

3.1.11.2.1 Não se aplica.

3.2 GERAÇÃO DE NOVO PAR DE CHAVES ANTES DA EXPIRAÇÃO DO ATUAL

3.2.1 Antes da expiração do certificado de pessoa física e jurídica, o titular de certificado pode solicitar um novo certificado, enviando à AC DEFESA uma solicitação por meio eletrônico, assinada digitalmente com o uso do certificado a ser renovado.

3.2.2 A renovação de certificado no âmbito da AC DEFESA será limitada a uma única ocorrência, de acordo com o processo especificado no item 3.2.1.

3.2.3 Nos demais casos devem ser observados os mesmos requisitos e procedimentos exigidos para a solicitação inicial do certificado descritos na PC correspondente, item 4.1.

3.3 GERAÇÃO DE NOVO PAR DE CHAVES APÓS EXPIRAÇÃO OU REVOGAÇÃO

3.3.1 O processo de identificação do solicitante quando da geração de novo par de chaves e emissão pela AC DEFESA de novo certificado, após expiração ou revogação do anterior, será o mesmo da primeira emissão.

3.3.2 A AC DEFESA não emite certificado para outra AC.

3.4 SOLICITAÇÃO DE REVOGAÇÃO

3.4.1 A confirmação da identidade do Titular do Certificado será feita com base em um dos documentos de identidade descritos no item 3.1.9 ou pela "Frase Senha".

3.4.2 Os procedimentos para confirmação da identidade do solicitante são feitos conforme o que se segue:

a) para as solicitações por escrito: confrontação entre as assinaturas e os dados contidos na Solicitação de Revogação com as assinaturas constantes no Termo de Titularidade ou de Responsabilidade e nos documentos entregues quando da solicitação de certificado;

b) para as solicitações diretamente na página *https://www.acefesa.mil.br:* pela frase senha informada na opção solicitação de revogação;

c) solicitação da AC Raiz ou do CG da ICP-Brasil - a confirmação será feita verificando se é um documento oficial válido (ofício ou memorando) assinado pelo responsável do órgão solicitante.

3.4.3 Nos casos descritos nos itens "a" e "b", a solicitação será arquivada junto aos documentos do titular do certificado.

3.4.4 Quando a revogação for por iniciativa da AC DEFESA ou da AR, não será preenchida solicitação de revogação. Os dados e motivos da revogação são registrados diretamente pelo sistema, cujo acesso se dá por intermédio de assinatura digital de uma AR.

4 REQUISITOS OPERACIONAIS

4.1 SOLICITAÇÃO DE CERTIFICADO

4.1.1 Os requisitos e procedimentos mínimos necessários para a solicitação de emissão de certificado são:

a) a comprovação de atributos de identificação constantes do certificado, conforme item 3.1;

b) a autenticação do agente de registro responsável pelas solicitações de emissão e de revogação de certificados mediante o uso de certificado digital do tipo A3;

c) um Termo de Titularidade assinado pelo titular do certificado e pelo responsável pelo uso do certificado, no caso de pessoa jurídica, conforme o adendo referente ao TERMO DE TITULARIDADE específico.

4.1.2 Não se aplica.

4.1.3 Não se aplica.

4.1.4 Não se aplica.

4.2 EMISSÃO DE CERTIFICADO

4.2.1 Os certificados são emitidos pela AC DEFESA após o completo e correto preenchimento da solicitação do certificado, e apresentação da documentação do solicitante. Após o processo de validação das informações fornecidas, o certificado será emitido e o titular notificado, por e-mail.

4.2.2 O certificado é considerado válido a partir do momento de sua emissão.

4.3 ACEITAÇÃO DE CERTIFICADO

4.3.1 O titular do certificado ou pessoa física responsável, verifica as informações contidas no certificado e o aceita caso as informações sejam íntegras, corretas e verdadeiras. Caso contrário, o titular do certificado não pode utilizar o certificado e deve solicitar imediatamente a revogação do mesmo. Ao aceitar o certificado, o titular do certificado:

a) concorda com as responsabilidades, obrigações e deveres nesta DPC e na PC correspondente;

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

c) afirma que todas as informações contidas no certificado, fornecidas na solicitação, são verdadeiras e estão reproduzidas no certificado de forma correta e completa.

O titular do certificado é informado, quando da emissão do mesmo, do disposto no item 4.3.

4.3.2 A aceitação do certificado e do seu conteúdo é declarada, pelo titular do certificado, na primeira utilização da chave privada correspondente.

4.3.3 Não há termos de acordo ou instrumentos similares requeridos pela AC DEFESA.

4.4 SUSPENSÃO E REVOGAÇÃO DE CERTIFICADO

4.4.1 Circunstâncias para revogação

4.4.1.1 A AC DEFESA pode revogar um certificado por ela emitido pelos seguintes motivos:

a) exoneração ou suspensão do titular;

b) mudança de cargo, função ou permissões do titular;

c) falha do titular no cumprimento de suas obrigações ou qualquer compromisso, regulamento ou lei em vigor;

d) solicitação de um dos responsáveis descritos no item 4.4.2;

e) devolução da mídia armazenadora do certificado.

4.4.1.2 Um certificado é revogado obrigatoriamente pelos seguintes motivos:

a) quando constatada emissão imprópria ou defeituosa do certificado;

b) quando for necessária a alteração de qualquer informação nele contida;

c) no caso de dissolução de AC;

d) no caso de comprometimento da chave privada correspondente ou da sua mídia armazenadora.

4.4.1.3 Em relação à revogação, deve ainda ser observado que:

a) a AC DEFESA revogará, no prazo definido no item 4.4.3.3, o certificado da entidade que deixar de cumprir as políticas, normas e regras estabelecidas pela ICP-Brasil;

b) o CG da ICP-Brasil ou a AC Raiz determinará a revogação do certificado da AC que deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas pela ICP-Brasil.

4.4.2 Quem pode solicitar revogação

A solicitação para a revogação de um certificado somente poderá ser feita:

a) pelo titular do certificado;

b) pelo responsável do certificado, no caso de certificado de pessoas jurídicas;

c) pelo órgão, quando o titular do certificado for seu empregado, funcionário ou servidor;

d) pela AC DEFESA;

e) por uma AR vinculada;

f) por determinação do CG da ICP-Brasil ou da AC Raiz.

4.4.3 Procedimento para solicitação de revogação

4.4.3.1 O procedimento para a solicitação de uma revogação varia dependendo de quem a origina.

A solicitação de revogação de certificado pode ser realizada de duas formas:

a) por intermédio da página *web* da AC DEFESA na opção "Revogar Certificado", deverá ser informado o "identificador" do certificado e a "frase senha";

b) envio do formulário específico existente no endereço que foi utilizado para solicitação, o formulário deverá ser encaminhado devidamente preenchido.

4.4.3.2 Como diretrizes gerais ficam estabelecidas que:

a) o solicitante da revogação de um certificado deve ser identificado;

b) as solicitações de revogação, bem como as ações delas decorrentes deverão ser registradas e armazenadas;

c) as justificativas para a revogação de um certificado são documentadas;

d) o processo de revogação de um certificado terminará com a geração e a publicação de uma LCR que contenha o número de série do certificado revogado.

4.4.3.3 O prazo máximo admitido para a conclusão do processo de revogação de certificado, após o recebimento da respectiva solicitação, para todos os tipos de certificado previstos pela ICP-Brasil é de 12 horas.

4.4.3.4 Não se aplica.

4.4.3.5 A AC DEFESA responde plenamente por todos os danos causados pelo uso de um certificado no período compreendido entre a solicitação de sua revogação e a emissão da correspondente LCR.

4.4.3.6 Não se aplica.

4.4.4 Prazo para solicitação de revogação

4.4.4.1 A solicitação de revogação deve ser imediata quando configuradas as circunstâncias definidas no item 4.4.1.

4.4.4.2 Não se aplica.

4.4.5 Circunstâncias para suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil.

4.4.6 Quem pode solicitar suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil.

4.4.7 Procedimento para solicitação de suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil.

4.4.8 Limites no período de suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil.

4.4.9 Frequência de emissão de LCR

4.4.9.1 As LCR referentes aos certificados emitidos pela AC DEFESA são geradas a cada 1 hora.

4.4.9.2 A frequência máxima admitida para a emissão de LCR para os certificados de usuário finais é de 6 horas.

4.4.9.3 Não se aplica.

4.4.9.4 Não se aplica.

4.4.10 Requisitos para verificação de LCR

4.4.10.1 Todo certificado deve ter a sua validade verificada, na respectiva LCR, antes de ser utilizado.

4.4.10.2 A autenticidade da LCR deve ser confirmada por intermédio da verificação da assinatura da AC DEFESA e do seu período de validade.

4.4.11 Disponibilidade para revogação/verificação de status *on-line*

A AC DEFESA não suporta o processo de verificação da situação de estado de certificados de forma online (OCSP). O processo de revogação on-line está disponível ao Titular do Certificado, conforme descrito no item 3.4.

4.4.12 Requisitos para verificação de revogação *on-line*

Não se aplica.

4.4.13 Outras formas disponíveis para divulgação de revogação

Não se aplica.

4.4.14 Requisitos para verificação de outras formas de divulgação de revogação

Não se aplica.

4.4.15 Requisitos especiais para o caso de comprometimento de chave

4.4.15.1 Caso ocorra perda, roubo, modificação, acesso indevido ou comprometimento de chave privada ou de sua mídia armazenadora, o titular deve notificar imediatamente a AC DEFESA e solicitar a revogação de seu certificado conforme descrito no item 4.4.3.

4.4.15.2 Quando houver comprometimento ou suspeita de comprometimento da chave privada, o Titular do Certificado deverá comunicar imediatamente a AC DEFESA, também em conformidade com o item 4.4.3.

4.5 PROCEDIMENTOS DE AUDITORIA DE SEGURANÇA

4.5.1 Tipos de Evento Registrados

4.5.1.1 Todas as ações executadas pelo pessoal da AC DEFESA, no desempenho de suas atribuições, são registradas de modo que cada ação esteja associada à pessoa que a realizou. A AC DEFESA registra em arquivos para fins de auditoria os seguintes eventos relacionados à segurança do seu sistema de certificação:

a) iniciação e desligamento do sistema de certificação;

b) tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AC DEFESA;

c) mudanças na configuração da AC DEFESA ou nas suas chaves;

d) mudanças nas políticas de criação de certificados;

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

f) tentativas não autorizadas de acesso aos arquivos de sistema;

g) geração de chaves próprias da AC DEFESA ou de chaves de Titulares de Certificados;

h) emissão e revogação de certificados;

i) geração de LCR;

j) tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas, e de atualizar e recuperar suas chaves;

k) operações falhas de escrita ou leitura no repositório de certificados e da LCR, quando aplicável;

l) operações de escrita nesse repositório, quando aplicável.

4.5.1.2 A AC DEFESA registra eletrônica ou manualmente as seguintes informações de segurança não geradas diretamente pelo seu sistema de certificação:

a) registros de acessos físicos;

b) manutenção e mudanças na configuração de seus sistemas;

c) mudanças de pessoal e de perfis qualificados;

d) relatórios de discrepância e comprometimento;

e) registros de destruição de mídias de armazenamento contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuários.

4.5.1.3 Os registros de auditoria mínimos a serem mantidos pela AC DEFESA incluem além dos acima:

a) registros de solicitação, inclusive registros relativos a solicitações rejeitadas;

b) pedidos de geração de certificado, mesmo que a geração não tenha êxito;

c) registros de solicitação de emissão de LCR.

4.5.1.4 Todo o registro de auditoria, eletrônico ou manual, contém a data e a hora do evento registrado e a identidade do agente que o causou.

4.5.1.5 Para facilitar os processos de auditoria, toda a documentação relacionada aos serviços da AC DEFESA é armazenada, eletrônica ou manualmente, em local único, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

4.5.1.6 A AR vinculada a AC DEFESA registra eletronicamente em arquivos de auditoria todos os eventos relacionados à validação e aprovação da solicitação, bem como, à revogação de certificados. Os seguintes eventos, obrigatórios, estão incluídos em arquivos de auditoria:

a) os agentes de registro que realizam as operações;

b) data e hora das operações;

c) a associação entre os agentes que realizam a validação e aprovação e o certificado gerado;

d) a assinatura digital do executante.

4.5.1.7 O local de arquivamento das cópias dos documentos para identificação apresentadas no momento da solicitação e revogação de certificados e dos termos de titularidade está definido em documento que faz parte da lista de documentos disponibilizados para as auditorias de conformidade.

4.5.2 Frequência de auditoria de registros (*logs*)

A periodicidade de auditoria de registros não será superior a uma semana, sendo que os registros de auditoria são analisados pelo pessoal operacional da AC DEFESA. Todos os eventos significativos são explicados em relatório de auditoria de registros. Tal análise envolve uma inspeção breve de todos os registros para verificar se não foram alterados. Em seguida procede-se a uma investigação mais detalhada de quaisquer alertas ou irregularidades nesses registros. Todas as ações tomadas em decorrência dessa análise são documentadas.

4.5.3 Período de Retenção para registros (*logs*) de Auditoria

A AC DEFESA mantém localmente, em suas próprias instalações, os seus registros de auditoria por pelo menos 2 meses e, subsequentemente, faz o armazenamento da maneira descrita no item 4.6.

4.5.4 Proteção de registro (*log*) de Auditoria

4.5.4.1 Os registros de auditoria gerados eletronicamente são obrigatoriamente protegidos contra leitura não autorizada, modificação e remoção. Estes registros são classificados e mantidos conforme sua classificação, segundo os requisitos da POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

4.5.4.2 As informações de auditoria geradas manualmente são obrigatoriamente protegidas contra leitura não autorizada, modificação e remoção. Estes registros são classificados e mantidos conforme sua classificação, segundo os requisitos da POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

4.5.4.3 Os mecanismos de proteção descritos neste item obedecem a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

4.5.5 Procedimentos para cópia de segurança (*backup*) de registro (*log*) de auditoria

A AC DEFESA executa procedimentos de *backup*, de todo o sistema de certificação (Sistema Operacional, Sistema de Aplicação e Banco de Dados) de duas formas:

a) diariamente: cópia de segurança;

b) semanalmente: cópia armazenada para processos de auditoria.

4.5.6 Sistema de coleta de dados de auditoria

O sistema de coleta de dados de auditoria é interno à AC DEFESA e utiliza processos manuais e automáticos.

4.5.7 Notificação de agentes causadores de eventos

Eventos registrados pelo conjunto de sistemas de auditoria da AC DEFESA não são notificados à pessoa, organização, dispositivo ou aplicação que causou o evento.

4.5.8 Avaliações de vulnerabilidade

Eventos que indiquem possível vulnerabilidade, detectados na análise periódica dos registros de auditoria da AC DEFESA, são analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes são implementadas e registradas para fins de auditoria.

4.6 ARQUIVAMENTO DE REGISTROS

4.6.1 Tipos de registros arquivados

As seguintes informações são registradas e arquivadas pela AC DEFESA:

a) solicitações de certificados;

b) solicitações de revogação de certificados;

c) notificações de comprometimento de chaves privadas;

d) emissões e revogações de certificados;

e) emissões de LCR;

f) trocas de chaves criptográficas da AC DEFESA;

g) informações de auditoria previstas no item 4.5.1.

4.6.2 Período de retenção para arquivo

Os períodos de retenção para cada registro arquivado são os seguintes:

a) as LCR e os certificados de assinatura digital são retidos permanentemente para fins de consulta histórica.

b) as cópias dos documentos para identificação apresentadas no momento da solicitação e da revogação de certificados, e os termos de titularidade e responsabilidade devem ser retidos, no mínimo, por 10 anos a contar da data da expiração ou revogação do certificado. O prazo de retenção já em curso, quando da alteração desta alínea, será reiniciado;

c) as demais informações, inclusive arquivos de auditoria, são retidas por, no mínimo, 7 anos.

4.6.3 Proteção de arquivos

Todos os registros arquivados são classificados e armazenados com requisitos de segurança compatíveis com sua classificação, conforme a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

4.6.4 Procedimentos para cópia de segurança (*backup*) de arquivos

4.6.4.1 Uma segunda cópia de todo o material arquivado é armazenada em ambiente externo ao sistema de certificação da AC DEFESA, e recebe o mesmo tipo de proteção utilizada no arquivo principal.

4.6.4.2 As cópias de segurança seguem os períodos de retenção definidos para os registros dos quais são cópias.

4.6.4.3 É feita a verificação da integridade dessas cópias de segurança, no mínimo, a cada 6 meses.

4.6.5 Requisitos para datação de registros

4.6.5.1 Os servidores de dados utilizados pela AC DEFESA são sincronizados com a hora GMT fornecida pela Fonte Confiável de Tempo da AC Raiz. Todas as informações geradas que possuam alguma identificação de horário recebem o horário GMT, inclusive os certificados emitidos por esses equipamentos.

4.6.5.2 No caso dos registros feitos manualmente, estes contêm a Hora Oficial do Brasil.

4.6.6 Sistema de coleta de dados de arquivo

Todos os sistemas de coleta de dados de arquivos utilizados pela AC DEFESA em seus procedimentos operacionais são automatizados e manuais e internos.

4.6.7 Procedimentos para obter e verificar informação de arquivo

As informações de arquivos podem ser acessadas da seguinte forma:

a) por pessoas autorizadas e corretamente identificadas, mediante apresentação de um instrumento devidamente constituído;

b) por titulares de certificados ou seus representantes legais, mediante solicitação formal, conforme definido no item 2.8.6;

c) a própria AC por meio de seus funcionários ou os Agentes de Registros das AR vinculadas.

4.7 TROCA DE CHAVE

4.7.1 A AC DEFESA comunica ao Titular de Certificado, por *e-mail*, a necessidade de renovação do certificado, com antecedência mínima de 45 dias. A solicitação de renovação do certificado deverá ser feita pelo próprio Titular do Certificado quando do recebimento dessa notificação, solicitando por meio eletrônico, assinado digitalmente com o uso do certificado vigente a ser renovado.

4.7.2 Não se aplica.

4.8 COMPROMETIMENTO E RECUPERAÇÃO DE DESASTRE

Nos itens a seguir estão relacionados procedimentos de notificação e de recuperação de desastres previstos no Plano de Continuidade de Negócio (PCN) da AC DEFESA, conforme estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

4.8.1 Recursos computacionais, *software* e dados corrompidos

A AC DEFESA possui um PCN que especifica as ações a serem tomadas no caso em que recursos computacionais, *software* ou dados, são corrompidos, e que podem ser resumidas no seguinte:

a) é feita a identificação de todos os elementos corrompidos;

b) o instante do comprometimento é determinado e é crítico para invalidar as transações executadas após aquele instante;

c) é feita uma análise do nível do comprometimento para a determinação das ações a serem executadas, que podem variar de uma simples restauração de um backup de segurança até a revogação do certificado da AC DEFESA.

4.8.2 Certificado de entidade é revogado

A AC DEFESA possui um PCN que especifica as ações a serem tomadas no caso em que seu certificado tenha que ser revogado. Tais procedimentos podem ser resumidos no seguinte:

a) a AC Raiz é informada por comunicações seguras e são também notificados os titulares de certificado;

b) a AC DEFESA revoga os certificados por ela emitidos;

c) a AC DEFESA pede um novo certificado à AC Raiz;

d) iniciam-se os procedimentos para emissão dos novos certificados de usuários.

Nota: *Os usuários são instruídos a solicitar um novo certificado que será validado e aprovado de acordo com essa DPC.*

4.8.3 Chave de entidade é comprometida

A AC DEFESA possui um PCN no qual está especificado que, em caso de comprometimento da chave da AC DEFESA, após a identificação da crise, são notificados os gestores do processo de certificação digital, que acionam as equipem envolvidas para ativar o *site* de contingência.

4.8.4 Segurança dos recursos após desastre natural ou de outra natureza

4.8.4.1 A AC DEFESA possui um PCN que especifica as ações a serem tomadas no caso de desastre natural ou de outra natureza. O propósito deste plano é restabelecer as principais operações da AC DEFESA quando a operação de sistemas é significativamente e adversamente abalada por fogo, greves etc.

4.8.4.2 O plano garante que qualquer impacto em operações de sistema não causará um impacto operacional direto e imediato dentro da ICP-Brasil, da qual a AC DEFESA faz parte. Isto significa que o plano tem como meta primária, restabelecer a AC DEFESA para tornar acessíveis os registros lógicos mantidos dentro do software. Serão tomadas as ações de recuperação aprovadas dentro do plano, segundo ordem de prioridade estabelecida.

4.8.5 Atividades das Autoridades de Registro

No PCN das AR vinculadas são previstos os seguintes procedimentos para recuperação total ou parcial das atividades das AR:

a) identificação dos eventos que causaram interrupções nos processos do negócio;

b) identificação das responsabilidades e procedimentos de emergência;

c) implementação dos procedimentos de emergência que permitam a recuperação e restauração nos prazos necessários. Atenção especial é dada à recuperação das documentações armazenadas nas instalações técnicas atingidas pelo desastre;

d) documentação dos processos e procedimentos adotados;

e) treinamento adequado do pessoal nos procedimentos e processos de emergência definidos, incluindo o gerenciamento de crise;

f) teste e atualização dos planos.

4.9 EXTINÇÃO DOS SERVIÇOS DA AC, AR OU PSS

4.9.1 Caso seja necessária a extinção dos serviços de AC, AR ou PSS, a AC DEFESA efetuará os procedimentos aplicáveis descritos no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6]

4.9.2 Os procedimentos para notificação dos usuários e para a transferência da guarda de seus dados e registros de arquivos incluem:

a) notificação para o e-mail do titular do certificado;

b) transferência progressiva do serviço e dos registros operacionais para um sucessor que tenha os mesmos requisitos de segurança da entidade extinta;

c) preservação de quaisquer registros não transferidos a um sucessor;

d) as chaves públicas dos certificados emitidos pela AC dissolvida serão armazenadas por outra AC após aprovação da AC Raiz;

e) quando houver mais de uma AC interessada, assumirá a responsabilidade do armazenamento das chaves públicas, aquela indicada pela AC DEFESA;

f) a AC DEFESA, ao encerrar as suas atividades transferirá, se for o caso, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas;

g) caso as chaves públicas não tenham sido assumidas por outra AC, os documentos referentes aos certificados digitais e as respectivas chaves públicas serão repassados à AC Raiz.

5 CONTROLES DE SEGURANÇA FÍSICA, PROCEDIMENTAL E DE PESSOAL

Nos itens seguintes estão descritos os controles de segurança implementados pela AC DEFESA e pela AR a ela vinculada para executar de modo seguro suas funções de geração de chaves, identificação, certificação, auditoria e arquivamento de registros.

5.1 CONTROLE FÍSICO

5.1.1 Construção e localização das instalações de AC

5.1.1.1 A localização e o sistema de certificação utilizado para a operação da AC DEFESA não são publicamente identificados. Internamente, não são admitidos ambientes compartilhados que permitam visibilidade nas operações de emissão e revogação de certificados. Essas operações são segregadas em compartimentos fechados e fisicamente protegidos.

5.1.1.2 Todos os aspectos de construção das instalações da AC DEFESA, relevantes para os controles de segurança física, foram executadas por técnicos especializados, especialmente os descritos abaixo:

a) Todas as instalações de equipamentos de apoio, tais como: máquinas de ar condicionado, grupos geradores, no-breaks, baterias, quadros de distribuição de energia e de telefonia, retificadores e estabilizadores e similares;

b) instalações para sistemas de telecomunicações;

c) sistema de aterramento e de proteção contra descargas atmosféricas;

d) iluminação de emergência.

5.1.2 Acesso físico nas instalações de AC

O acesso físico às dependências da AC DEFESA é gerenciado e controlado internamente conforme o previsto na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

5.1.2.1 Níveis de Acesso

5.1.2.1.1 São implementados 4 níveis de acesso físico aos diversos ambientes onde estão instalados os equipamentos utilizados na operação da AC DEFESA, e mais 2 níveis relativos à proteção da chave privada de AC.

5.1.2.1.2 O primeiro nível - ou nível 1 - situa-se após a primeira barreira de acesso às instalações da AC DEFESA. Para entrar em uma área de nível 1, cada indivíduo é identificado e registrado por segurança armada. A partir desse nível, pessoas estranhas à operação da AC DEFESA transitam devidamente identificadas e acompanhadas. Nenhum tipo de processo operacional ou administrativo da AC DEFESA é executado nesse nível.

5.1.2.1.3 Excetuados os casos previstos em lei, o porte de armas não é admitido nas instalações do ambiente onde estão instalados os equipamentos utilizados na operação da AC DEFESA, em níveis superiores ao nível 1. A partir desse nível, equipamentos de gravação, fotografia, vídeo, som ou similares, bem como computadores portáteis, tem sua entrada controlada e somente podem ser utilizados mediante autorização formal e supervisão.

5.1.2.1.4 O segundo nível - ou nível 2 - é interno ao primeiro nível e requer, da mesma forma que o primeiro, a identificação individual das pessoas que nele entram. Esse é o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da AC DEFESA. A passagem do primeiro para o segundo nível exige identificação por meio eletrônico, e o uso de crachá.

5.1.2.1.5 O terceiro nível - ou nível 3 - é interno ao segundo nível e é o primeiro nível a abrigar material e atividades sensíveis da operação da AC DEFESA. Qualquer atividade relativa ao ciclo de vida dos certificados digitais está localizada a partir desse nível. Pessoas que não estejam envolvidas com essas atividades não têm permissão para acesso a esse nível. Pessoas que não possuem permissão de acesso não podem permanecer nesse nível se não estiverem devidamente autorizadas, identificadas e acompanhadas por pelo menos um funcionário que tenha esta permissão.

5.1.2.1.6 No terceiro nível são controladas tanto as entradas quanto as saídas de cada pessoa autorizada. Dois tipos de mecanismos de controle são requeridos para a entrada nesse nível: a identificação individual, como cartão eletrônico e a identificação biométrica.

5.1.2.1.7 Telefones celulares, bem como quaisquer outros equipamentos portáteis de comunicação, exceto aqueles exigidos para a operação da AC DEFESA, não são admitidos a partir do nível 3.

5.1.2.1.8 **quarto nível - ou nível 4** - é interno ao terceiro nível, é aquele no qual ocorrem atividades especialmente sensíveis de operação da AC DEFESA, tais como: emissão e revogação de certificados e emissão de LCR. Todos os sistemas e equipamentos necessários a estas atividades estão localizados a partir desse nível. O nível 4 possui os mesmos controles de acesso do nível 3 e, adicionalmente, exige em cada acesso ao seu ambiente, a identificação de, no mínimo, 2 (duas) pessoas autorizadas. Nesse nível, a permanência dessas pessoas é exigida enquanto o ambiente estiver ocupado.

5.1.2.1.9 No quarto nível, as paredes, piso e o teto são inteiriços e revestidos de aço e concreto, constituindo uma célula estanque contra ameaças de acesso indevido, água, vapor, gases e fogo. Os dutos de refrigeração e de energia, bem como os dutos de comunicação, não permitem a invasão física das áreas de quarto nível. Adicionalmente, esses ambientes de nível 4 que constituem a chamada sala cofre possuem proteção contra interferência eletromagnética externa.

5.1.2.1.10 A sala cofre é construída segundo as normas brasileiras aplicáveis. Eventuais omissões dessas normas devem ser sanadas por normas internacionais pertinentes.

5.1.2.1.11 São três os ambientes de quarto nível abrigados pela sala cofre:

a) sala de equipamentos de suporte (ar-condicionados e quadros de distribuição)

b) sala de equipamentos de produção *on-line* e cofre de armazenamento;

c) sala de equipamentos de rede e infraestrutura *(firewall, roteadores, switches e servidores).*

5.1.2.1.12 **O quinto nível - ou nível 5** - é interno aos ambientes de nível 4, e compreende cofres e gabinetes reforçados trancados. Materiais criptográficos tais como chaves, dados de ativação, suas cópias e equipamentos criptográficos são armazenados em ambiente de nível 5 ou superior.

5.1.2.1.13 Para garantir a segurança do material armazenado, o cofre ou o gabinete obedecem às seguintes especificações mínimas:

a) ser feito em aço ou material de resistência equivalente;

b) possuir tranca com chave.

5.1.2.1.14 O sexto nível - ou nível 6 - consiste de pequenos depósitos localizados no interior do cofre ou gabinete de quinto nível. Cada um desses depósitos dispõe de fechadura individual. Os dados de ativação da AC DEFESA estão armazenados em um desses depósitos.

5.1.2.2 Sistema físico de detecção

5.1.2.2.1 Todas as passagens entre os níveis de acesso, bem como as salas de operação de nível 4, são monitoradas por câmaras de vídeo ligadas a um sistema de gravação 24x7. O posicionamento e a capacidade dessas câmaras não permitem a recuperação de senhas digitadas nos controles de acesso.

5.1.2.2.2 Os vídeos resultantes da gravação 24x7 são armazenadas por, no mínimo, 1 (um) ano. Eles são testados (verificação de trechos aleatórios no início, meio e final dos vídeos) pelo menos a cada 3 (três) meses, com a escolha de, no mínimo, um lote de arquivos de vídeo referente a cada semana. Esses vídeos são armazenadas em ambiente de terceiro nível.

5.1.2.2.3 Todas as portas de passagem entre os níveis de acesso 3 e 4 do ambiente são monitoradas por sistema de notificação de alarmes.

5.1.2.2.4 Em todos os ambientes de quarto nível, um alarme de detecção de movimentos permanece ativo enquanto não for satisfeito o critério de acesso ao ambiente. Assim que, devido à saída de um ou mais funcionários de confiança, o critério mínimo de ocupação deixar de ser satisfeito, ocorre a reativação automática dos sensores de presença.

5.1.2.2.5 O sistema de notificação de alarmes utiliza 2 (dois) meios de notificação: sonoro e visual.

5.1.2.2.6 O sistema de monitoramento das câmeras de vídeo, bem como o sistema de notificação de alarmes, são permanentemente monitorados por guarda armado e estão localizados em ambiente de nível 3. As instalações do sistema de monitoramento, por sua vez, são monitoradas por câmaras de vídeo cujo posicionamento permite o acompanhamento das ações do guarda.

5.1.2.3 Sistema de Controle de Acesso

O sistema de controle de acesso está baseado em um ambiente de nível 4.

5.1.2.4 Mecanismos de emergência

5.1.2.4.1 Mecanismos específicos foram implantados para garantir a segurança do pessoal e dos equipamentos da AC DEFESA em situações de emergência. Esses mecanismos permitem o destravamento de portas por meio de acionamento mecânico, para a saída de emergência de todos os ambientes com controle de acesso. A saída efetuada por meio desses mecanismos aciona imediatamente os alarmes de abertura de portas.

5.1.2.4.2 Todos os procedimentos referentes aos mecanismos de emergência estão documentados. Os mecanismos e procedimentos de emergência são verificados semestralmente, por meio de simulação de situações de emergência.

5.1.3 Energia e ar-condicionado nas instalações da AC

5.1.3.1 A infraestrutura do ambiente de certificação da AC DEFESA é dimensionada com sistemas e dispositivos que garantem o fornecimento ininterrupto de energia elétrica às instalações. As condições de fornecimento de energia são mantidas de forma a atender os requisitos de disponibilidade dos sistemas da AC DEFESA e seus respectivos serviços. Um sistema de aterramento está implantado.

5.1.3.2 Todos os cabos elétricos são protegidos por tubulações ou dutos apropriados.

5.1.3.3 São utilizadas tubulações, dutos, calhas, quadros e caixas de passagem, de distribuição e de terminação, projetados e construídos de forma a facilitar vistorias e a detecção de tentativas de violação. São utilizados dutos separados para os cabos de energia, de telefonia e de dados.

5.1.3.4 Todos os cabos são catalogados, identificados e periodicamente vistoriados, no mínimo a cada 6 meses, na busca de evidências de violação ou de outras anormalidades.

5.1.3.5 São mantidos atualizados os registros sobre a topologia da rede de cabos, observados os requisitos de sigilo estabelecidos pela POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8]. Qualquer modificação nessa rede é previamente documentada.

5.1.3.6 Não são admitidas instalações provisórias, fiações expostas ou diretamente conectadas às tomadas sem a utilização de conectores adequados.

5.1.3.7 O sistema de climatização atende aos requisitos de temperatura e umidade exigida pelos equipamentos utilizados no ambiente e dispõe de filtros de poeira. Nos ambientes de nível 4, o sistema de climatização é independente e tolerante a falhas.

5.1.3.8 A temperatura dos ambientes atendidos pelo sistema de climatização é permanentemente monitorada pelo sistema de notificação de alarmes.

5.1.3.9 O sistema de ar condicionando dos ambientes de nível 4 é interno, com troca de ar realizada apenas por abertura da porta.

5.1.3.10 A capacidade de redundância de toda a estrutura de energia e ar-condicionado da AC é garantida por meio de:

a) geradores de porte compatível;

b) geradores de reserva;

c) sistemas de *no-breaks* redundantes;

d) sistemas redundantes de ar-condicionado.

5.1.4 Exposição à água nas instalações da AC

A estrutura inteiriça do ambiente de nível 4, construído na forma de célula estanque, provê proteção física contra exposição à água, infiltrações e inundações, provenientes de qualquer fonte externa.

5.1.5 Prevenção e proteção contra incêndio nas instalações da AC

5.1.5.1 Os sistemas de prevenção contra incêndios das áreas de nível 4 possibilitam alarmes preventivos antes de fumaça visível, disparando alarmes com a presença de partículas que caracterizam o sobreaquecimento de materiais elétricos e outros materiais combustíveis presentes nas instalações.

5.1.5.2 Nas instalações da AC DEFESA não é permitido fumar ou portar objetos que produzam fogo ou faísca.

5.1.5.3 A sala cofre possui sistema para detecção precoce de fumaça e sistema de extinção de incêndio por gás. As portas de acesso à sala cofre são eclusas, uma porta só se abre quando a anterior está fechada.

5.1.5.4 Em caso de incêndio nas instalações da AC DEFESA, a temperatura interna da sala cofre não excede 50 graus Celsius, e a sala suporta esta condição por, no mínimo, uma hora.

5.1.6 Armazenamento de mídia nas instalações da AC

A AC DEFESA atende a norma brasileira NBR 11.515/NB 1334 (“Critérios de Segurança Física Relativos ao Armazenamento de Dados”).

5.1.7 Destruição de lixo nas instalações da AC

5.1.7.1 Todos os documentos em papel que contenham informações classificadas como sensíveis são triturados antes de ir para o lixo.

5.1.7.2 Todos os dispositivos eletrônicos não mais utilizáveis, e que tenham sido anteriormente utilizados para o armazenamento de informações sensíveis, são fisicamente destruídos.

5.1.8 Instalações de segurança (backup) externas (off-site) para AC

As instalações de backup atendem os requisitos mínimos estabelecidos por este documento. Sua localização é tal que, em caso de sinistro que torne inoperantes as instalações principais, as instalações de backup não serão atingidas e tornar-se-ão totalmente operacionais em, no máximo, 48 horas.

5.1.9 Instalações técnicas de AR

As instalações técnicas de AR atendem aos requisitos estabelecidos no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1].

5.2 CONTROLES PROCEDIMENTAIS

Nos itens seguintes estão descritos os requisitos para a caracterização e o reconhecimento de perfis qualificados na AC DEFESA, juntamente com as responsabilidades definidas para cada perfil. Para cada tarefa associada aos perfis definidos, é estabelecido o número de pessoas requerido para sua execução.

5.2.1 Perfis qualificados

5.2.1.1 A separação das tarefas para funções críticas é uma prática adotada, com o intuito de evitar que um militar ou funcionário utilize indevidamente o sistema de certificação sem ser detectado. As ações de cada empregado estão limitadas de acordo com o seu perfil.

5.2.1.2 A AC DEFESA estabelece um mínimo de 3 (três) perfis distintos para sua operação, distinguindo as operações do dia-a-dia do sistema, o gerenciamento e a auditoria dessas operações, bem como o gerenciamento de mudanças substanciais no sistema.

5.2.1.3 Todos os operadores do sistema de certificação da AC DEFESA recebem treinamento específico antes de obter qualquer tipo de acesso. O tipo e o nível de acesso são determinados, em documento formal, com base nas necessidades de cada perfil.

5.2.1.4 Quando um empregado se desliga da AC, suas permissões de acesso são revogadas imediatamente.

5.2.1.5 Quando há mudança na posição ou função que o empregado ocupa dentro da AC, são revistas suas permissões de acesso. Existe uma lista de revogação, com todos os recursos, antes disponibilizados, que o empregado deverá devolver à AC no ato de seu desligamento.

5.2.2 Número de pessoas necessário por tarefa

5.2.2.1 Controle multiusuário é requerido para a geração e a utilização da chave privada da AC DEFESA, conforme o descrito em 6.2.2.

5.2.2.2 Todas as tarefas executadas no ambiente onde está localizado o equipamento de certificação da AC DEFESA necessitam da presença de no mínimo 2 operadores (funcionários). As demais tarefas da AC DEFESA podem ser executadas por um único operador.

5.2.3 Identificação e autenticação para cada perfil

5.2.3.1 Pessoas que ocupam os perfis designados pela AC DEFESA passam por um processo rigoroso de seleção. Todo funcionário da AC DEFESA tem sua identidade e perfil verificados antes de:

a) ser incluído em uma lista de acesso às instalações da AC DEFESA;

b) ser incluído em uma lista para acesso físico ao sistema de certificação da AC DEFESA;

c) receber um certificado para executar suas atividades operacionais na AC DEFESA;

d) receber uma conta no sistema de certificação da AC DEFESA.

5.2.3.2 Os certificados, contas e senhas utilizadas para identificação e autenticação dos funcionários:

a) são diretamente atribuídos a um único operador (funcionário da AC DEFESA devidamente qualificado);

b) não são compartilhados;

c) são restritos às ações associadas ao perfil para o qual foram criados.

5.2.3.3 A AC DEFESA implementa um padrão de utilização de "senhas fortes", definido em seu Manual de Segurança e em conformidade com a POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

5.3 CONTROLES DE PESSOAL

Nos itens seguintes estão descritos requisitos e procedimentos, implementados pela AC DEFESA, pelas AR e PSS vinculados em relação a todo o seu pessoal, referentes a aspectos como: verificação de antecedentes e de idoneidade, treinamento e reciclagem profissional, rotatividade de cargos, sanções por ações não autorizadas, controles para contratação e documentação a ser fornecida. Todos os integrantes da AC DEFESA e das AR e PSS vinculados, encarregados de tarefas operacionais, têm registrado em contrato ou termo de responsabilidade:

a) os termos e as condições do perfil que ocupam;

b) o compromisso de observar as normas, políticas e regras aplicáveis da AC DEFESA;

c) o compromisso de observar as normas, políticas e regras aplicáveis da ICP-Brasil;

d) o compromisso de não divulgar informações sigilosas a que tenham acesso.

5.3.1 Antecedentes, qualificação, experiência e requisitos de idoneidade

Todo o pessoal da AC DEFESA e AR vinculadas envolvidos em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é admitido conforme o estabelecido na Política de Segurança da AC DEFESA e na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

5.3.2 Procedimentos de Verificação de Antecedentes

5.3.2.1 Com o propósito de resguardar a segurança e a credibilidade da AC DEFESA, todo o pessoal envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados, são submetidos aos seguintes processos, antes do começo das atividades de:

a) VERIFICAÇÃO de antecedentes criminais;

b) VERIFICAÇÃO de situação de crédito;

c) VERIFICAÇÃO de histórico de empregos anteriores;

d) COMPROVAÇÃO de escolaridade e de residência.

5.3.2.2 A AC DEFESA poderá definir requisitos adicionais para a verificação de antecedentes.

5.3.3 Requisitos de treinamento

Todo o pessoal da AC DEFESA e das AR vinculadas, envolvidos em atividades diretamente relacionadas com os processos de emissão, expedição , distribuição, revogação e gerenciamento de certificados recebem treinamento documentado, suficiente para o domínio dos seguintes temas:

a) princípios e mecanismos de segurança da AC DEFESA e das AR vinculadas;

b) sistema de certificação em uso na AC DEFESA;

c) procedimentos de recuperação de desastres e de continuidade do negócio;

d) reconhecimento de assinaturas e validade dos documentos apresentados, na forma do item 3.1.9, 3.1.10 e 3.1.11;

e) outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4 Frequência e requisitos para reciclagem técnica

Todo o pessoal da AC DEFESA e das AR vinculadas envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é mantido atualizado sobre eventuais mudanças tecnológicas no sistema de certificação da AC DEFESA. Treinamentos de reciclagem são realizados pela AC DEFESA sempre que necessário.

5.3.5 Frequência e sequência de rodízios de cargos

A AC DEFESA não implementa rodízio de cargos.

5.3.6 Sanções para ações não autorizadas

5.3.6.1 A AC DEFESA, na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional da AC DEFESA ou de uma AR vinculada, suspenderá de imediato o acesso dessa pessoa ao seu sistema de certificação e instaurará processo administrativo para apurar os fatos e, se for o caso, adotará as medidas legais cabíveis.

5.3.6.2 O processo administrativo referido acima conterá, no mínimo, os seguintes itens:

a) relato da ocorrência com *modus operandi*;

b) identificação dos envolvidos;

c) eventuais prejuízos causados;

d) punições aplicadas se for o caso; e

e) conclusões.

5.3.6.3 Concluído o processo administrativo, a AC DEFESA encaminhará suas conclusões à AC Raiz.

5.3.6.4 As punições passíveis de aplicação, em decorrência de processo administrativo, são:

a) advertência;

b) suspensão por prazo determinado;

c) impedimento definitivo de exercer funções no âmbito da ICP-Brasil.

5.3.7 Requisitos para designação de pessoal

O pessoal da AC DEFESA e das AR vinculadas, no exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados, é designado conforme o estabelecido na POLÍTICA DE SEGURANÇA DA ICP-BRASIL [8].

5.3.8 Documentação fornecida ao pessoal

5.3.8.1 A AC DEFESA disponibiliza para todo o seu pessoal e para o pessoal das AR vinculadas, no mínimo:

a) esta DPC;

b) a Política de Segurança da ICP-Brasil;

c) a Política de Segurança da AC DEFESA;

d) documentação operacional relativa às suas atividades;

e) contratos, normas e políticas relevantes para suas atividades.

5.3.8.2 Toda a documentação é classificada e mantida atualizada, segundo a política de classificação de informação, definida pela AC DEFESA.

6 CONTROLES TÉCNICOS DE SEGURANÇA

6.1 GERAÇÃO E INSTALAÇÃO DO PAR DE CHAVES

6.1.1 Geração do Par de Chaves

6.1.1.1 O par de chaves criptográficas da AC DEFESA é gerado por ela própria, em módulo criptográfico de hardware com padrão de segurança conforme definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9], após o deferimento do seu pedido de credenciamento e a consequente autorização de funcionamento no âmbito da ICP-Brasil.

6.1.1.2 Somente os titulares dos certificados emitidos pela AC DEFESA geram os seus respectivos pares de chaves. Os procedimentos específicos estão descritos em cada PC implementada pela AC DEFESA.

6.1.1.3 Cada PC implementada pela AC DEFESA define o meio utilizado para armazenamento da chave privada, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICPBRASIL [7].

6.1.2 Entrega da chave privada à entidade titular

Não se aplica. É responsabilidade exclusiva do titular do certificado a geração e a guarda da sua chave privada.

6.1.3 Entrega da chave pública para emissor de certificado

6.1.3.1 A AC DEFESA entregará à AC RAIZ cópia de sua chave pública, em formato PKCS#10. Essa entrega será feita por representante legal da AC DEFESA, em cerimônia específica, em data e hora previamente estabelecidas pela AC Raiz.

6.1.3.2 Chaves públicas são entregues ao emissor de certificado por intermédio de uma troca on-line utilizando funções automáticas do *software* de certificação da AC DEFESA.

6.1.4 Disponibilização de chave pública da AC DEFESA para usuários

As formas para a disponibilização do certificado da AC DEFESA, e de todos os certificados da cadeia de certificação, para os usuários da AC DEFESA, compreendem:

a) no momento da disponibilização de um certificado para seu titular, será utilizado o formato definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9];

b) página *web* da AC DEFESA (http://www.acdefesa.mil.br);

c) outros meios seguros aprovados pelo CG da ICP-Brasil.

6.1.5 Tamanhos de chave

6.1.5.1 As PC implementadas pela AC DEFESA definirão os tamanhos das chaves criptográficas associadas aos certificados emitidos, com base nos requisitos aplicáveis estabelecidos pelo documento "REQUISITOS MINIMOS PARA AS POLITICAS DE CERTIFICADO NA ICP-BRASIL" [7].

6.1.5.2 Não se aplica.

6.1.6 Geração de parâmetros de chaves assimétricas

Os parâmetros de geração de chaves assimétricas da AC DEFESA seguem o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.7 Verificação da qualidade dos parâmetros

A verificação dos parâmetros de geração de chave é feita de acordo com o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.1.8 Geração de chave por *hardware ou software*

6.1.8.1 O processo de geração do par de chaves da AC DEFESA é feito por *hardware* padrão FIPS *(Federal Information Processing Standards)* 140-2, level 3.

6.1.8.2 As PC implementadas pela AC DEFESA definem o processo utilizado para a geração de chaves criptográficas dos titulares de certificados, com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

6.1.9 Propósitos de uso de chave (conforme campo *key usage* na X.509 v3)

6.1.9.1 Os certificados de assinatura emitidos pela AC DEFESA têm ativados os bits *digitalSignature, nonRepudiation e keyEncipherment* enquanto que os certificados de sigilo têm ativados apenas os bits *dataEncipherment e keyEncipherment.*

Os propósitos para os quais podem ser utilizadas as chaves criptográficas dos titulares de certificados emitidos pela AC DEFESA, bem como as possíveis restrições cabíveis, em conformidade com as aplicações definidas para os certificados correspondentes estão especificados em cada PC que implementa.

6.1.9.2 A chave privada da AC DEFESA é utilizada apenas para a assinatura dos certificados por ela emitidos e de sua LCR.

6.2 PROTEÇÃO DA CHAVE PRIVADA

Nos itens seguintes são definidos os requisitos para a proteção das chaves privadas da AC DEFESA. A chave privada da AC DEFESA é gerada, armazenada e utilizada apenas em *hardware* criptográfico específico, classificado como FIPS 140-2 level 3, não havendo portanto tráfego em nenhum momento.

6.2.1 Padrões para módulo criptográfico

6.2.1.1 O módulo criptográfico de geração de chaves assimétricas da AC DEFESA utiliza *hardware* criptográfico, classificado como FIPS 140-2 level 3 . Este padrão está definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9].

6.2.1.2 Os módulos de geração de chaves criptográficas dos Titulares de Certificados são aqueles definidos no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9] - Cada PC implementada especifica os requisitos adicionais aplicáveis.

6.2.2 Controle "*n* de *m*" para chave privada

6.2.2.1 A AC DEFESA implementa o controle múltiplo para a ativação e a desativação da sua chave privada por intermédio de controles de acesso físico e do *software* de certificação.

6.2.2.2 É exigida a presença, no mínimo, de 2 detentores da chave de ativação (n) de um grupo de 11 (m) para a ativação da chave da AC DEFESA.

6.2.3 Recuperação *(escrow)* de chave privada

Não é permitido, no âmbito da ICP-Brasil, a recuperação *(escrow)* de chaves privadas, isto é, não se permite que terceiros possam legalmente obter uma chave privada sem o consentimento de seu titular.

6.2.4 Cópia de segurança *(backup)* de chave privada.

6.2.4.1 Como diretriz geral, qualquer entidade titular de certificado poderá, a seu critério, manter cópia de segurança de sua própria chave privada.

6.2.4.2 A AC DEFESA mantém cópia de segurança de sua própria chave privada. Esta cópia é armazenada cifrada e protegida com um nível de segurança não inferior àquele definido para a versão original da chave aprovado pelo CG da ICP-Brasil e mantida pelo prazo de validade do certificado correspondente.

6.2.4.3 A AC DEFESA não mantém cópia de segurança das chaves privadas de titulares de certificados por ela emitidos.

6.2.4.4 A cópia de segurança deve ser armazenada, cifrada, por algoritmo simétrico definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL [9], e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.5 Arquivamento de chave privada

6.2.5.1 As chaves privadas dos titulares de certificados emitidos pela AC DEFESA não são arquivadas.

6.2.5.2 Define-se arquivamento como o armazenamento da chave privada para seu uso futuro, após o período de validade do certificado correspondente.

6.2.6 Inserção de chave privada em módulo criptográfico

A chave privada da AC DEFESA é inserida no módulo criptográfico de acordo com o estabelecido na RFC 4210.

6.2.7 Método de ativação de chave privada

A ativação da chave privada da AC DEFESA é implementada por meio de cartões criptográficos, protegidos com senha, após a identificação de “2” de “11” dos detentores da chave de ativação da chave criptográfica. Os detentores da chave de ativação são Oficiais das Forças Armadas indicados pela AC DEFESA para essa função. As senhas utilizadas obedecem à política de senhas estabelecida pela AC DEFESA.

6.2.8 Método de desativação de chave privada

A chave privada da AC DEFESA, armazenada em módulo criptográfico, é desativada quando não mais é necessária, através de mecanismo disponibilizado pelo *software* de certificação que permite o apagamento de todas as informações contidas no módulo criptográfico. Este procedimento é implementado por meio de cartões criptográficos, protegidos com senha, após a identificação de "2" de "11" dos detentores da chave de ativação da chave criptográfica. Os detentores da chave de ativação são Oficiais das Forças Armadas indicados pela AC DEFESA para essa função. As senhas utilizadas obedecem à política de senhas por ele estabelecida.

6.2.9 Método de destruição de chave privada

Quando a chave privada da AC DEFESA for desativada, em decorrência de expiração ou revogação, esta será eliminada da memória do módulo criptográfico. Qualquer espaço em memória, onde a chave estava armazenada, será sobrescrito. Todas as cópias de segurança da chave privada da AC DEFESA e os cartões criptográficos dos detentores serão destruídos. Os agentes autorizados para realizar estas operações são os administradores e os detentores das chaves de ativação da AC DEFESA.

6.3 OUTROS ASPECTOS DO GERENCIAMENTO DO PAR DE CHAVES

6.3.1 Arquivamento de chave pública

A AC DEFESA armazena as chaves públicas da própria AC DEFESA e dos titulares de certificados de assinatura digital, bem como as LCR emitidas permanentemente para verificação de assinaturas geradas durante seu período de validade.

6.3.2 Períodos de uso para as chaves pública e privada

6.3.2.1 A chave privada da AC DEFESA e dos titulares de certificados por ela emitidos são utilizadas apenas durante o período de validade dos certificados correspondentes. A chave pública da AC DEFESA pode ser utilizada durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade do certificado correspondente.

6.3.2.2 Os períodos de uso das chaves correspondentes aos certificados de sigilo emitidos pela AC DEFESA são definidos nas respectivas PC.

6.3.2.3 As PCs implementadas pela AC DEFESA definem o período máximo de validade de seus certificados com base nos requisitos aplicáveis estabelecidos pelo documento REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL [7].

6.3.2.4 O período máximo de validade admitido para o certificado da AC DEFESA são de 10 anos.

6.4 DADOS DE ATIVAÇÃO

Nos itens seguintes, são descritos os requisitos gerais de segurança referentes aos dados de ativação. Os dados de ativação, distintos das chaves criptográficas, são aqueles requeridos para a operação de alguns módulos criptográficos. Os requisitos específicos, quando existirem, serão descritos nas PC correspondentes.

6.4.1 Geração e instalação dos dados de ativação

6.4.1.1 A AC DEFESA garante que os dados de ativação da sua chave privada são únicos e aleatórios.

6.4.1.2 Todas as PC implementadas garantem que os dados de ativação da chave privada do titular do certificado, se utilizados, são únicos e aleatórios.

6.4.2 Proteção dos dados de ativação.

6.4.2.1 Os dados de ativação são protegidos contra o uso não autorizado, por cartões criptográficos individuais com senha, e são armazenados em ambiente de nível 6 de segurança.

6.4.2.2 Todas as PCs implementadas garantem que os dados de ativação da chave privada da entidade titular do certificado, se utilizados, são protegidos contra uso não autorizado

6.4.3 Outros aspectos dos dados de ativação

Item não aplicável.

6.5 CONTROLES DE SEGURANÇA DOS COMPUTADORES

6.5.1 Requisitos técnicos específicos de segurança computacional

6.5.1.1 A AC DEFESA garante que a geração de seu par de chaves é realizada em ambiente off-line, para impedir o acesso remoto não autorizado.

6.5.1.2 Os requisitos gerais de segurança computacional do equipamento onde são gerados os pares de chaves criptográficos dos titulares de certificados emitidos pela AC DEFESA estão descritos no item 6.5.1 das PC implementadas.

6.5.1.3 Os computadores servidores, utilizados pela AC DEFESA, relacionados diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, implementam, entre outras, as seguintes características:

a) controle de acesso aos serviços e perfis da AC DEFESA;

b) clara separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC DEFESA;

c) acesso restrito aos bancos de dados da AC DEFESA;

d) uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações;

e) geração e armazenamento de registros de auditoria da AC DEFESA;

f) mecanismos internos de segurança para garantia da integridade de dados e processos críticos;

g) mecanismos para cópias de segurança *(backup).*

6.5.1.4 Essas características são implementadas pelo sistema operacional ou por meio da combinação deste, com o sistema de certificação e com mecanismos de segurança física.

6.5.1.5 Qualquer equipamento, ou parte deste, ao ser enviado para manutenção tem as informações sensíveis nele contidas seguramente retiradas e é efetuado controle de entrada e saída, registrando número de série e as datas de envio e de recebimento. Ao retornar às instalações onde reside é inspecionado. Todo equipamento que deixar de ser utilizado em caráter permanente terão suas informações sensíveis relativas à atividade da AC DEFESA destruídas de maneira definitiva. Todos esses eventos são registrados para fins de auditoria.

6.5.1.6 Qualquer equipamento incorporado à AC DEFESA, é preparado e configurado como previsto na política de segurança implementada ou em outro documento aplicável, de forma a apresentar o nível de segurança necessário à sua finalidade.

6.5.2 Classificação da segurança computacional

A segurança computacional da AC DEFESA segue as recomendações *Common Criteria.*

6.5.3 Controle de segurança para as Autoridades de Registro

Os requisitos correspondem aos especificados no documento CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL [1].

6.6 CONTROLES TÉCNICOS DO CICLO DE VIDA

6.6.1 Controles de desenvolvimento de sistemas

6.6.1.1 A AC DEFESA adota um Sistema de Certificação Digital desenvolvido em código aberto. Todas as customizações são realizadas inicialmente em um ambiente de desenvolvimento e após conclusão dos testes é colocado em um ambiente de homologação. Finalizando o processo de homologação das customizações, o Chefe da AC Principal avalia e decide quando será a implementação no ambiente de produção.

6.6.1.2 Os processos de projeto e desenvolvimento conduzidos pela AC DEFESA proveem documentação suficiente para suportar avaliações externas de segurança dos componentes da AC DEFESA.

6.6.2 Controle de gerenciamento de segurança

6.6.2.1 A AC DEFESA verifica os níveis configurados de segurança com periodicidade semanal e através de ferramentas do próprio sistema operacional. As verificações são feitas por intermédio da emissão de comandos de sistema e comparando-se com as configurações aprovadas. Em caso de divergência, são tomadas as medidas para recuperação da situação, conforme a natureza do problema e averiguação do fato gerador do problema para evitar sua recorrência.

6.6.2.2 A AC DEFESA utiliza metodologia formal de gerenciamento de configuração para a instalação e a contínua manutenção do sistema.

6.6.3 Classificação de segurança de ciclo de vida

Não se aplica.

6.6.4 Controles na Geração de LCR

Antes de publicadas, todas as LCR geradas pela AC são checadas quanto à consistência de seu conteúdo, comparando-o com o conteúdo esperado em relação ao número da LCR, data/hora de emissão e outras informações relevantes.

6.7 CONTROLES DE SEGURANÇA DE REDE

6.7.1 Diretrizes Gerais.

6.7.1.1 Os controles implementados para garantir a confidencialidade, a integridade e a disponibilidade dos serviços da AC DEFESA em ambiente de rede são os seguintes:

a) os servidores e elementos de infraestrutura e proteção de rede, tais como roteadores, *hubs, switches, firewalls* e sistemas de detecção de intrusão (IDS), que atendem o segmento de rede dos servidores *web* do sistema de certificação da AC DEFESA estão localizados e operam em ambiente protegido por três perímetros de segurança: os dois primeiros controlados por vigilantes e o terceiro constituído por controle de acesso biométrico;

b) as versões mais recentes dos sistemas operacionais e dos aplicativos servidores, bem como as eventuais correções e atualizações, disponibilizadas pelos respectivos fabricantes são implantadas imediatamente após testes em ambiente de desenvolvimento e homologação;

c) o acesso lógico aos elementos de infraestrutura e proteção de rede é restrito por meio de sistema de autenticação e autorização de acesso. Os roteadores conectados a redes externas implementam filtros de pacotes de dados, que permitam somente as conexões aos serviços e servidores previamente definidos como passíveis de acesso externo;

d) infraestrutura de conectividade, incluindo:
   1) alojamento seguro de equipamento de comunicação;
   2) *firewall* seguro e serviços de roteamento;
   3) serviço de LAN seguro;
   4) serviço *back office* seguro;
   5) serviço de Internet seguro e redundante.

e) prevenção de incidentes e avaliação, incluindo:
   1) descoberta de intrusão;
   2) análise de vulnerabilidades;
   3) configuração segura de servidor;
   4) auditorias técnicas.

f) administração de infraestrutura, incluindo:
   1) monitoramento de servidor;
   2) monitoramento de rede;
   3) monitoramento de URL;
   4) relatórios de níveis de serviço.

6.7.1.2 Nos servidores e elementos de infraestrutura e proteção de rede utilizada pela AC DEFESA, somente os serviços estritamente necessários são habilitados.

6.7.1.3 Os servidores e elementos de infraestrutura e proteção de rede tais como roteadores, *hubs, switches, firewalls* localizados no segmento de rede que hospeda o sistema de certificação da AC DEFESA, estão localizados e operam em ambiente de nível 4.

6.7.1.4 As versões mais recentes dos sistemas operacionais e dos aplicativos servidores, bem como as eventuais correções e atualizações, disponibilizadas pelos respectivos fabricantes são implantadas imediatamente após testes em ambiente de desenvolvimento e homologação.

6.7.1.5 O acesso lógico aos elementos de infraestrutura e proteção de rede é restringido por meio de sistema de autenticação e autorização de acesso. Os roteadores conectados a redes externas implementam filtros de pacotes de dados que permitam somente as conexões aos serviços e servidores previamente definidos como passíveis de acesso externo.

6.7.2 *Firewall*

6.7.2.1 Mecanismos de *firewall* estão implementados em equipamentos de utilização específica, configurados exclusivamente para tal função. O *firewall* promove o isolamento, por intermédio de zona desmilitarizada, em subredes específicas dos equipamentos servidores com acesso externo em relação aos equipamentos com acesso exclusivamente interno à AC DEFESA.

6.7.2.2 O *software de firewall*, entre outras características, implementa registros de auditoria.

6.7.3 Sistema de detecção de intrusão (IDS)

6.7.3.1 O IDS tem capacidade de reconhecer ataques em tempo real e respondê-los automaticamente com medidas tais como: enviar *traps* SNMP, executar programas definidos pela administração da rede, enviar e-mail aos administradores, enviar mensagens de alerta ao *firewall* ou ao terminal de gerenciamento, promover a desconexão automática de conexões suspeitas, ou ainda a reconfiguração do *firewall*.

6.7.3.2 O IDS tem capacidade de reconhecer diferentes padrões de ataques, inclusive contra o próprio sistema, apresentando a possibilidade de atualização da sua base de reconhecimento.

6.7.3.3 O IDS provê registros de eventos *(log)*, recuperáveis em arquivos do tipo texto, além de implementar uma gerência de configuração.

6.7.4 Registro de acessos não autorizados à rede

As tentativas de acesso não autorizado - em roteadores, *firewalls* ou IDS - são registradas em arquivos para análise. A frequência de exame dos arquivos de *log* é diária e todas as ações tomadas em decorrência desse exame são documentadas.

6.8 CONTROLES DE ENGENHARIA DO MÓDULO CRIPTOGRÁFICO

O módulo criptográfico utilizado pela AC DEFESA para o armazenamento de sua chave privada é certificado como FIPS 140-2, nível 3.

7 PERFIS DE CERTIFICADO E LCR

7.1 DIRETRIZES GERAIS

7.1.1 Nos seguintes itens são descritos os aspectos dos certificados e LCR emitidos pela AC DEFESA.

7.1.2 As Políticas de Certificados abaixo, implementadas pela AC DEFESA, especificam os formatos dos certificados gerados e das correspondentes LCR. São incluídas informações sobre os padrões adotados, seus perfis, versões e extensões.

Política de Certificado	Nome Conhecido	OID
Política de Certificados da AC DEFESA A1	PC AC DEFESA A1	2.16.76.1.2.1.78
Política de Certificados da AC DEFESA A3	PC AC DEFESA A3	2.16.76.1.2.3.75
Política de Certificados da AC DEFESA A4	PC AC DEFESA A4	2.16.76.1.2.4.44
Política de Certificados da AC DEFESA S1	PC AC DEFESA S1	2.16.76.1.2.101.17
Política de Certificados da AC DEFESA S3	PC AC DEFESA S3	2.16.76.1.2.103.15
Política de Certificados da AC DEFESA S4	PC AC DEFESA S4	2.16.76.1.2.104.12

7.1.3 Não se aplica.

7.2 PERFIL DO CERTIFICADO

Todos os certificados emitidos pela AC DEFESA estão em conformidade com o formato definido pelo padrão ITU X. 509 ou ISO/IEC 9594-8.

7.2.1 Número de versão

Todos os certificados emitidos pela AC DEFESA implementam a **versão 3** do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.2.2 Extensões de certificados

Não se aplica. A AC DEFESA não emite certificados de AC.

7.2.3 Identificadores de algoritmos

Não se aplica. A AC DEFESA não emite certificados de AC.

7.2.4 Formatos de nome

Não se aplica. A AC DEFESA não emite certificados de AC.

7.2.5 Restrições de nome

Não se aplica. A AC DEFESA não emite certificados de AC.

7.2.6 OID *(Object Identifier)* de DPC

O Identificador de Objeto (OID) desta DPC, atribuído pela ICP-Brasil para a AC DEFESA após conclusão do processo de seu credenciamento, é **2.16.76.1.1.92**.

7.2.7 Uso da extensão *"Policy Constraints"*

Não se aplica. A AC DEFESA não emite certificados de AC.

7.2.8 Sintaxe e semântica dos qualificadores de política

O campo *policyQualifiers* da extensão "*Certificate Policies*" contém o endereço *web* da DPC da AC Defesa, *http://repositorio-acp.acdefesa.mil.br/docs/dpc-acdefesa.pdf*.

7.2.9 Semântica de processamento para extensões críticas

Extensões críticas devem ser interpretadas conforme a RFC 5280.

7.3 PERFIL DE LCR

7.3.1 Número de versão

As LCR geradas pela AC DEFESA implementam a **versão 2** do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

7.3.2 Extensões de LCR e de suas entradas

7.3.2.1 AC DEFESA adota as seguintes extensões de LCR definidas como obrigatórias pela ICP-Brasil:

a) ***Authority Key Identifier***, não crítica: contém o resumo SHA-1 da chave pública da AC DEFESA;

b) ***CRL Number***, não crítica: contém número sequencial para cada LCR emitida.

7.3.2.2 A ICP-Brasil define como obrigatórias as seguintes extensões de LCR:

a) ***Authority Key Identifier***, deve conter o hash SHA1 da chave pública da AC que assina a LCR;

b) ***CRL Number***, não crítica: deve conter um número sequencial para cada LCR emitida pela AC.

8 ADMINISTRAÇÃO DE ESPECIFICAÇÃO

8.1 PROCEDIMENTOS DE MUDANÇA DE ESPECIFICAÇÃO

Qualquer alteração nesta DPC da AC DEFESA será submetida previamente à aprovação do CG da ICP-Brasil. A DPC será alterada sempre que uma nova PC implementada o exigir.

8.2 POLÍTICAS DE PUBLICAÇÃO E DE NOTIFICAÇÃO

A AC DEFESA publica esta DPC, em sua página *web* acessível pela URL http://repositorio-acp.acdefesa.mil.br/docs/dpc-acdefesa.pdf. Sempre que esta DPC for atualizada será alterado o arquivo disponibilizado na *web*.

8.3 PROCEDIMENTOS DE APROVAÇÃO

Todas as DPC no âmbito da ICP-Brasil são submetidas à aprovação durante o processo de credenciamento da AC DEFESA, conforme o estabelecido no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL [6].

9 DOCUMENTOS REFERENCIADOS

9.1 Os documentos abaixo são aprovados por Resoluções do Comitê-Gestor da ICP-Brasil, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sítio *http://www.iti.gov.br* publica a versão mais atualizada desses documentos e as Resoluções que os aprovaram.

Ref.	Nome do documento	Código
[2]	CRITÉRIOS E PROCEDIMENTOS PARA FISCALIZAÇÃO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-09
[3]	CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-08
[6]	CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL	DOC-ICP-03
[7]	REQUISITOS MÍNIMOS PARA AS POLÍTICAS DE CERTIFICADO NA ICP-BRASIL	DOC-ICP-04
[8]	POLÍTICA DE SEGURANÇA DA ICP-BRASIL	DOC-ICP-02

9.2 Os documentos abaixo são aprovados por Instrução Normativa da AC Raiz, podendo ser alterados, quando necessário, pelo mesmo tipo de dispositivo legal. O sitio *http://www.iti.gov.br* publica a versão mais atualizada desses documentos e as instruções Normativas que os aprovam.

Ref.	Nome do documento	Código
[1]	CARACTERÍSTICAS MÍNIMAS DE SEGURANÇA PARA AS AR DA ICP-BRASIL	DOC-ICP-03.01
[9]	PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL	DOC-ICP-01.01

9.3 Os documentos abaixo são aprovados pela AC Raiz, podendo ser alterados, quando necessário, mediante publicação de uma nova versão no sítio *htt p://www.iti.gov.br*.

Ref.	Nome do documento	Código
[4]	MODELO DE TERMO DE TITULARIDADE	ADE-ICP-05.A
[5]	MODELO DE TERMO DE RESPONSABILIDADE	ADE-ICP-05.B