RESOLUÇÃO CONJUNTA Nº 002 DE 08 DE MARÇO DE 2005
SUPERIOR TRIBUNAL DE JUSTIÇA – STJ E CONSELHO DA JUSTIÇA FEDERAL - CJF

Revogada pela Resolução Conjunta n. 004//STJ/CJF, de 28.9.2005

~~Altera dispositivos da Resolução Conjunta nº 001, de 20 de dezembro de 2004, que cria a Autoridade Certificadora do Sistema Justiça Federal (AC-JUS) e dispõe sobre a sistemática de funcionamento.~~

~~O PRESIDENTE DO SUPERIOR TRIBUNAL DE JUSTIÇA E DO CONSELHO DA JUSTIÇA FEDERAL, no uso de suas atribuições legais e tendo em vista o decidido no Processo nº 2004161839, em sessão do Conselho realizada no dia 24 de fevereiro de 2005, resolve:~~

~~Art. 1º O considerando constante da alínea "b" do *caput*, e os Arts. 1º e 3º da Resolução Conjunta nº 001, de 20 de dezembro de 2004, passam a ter as seguintes redações:~~

~~"b) a necessidade de garantir a autenticidade, a integridade e a validade jurídica de documentos produzidos em forma eletrônica, em conformidade com o que dispõe o §1º do Art. 10 da Medida Provisória nº 2.200-2, de 24 de agosto de 2001, que institui a Infra-estrutura de Chaves Públicas Brasileiras – ICP-Brasil;"~~

~~"Art.1º .....~~

~~Parágrafo único. A AC-JUS funcionará como Autoridade Certificadora de primeiro nível vinculada à Autoridade Certificadora Raiz da Infra-estrutura de chaves Públicas Brasileira – ICP-Brasil (AC-Raiz), tão logo seja deferida sua solicitação de credenciamento no âmbito dessa Infra-estrutura e emitido e distribuído o certificado correspondente pela AC-Raiz."~~

~~"Art. 3º .....~~

~~I - .....~~

~~II - .....~~

~~III - a publicação de certificados por ela emitidos;~~

~~IV - a revogação de certificados por ela emitidos;~~

~~V - a emissão, o gerenciamento e a publicação de sua Lista de Certificados Revogados (LCR);"~~

~~Art. 2º Esta Resolução entra em vigor na data de sua publicação.~~

~~PUBLIQUE-SE. REGISTRE-SE. CUMPRA-SE.~~

~~Ministro *Edson Vidigal*~~
~~Presidente~~

Publicada no Diário Oficial
Em 10/03/2005 Seção 1 pág. 199

Política de Certificados
da
Autoridade Certificadora do Sistema Justiça Federal
(PC AC-JUS)

Versão 1.0

CONSELHO DA JUSTIÇA FEDERAL

Declaração de Práticas de Certificação da Autoridade Certificadora do Sistema Justiça Federal

DPC AC-JUS

SUMÁRIO

1. INTRODUÇÃO

1.1 Visão Geral

Este documento descreve a Política de Certificados da Autoridade Certificadora do Sistema Justiça Federal (AC-JUS), doravante denominada PC AC-JUS, implementada sob a Declaração de Práticas de Certificação da Autoridade Certificadora do Sistema Justiça Federal (DPC AC-JUS).
Ela é dirigida a todos aqueles que necessitam verificar a confiabilidade da AC-JUS e verificar a adequabilidade de seus certificados às exigências de segurança da AC-JUS.

1.2 Identificação

Esta PC AC-JUS segue as recomendações da ICP-Brasil para emissão de certificados digitais para autoridades certificadoras de nível imediatamente subseqüente ao da AC-JUS.
O OID desta PC AC-JUS é: 2.16.76.1.2.201.5

1.3 Comunidade e Aplicabilidade

1.3.1 Autoridades Certificadoras

Esta PC AC-JUS é implementada pela AC-JUS cuja DPC AC-JUS encontra-se publicada na página http://www.acjus.gov.br/acjus/dpcacjus.pdf.

1.3.2 Autoridade de Registro (AR)

A responsável pelo processo de recebimento, validação e encaminhamento de solicitações de emissão e revogação de certificados digitais para AC de nível imediatamente subseqüente ao da AC-JUS, e pela confirmação da identidade de seus solicitantes, é a Autoridade de Registro do Sistema Justiça Federal (AR-JUS), cujos procedimentos estão em conformidade com esta Política de Certificado.

1.3.3 Titulares de Certificado

Os titulares dos certificados são Órgãos do Poder Judiciário Federal, representados inicialmente pelo Superior Tribunal de Justiça, Conselho da Justiça Federal, Tribunais Regionais Federais e Seções Judiciárias , e entidades e pessoas jurídicas de direito

publico e privado, autorizadas pela AR-JUS a receberem certificados digitais emitidos pela AC-JUS, cujos nomes aparecem no certificado digital, no campo "D*istinguished Name (DN)"*.
Será designada pessoa física como responsável pelo certificado, que será a detentora da chave privada.

Preferencialmente, será designado como responsável pelo certificado, o dirigente máximo do Órgão, o representante legal da pessoa jurídica ou um de seus representantes legais.

1.3.4 Aplicabilidade

Os certificados definidos por esta PC AC-JUS têm sua utilização exclusiva para a assinatura de certificados digitais e de Lista de Certificados Revogados (LCR), emitidos pelas ACs de nível imediatamente subseqüentes ao da AC-JUS

1.4 Dados de Contato

1.4.1 Organização da Administração da PC AC-JUS

Esta PC é administrada pelo Comitê Gestor da AC-JUS, assessorado pela Comissão Técnica por ele designada e pela estrutura administrativa de certificação digital do CJF.

Nome: Conselho da Justiça Federal
Endereço: SEPN 510 Bloco "C" lote 8
Edifício Conselho da Justiça Federal Asa Norte - Brasília-DF Brasil
Telefone: **(61) 348-3113 (PABX)**
Fax: **(61) 349-1524**
Página *Web*: http://www.acjus.gov.br/acjus/
E-mail: AC-JUS@cjf.gov.br

1.4.2 Pessoas de Contato

Nome: Paulo Martins Inocêncio
E-mail: paulo.martins@cjf.gov.br

Nome: Wilson Nogueira de Aquino Jr.
E-mail: wilsonjr@cjf.gov.br

Endereço: SEPN 510 Bloco "C" lote 8
Edifício Conselho da Justiça Federal Asa Norte - Brasília-DF Brasil

Telefone: **(61) 348-3113 (PABX)**
Fax: **(61) 349-1542**
Página *Web*: http://www.acjus.gov.br/acjus/

2. DISPOSIÇÕES GERAIS

2.1 Obrigações e direitos

2.1.1 Obrigações da Autoridade Certificadora

As obrigações da AC-JUS são as abaixo relacionadas:

- Operar de acordo com a DPC AC-JUS e com esta PC AC-JUS;
- Adotar as medidas cabíveis para assegurar que usuários e demais entidades envolvidas tenham conhecimento de seus respectivos direitos e obrigações;
- Gerar e gerenciar o seu par de chaves criptográficas;
- Assegurar a proteção de sua chave privada;
- Notificar a AC-Raiz da ICP-Brasil, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação deste certificado;
- Notificar as AC de nível imediatamente subseqüente ao seu quando ocorrer: suspeita de comprometimento de sua chave, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;
- Distribuir o seu próprio certificado;
- Emitir, expedir e distribuir os certificados das AC de nível imediatamente subseqüente ao seu;
- Informar a emissão do certificado ao respectivo solicitante;
- Revogar os certificados por ela emitidos;
- Emitir, gerenciar e publicar sua Lista de Certificados Revogados (LCR);
- Identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo Comitê Gestor da ICP-Brasil (CG ICP-Brasil);
- Publicar em sua página *web* http://www.acjus.gov.br/acjus/ a DPC AC-JUS e a PC AC-JUS aprovadas;
- Adotar as medidas de segurança e controle previstas na PC, DPC e Política de Segurança que implementar, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios, práticas e procedimentos da ICP-Brasil;

- Manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;
- Manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;
- Manter e testar regularmente seu Plano de Continuidade do Negócio;
- Não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado;
- Publicar os certificados por ela emitidos; e
- Fiscalizar as AC e auditar as AR e os prestadores de serviço habilitados em conformidade com os critérios estabelecidos pelo Comitê Gestor (CG) da ICP-Brasil.

2.1.2 Obrigações da AR-JUS

As obrigações da AR-JUS são as abaixo relacionadas:

- Receber solicitações de emissão e revogação de certificados e respectivos documentos de identificação armazenado-os conforme critérios estabelecidos pelo CG da ICP-Brasil;
- Confirmar a identidade do solicitante e a validade da solicitação, de acordo com os requisitos estabelecidos pelos itens 3 e 4 desta PC AC-JUS;
- Encaminhar a solicitação de emissão e de revogação de certificado à AC-JUS utilizando VPN (virtual private network - rede privativa virtual), SSL (secure socket layer - protocolo de comunicação seguro) ou outra tecnologia de igual ou superior nível de segurança e privacidade;
- Utilizar VPN (virtual private network - rede privativa virtual), SSL (secure socket layer - protocolo de comunicação seguro) ou outra tecnologia de igual ou superior nível de segurança e privacidade, ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via web;
- Informar aos respectivos titulares a emissão ou a revogação de seus certificados;
- Disponibilizar os certificados emitidos pela AC-JUS aos seus respectivos solicitantes;
- Identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
- Manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC-JUS;
- Manter e garantir a segurança da informação por elas tratada, de acordo com o estabelecido nas normas, critérios, práticas e procedimentos da ICP – Brasil;

- Oferecer treinamento aos seus agentes de registro, especialmente quanto ao reconhecimento de assinaturas e validade dos documentos apresentados na forma dos itens 3.1.8 e 3.1.9; e
- Orientar os portadores de certificados emitidos pela AC-JUS nas boas práticas de utilização e de preservação de certificados digitais.

2.1.3 Obrigações do Titular do Certificado

As obrigações do titular do certificado emitido de acordo com esta PC AC-JUS são as abaixo relacionadas:

- Fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação;
- Garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos;
- Utilizar os seus certificados e suas respectivas chaves privadas de modo apropriado, conforme o previsto nesta PC AC-JUS;
- Conhecer os seus direitos e obrigações, contemplados nesta PC AC-JUS, na DPC da AC-JUS e em outros documentos aplicáveis da ICP-Brasil; e
- Informar à AC-JUS qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente.

Por se tratar de certificado emitido para pessoa jurídica, estas obrigações se aplicam ao responsável pelo uso do certificado.

2.1.4 Direitos da terceira parte (Relying Party)

Considera-se terceira parte, a parte usuária que confia no teor, validade e aplicabilidade do certificado digital.
Constituem direitos da terceira parte:

- Recusar a utilização do certificado para fins diversos dos previstos nesta PC AC-JUS;
- Verificar, a qualquer tempo, a validade do certificado.
- Um certificado emitido por AC integrante da ICP-Brasil é considerado válido quando:
    - não constar da LCR da AC emitente;
    - não estiver expirado; e
    - puder ser verificado com o uso de certificado válido da AC emitente.

O não exercício desses direitos não afasta a responsabilidade da AC-JUS e do titular do certificado.

2.1.5 Obrigações do Repositório

O repositório da AC-JUS está disponível para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana, possuindo os recursos necessários para a segurança dos dados nele armazenados. Disponibiliza, ainda, logo após a sua emissão, os certificados emitidos pela AC-JUS e sua LCR.

2.2 Responsabilidades

2.2.1 Responsabilidades da AC-JUS

A AC-JUS responde pelos danos a que der causa.
A AC-JUS responde solidariamente pelos atos das AC da cadeia a ela subordinadas.

2.2.2 Responsabilidades da AR-JUS

A AR-JUS será responsável pelos danos a que der causa.

2.3 Responsabilidade Financeira

2.3.1. Indenizações devidas pela terceira parte (Relying Party)

Não existe situação específica de utilização do certificado da AC-JUS que requeira prática de indenização pelos Usuários de Certificados, exceto na prática de ato ilícito.

2.3.2. Relações Fiduciárias

A AC-JUS ou a AR-JUS indenizará integralmente os danos a que der causa. Em situações justificáveis, pode ocorrer limitação da indenização, quando o titular do certificado for pessoa jurídica.

2.3.3. Processos Administrativos

Será seguida lei 9784 de 29 de janeiro de 1999 e qualquer outra legislação específica, uma vez que a AC-JUS e a AR-JUS são administradas pelo Conselho da Justiça Federal, órgão da Administração Pública Federal.

2.4 Interpretação e Execução

2.4.1 Legislação

A PC AC-JUS 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 e a Resolução conjunta CJF/STJ nº 01 de 20 de dezembro der 2004.

2.4.2 Forma de interpretação e notificação

Caso uma ou mais disposições desta PC, por qualquer razão, sejam consideradas inválidas, ilegais, ou não aplicáveis, somente essa disposição será afetada. Todas as demais permanecem válidas dentro do escopo de abrangência deste documento.
Nesse caso, o corpo técnico, da AC-JUS, examinará a disposição inválida e proporá à Comissão Técnica, no prazo máximo de 30 dias, nova redação ou retirada da disposição afetada.
As práticas descritas nesta PC não prevalecerão sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.
Todas solicitações, notificações ou quaisquer outras comunicações necessárias sujeitas às práticas descritas na PC serão realizadas por iniciativa da AC-JUS por intermédio de seus responsáveis, e encaminhadas formalmente ao CG da ICP-Brasil e às AC´s subsequentes se for o caso.

2.4.3 Procedimentos de solução de disputa

Esta PC AC-JUS não prevalece sobre as normas, critérios, práticas e procedimentos da ICP-Brasil, sendo a norma, critério ou prática divergentes, alteradas nesta PC AC-JUS de forma a torná-las compatíveis.

2.5 Tarifas de Serviço

Não há tarifas previstas pela AC-JUS para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.5.1 Tarifas de emissão e renovação de certificados

Não há tarifas previstas pela AC-JUS para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.5.2 Tarifas de acesso ao certificado

Não há tarifas previstas pela AC-JUS para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.5.3 Tarifas de revogação ou de acesso a informação de status

Não há tarifas previstas pela AC-JUS para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.5.4 Tarifas para outros serviços

Não há tarifas previstas pela AC-AC-JUS para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.5.5 Política de reembolso

Não há política de reembolso prevista pela AC-JUS pelos serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.6 Publicação e Repositório

2.6.1 Publicação de informação da AC-JUS

A AC-JUS publica em sua página *web,* http://www.acjus.gov.br/acjus/ , as seguintes informações:

- seu próprio certificado;
- sua LCR;
- sua DPC AC-JUS;
- esta PC AC-JUS;
- legislação especifica aplicável a esta a AC e as suas AC subseqüentes;
- o endereço da instalação técnica da AR-JUS;

- leiaute do certificado emitido pela AC-JUS; e
- lista de certificados emitidos

A disponibilidade da página web é de, no mínimo, 99,0% (noventa e nove vírgula zero por cento) do mês, 24 (vinte e quatro) horas por dia, 7(sete) dias por semana.
A AC-JUS inclui nos certificados emitidos a identidade da sua página *web*.

2.6.2 Freqüência de publicação

As informações de que trata o item anterior serão publicadas tão logo sofram alterações exceto a LCR que será publicada imediatamente após sua emissão e a cada 15 dias independentemente de haver alteração.

2.6.3 Controles de acesso

Não há qualquer restrição ao acesso para consulta a esta DPC, à sua PC, aos certificados emitidos e à LCR da AC-JUS.
Acessos para escrita nos locais de armazenamento e publicação serão permitidos apenas às pessoas responsáveis designadas especificamente para esse fim. Os controle de acesso incluirão identificação pessoal para acesso aos equipamentos, utilização de senhas.

2.6.4 Repositório

O repositório da AC-JUS pode ser acessado através da página http://www.acjus.gov.br,/acjus/ utilizando os protocolos de acesso https e http.
Os repositórios estão disponíveis em no mínimo 99,0% (noventa e nove vírgula zero por cento), 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.
Somente a AC-JUS, por seus funcionários competentes e designados especialmente para esse fim, pode alterar as informações constantes nos repositórios. Os requisitos do item 5 desta PC AC-JUS serão observados para os repositórios.

2.7 Auditoria de Conformidade

A AC Raiz da ICP-Brasil é a responsável pela auditoria dos processos, procedimentos e atividades de todas as AC integrantes da ICP-Brasil e das AR e prestadores de serviço de suporte a elas vinculadas. A AC Raiz audita a AC-JUS no âmbito da ICP-Brasil. A auditoria é realizada com o objetivo de verificar a conformidade com suas respectivas DPC, PC, PS (Política de Segurança) e demais normas e procedimentos estabelecidos pela ICP-Brasil.
Os serviços de auditoria poderão ser executados:

- por empresas independentes, autorizadas pela AC Raiz e contratadas pela AC-JUS ; ou

- pela AC-JUS, em AR´s e PSS (prestadores de serviço de suporte) a ela vinculados, de acordo com os procedimentos estabelecidos pela ICP-Brasil.

2.7.1 Freqüência de auditoria de conformidade de entidade

As AC credenciadas pelo CG da ICP-Brasil subordinadas à AC-JUS, suas AR e seus prestadores de serviço sofrem auditoria:

- previamente ao seu credenciamento pela AC-Raiz e à sua habilitação pela AC-JUS;
- anuais, em data a ser designada pela AC-Raiz ou pela AC-JUS; e
- a qualquer tempo, sem aviso prévio, pela AC Raiz.

Adicionalmente, as AC de nível imediatamente subseqüente ao da AC-JUS, para fins de continuidade do credenciamento, apresentarão anualmente relatório de auditoria.
A AC-JUS conduz anualmente auditorias de conformidade na AR-JUS, podendo também executar, a qualquer momento, auditorias não programadas.

2.7.2 Identidade/Qualificações do Auditor

A auditoria será executada por empresa de auditoria independente e especializada, com comprovada experiência em serviços de auditoria e tecnologias de certificação, de acordo com os procedimentos estabelecidos pela ICP-Brasil.
As auditorias nas AR e prestadores de serviço de suporte vinculadas, poderão ser executadas pela AC-JUS.

2.7.3 Relação entre auditor e parte auditada

No caso de contratação de auditoria, o auditor deve ser totalmente independente da AC auditada. Ao auditor, sem prejuízo do disposto nesta PC, aplicam-se, no que couber, as regras de suspeição e impedimento estabelecidas nos arts. 134 e 135 do Código de Processo Civil.
O auditor, tanto no caso de contratação de auditoria independente como nas auditorias realizada pela AC-JUS, será declarado impedido de realizar auditoria, quando:

- houver motivo íntimo declarado;
- for amigo íntimo ou inimigo capital de membros da AC auditada;
- for credor ou devedor da AC auditada ou de um de seus membros;
- tiver recebido, nos últimos 5 anos, da AC auditada, pagamentos referentes à prestação de serviços de outra natureza;
- tiver interesse no resultado da auditoria da AC auditada; e
- houver relacionamento, de fato ou de direito, como cônjuge, parente, consangüíneo ou afim, com algum dos membros da AC auditada, em linha reta ou na colateral até o terceiro grau.

O auditor firmará declaração, sob as penas da lei, de que não se enquadra em qualquer dessas causas de impedimento. Declarará, ainda, em outro documento, o seu compromisso de manter em sigilo todas e quaisquer informações que obtiver no curso dos trabalhos, mesmo depois do término destes, sendo responsável civil e criminalmente pela divulgação indevida das mesmas.

2.7.4 Tópicos cobertos pela auditoria

As auditorias de conformidade verificam todos os aspectos relacionados com a emissão e o gerenciamento de certificados digitais, incluindo o controle dos processos de solicitação, identificação, autenticação, geração, publicação, distribuição, renovação e revogação de certificados.
Todos os eventos significativos ocorridos em um sistema de AC ou de AR serão armazenados em trilhas seguras de auditoria, onde cada entrada possua o registro de data, hora e tipo de evento, com assinatura, para garantir que as entradas não possam ser falsificadas.
Os tópicos cobertos por uma auditoria de conformidade incluem, dentre outros:

- Política de Segurança;
- Segurança física;
- Avaliação de tecnologia;
- Administração dos serviços;
- Investigação de pessoal;
- PC e DPC utilizadas;
- Contratos; e
- Considerações de sigilo.

2.7.5 Medidas adotadas em caso de não conformidade

Cabe à entidade auditada cumprir, no menor dos prazos estipulados, as recomendações dos auditores para corrigir os casos de não conformidade com a legislação ou com as políticas, normas, práticas e regras estabelecidas. O não cumprimento das recomendações, no prazo estipulado, acarretará a revogação do seu certificado pela AC-JUS.
A AC-JUS, em casos de iminente dano irreparável ou de difícil reparação a terceiros, poderá suspender cautelarmente, no todo ou em parte, a emissão de certificados pela AC de nível imediatamente subseqüente ao seu.

2.7.6 Comunicação de resultados

Os auditores somente informam os resultados da auditoria à entidade auditada, à AC-JUS e à AC Raiz da ICP-Brasil, nos termos da declaração que firmarem, como exigida pelo item 2.7.3.

2.8 Sigilo

A chave privada de assinatura digital da AC-JUS foi gerada e é mantida pela própria AC-JUS, que é responsável pelo seu sigilo.

A divulgação ou utilização indevida da chave privada de assinatura pela AC-JUS é de sua inteira responsabilidade.

Os titulares de certificados emitidos pela AC-JUS, 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 Tipos de informações sigilosas

Todas as informações coletadas, geradas, transmitidas e mantidas pela AC-JUS são consideradas sigilosas, exceto os certificados de chaves públicas e LCR, os quais são consideradas não sigilosas, assim como a versão desta PC AC-JUS, da DPC AC-JUS e daquelas informações citadas no item 2.8.2.
Essas informações serão arquivadas de acordo com sua classificação, que será especificada na Política de Segurança.
Como princípio geral, nenhum documento, informação ou registro fornecido à AC-JUS ou AR-JUS deverá ser divulgado.

2.8.2 Tipos de informações não sigilosas

Certificados, LCR e informações corporativas ou pessoais que necessariamente façam parte deles ou de diretórios públicos são consideradas informações não sigilosas.
Os seguintes documentos da AC-JUS são considerados documentos não sigilosos:

- qualquer PC aplicável;
- qualquer DPC;
- versões públicas de Políticas de Segurança; e
- resultados finais de auditoria.

2.8.3 Divulgação de informação de revogação e de suspensão de certificado

No endereço **http://www.acjus.gov.br/acjus/acjus.crl,** estará disponibilizada a lista de certificados revogados.
As razões para revogação do certificado sempre serão informadas para o seu titular.

Código de campo alterado

Os motivos que justificaram a revogação são mantidos confidenciais pela AC-JUS e pela AR-JUS, exceto quando:

- o titular do certificado revogado autorizar expressamente a sua divulgação a terceiros;
- esses motivos tenham sido publicados, ou sejam ou venham a se tornar de domínio público, desde que tal publicação ou publicidade não tenha sido, de qualquer forma, ocasionada por culpa ou interferência indevida da AC-JUS ou da AR-JUS;
- tais motivos sejam requisitados por determinação judicial ou governamental, caso em que a AC-JUS ou a AR-JUS, se estiver obrigada a divulgá-los, comunicará previamente ao titular do certificado a existência de tal determinação.

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

2.8.4 Quebra de sigilo por motivos legais

Como princípio geral, nenhum documento, informação ou registro que pertençam ou estejam sob a guarda da AC-JUS e suas AR é divulgado a entidades legais ou seus funcionários, exceto quando:

- Exista uma ordem judicial corretamente constituída; e
- Esteja corretamente identificado o representante da lei.

2.8.5 Informações a terceiros

A AC-JUS não fornece nem fornecerá a terceiros nenhum documento, informação ou registro sob sua guarda, exceto nas hipóteses mencionadas nos itens 2.8.4, 2.8.6 e 2.8.7 desta PC AC-JUS.

2.8.6 Divulgação por solicitação do titular

O titular de certificado ou 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.

Autorizações formais podem ser apresentadas de duas formas:

- por meio eletrônico, contendo assinatura válida garantida por certificado reconhecido pela AC-JUS; ou
- por meio de pedido escrito com firma reconhecida.

Nenhuma liberação de informação é permitida sem autorização formal do titular do certificado, exceto nos casos do item 2.8.4.

2.8.7 Outras circunstâncias de divulgação de informação

Nenhuma outra liberação de informação, que não expressamente descrita na DPC da AC-JUS, é permitida.

2.9 Direitos de Propriedade Intelectual

Todos os direitos de propriedade intelectual inclusive todos os direitos autorais em todos os certificados e todos os documentos gerados para a AC-JUS (eletrônico ou não) pertencem e continuarão sendo propriedade **do** Conselho da Justiça Federal – **CJF.**
A AC subsequente concede à AC-JUS, o direito de publicar e divulgar em página *web* a chave pública que corresponde à chave privada da AC subsequente.
Direitos sobre Identificadores de Objeto (OID) atribuídos à AC-JUS após o processo de credenciamento, cabem única e exclusivamente ao ITI, designado como a AC Raiz da ICP-Brasil.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1 Registro Inicial

A AR-JUS efetua a identificação e autenticação da AC subordinada, com base nos dados fornecidos no formulário de solicitação e nos documentos exigidos nesta PC AC-JUS.
A AR-JUS realiza a autenticação da identidade de uma organização (item 3.1.8) e a autenticação da identidade de um indivíduo (item 3.1.9) por meio de, no mínimo, **dois agentes** de registro responsáveis pelo recolhimento e verificação da validade dos documentos apresentados.

3.1.1 Tipos de nomes

A AC-JUS emite certificados com nomes que permitem a identificação unívoca. Para isso utiliza o "distinguished name" do padrão ITU X.500.
Os certificados emitido para as AC subordinadas, não incluirão o nome da pessoa física responsável.

3.1.2 Necessidade de nomes significativos

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

3.1.3 Regras para interpretação de vários tipos de nomes

Não se aplica.

3.1.4 Unicidade de nomes

Os identificadores do tipo "Distinguished Name" (DN) são únicos para cada entidade titular de certificado, no âmbito da AC-JUS. Números ou letras adicionais podem ser incluídos ao nome de cada entidade para assegurar a unicidade do campo.
A extensão “unique identifiers” não será admitida para diferenciar as AC com nomes idênticos.

3.1.5 Procedimento para resolver disputa de nomes

A AC-JUS se reserva o direito de tomar todas as decisões referentes a disputas de nomes das entidades solicitantes de certificados. Durante o processo de confirmação de identidade, cabe à entidade solicitante do certificado provar o seu direito de uso de um nome específico.

3.1.6 Reconhecimento, autenticação e papel de marcas registradas

De acordo com a legislação em vigor.

3.1.7 Método para comprovar a posse de chave privada

A confirmação que a entidade solicitante possui a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital é realizada seguindo o padrão RFC 2510, item 2.3.

3.1.8 Autenticação da identidade de uma organização

A confirmação da identidade de uma AC subsequente é feita com base nos "CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL", conforme aprovados pela Resolução nº 6, de 22 de novembro de 2001, do Comitê Gestor da ICP, com as alterações introduzidas pela resolução 31 de 29 de janeiro de 2004, do CG da ICP-Brasil.

A confirmação da identidade de pessoa jurídica responsável pela solicitação de certificado da AC subseqüente é feita mediante a apresentação dos seguintes documentos;

- Registro comercial, no caso de empresa individual:
- Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais ou civis, e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores;
- Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ);
- Prova de inscrição no Cadastro Especifico do INSS (CEI), se aplicável.

A pessoa física responsável pela AC subordinada será identificada na forma descrita no item seguinte.

3.1.9 Autenticação da identidade de um indivíduo

A confirmação da identidade de um indivíduo será realizada mediante a presença física do interessado, com base em documentos legalmente aceitos.
É mantido arquivo contendo o tipo e os detalhes do procedimento de identificação utilizado pela AR-JUS.

3.1.9.1 Documentos para identificação

Deve ser apresentada uma foto recente e, no mínimo, os seguintes documentos acompanhados de cópia:

- Cédula de Identidade ou Passaporte, se estrangeiro;
- Cadastro de Pessoa Física;
- comprovante de residência;
- Número de Identificação social – NIS (PIS/PASEP ou Cadastro de Contribuintes Individuais do INSS - CI), se aplicável;
- Cadastro Específico do INSS – CEI, se aplicável;
- Título de Eleitor, se aplicável;
- Mais um documento oficial com fotografia, no caso de certificados de tipos A4 e S4; e

- Os documentos acima mencionados do responsável, caso o solicitante seja incapaz

Entende-se por cédula de identidade as carteiras instituídas por lei, desde que contenham foto e às mesmas seja atribuída fé pública em todo o território nacional, tais como: Carteira de Identidade emitida pela Secretaria de Segurança Pública, Carteira Nacional de Habilitação, Carteira de Identidade Funcional, Carteira de Identidade Profissional.
O representante legal da AC subordinada assina o termo de titularidade denominado "Termo de Titularidade" e é, para todos os efeitos legais Titular do Certificado emitido.
A pessoa física indicada como responsável pelo certificado assina o Termo de Responsabilidade.
Os Termos de Titularidade e de Responsabilidade serão mantidos junto à documentação exigida neste item.
Tanto a pessoa jurídica titular do certificado, como a pessoa física designada como responsável pelo certificado, serão responsáveis, pela correta utilização deste conforme as normas da ICP-Brasil, assim como pelos danos a que derem causa pelo uso indevido do certificado.

3.2 Geração de novo par de chaves antes da expiração do atual

Antes de sua expiração pode ser solicitado um novo certificado, enviando à AR-JUS uma solicitação, observando os mesmos requisitos e procedimentos exigidos para solicitação do certificado. A emissão de um novo certificado obedece ao estabelecido nesta PC AC-JUS.

3.3 Geração de novo par de chaves após revogação

Após a revogação do certificado de AC de nível imediatamente subseqüente ao da AC-JUS, a AC subordinada executará os processos regulares de geração de seu novo par de chaves.

3.4 Solicitação de Revogação

A solicitação de revogação de certificado da AC-JUS será feita formalmente pelo representante da AC-JUS à AC-Raiz.
A solicitação de revogação de certificado de AC imediatamente subseqüente será feita pelo representante da AC imediatamente subseqüente, encaminhado formalmente à AC-JUS e a com a presença física do representante legal da AC subseqüente, a fim de possibilitar a sua identificação inequívoca.

A solicitação de revogação poderá ainda ser feita por decisão judicial, ou determinação da AC-Raiz.

4. REQUISITOS OPERACIONAIS

4.1 Solicitação de Certificado

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

1) A comprovação de atributos de identificação constantes do certificado;
2) Para a aprovação de certificados a chave da AC-JUS é ativada com a presença de no mínimo 2 (dois) dos custodiantes da chave de ativação;
3) Assinatura do Termo de Titularidade e de Responsabilidade (item 3.1.9.1);

A solicitação de certificado para AC de nível imediatamente subseqüente ao da AC-JUS somente é possível após o deferimento do pedido de credenciamento e a respectiva autorização de funcionamento da AC em questão pela AC-Raiz.

Nesse caso, aquela AC deve encaminhar a solicitação de seu certificado à AC-JUS por meio de seus representantes legais, utilizando o padrão de solicitação de certificado PKCS#10 (Public Key Cryptographic Standards).

4.2 Emissão de Certificado

A emissão de um certificado pela AC-JUS é feita em cerimônia específica, com a presença dos representantes da AC-JUS, da AC habilitada, de auditores e convidados, na qual são registrados todos os procedimentos executados.
A AC-JUS garante que a cerimônia de emissão de um certificado para AC de nível imediatamente subseqüente ao seu ocorre em, no máximo, 10 (dez) dias úteis após a autorização de funcionamento da AC em questão pelao AC-RAIZ.
A AC-JUS entrega o certificado emitido, em formato padrão PKCS#7, para os representantes legais da AC habilitada.
A emissão dos certificados das AC de nível imediatamente subseqüente à AC-JUS é feita em equipamentos que operam *off-line*.

O certificado é considerado válido a partir da assinatura do “Termo de Acordo”.

4.3 Aceitação de Certificado

O certificado é considerado aceito assim que for utilizado. A aceitação implica que a Ac subseqüente responsável pelo certificado reconhece a veracidade dos dados contidos no certificado.

4.4 Suspensão e Revogação de Certificado

4.4.1 Circunstâncias para revogação

Um certificado é obrigatoriamente revogado nas seguintes circunstâncias:

- quando constatada emissão imprópria ou defeituosa do mesmo;
- quando for necessária a alteração de qualquer informação constante no mesmo;
- no caso de dissolução da AC titular do certificado; ou
- no caso de perda, roubo, modificação, acesso indevido, comprometimento ou suspeita de comprometimento da chave privada correspondente ou da sua mídia armazenadora.

A AC-JUS pode a seu critério revogar, conforme prazo definido no item 4.4.3, o certificado da entidade que deixar de cumprir as políticas, normas e regras estabelecidas para a ICP-Brasil e pela AC-JUS;
O CG da ICP-Brasil pode, a seu critério, determinar a revogação do certificado da AC que deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas para a ICP-Brasil.

4.4.2 Quem pode solicitar revogação

A revogação de um certificado somente pode ser solicitada:

- pelo titular do certificado;
- pelo responsável pela utilização do certificado;
- pela AC-JUS;
- pela AR-JUS;
- por determinação do CG da ICP-Brasil;
- por determinação da AC Raiz; ou
- por decisão judicial.

4.4.3 Procedimento para solicitação de revogação

A solicitação de revogação de certificado é feita através de formulário específico, disponível na página **http://www.acjus.gov.br/acjus/**, permitindo a identificação inequívoca do solicitante. Os agentes habilitados, conforme o item 4.4.2, podem a qualquer tempo solicitar a revogação de seus respectivos certificados. Os procedimentos detalhados de solicitação de revogação estão descritos na correspondente PC.
Como diretrizes gerais, fica estabelecido que:

- O solicitante da revogação de um certificado deve ser identificado;
- As solicitações de revogação, bem como as ações delas decorrentes deverserão ser registradas e armazenadas;
- As justificativas para a revogação de um certificado são documentadas; e
- O processo de revogação de um certificado terminará com a geração e a publicação de uma LCR que contenha o certificado revogado.

O prazo limite para a conclusão do processo de revogação de certificado, após o recebimento da respectiva solicitação é de 24 (vinte e quatro) horas.

4.4.4 Prazo para solicitação de revogação

A solicitação de revogação será imediata quando configuradas as circunstâncias definidas no seu item 4.4.1.
A AC titular do certificado pode solicitar a sua revogação no prazo de (5) cinco dias úteis após o recebimento do mesmo, sem quaisquer ônus.

4.4.5 Circunstâncias para suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil, não sendo, portanto, admitida no âmbito da AC-JUS.

4.4.6 Quem pode solicitar suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil, não sendo, portanto, admitida no âmbito da AC-JUS.

4.4.7 Procedimento para solicitação de suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil, não sendo, portanto, admitida no âmbito da AC-JUS.

4.4.8 Limites no período de suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil, não sendo, portanto, admitida no âmbito da AC-JUS.

4.4.9 Freqüência de emissão de LCR

O prazo máximo admitido para a emissão de LCR referente a certificados de AC subordinadas é de 15 (quinze) dias.

Na revogação de certificado de AC de nível imediatamente subseqüente ao seu, a AC-JUS deverá emitir nova LCR no prazo máximo de 24 (vinte e quatro) horas e notificar todas as AC de nível imediatamente subseqüente ao seu.

São emitidas LCR na freqüência determinada na PC, mesmo quando não houver nenhuma mudança ou atualização, para assegurar a periodicidade da informação.

4.4.10 Requisitos para verificação de LCR

Todos os certificados revogados no domínio da AC-JUS são listados na LCR que pode ser acessada no endereço *web* contido no próprio certificado.
Todo certificado deve ter a sua validade verificada, na respectiva LCR, antes de ser utilizado.

Os números de série de certificados revogados, de qualquer das AC de nível imediatamente subseqüente, entidade final que estejam revogados aparecem na LCR emitida pela AC-JUS emitida pela AC-JUS. Estes números permanecem nas LCR emitidas até a data de expiração dos certificados ser atingida, sendo removidos na primeira LCR emitida após essa data.
A autenticidade da LCR deve também ser confirmada por meio da verificação da assinatura da AC-JUS e do período de validade da LCR.

4.4.11 Disponibilidade para revogação/verificação de status on-line

A AC-JUS não disponibiliza recursos para revogação ou verificação *on-line* de estado de certificados.

4.4.12 Requisitos para verificação de revogação on-line

A AC-JUS não disponibiliza diretório *on-line* ou um servidor de OCSP para verificar o estado dos certificados emitidos pela AC-JUS.

4.4.13 Outras formas disponíveis para divulgação de revogação

Informações de revogação de certificado de AC de nível imediatamente subseqüente ao da AC-JUS serão divulgadas por meio de sua publicação no Diário Oficial, Caderno III, Diário de Justiça e na página WEB **http://www.acjus.gov.br/acjus/.**

4.4.14 Requisitos para verificação de outras formas de divulgação de revogação

As formas de verificação de revogação descritas no item 4.4.10, são meramente informativas. Onde forem aplicáveis, outras formas de divulgação de revogação, os requisitos de verificação são especificados nas PC implementadas pela AC-JUS.

4.4.15 Requisitos especiais para o caso de comprometimento de chave

No caso do comprometimento da chave privada de uma AC de nível imediatamente subseqüente ao da AC-JUS, a mesma deve notificar imediatamente à AC-JUS, solicitando a revogação de seu certificado, por meio de formulário específico disponibilizado pela AC-JUS em sua página WEB, http://www.acjus.gov.br/acjus/.

4.5 Procedimentos de Auditoria de Segurança

Os itens a seguir estão definidos na DPC da AC-JUS sob a mesma numeração.

4.5.1 Tipos de evento registrados

4.5.2 Freqüência de auditoria de registros (logs)

4.5.3 Período de retenção para registros (logs) de auditoria

4.5.4 Proteção de registro (log) de auditoria

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

4.5.6 Sistema de coleta de dados de auditoria

4.5.7 Notificação de agentes causadores de eventos

4.5.8 Avaliações de vulnerabilidade

4.6 Arquivamento de Registros

Os itens a seguir estão definidos na DPC da AC-JUS sob a mesma numeração.

4.6.1 Tipos de eventos registrados

4.6.2 Período de retenção para arquivo

4.6.3 Proteção de arquivo

4.6.4 Procedimentos para cópia de segurança (backup) de arquivo

4.6.5 Requisitos para datação (time-stamping) de registros

4.6.6 Sistema de coleta de dados de arquivo

4.6.7 Procedimentos para obter e verificar informação de arquivo

4.7 Troca de chave

A AC-JUS comunica através de oficio, com 90 dias de antecedência, à AC subseqüente o vencimento do seu certificado, junto com as informações necessárias para a solicitação de uma nova chave.

4.8 Comprometimento e Recuperação de Desastre

Os itens a seguir estão definidos na DPC da AC-JUS sob a mesma numeração.

4.8.1 Recursos computacionais, software, e dados corrompidos

4.8.2 Certificado de entidade é revogado

4.8.3 Chave de entidade é comprometida

4.8.4 Segurança dos recursos após desastre natural ou de outra natureza

4.9 Extinção da AC-JUS ou AR-JUS

Quando for necessário encerrar as atividades da AC-JUS ou da AR-JUS, o impacto deste término deve ser minimizado da melhor forma possível tendo em vista as circunstâncias prevalecentes. Isto inclui:

- Prover com maior antecedência possível notificação para:
  - a AC Raiz da ICP-Brasil;
  - todas as entidades subordinadas.
- A transferência progressiva do serviço e dos registros operacionais, para um sucessor, que deverá observar os mesmos requisitos de segurança exigidos para a AC-JUS ou para a AR-JUS extinta;
- Preservar qualquer registro não transferido a um sucessor.

As chaves públicas dos certificados emitidos pela AC-JUS, dissolvida, serão armazenadas por outra AC, após aprovação da AC Raiz.
Quando houver mais de uma AC interessada, assumirá a responsabilidade do armazenamento das chaves públicas, aquela indicada pela AC-JUS.
A AC-JUS, 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.

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

Os itens a seguir estão definidos na DPC da AC-JUS sob a mesma numeração.

5.1 Controles Físicos

5.1.1 Construção e localização das instalações

5.1.2 Acesso físico

5.1.3 Energia e ar condicionado

5.1.4 Exposição à água.

5.1.5 Prevenção e proteção contra incêndio

5.1.6 Armazenamento de mídia

5.1.7 Destruição de lixo

5.1.8. Instalações de segurança (backup) externas (off-site)

5.2. Controles Procedimentais

5.2.1. Perfis qualificados

5.2.2. Número de pessoas necessário por tarefa

5.2.3. Identificação e autenticação para cada perfil

5.3 Controles de Pessoal

5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade

5.3.2. Procedimentos de verificação de antecedentes

5.3.3. Requisitos de treinamento

5.3.4. Freqüência e requisitos para reciclagem técnica

5.3.5. Freqüência e seqüência de rodízio de cargos

5.3.6. Sanções para ações não autorizadas

5.3.7. Requisitos para contratação de pessoal

5.3.8. Documentação fornecida ao pessoal

6. CONTROLES TÉCNICOS DE SEGURANÇA

6.1. Geração e Instalação do Par de Chaves

6.1.1. Geração do par de chaves

Os pares de chaves criptográficas da AC-JUS e das AC subordinadas são gerados pelas mesmas, após seu credenciamento pela ICP-Brasil. As AC subordinadas indicarão, por intermédio de seus representantes legais, a pessoa responsável pela geração dos pares de chaves criptográficas e pelo uso do certificado.
Ao ser gerada, a chave privada da entidade titular é gravada cifrada, por algoritmo simétrico como 3-DES, IDEA, SAFER+ ou outros aprovados pelo CG da ICP-Brasil, em hardware criptográfico aprovado pelo CG da ICP - Brasil.
A chave privada trafega cifrada, empregando os mesmos algoritmos citados no parágrafo anterior, entre o dispositivo gerador e a mídia utilizada para o seu armazenamento.
O meio de armazenamento da chave privada assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

- a chave privada é única e seu sigilo é suficientemente assegurado;
- a chave privada não pode, com uma segurança razoável, ser deduzida;
- a chave privada está protegida contra falsificações realizadas através das tecnologias atualmente disponíveis;
- a chave privada pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros;

Esse meio de armazenamento não modifica os dados a serem assinados, nem impede que esses dados sejam apresentados ao signatário antes do processo de assinatura.
Os pares de chaves da AC-JUS e das AC subordinadas são gerados em módulo criptográfico de hardware com padrão de segurança FIPS 140-1 nível 2,ou superior, utilizando algoritmo RSA para geração do par de chaves.
Os pares de chaves da AC-JUS e das AC subordinadas são gerados somente pelo Titular do Certificado correspondente.

6.1.2. Entrega da chave privada à entidade titular

A geração e a guarda de uma chave privada é de responsabilidade exclusiva do titular do certificado correspondente.

6.1.3. Entrega da chave pública para emissor de certificado

Para a entrega de sua chave pública à AC-JUS, encarregada da emissão de seu certificado, a AC solicitante faz uso do padrão PKCS#10. Essa entrega é feita por representante legalmente constituído da AC subordinada, em data e hora previamente estabelecida pela AC-JUS.

6.1.4. Disponibilização de chave pública da AC-JUS para usuários

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

- formato PKCS#7 (RFC 2315), que inclui toda a cadeia de certificação, no momento da disponibilização de um certificado para seu titular;
- diretório;
- página Web da AC-JUS (http://www.acjus.gov.br/acjus/)
- outros meios seguros aprovados pelo CG da ICP-Brasil.

Código de campo alterado

6.1.5. Tamanhos de chave

O tamanho das chaves criptográficas associadas a certificados emitidos pela AC-JUS será de, no mínimo 2048 (dois mil e quarenta e oito) bits, conforme estabelecido pela ICP-Brasil para chaves criptográficas associadas a certificados de AC.

6.1.6. Geração de parâmetros de chaves assimétricas

As entidades titulares de certificados adotarão o padrão FIPS (Federal Information Processing Standards) 140-1 nível 2 ou superior, para a geração de chaves assimétricas de sua propriedade.

6.1.7. Verificação da qualidade dos parâmetros

Os parâmetros são verificados de acordo com as normas estabelecidas pelo CMVP (Cryptographic Module Validation Program) do NIST (National Institute of Standards and Technology).

6.1.8. Geração de chave por hardware ou software

A AC-JUS utiliza componentes seguros de hardware para a geração de seu par de chaves, de seu certificado, dos certificados das AC subsequentes ao seu e para a geração e assinatura de sua LCR. O componente seguro de hardware utiliza um mecanismo de detecção de violação.

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

A chave privada da AC-JUS é utilizada apenas para a assinatura dos certificados por ela emitidos e de suas LCR.
As chaves privadas dos titulares de certificados emitidos pela AC-JUS são utilizadas apenas para a assinatura dos certificados por ela emitidos e de suas LCR.

6.2. Proteção da Chave Privada

6.2.1. Padrões para módulo criptográfico

A chave privada da AC-JUS é gerada, armazenada e utilizada apenas em *hardware* criptográfico específico, classificado como FIPS 140-1 nível 3, não havendo portanto tráfego da mesma em nenhum momento.

6.2.2. Controle "n de m" para chave privada

A chave criptográfica de ativação do componente seguro de hardware que armazena a chave privada da AC-JUS é dividida em “6” (m) partes e distribuídas por “6” custodiantes designados pela AC-JUS, É necessário a presença de no mínimo “2” (n) custodiantes para a ativação do componente e a consequente utilização da chave privada.

6.2.3. Recuperação (escrow) de chave privada

Não é permitida, 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

A AC-JUS 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 e aprovado pelo CG da ICP-Brasil, e mantida pelo prazo de validade do certificado correspondente.

A AC-JUS não mantém cópia de segurança das chaves privadas das AC de nível imediatamente subseqüentes ao seu.

Qualquer entidade titular de certificado pode, a seu critério, manter cópia de sua própria chave privada.

A cópia de segurança deve ser armazenada, cifrada, por algoritmo simétrico como 3-DES, IDEA, SAFER+, ou outros aprovados pelo CG da ICP-Brasil, e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.5. Arquivamento de chave privada

As chaves privadas dos titulares de certificados emitidos pela AC-JUS não são arquivadas.
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-JUS é inserida no módulo criptográfico de acordo com o estabelecido na RFC 2510.

6.2.7. Método de ativação de chave privada

A ativação da chave privada da AC-JUS é implementada por meio de cartões criptográficos, protegidos com senha, após a identificação de “2” de “6” dos custodiantes da chave de ativação da chave criptográfica. Os custodiantes da chave de ativação serão magistrados ou servidores do Judiciário Federal indicados pelo Comitê

Gestor da AC-JUS. As senhas obedecem à política de senhas estabelecida pela AC-JUS.

6.2.8. Método de desativação de chave privada

A chave privada da AC-JUS, armazenada em módulo criptográfico é desativada, quando não mais 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 "6" dos *custodiantes* da chave de ativação da chave criptográfica. As senhas obedecem à política de senhas estabelecida pela AC-JUS.

6.2.9. Método de destruição de chave privada

Além do estabelecido no item 6.2.8 desta PC, todas as cópias de segurança da chave privada da AC–JUS serão destruídas.

As mídias de armazenamento das chaves privadas serão reinicializadas de forma a não restarem nelas informações sensíveis.

6.3. Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1. Arquivamento de chave pública

As chaves públicas da AC-JUS e dos titulares de certificados de assinatura para Autoridade Certificadora subordinada por ela emitidos permanecem armazenadas após a expiração dos certificados correspondentes, por no mínimo 30 (trinta) anos, na forma da legislação em vigor, para a verificação de assinaturas geradas durante seu período de validade.

6.3.2. Períodos de uso para as chaves pública e privada

A chave privada da AC-JUS é utilizada apenas durante o período de validade do certificado correspondente, cuja validade máxima é de 8 anos. A chave pública da AC-JUS 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.
Os certificados emitidos pela AC-JUS para as AC´s de nível imediatamente subseqüente ao seu terão validade de no máximo 5 anos.

6.4. Dados de Ativação

6.4.1. Geração e instalação dos dados de ativação

São necessários as presenças de no mínimo dois custodiantes, com os cartões criptográficos e senha de ativação do módulo criptográfico.

6.4.2. Proteção dos dados de ativação

Os dados de ativação são protegidos por cartões criptográficos individuais com senha, e são armazenados em ambiente de nível 6 de segurança.

6.4.3. Outros aspectos dos dados de ativação

Não aplicável.

6.5. Controles de Segurança Computacional

6.5.1. Requisitos técnicos específicos de segurança computacional

A geração do par de chaves das AC subordinadas é realizada off-line, para impedir o acesso remoto não autorizado.
Cada computador servidor das AC subordinadas relacionado diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, implementa, entre outras, as seguintes características:

- controle de acesso aos serviços e perfis da AC;
- clara separação das tarefas e atribuições relacionadas a cada perfil das AC subordinadas;
- uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações;
- geração e armazenamento de registros de auditoria das AC subordinadas;
- mecanismos internos de segurança para garantia da integridade de dados e processos críticos;
- mecanismos para cópias de segurança (backup);e
- acesso restrito aos bancos de dados das AC.

Essas características são implementadas pelo sistema operacional ou por meio da combinação deste com o sistema de certificação e com mecanismos de segurança física.
Qualquer equipamento, ou parte deste, ao ser enviado para manutenção, tem todas as informações sensíveis nele contidas apagadas e seu número de série e as datas de

envio e de recebimento controlados. Ao retornar às instalações das AC subordinadas, o equipamento que passa por manutenção é inspecionado. Em todo equipamento que deixe de ser utilizado em caráter permanente, são destruídas de maneira definitiva todas as informações sensíveis armazenadas, relativas à atividade das AC subordinadas. Todos esses eventos são registrados para fins de auditoria.
Qualquer equipamento incorporado às AC subordinadas é preparado e configurado como previsto na Política de Segurança implementada, de forma a apresentar o nível de segurança necessário à sua finalidade.

6.5.2. Classificação da segurança computacional

A AC-JUS aplica configurações de segurança conforme recomendações do SANS INSTITUTE. Também são seguidas as recomendações de segurança do ITSEC que avaliou a plataforma da solução implementada.

6.6. Controles Técnicos do Ciclo de Vida

6.6.1. Controles de desenvolvimento de sistema

A AC-JUS adota sistema de certificação próprio desenvolvido em código aberto.

6.6.2. Controles de gerenciamento de segurança

A administração de segurança de sistema é controlada pelos privilégios nomeados a contas de sistema operacional, e pelos papéis confiados descritos no item 5.2.1.

O gerenciamento de configuração, para a instalação e a contínua manutenção do sistema de certificação utilizado pela AC-JUS, envolve o teste de mudanças planejadas no Ambiente de Desenvolvimento e Homologação isolados antes de sua implantação no ambiente de Produção, incluindo as seguintes atividades:

- Instalação de novas versões ou de atualizações nos produtos que constituem a plataforma do sistema de certificação;
- Implantação ou modificação de Autoridades Certificadoras com customizações a nível de certificados, páginas web, scripts, etc.;
- Implantação de novos procedimentos operacionais relacionados com a plataforma de processamento incluindo módulos criptográficos; e
- Instalação de novos serviços na plataforma de processamento.

6.6.3. Classificações de segurança de ciclo de vida

Não aplicável.

6.7. Controles de Segurança de Rede

Item não se aplica, uma vez que a máquina e off-line.

6.8. Controles de Engenharia do Módulo Criptográfico

O módulo criptográfico utilizado pela AC-JUS para o armazenamento de sua chave privada é certificado como FIPS (*Federal Information Processing Standard*s) 140-1, *level* 3.

Ao ser gerada, a chave privada da entidade titular é gravada cifrada, por algoritmo simétrico como 3-DES, IDEA, SAFER+ ou outros aprovados pelo CG da ICP-Brasil, em hardware criptográfico aprovado pelo CG da ICP - Brasil.
O meio de armazenamento da chave privada assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

- a chave privada utilizada na geração de uma assinatura é única e seu sigilo é suficientemente assegurado;
- A chave privada utilizada na geração de uma assinatura não pode, com uma segurança razoável, ser deduzida e que está protegida contra falsificações realizadas através das tecnologias atualmente disponíveis;
- a chave privada utilizada na geração de uma assinatura pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

Esse meio de armazenamento não modifica os dados a serem assinados, nem impede que esses dados sejam apresentados ao signatário antes do processo de assinatura.

7. PERFIS DE CERTIFICADO E LCR

7.1. Perfil do Certificado

Os certificados emitidos pela AC-JUS estão em conformidade com o formato definido pelo padrão ITU X.509.

7.1.1. Número(s) de versão

Os certificados emitidos pela AC-JUS implementam a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 2459.

7.1.2. Extensões de certificado

Os certificados emitidos pela AC-JUS, sob esta PC AC-JUS, obedecem as resoluções da ICP-Brasil, que define como obrigatórias as seguintes extensões para certificados de AC:

- "*Authority Key Identifier*", não crítica: o campo keyIdentifier contém o resumo SHA-1 da chave pública da AC-JUS;
- *Subject Key Identifier*", não crítica: contém o *hash* SHA-1 da chave pública da AC titular do certificado;
- "*Key Usage*", crítica: somente os bits e keyCertSign e cRLSign são ativados;
- "*Certificate Policies*", não crítica:
  - o campo policyIdentifier contém o OID das PC que a AC titular do certificado implementa;
  - o campo policyQualifiers contém o endereço *URL* da página *Web, http://www.acjus.gov.br/acjus/dpcacjus.pdf,* onde se obtém a DPC da AC-JUS;
- "Basic Constraints", crítica: contém o campo CA=TRUE;
- "*CRL Distribution Points*", não crítica: contém o endereço *URL* da página *Web, http://www.acjus.gov.br /acjus/acjus.crl,* onde se obtém a LCR da AC-JUS.

7.1.3. Identificadores de algoritmo

Os certificados da AC-JUS e de titulares de certificado são assinados com o uso do algoritmo RSA com SHA-1 como função hash (OID= 1.2.840.113549.1.1.5), conforme o padrão PKCS#1 (RFC 2313).

7.1.4. Formatos de nome

Para os certificados emitidos sob esta PC AC-JUS, o nome da AC titular do certificado, constante do campo "*Subject*", adota o "*Distinguished Name"* (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C= BR
O= ICP-Brasil
OU= CONSELHO DA JUSTIÇA FEDERAL - CJF
CN= nome da AC

7.1.5. Restrições de nome

As restrições aplicáveis para os nomes dos titulares de certificados emitidos pela AC-JUS são as seguintes:

• não serão utilizados sinais de acentuação, tremas ou cedilhas;
• além dos caracteres alfanuméricos, podem ser utilizados somente os seguintes caracteres especiais:

Caractere	Código NBR9611 (hexadecimal)
Branco	20
!	21
"	22
#	23
$	24
%	25
&	26
'	27
(	28
)	29
*	2A
+	2B
,	2C
-	2D
.	2E
/	2F
:	3A
;	3B
=	3D
?	3F
@	40
\	5C

7.1.6. OID (Object Identifier) de Política de Certificado

O OID desta PC AC-JUS é 2.16.76.1.2.201.5.

7.1.7. Uso da extensão "Policy Constraints"

Não aplicável.

7.1.8. Sintaxe e semântica dos qualificadores de política

Nos certificados emitidos segundo esta PC AC-JUS, o campo policyQualifiers da extensão "Certificate Policies" contém o endereço Web da DPC da AC-JUS (http://www.acjus.gov.br /acjus/dpcacjus.pdf)

7.1.9. Semântica de processamento para extensões críticas

Extensões críticas são interpretadas conforme a RFC 2459.

7.2. Perfil de LCR

7.2.1. Número de versão

As LCR geradas pela AC-JUS, segundo esta PC AC-JUS, implementam a versão 2 de LCR definida no padrão ITU X.509, de acordo com o perfil estabelecido na RFC 2459.

7.2.2. Extensões de LCR e de suas entradas

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

- "Authority Key Identifier": conterá o hash SHA-1 da chave pública da AC-JUS.
- "CRL Number", não crítica: conterá um número seqüencial para cada LCR emitida pela AC-JUS.

8. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

8.1. Procedimentos de mudança de especificação.

Qualquer alteração nesta PC AC-JUS é submetida à aprovação do CG da ICP-Brasil.

Esta PC AC-JUS é atualizada sempre que a DPC da AC-JUS o exigir.

8.2. Políticas de publicação e notificação

Esta PC AC-JUS está disponível para a comunidade no endereço web http://www.acjus.gov.br/acjus/dpacjus.pdf .

8.3. Procedimentos de aprovação

Esta PC AC-JUS foi submetida à aprovação da AC RAIZ da ICP-Brasil, durante o processo de credenciamento da AC-JUS, conforme o determinado pelo documento Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil.

Declaração de Práticas de Certificação
da
Autoridade Certificadora
do Sistema Justiça Federal

(DPC AC-JUS)

Versão 1.0

SUMÁRIO

1. INTRODUÇÃO

1.1 Visão Geral

Esta Declaração de Práticas de Certificação (DPC) descreve as práticas e os procedimentos empregados pela Autoridade Certificadora do Sistema Justiça Federal (AC-JUS) integrante da Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil) na execução dos seus serviços.

A AC-JUS possui um certificado de nível intermediário na ICP-Brasil, sendo este certificado assinado pela AC Raiz da ICP-Brasil. O certificado da AC-JUS contém a chave pública correspondente à chave privada utilizada para assinar os certificados das AC de nível imediatamente subseqüente ao seu e a sua LCR (Lista de Certificados Revogados).

A AC-JUS utilizará o ambiente e os serviços Serviço Federal de Processamento de Dados - SERPRO para hospedar, operar e dar manutenção às suas atividades.

A estrutura desta DPC AC-JUS está baseada nas resoluções do Comitê Gestor da ICP-Brasil (CG ICP-Brasil) e na RFC 2527 (Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Framework).

1.2 Identificação

Esta DPC é chamada “Declaração de Práticas de Certificação da Autoridade Certificadora do Sistema Justiça Federal, integrante da ICP-Brasil”, e comumente referida como “DPC AC-JUS”. O Identificador de Objeto **(OID)** desta DPC, atribuído pela AC Raiz, após conclusão do processo de seu credenciamento, é **2.16.76.1.1.1.9**

1.3 Comunidade e Aplicabilidade

1.3.1 Autoridades Certificadoras

Esta DPC refere-se unicamente à Autoridade Certificadora do Sistema Justiça Federal (AC-JUS) e encontra-se publicada na página http://www.acjus.gov.br/ acjus/dpcacjus.pdf.

.

1.3.2 Autoridades de Registro

Os processos de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes, são de competência da AC-JUS através de sua Autoridade de Registro, doravante chamada de AR-JUS.

A PC operada pela AC-JUS no âmbito da ICP-Brasil possui sua própria Autoridade de Registro identificada neste mesmo item.

1.3.3 Titulares de Certificado

A AC-JUS emite certificados para Autoridades Certificadoras de nível imediatamente subseqüente ao seu.

Os titulares dos certificados são Órgãos do Poder Judiciário Federal, representados inicialmente pelo Superior Tribunal de Justiça, Conselho da Justiça

Federal, Tribunais Regionais Federais, Seções Judiciárias e entidades e pessoas jurídicas de direito publico e privado, autorizadas pela AR-JUS a receberem certificados digitais emitidos pela AC-JUS, cujos nomes aparecem no certificado digital, no campo "D*istinguished Name (DN)"*.

1.3.4 Aplicabilidade

Os certificados definidos por esta DPC AC-JUS têm sua utilização exclusiva para a assinatura de certificados digitais e de Lista de Certificados Revogados (LCR).

1.4 Dados de Contato

Esta DPC é administrada pelo Comitê Gestor da AC-JUS, assessorada pela Comissão Técnica por ele designada e pela estrutura administrativa de certificação digital do CJF.

Nome: Conselho da Justiça Federal
Endereço: SEPN 510 Bloco "C" lote 8
Edifício Conselho da Justiça Federal Asa Norte - Brasília-DF Brasil
Telefone: **(61) 348-3113 (PABX)**
Fax: **(61) 349-1542**
Página *Web*: http://www.acjus.gov.br/acjus/
E-mail: AC-JUS@cjf.gov.br

1.4.1 Pessoas de Contato

Nome: Paulo Martins Inocêncio
E-mail: paulo.martins@cjf.gov.br

Nome: Wilson Nogueira de Aquino Jr.
E-mail: wilsonjr@cjf.gov.br

Endereço: SEPN 510 Bloco "C" lote 8
Edifício Conselho da Justiça Federal Asa Norte - Brasília-DF Brasil
Telefone: **(61) 348-3113 (PABX)**
Fax: **(61) 349-9414**
Página *Web*: http://www.acjus.gov.br/acjus/
E-mail: paulo.martins@cjf.gov.br

2. DISPOSIÇÕES GERAIS

2.1 Obrigações e Direitos

2.1.1 Obrigações da AC-JUS

As obrigações da AC-JUS são as abaixo relacionadas:

- Operar de acordo com esta DPC e com a PC implementada;
- Adotar as medidas cabíveis para assegurar que usuários e demais entidades envolvidas tenham conhecimento de seus respectivos direitos e obrigações;
- Gerar e gerenciar o seu par de chaves criptográficas;

- Assegurar a proteção de sua chave privada;
- Notificar a AC Raiz da ICP-Brasil, emitente do seu certificado, quando ocorrer comprometimento de sua chave privada e solicitar a imediata revogação desse certificado;
- Notificar as AC de nível imediatamente subseqüente ao seu quando ocorrer: suspeita de comprometimento de sua chave, emissão de novo par de chaves e correspondente certificado ou o encerramento de suas atividades;
- Distribuir o seu próprio certificado;
- Emitir, expedir e distribuir os certificados das AC de nível imediatamente subseqüente ao seu e os certificados da AR-JUS.
- Informar a emissão do certificado ao respectivo solicitante;
- Revogar os certificados por ela emitidos;
- Emitir, gerenciar e publicar sua Lista de Certificados Revogados (LCR);
- Identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo Comitê Gestor da ICP-Brasil (CG ICP-Brasil);
- Publicar em sua página *web* http://www.acjus.gov.br/acjus/ a DPC AC-JUS e a PC AC-JUS aprovadas e implementadas;
- Adotar as medidas de segurança e controle previstas na DPC, PC e política de segurança que implementar, envolvendo seus processos, procedimentos e atividades, observadas as normas, critérios e procedimentos da ICP-Brasil;
- Manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras da ICP-Brasil e com a legislação vigente;
- Manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada;
- Manter e testar regularmente seu Plano de Continuidade do Negócio;
- Não emitir certificados com prazo de validade que se estenda além do prazo de validade de seu próprio certificado.
- Publicar os certificados por ela emitidos;
- Investigar comprometimento e suspeitas de comprometimento de sua chave privada.
- Fiscalizar e auditar as AC, as AR e os prestadores de serviço, habilitados em conformidade com os critérios estabelecidos pelo Comitê Gestor (CG) da ICP-Brasil; e
- Informar as terceiras partes e titulares de certificado acerca das garantias, coberturas, condicionantes e limitações estipuladas pela apólice de seguro de responsabilidade civil contratada pela AC.

2.1.2 Obrigações da AR-JUS

As obrigações da AR-JUS são as abaixo relacionadas:

- Receber solicitações de emissão e revogação de certificados e respectivos documentos de identificação armazenado-os conforme critérios estabelecidos pelo CG da ICP-Brasil;
- Confirmar a identidade do solicitante e a validade da solicitação, de acordo com os requisitos estabelecidos pelos itens 3 e 4 desta DPC AC-JUS;
- Encaminhar a solicitação de emissão e de revogação de certificado à AC-JUS utilizando VPN (virtual private network - rede privativa virtual), SSL (secure socket layer - protocolo de comunicação seguro) ou outra tecnologia de igual ou superior nível de segurança e privacidade;
- Utilizar VPN (virtual private network - rede privativa virtual), SSL (secure socket layer - protocolo de comunicação seguro) ou outra tecnologia de igual ou superior nível de segurança e privacidade, ao disponibilizar serviços para os solicitantes ou usuários de certificados digitais via *web*;
- Informar aos respectivos titulares a emissão ou a revogação de seus certificados;
- Disponibilizar os certificados emitidos pela AC-JUS aos seus respectivos solicitantes;
- Identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasi;
- Manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC-JUS;
- Manter e garantir a segurança da informação por elas tratada, de acordo com o estabelecido nas normas, critérios, práticas e procedimentos da ICP –Brasil;
- Oferecer treinamento aos seus agentes de registro, especialmente quanto ao reconhecimento de assinaturas e validade dos documentos apresentados na forma dos itens 3.1.8 e 3.1.9; e

2.1.3 Obrigações do Titular do Certificado

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

- Fornecer, de modo completo e preciso, todas as informações necessárias para sua identificação;
- Garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos;
- Utilizar os seus certificados e suas respectivas chaves privadas de modo apropriado, conforme o previsto na PC AC-JUS;

- Conhecer os seus direitos e obrigações, contemplados na PC da AC-JUS, nesta DPC e em outros documentos aplicáveis da ICP-Brasil;
- Informar à AC-JUS qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente;
- operar de acordo com a sua DPC e com a PC que implementa;
- emitir, expedir e distribuir os certificados de seus solicitantes;
- informar a emissão do certificado ao respectivo solicitante;
- revogar os certificados por ele emitidos;
- emitir, gerenciar e publicar sua Lista de Certificados Revogados (LCR);
- publicar em sua página *web* sua DPC e a PC aprovada e implementada;
- fiscalizar e auditar as AR e os prestadores de serviço habilitados em conformidade com os critérios estabelecidos pelo Comitê Gestor (CG) da ICP-Brasil; e
- identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil.

2.1.4 Direitos da Terceira Parte (*Relying Party*)

Considera-se terceira parte, a parte usuária que confia no teor, validade e aplicabilidade do certificado digital. Constituem direitos da terceira parte:

- utilizar o certificado para os propósitos previstos nesta DPC, bem como para outros fins lícitos;
- verificar a qualquer tempo a validade do certificado, sendo este considerado válido quando:
  - puder ser verificado com o uso de certificado válido da AC-JUS;
  - não constar da LCR da AC-JUS;
  - não estiver expirado; e
  - recusar a utilização do certificado para fins diversos dos previstos na PC correspondente.

O não exercício desses direitos não afasta a responsabilidade da AC-JUS e do titular do certificado.

2.1.5 Obrigações do Repositório

- disponibilizar, logo após a sua emissão, os certificados emitidos pela AC-JUS e a sua LCR;
- estar disponível para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana; e
- implementar os recursos necessários para a segurança dos dados nele armazenados.

2.2 Responsabilidades

2.2.1 Responsabilidades da AC-JUS

A Autoridade Certificadora do CJF responde pelos danos a que der causa.
A AC-JUS responde solidariamente pelos atos das AC da cadeia a ela subordinada.

2.2.2 Responsabilidades da AR

A AR-JUS será responsável pelos danos a que der causa.
A AC-JUS responde solidariamente pelos atos da AR-JUS.

2.3 Responsabilidade Financeira

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

Não existe situação específica de utilização do certificado da AC-JUS que requeira prática de indenização pelos Usuários de Certificados, exceto na prática de ato ilícito.

2.3.2 Relações Fiduciárias

A AC-JUS ou a AR-JUS indenizará integralmente os danos a que der causa. Em situações justificáveis, pode ocorrer limitação da indenização, quando o titular do certificado for pessoa jurídica.

2.3.3 Processos Administrativos

Será seguida lei 9784 de 29 de janeiro de 1999 e qualquer outra a legislação específica, uma vez que a AC-JUS e a AR-JUS são administradas pelo Conselho da Justiça Federal, órgão da Administração Pública Federal.

2.4 Interpretação e Execução

2.4.1 Legislação

A DPC AC-JUS 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 e a Resolução conjunta STJ/CJF nº 01 de 20 de Dezembro de 2004.

2.4.2 Forma de interpretação e notificação

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, o corpo técnico, da AC-JUS, examinará a disposição inválida e proporá à Comissão Técnica, no prazo máximo de 30 dias, nova redação ou retirada da disposição afetada.As práticas descritas nesta DPC não prevalecerão sobre as normas, critérios, práticas e procedimentos da ICP-Brasil.

Todas solicitações, notificações ou quaisquer outras comunicações necessárias sujeitas às práticas descritas na PC serão realizadas por iniciativa da AC-JUS por intermédio de seus responsáveis, e enviadas formalmente ao CG da ICP-Brasil e às AC´s subseqüentes se for o caso.

2.4.3 Procedimentos de solução de disputa

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.

2.5 Tarifas de Serviço

Não há tarifas previstas pela AC-JUS para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.5.1 Tarifas de emissão e renovação de certificados

Não há tarifas previstas pela AC-JUS para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.5.2 Tarifas de acesso ao certificado

Não há tarifas previstas pela AC-JUS para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.5.3 Tarifas de revogação ou de acesso à informação de status

Não há tarifas previstas pela AC-JUS para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.5.4 Tarifas para outros serviços, tais como informação de política

Não há tarifas previstas pela AC-JUS para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.5.5 Política de reembolso

Não há política de reembolso prevista pela AC-JUS para os serviços prestados às AC de nível imediatamente subseqüente ao seu.

2.6 Publicação e Repositório

2.6.1 Publicação de informação da AC-JUS

São publicados em página *web* da AC-JUS, http://www.acjus.gov.br/acjus/ :

- O certificado da AC-JUS;
- sua LCR;
- esta DPC e a PC que implementa;
- os certificados das AC de nível imediatamente subseqüente ao seu;
- a lista das Autoridades Certificadoras subordinadas à AC-JUS ;
- a legislação aplicável a esta AC e às suas AC subseqüentes;

- o endereço da instalação técnica da AR-JUS; e
- o leiaute dos certificados emitidos pela AC-JUS.

A disponibilidade das informações publicadas pela AC-JUS em página *web*, tais como certificados, sua LCR, sua DPC, entre outras, é de 99,00% (noventa e nove por cento) do mês, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

A AC-JUS inclui nos certificados emitidos a identificação da sua página *web* .(no certificado consta o endereço da LCR e da DPC).

2.6.2 Freqüência de publicação

Os certificados e a LCR são publicados imediatamente após sua primeira emissão pela AC-JUS. A LCR que será publicada a cada 15 dias independentemente de haver alteração. Esta DPC AC-JUS, a PC AC-JUS e o leiaute dos certificados da AC-JUS são publicadas após aprovação pela AC Raiz da ICP-Brasil e sempre que sofrerem atualizações.
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, à sua PC, aos certificados emitidos e à LCR da AC-JUS.
Acessos para escrita nos locais de armazenamento e publicação serão permitidos apenas às pessoas responsáveis designadas especificamente para esse fim. Os controle de acesso incluirão identificação pessoal para acesso aos equipamentos, utilização de senhas.

2.6.4 Repositórios

O repositório da AC-JUS está disponível para consulta, em no mínimo 99% (noventa e nove por cento), durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana e atende aos seguintes requisitos:

- localização: http://www.acjus.gov.br/acjus/;
- disponibilidade: aquela definida no item 2.6.1 desta DPC AC-JUS;
- protocolos de acesso: HTTP e HTTPS;
- requisitos de segurança: obedece aos requisitos definidos no item 5 desta DPC AC-JUS.

2.7 Auditoria de conformidade

A AC Raiz da ICP-Brasil é a responsável pela auditoria dos processos, procedimentos e atividades de todas as AC integrantes da ICP-Brasil e das AR e prestadores de serviço de suporte a elas vinculadas. A AC Raiz audita a AC-JUS no âmbito da ICP-Brasil. A auditoria é realizada com o objetivo de verificar a conformidade com suas respectivas DPC, PC, PS (Política de Segurança) e demais normas e procedimentos estabelecidos pela ICP-Brasil.
Os serviços de auditoria poderão ser executados:

- por empresas independentes, autorizadas pela AC Raiz e contratadas pela AC auditada; ou
- pela AC-JUS, em AR´s e PSS (prestadores de serviço de suporte) vinculados, de acordo com os procedimentos estabelecidos pela ICP-Brasil.

2.7.1 Freqüência de auditoria de conformidade de entidade

As AC credenciadas pelo CG da ICP-Brasil, subordinadas à AC-JUS, suas AR e seus prestadores de serviço sofrem auditoria:

- previamente ao seu credenciamento pela AC-Raiz e à sua habilitação pela AC-JUS;
- anuais, em data a ser designada pela AC-Raiz ou pela AC-JUS; e
- a qualquer tempo, sem aviso prévio, pela AC Raiz.

Adicionalmente, as AC de nível imediatamente subseqüente ao da AC-JUS, para fins de continuidade do credenciamento, apresentarão anualmente relatório de auditoria.

A AC-JUS conduz anualmente auditorias de conformidade na AR-JUS, podendo também executar, a qualquer momento, auditorias não programadas.

2.7.2 Identidade/Qualificações do Auditor

A auditoria será executada por empresa de auditoria independente e especializada, com comprovada experiência em serviços de auditoria e tecnologias de certificação, de acordo com os procedimentos estabelecidos pela ICP-Brasil.

As auditorias nas AR e prestadores de serviço vinculadas, poderão ser executadas pela AC-JUS.

2.7.3 Relação entre auditor e parte auditada

No caso de contratação de auditoria, o auditor deve ser totalmente independente da AC auditada. Ao auditor, sem prejuízo do disposto nesta PC, aplicam-se, no que couber, as regras de impedimento e suspeição estabelecidas nos arts. 134 e 135 do Código de Processo Civil.

O auditor, tanto no caso de contratação de auditoria independente como nas auditorias realizada pela AC-JUS, será declarado impedido de realizar auditoria, quando::

- houver motivo de foro íntimo declarado;
- for amigo íntimo ou inimigo capital de membros da AC auditada;
- for credor ou devedor da AC auditada ou de um de seus membros;
- tiver recebido, nos últimos 5 anos, da AC auditada, pagamentos referentes à prestação de serviços de outra natureza;
- tiver interesse no resultado da auditoria da AC auditada; e
- houver relacionamento, de fato ou de direito, como cônjuge, parente, consangüíneo ou afim, com algum dos membros da AC auditada, em linha reta ou na colateral até o terceiro grau.

O auditor firmará declaração, sob as penas da lei, de que não se enquadra em qualquer dessas ou outras causas de impedimento. Declarará, ainda, em outro documento, o seu compromisso de manter em sigilo todas e quaisquer informações que obtiver no curso dos trabalhos, mesmo depois do término destes, sendo responsável civil e criminalmente pela divulgação indevida.

2.7.4 Tópicos cobertos pela auditoria

As auditorias de conformidade verificam todos os aspectos relacionados com a emissão e o gerenciamento de certificados digitais, incluindo o controle dos processos de solicitação, identificação, autenticação, geração, publicação, distribuição, renovação e revogação de certificados.
Todos os eventos significativos ocorridos em um sistema de AC ou de AR serão armazenados em trilhas seguras de auditoria, onde cada entrada possua o registro de data, hora e tipo de evento, com assinatura, para garantir que as entradas não possam ser falsificadas.
Os tópicos cobertos por uma auditoria de conformidade incluem, entre outros:

- Política de Segurança;
- Segurança física;
- Avaliação de tecnologia;
- Administração dos serviços;
- Investigação de pessoal;
- PC e DPC utilizadas;
- Contratos; e
- Considerações de sigilo.

2.7.5 Medidas a serem adotadas em caso de não conformidade

Cabe à entidade auditada cumprir, no menor dos prazos estipulados, as recomendações dos auditores para corrigir os casos de não conformidade com a legislação ou com as políticas, normas, práticas e regras estabelecidas. O não cumprimento das recomendações, no prazo estipulado, acarretará a revogação do seu certificado pela AC-JUS.
A AC-JUS, em casos de iminente dano irreparável ou de difícil reparação a terceiros, poderá suspender cautelarmente, no todo ou em parte, a emissão de certificados pela AC de nível imediatamente subseqüente ao seu.

2.7.6 Comunicação de resultados

Os auditores somente informam os resultados da auditoria à entidade auditada, à AC-JUS e à AC Raiz da ICP-Brasil, nos termos da declaração que firmarem, como exigida pelo item 2.7.3.

2.8 Sigilo

A chave privada de assinatura digital da AC-JUS foi gerada e é mantida pela própria AC-JUS, que é responsável pelo seu sigilo.
A divulgação ou utilização indevida da chave privada de assinatura pela AC-JUS é de sua inteira responsabilidade.
Os titulares de certificados emitidos pela AC-JUS, 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 Tipos de informações sigilosas

Todas as informações coletadas, geradas, transmitidas e mantidas pela AC-JUS e a AR-JUS são consideradas sigilosas, exceto aquelas informações citadas no item 2.8.2.
Essas informações serão arquivadas de acordo com sua classificação que será especificada na Política de Segurança.
Como princípio geral, nenhum documento, informação ou registro fornecido à AC-JUS ou AR-JUS deverá ser divulgado.

2.8.2 Tipos de informações não sigilosas

Certificados, LCR e informações corporativas ou pessoais que necessariamente façam parte deles ou de diretórios públicos são consideradas informações não sigilosas.
Os seguintes documentos da AC-JUS e AR-JUS são considerados documentos não sigilosos:

- qualquer PC aplicável;
- qualquer DPC;
- versões públicas de Políticas de Segurança; e
- resultados finais de auditoria.

2.8.3 Divulgação de informação de revogação/suspensão de certificado

A AC-JUS disponibiliza permanentemente em sua página **http://www.acjus.gov.br/acjus/acjus.crl**, lista de certificados revogados.
As razões para revogação do certificado sempre serão informadas para o seu titular.
Os motivos que justificaram a revogação são mantidos confidenciais pela AC-JUS e pela AR-JUS, exceto quando:

- o titular do certificado revogado autorizar expressamente a sua divulgação a terceiros;
- esses motivos tenham sido publicados, ou sejam ou venham a se tornar de domínio público, desde que tal publicação ou publicidade não tenha sido, de qualquer forma, ocasionada por culpa ou interferência indevida da AC-JUS ou da AR-JUS;
- tais motivos sejam requisitados por determinação judicial ou governamental, caso em que a AC-JUS ou a AR-JUS, se estiver obrigada a divulgá-los, comunicará previamente ao titular do certificado a existência de tal determinação.

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

2.8.4 Quebra de sigilo por motivos legais

Como princípio geral, nenhum documento, informação ou registro que pertençam ou estejam sob a guarda da AC-JUS e suas AR é divulgado a entidades legais ou seus funcionários, exceto quando:

- Exista uma ordem judicial corretamente constituída; e

- Esteja corretamente identificado o representante da lei.

2.8.5 Informações a terceiros

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

2.8.6 Divulgação por solicitação do titular

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.
Autorizações formais podem ser apresentadas de duas formas:

- por meio eletrônico, contendo assinatura válida garantida por certificado reconhecido pela AC-JUS; ou
- por meio de pedido escrito com firma reconhecida.

Nenhuma liberação de informação é permitida sem autorização formal do titular do certificado, exceto nos casos do item 2.8.4.

2.8.7 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

Todos os direitos de propriedade intelectual inclusive todos os direitos autorais em todos os certificados e todos os documentos gerados para a AC-JUS (eletrônicos ou não) pertencem e continuarão sendo propriedade do Conselho da Justiça Federal - CJF.
O Titular de Certificado concede à AC-JUS, o direito de publicar e divulgar em página *web* a chave pública que corresponde à chave privada que está sob posse do Titular de Certificado.
Direitos sobre Identificadores de Objeto (OID) atribuídos à AC-JUS após o processo de credenciamento, cabem única e exclusivamente ao ITI, designado como a AC Raiz da ICP-Brasil.

3. IDENTIFICAÇÃO E AUTENTICAÇÃO

3.1 Registro Inicial

Neste item e nos seguintes a DPC descreve os requisitos e os procedimentos gerais utilizados pela AR-JUS, vinculada à AC-JUS, responsável no processo inicial de identificação dos solicitantes de certificado.
A AR-JUS realiza a autenticação da identidade de uma organização (item 3.1.8) e a autenticação da identidade de um indivíduo (item 3.1.9) por meio de, no mínimo, dois agentes de registro responsáveis pelo recolhimento e verificação da validade dos documentos apresentados.

3.1.1 Tipos de nomes

As AC de nível imediatamente subseqüente ao da AC-JUS, titulares de certificados de AC habilitada, terão um nome que as identifique univocamente no

âmbito da AC-JUS, no padrão ITU X.500, não incluindo no certificado o nome da pessoa física responsável pelo mesmo.
A AC-JUS segue as regras de identificação de nomes da AC Raiz da ICP-Brasil.

3.1.2 Necessidade de nomes significativos

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

3.1.3 Regras para interpretação de vários tipos de nomes

Item não aplicável.

3.1.4 Unicidade de nomes

Os identificadores "*Distinguished Name"* (DN) são únicos para cada AC de nível imediatamente subseqüente ao da AC-JUS. Para cada AC, números ou letras adicionais podem ser incluídos ao nome para assegurar a unicidade do campo, conforme o padrão ITU X.509.
A extensão "*Unique Identifiers*" não será admitida para diferenciar as AC com nomes idênticos.

3.1.5 Procedimento para resolver disputa de nomes

A AC-JUS reserva-se o direito de tomar todas as decisões referentes a disputas de nomes das AC de nível imediatamente subseqüente ao seu. Durante o processo de confirmação de identidade, a AC solicitante deve provar o seu direito de uso de um nome específico (DN) em seu certificado.

3.1.6 Reconhecimento, autenticação e papel de marcas registradas

De acordo com a legislação em vigor.

3.1.7 Método para comprovar a posse de chave privada

A confirmação que a entidade solicitante possui a chave privada correspondente à chave pública para a qual está sendo solicitado o certificado digital é realizada seguindo o padrão RFC 2510, item 2.3.

3.1.8 Autenticação da Identidade de uma organização

A confirmação da identidade de uma AC subordinada é feita com base nos "CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICP-BRASIL", conforme aprovados pela Resolução nº 6, de 22 de novembro de 2001, do Comitê Gestor da ICP.

A confirmação da identidade de pessoa jurídica responsável pela solicitação de certificado da AC subseqüente é feita mediante a apresentação dos seguintes documentos;

- Registro comercial, no caso de empresa individual:

- Ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais ou civis, e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores;
- Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ);
- Prova de inscrição no Cadastro Especifico do INSS (CEI), se aplicável.

A pessoa física responsável pela AC subordinada será identificada na forma descrita no item seguinte.

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.
A PC AC-JUS definirá os documentos exigidos com base nos requisitos aplicáveis estabelecidos pelo documento “Requisitos Mínimos para Certificados da ICP-Brasil”.

As solicitações de certificados, para a AC subordinada, devem ser realizadas por pessoa física legalmente responsável.

Cabe a AR-JUS verificar a autorização atribuída ao solicitante, bem como a presença dos documentos exigidos. Os procedimentos utilizados pela AR-JUS, para identificação e verificação da autorização do solicitante, estão descritos na PC AC-JUS.

Todos os documentos de identificação exigidos serão arquivados pela AR-JUS, conforme definido na PC AC-JUS.

O representante legal da AC subordinada assina o termo de titularidade denominado “Termo de Titularidade” e é, para todos os efeitos legais, titular do certificado emitido.
A pessoa física indicada como responsável pelo certificado assina o “Termo de Responsabilidade”.

Os Termos de Titularidade e de Responsabilidade serão mantidos junto à documentação exigida neste item.

Tanto a pessoa jurídica titular do certificado, como a pessoa física designada como responsável pelo certificado, serão responsáveis pela correta utilização deste, conforme as normas da ICP-Brasil, assim como pelos danos a que derem causa pelo uso indevido do certificado.

É mantido arquivo contendo o tipo e os detalhes do procedimento de identificação utilizado pela AR-JUS.

3.2 Geração de novo par de chaves antes da expiração do atual

Pode ser solicitado um novo certificado antes da expiração do atual, observando os mesmos requisitos e procedimentos exigidos inicialmente.

3.3 Criação de novo par de chaves após revogação

Após a revogação de seu certificado, uma AC deve executar os processos regulares de geração de novo par de chaves.

3.4 Solicitação de Revogação

A solicitação de revogação de certificado da AC-JUS será feita formalmente pelo representante da AC-JUS à AC-Raiz.
A solicitação de revogação de certificado de AC imediatamente subseqüente será feita formal pelo representante da AC imediatamente subseqüente, e com a presença física do mesmo, a fim de possibilitar a sua identificação inequívoca.

A solicitação de revogação poderá ainda ser feita por decisão judicial, ou determinação da AC-Raiz.

4. REQUISITOS OPERACIONAIS

4.1 Solicitação de Certificado

A solicitação de emissão de um Certificado Digital para Autoridade Certificadora Habilitada será feita mediante o formulário colocado à disposição do solicitante na página http://www.acjus.gov.br/acjus/acjus.crl, Toda referência a formulário será entendida também como referência a outras formas que a AC-JUS possa vir a adotar.

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

4) A comprovação de atributos de identificação constantes do certificado;
5) Para a aprovação de certificados a chave da AC-JUS é ativada com a presença de no mínimo 2 (dois) dos custodiantes da chave de ativação;
6) Assinatura do Termo de Titularidade e de Responsabilidade (item 3.1.9.1);

A solicitação de certificado para AC de nível imediatamente subseqüente ao da AC-JUS somente é possível após o deferimento do pedido de credenciamento e a respectiva autorização de funcionamento da AC em questão pela AC-Raiz.

Nesse caso, aquela AC deve encaminhar a solicitação de seu certificado à AC-JUS por meio de seus representantes legais, utilizando o padrão de solicitação de certificado PKCS#10 (Public Key Cryptographic Standards).

4.2 Emissão de Certificado

A emissão de um certificado pela AC-JUS é feita em cerimônia específica, com a presença dos representantes da AC-JUS, da AC habilitada, de auditores e convidados, na qual são registrados todos os procedimentos executados.

A AC-JUS garante que a cerimônia de emissão de um certificado para AC de nível imediatamente subseqüente ao seu ocorre em, no máximo, 10 (dez) dias úteis após a autorização de funcionamento da AC em questão pela AC-RAIZ.
A AC-JUS entrega o certificado emitido, em formato padrão PKCS#7, para os representantes legais da AC habilitada.
A emissão dos certificados das AC de nível imediatamente subseqüente à AC-JUS é feita em equipamentos que operam *off-line*.
O certificado é considerado válido a partir do momento de sua emissão.

4.3 Aceitação de Certificado

A AC de nível imediatamente subseqüente irá declarar, através de seus representantes legais, mediante assinatura do "Termo de Acordo", que aceita o certificado emitido. A aceitação implica que o solicitante reconhece a veracidade dos dados contidos no certificado. A PC correspondente detalha os procedimentos referentes à aceitação do certificado.

4.4 Suspensão e Revogação de Certificado

4.4.1 Circunstâncias para revogação

Um certificado de AC de nível imediatamente subseqüente ao da AC-JUS pode ser revogado a qualquer momento nas seguintes circunstâncias: por solicitação da AC titular do certificado, por decisão da AC-JUS , do CG da ICP-Brasil ou da AC Raiz.
Um certificado é obrigatoriamente revogado nas seguintes circunstâncias:

- quando constatada emissão imprópria ou defeituosa;
- quando for necessária a alteração de qualquer informação constante no mesmo;
- no caso de dissolução da AC titular do certificado;
- no caso de perda, roubo, modificação, acesso indevido ou comprometimento da chave privada correspondente ou da sua mídia armazenadora; ou
- por decisão judicial.

Em relação à revogação, deve ainda ser observado que:

- A AC-JUS revogará, no prazo definido no item 4.4.3, o certificado da entidade que deixar de cumprir as políticas, normas e regras estabelecidas pela ICP-Brasil;
- 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 revogação do certificado de uma AC de nível imediatamente subseqüente ao da AC-JUS somente pode ser feita:

- pela AC-JUS;
- pela AR-JUS;

- pela AC Titular do Certificado;
- pelo CG da ICP-Brasil;
- pela AC Raiz;
- **por decisão judicial**.

4.4.3 Procedimento para solicitação de revogação

A solicitação de revogação de certificado é feita através de formulário específico, disponível na página **http://www.acjus.gov.br/acjus/**, permitindo a identificação inequívoca do solicitante. Os agentes habilitados, conforme o item 4.4.2, podem a qualquer tempo solicitar a revogação de seus respectivos certificados. Os procedimentos detalhados de solicitação de revogação estão descritos na correspondente PC.

Como diretrizes gerais, fica estabelecido que:

- O solicitante da revogação de um certificado deve ser identificado;
- As solicitações de revogação, bem como as ações delas decorrentes deverão ser registradas e armazenadas;
- As justificativas para a revogação de um certificado são documentadas; e
- O processo de revogação de um certificado terminará com a geração e a publicação de uma LCR que contenha o certificado revogado.

O prazo limite para a conclusão do processo de revogação de certificado, após o recebimento da respectiva solicitação é de 24 (vinte e quatro) horas.

4.4.4 Prazo para solicitação de revogação

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

A PC implementada pela AC-JUS estabelece os prazos dentro dos quais a revogação do certificado poderá ser solicitada, sem ônus.

4.4.5 Circunstâncias para suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil, não sendo, portanto, admitida no âmbito da AC-JUS.

4.4.6 Quem pode solicitar suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil, não sendo, portanto, admitida no âmbito da AC-JUS.

4.4.7 Procedimento para solicitação de suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil, não sendo, portanto, admitida no âmbito da AC-JUS.

4.4.8 Limites no período de suspensão

A suspensão de certificados não é admitida no âmbito da ICP-Brasil, não sendo, portanto, admitida no âmbito da AC-JUS.

4.4.9 Freqüência de emissão de LCR

O prazo máximo admitido para a emissão de LCR referente a certificados de AC subordinadas é de 15 (quinze) dias.

Na revogação de certificado de AC de nível imediatamente subseqüente ao seu, a AC-JUS deverá emitir nova LCR no prazo máximo de 24 (vinte e quatro) horas e notificar todas as AC de nível imediatamente subseqüente ao seu.

São emitidas LCR na freqüência determinada na PC, mesmo quando não houver nenhuma mudança ou atualização, para assegurar a periodicidade da informação.

4.4.10 Requisitos para verificação de LCR

Todos os certificados revogados no domínio da AC-JUS são listados na LCR que pode ser acessada no endereço *web* contido no próprio certificado.
Todo certificado deve ter a sua validade verificada, na respectiva LCR, antes de ser utilizado.
Os números de série de certificados revogados, das AC de nível imediatamente subseqüente, aparecem na LCR emitida pela AC-JUS. Estes números permanecem nas LCR emitidas até a data de expiração dos certificados ser atingida, sendo removidos na primeira LCR emitida após essa data.

A autenticidade da LCR deve também ser confirmada por meio da verificação da assinatura da AC-JUS e do período de validade da LCR.

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

A AC-JUS não disponibiliza recursos para revogação ou verificação *on-line* de estado de certificados.

4.4.12 Requisitos para verificação de revogação *on-line*

A AC-JUS não disponibiliza diretório *on-line* ou um servidor de OCSP para verificar o estado dos certificados emitidos pela AC-JUS.

4.4.13 Outras formas disponíveis para divulgação de revogação

Informações de revogação de certificado de AC de nível imediatamente subseqüente ao da AC-JUS serão divulgadas por meio de sua publicação no Diário Oficial, Caderno III, Diário da Justiça e na página WEB **http://www.acjus.gov.br/acjus/.**

4.4.14 Requisitos para verificação de outras formas de divulgação de revogação

item não aplicável

4.4.15 Requisitos especiais para o caso de comprometimento de chave

No caso do comprometimento da chave privada de uma AC de nível imediatamente subseqüente ao da AC-JUS, a mesma deve notificar imediatamente à AC-JUS, solicitando a revogação de seu certificado, por meio de formulário específico disponibilizado pela AC-JUS em sua página *web*, http://www.acjus.gov.br/acjus/.

4.5 Procedimentos de Auditoria de Segurança

4.5.1 Tipos de Evento Registrados

Todas as ações executadas pelo pessoal da AC-JUS, no desempenho de suas atribuições, são registradas de modo que cada ação esteja associada à pessoa que a realizou.

A AC-JUS registra em arquivos para fins de auditoria todos os eventos relacionados à segurança do seu sistema de certificação, quais sejam:

- Iniciação e desligamento do sistema de certificação;
- Tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AC-JUS;
- Mudanças na configuração da AC-JUS ou nas suas chaves;
- Mudanças nas políticas de criação de certificados;
- Tentativas de acesso (*login*) e de saída do sistema (*logoff*);
- Tentativas não autorizadas de acesso aos arquivos de sistema;
- Geração de chaves próprias da AC-JUS ou de chaves de Titulares de Certificados;
- Emissão e revogação de certificados;
- Geração de LCR;
- Tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas, e de atualizar e recuperar suas chaves;
- Operações falhas de escrita ou leitura no repositório de certificados e da LCR, quando aplicável; e
- Operações de escrita nesse repositório, quando aplicável.

A AC-JUS registra, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo seu sistema de certificação, quais sejam:

- Registros de acessos físicos;
- Manutenção e mudanças na configuração de seus sistemas;
- Mudanças de pessoal e de perfis qualificados;
- Relatórios de discrepância e comprometimento; e
- Registros de destruição de meios de armazenamento contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuários.

Os registros de auditoria mínimos a serem mantidos pela AC-JUS incluem além dos acima:

- Registros de solicitação, inclusive registros relativos a solicitações rejeitadas;
- Pedidos de geração de certificado, mesmo que a geração não tenha êxito;
- Registros de solicitação de emissão de LCR.

Todos os registros de auditoria, eletrônicos ou manuais, contém a data e a hora do evento registrado e a identidade do agente que o causou.
Para facilitar os processos de auditoria, toda a documentação relacionada aos serviços da AC-JUS é armazenada, eletrônica ou manualmente, em local único, conforme a Política de Segurança da ICP-Brasil.

4.5.2 Freqüência de auditoria de registros (*logs*)

A auditoria de registro será realizada sempre que houver utilização do sistema de certificação.

Os registros de auditoria são analisados pelo pessoal operacional da AC-JUS. Todos os eventos significativos são explicados em relatório de auditoria de registros. Tal análise envolve uma inspeção breve de todos os registros verificando-se que 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-JUS mantém localmente, nas instalações do SERPRO, os seus registros de auditoria por pelo menos 2 (dois) meses e, subseqüentemente, faz o armazenamento da maneira descrita no item 4.6.

4.5.4 Proteção de registro (*log*) de Auditoria

Os equipamentos da AC-JUS, onde são gerados os diversos registros de sistemas pelo sistema operacional, banco de dados e aplicativo de AC, encontram-se fisicamente em um ambiente classificado como nível 4 de segurança.
A inspeção contínua dos diversos registros dos sistemas é feita por meio das ferramentas nativas do sistema operacional, do banco de dados e do aplicativo de AC, e estão disponíveis somente para leitura. Pode ser feita também por relatórios emitidos a partir destas ferramentas. Estes dados de auditoria são coletados e armazenados toda a vez que existir utilização do equipamento em uma sala de arquivos de nível de segurança 3.
Os registros de auditoria gerados eletrônica ou manualmente 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.

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

A AC-JUS executa procedimentos de backup de todo o sistema de certificação, sempre que houver utilização do mesmo, seguindo scripts previamente desenvolvidos para estas atividades.

4.5.6 Sistema de coleta de dados de auditoria

O sistema de coleta de dados de auditoria da AC-JUS é uma combinação de processos automatizados e manuais executados pelo sistema operacional, pelos

sistemas de certificação de AC-JUS, pelo sistema de controle de acesso e pelo pessoal operacional.

Tipo de evento	Sistema de coleção	Registrado por
Sucesso e fracasso de tentativas a mudanças nos parâmetros de segurança do sistema operacional	Automático	Sistema operacional
Início e parada de aplicação	Automático	Sistema operacional
Sucesso e fracasso de tentativas de *log-in* e *log-out*	Automático	Sistema operacional
Sucesso e fracasso de tentativas para criar, modificar, ou apagar contas de sistema	Automático	Sistema operacional
Sucesso e fracasso de tentativas para criar, modificar ou apagar usuários de sistemas autorizados	Automático	Sistema operacional
Sucesso e fracasso de tentativas para pedir, gerar, assinar, emitir ou revogar chaves e certificados	Automático	AC ou Software de AR
Sucesso e fracasso de tentativas para criar, modificar ou apagar informação de Titular de Certificado	Automático	Software de AR
Logs de *Backup* e restauração	Automático e manual	Sistema operacional e pessoal de operações
Mudanças de configuração de sistema	Manual	Pessoal de operações
Atualizações de *software* e *hardware*	Manual	Pessoal de operações
Manutenção de sistema	Manual	Pessoal de operações
Mudanças de pessoal	Manual	Pessoal de operações
Registros de acessos físicos	Automático e manual	*Software* de controle de acesso e pessoal de operações

4.5.7 Notificação de agentes causadores de eventos

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

4.5.8 Avaliações de vulnerabilidade

Uma Avaliação de Riscos de Segurança foi realizada para a AC-JUS. Esta avaliação cobre a incidência de riscos e ameaças que podem impactar na operação dos serviços de certificação.
Eventos que indiquem possível vulnerabilidade, detectados na análise dos registros de auditoria da AC-JUS, 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-JUS:

- solicitações de certificados;
- solicitações de revogação de certificados;
- notificações de comprometimento de chaves privadas;
- emissões e revogações de certificados;
- emissões de LCR;
- trocas de chaves criptográficas da AC-JUS;
- informações de auditoria previstas no item 4.5.1;
- correspondências formais;
- Processos de credenciamento de AC de nível imediatamente subseqüente ao da AC-JUS.

4.6.2 Período de retenção para arquivo

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

- as LCR referentes a certificados de assinatura digital são retidas por, no mínimo, período igual ao do arquivamento dos respectivos certificados;
- as demais informações são retidas por, no mínimo, 6 (seis) anos.

Períodos de retenção específicos são definidos nas PC implementadas pela AC-JUS, quando necessário.

4.6.3 Proteção de arquivos

Mídias de arquivos são guardadas em local seguro, sendo que a proteção criptográfica das mídias é adotada quando a classificação da informação assim o exigir. Também são protegidas de fatores ambientais como temperatura, umidade e magnetismo.

Todos os registros arquivados são classificados e armazenados com requisitos de segurança compatíveis com sua classificação, conforme a Política de Segurança da ICP-Brasil.

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

Uma segunda cópia de todo o material arquivado é armazenada em ambiente externo ao sistema de certificação da AC-JUS, protegido com nível 3 de segurança.

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

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

4.6.5 Requisitos para datação (*time-stamping*) de registros

Os servidores da AC-JUS são sincronizados com a hora GMT fornecida pelo Observatório Nacional. Todas as informações geradas que possuam alguma identificação de horário recebem o horário em GMT, inclusive os certificados emitidos por esses equipamentos.
No caso dos registros feitos manualmente, estes contêm a Hora Oficial do Brasil.

4.6.6 Sistema de coleta de dados de arquivo

O sistema de coleta de dados de arquivos da AC-JUS é uma combinação de processos automatizados e manuais executados pelo sistema operacional, pelos sistemas de certificação de AC e pelo pessoal operacional.

Tipo de evento	Sistema de coleção	Registrado por
Solicitações de certificados	Automático e manual	*Software* de AC/AR e pessoal de operações
Solicitações de revogação de certificados	Automático e manual	*Software* de AC/ARe pessoal de operações
Notificações de comprometimento de chaves privadas	Manual	Pessoal de operações
Emissões e revogações de certificados	Automático	*Software* de AC/AR
Emissões de LCR	Automático	*Software* de AC/AR
Correspondências formais	Manual	Pessoal de operações

4.6.7 Procedimentos para obter e verificar informação de arquivo

A integridade dos arquivos da AC-JUS e da AR-JUS é verificada:

- Na ocasião em que o arquivo é preparado;
- Semestralmente no momento de uma auditoria de segurança programada;
- Em qualquer outro momento quando uma auditoria de segurança completa é requerida.

Somente podem ter acesso às informações de arquivo da AR-JUS:

- Pessoas corretamente identificadas e devidamente autorizadas, por meio de instrumento devidamente constituído, conforme definido no item 2.8.5;
- Titulares de Certificados, ou seus representantes legais, mediante solicitação formal, conforme definido no item 2.8.6.

4.7 Troca de chave

A AC-JUS comunica através de oficio, com 90 dias de antecedência, à AC subseqüente o vencimento do seu certificado, junto com as informações necessárias para a solicitação de uma nova chave.

4.8 Comprometimento e Recuperação de Desastre

A AC-JUS:

Estabelece e mantém documentação detalhada composta por:

- Plano de Contingência, incluindo o comprometimento de chaves, *hardware*, *software,* falhas de comunicações, e desastres naturais como fogo e inundação;
- Padrões de configuração, incluindo sistema operacional, *software* de anti-vírus e programas aplicativos específicos;
- Procedimentos de *backup*, arquivamento e armazenamento externo de segurança;
- Provê a documentação a pedido:
- do CG da ICP-Brasil, quando da auditoria de práticas de DPC;
- de pessoas que administram a segurança ou auditoria de conformidade;
- Provê treinamento apropriado a todo pessoal pertinente em contingência e procedimentos de recuperação de desastre.

4.8.1 Recursos computacionais, *software* ou dados corrompidos

A AC-JUS possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso em que recursos computacionais, *software* e/ou dados são corrompidos, e que podem ser resumidas no seguinte:

- É feita a identificação de todos os elementos corrompidos;
- O instante do comprometimento é determinado e é crítico para invalidar as transações executadas após aquele instante;
- 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-JUS.

4.8.2 Certificado de entidade revogado

A AC-JUS possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso em que o certificado da AC-JUS é revogado, e que podem ser resumidas da seguinte forma:

1. m caso de revogação do certificado da AC-JUS, após a identificação do incidente, são notificados os gestores do processo de certificação digital, que acionam as equipes envolvidas, de forma a indisponibilizar temporariamente os serviços de autoridade certificadora. Na confirmação do incidente, são revogados os certificados das AC de nível imediatamente subseqüente, é gerado o novo par de chaves da AC-JUS, sendo emitido, pela AC Raiz, certificado associado ao novo par de chaves gerado e emitidos, pela AC-JUS, novos certificados digitais para as AC de nível imediatamente subseqüente.

4.8.3 Chave de entidade comprometida

A AC-JUS possui um Plano de Continuidade de Negócio que especifica as ações a serem tomadas no caso em que a chave privada da AC-JUS é comprometida, e que podem ser resumidas nas ações listadas a seguir:

1) m caso de comprometimento da chave da AC-JUS, após a identificação da crise, são notificados os gestores do processo de certificação digital, que acionam as equipes envolvidas, de forma a indisponibilizar temporariamente os serviços de autoridade certificadora. Na confirmação do incidente, são revogados os certificados da AC-JUS e das AC de nível imediatamente subseqüente. É gerado, então, um novo par de chaves e emitido, pela AC Raiz, certificado associado ao novo par de chaves gerado e emitidos, pela AC-JUS, novos certificados digitais para as AC de nível imediatamente subseqüente.

4.8.4 Segurança dos recursos após desastre natural ou de outra natureza

A AC-JUS possui um Plano de Continuidade de Negócio 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-JUS quando a operação de sistemas é significativamente e adversamente abalada por fogo, greves, etc.
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-JUS faz parte. Isto significa que o plano deve ter como meta primária, restabelecer a AC-JUS para tornar acessível os registros lógicos mantidos dentro do *software*. Serão tomadas as ações de recuperação aprovadas dentro do plano, segundo uma ordem de prioridade.

4.9 Extinção da AC-JUS ou AR-JUS

Quando for necessário encerrar as atividades da AC-JUS ou da AR-JUS, o impacto deste término deve ser minimizado da melhor forma possível tendo em vista as circunstâncias prevalecentes. Isto inclui:

- Prover com maior antecedência possível notificação para:
- a AC Raiz da ICP-Brasil;
- todas as entidades subordinadas.
- A transferência progressiva do serviço e dos registros operacionais, para um sucessor, que deverá observar os mesmos requisitos de segurança exigidos para a AC-JUS ou para a AR-JUS extinta;
- Preservar qualquer registro não transferido a um sucessor.

As chaves públicas dos certificados emitidos pela AC-JUS, dissolvida, serão armazenadas por outra AC, após aprovação da AC Raiz.
Quando houver mais de uma AC interessada, assumirá a responsabilidade do armazenamento das chaves públicas, aquela indicada pela AC-JUS.

A AC-JUS, 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.

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 Pessoas

5.1 Controle Físico

5.1.1 Construção e localização das instalações

A operação da AC-JUS é executada dentro de um ambiente físico seguro em área de instalação altamente protegida.

Os componentes do sistema de certificação utilizados para a operação da AC-JUS estão situados nas instalações **do SERPRO Rio de Janeiro, Horto.**

A localização e o sistema de certificação utilizado para a operação da AC-JUS 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. Nenhuma das linhas telefônicas dentro do ambiente de certificação da AC oferece suporte a modems

Alguns aspectos de construção das instalações da AC-JUS relevantes para os controles de segurança física são descritos abaixo. Outros detalhes estão descritos no restante do item 5.1.

- 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, instalações para sistemas de telecomunicações e sistema de aterramento e de proteção contra descargas atmosféricas, foram executadas por técnicos especializados para garantir a proteção física da AC-JUS.

5.1.2 Acesso físico

O acesso físico às dependências da AC-JUS é gerenciado e controlado internamente conforme o previsto na Política de Segurança da AC-JUS. Chaves, senhas, cartões, identificações biométricas ou outros dispositivos são utilizados para controle de acesso.

O acesso físico é monitorado e o seu controle assegura que apenas pessoas autorizadas participem das atividades pertinentes.

O sistema de certificação da AC-JUS está situado em uma sala-cofre. Segurança patrimonial e controles de segurança biométricos restringem o acesso aos equipamentos da sala-cofre.

5.1.2.1 Níveis de Acesso

São implementados 4 (quatro) níveis de acesso físico aos diversos ambientes onde estão instalados os equipamentos utilizados na operação da AC-JUS, e mais 2 (dois) níveis relativos à proteção da chave privada de AC.

O primeiro nível – ou nível 1 – Situa-se após a primeira barreira de acesso às instalações da AC-JUS. 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-JUS transitam devidamente identificadas e acompanhadas. Nenhum tipo de processo operacional ou administrativo da AC-JUS é executado nesse nível.
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-JUS, em níveis superiores ao nível 1. A partir desse nível, equipamentos de gravação, fotografia, telefones celulares, *pagers*, vídeo, som ou similares, bem como computadores portáteis, tem sua entrada controlada e somente podem ser utilizados mediante autorização formal e supervisão.

O segundo nível – ou nível 2 – é interno ao primeiro nível. A passagem do primeiro para o segundo nível exige identificação das pessoas autorizadas por meio eletrônico, e o uso de crachá. Esse é o nível mínimo de segurança requerido para a execução de qualquer processo operacional ou administrativo da AC-JUS.

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-JUS. 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 estejam envolvidas com essas atividades não podem permanecer nesse nível se não estiverem devidamente autorizadas, identificadas e acompanhadas por pelo menos um funcionário que tenha esta permissão.
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.

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

O quarto nível - ou nível 4 – é interno ao terceiro nível, é aquele no qual ocorrem atividades especialmente sensíveis de operação da AC-JUS, 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.
No quarto nível todas as paredes, o piso e o teto são revestidos de aço e concreto. As paredes, piso e o teto são inteiriços, 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.
A sala cofre é construída segundo as normas brasileiras aplicáveis. Eventuais omissões dessas normas devem ser sanadas por normas internacionais pertinentes.
São dois os ambientes de quarto nível abrigados pela sala cofre:

- Sala de equipamentos de produção *off-line* e cofre de armazenamento.

No quarto 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: algum tipo de identificação individual, como cartão eletrônico, e identificação biométrica.

O quinto nível – ou nível 5 – é interno aos ambientes de nível 4, e compreende cofres e gabinetes trancados. Materiais criptográficos tais como chaves, dados de ativação, suas cópias e equipamentos criptográficos são armazenados em nível 5 ou superior.
Para garantir a segurança do material armazenado, o cofre ou o gabinete obedecem às seguintes especificações mínimas:

- Ser feito em aço ou material de resistência equivalente;
- Possuir tranca com chave.

O sexto nível – ou nível 6 - consiste de pequenos depósitos localizados no interior do cofre ou gabinete de quinto nível, ou hardware criptográfico. Cada um desses depósitos dispõe de fechadura individual. A chave privada da AC-JUS esta armazenada em um desses depósitos quando não estiver em operação. Quando em operação, a chave privada da AC-JUS é armazenada em cartões criptográfico, em gabinete de nível 5.

5.1.2.2 Sistema físico de detecção

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.

As mídias de vídeo resultantes da gravação 24x7 são armazenadas por, no mínimo, um ano. Elas são testadas (verificação de trechos aleatórios no início, meio e final da fita) pelo menos a cada 3 (três) meses, com a escolha de, no mínimo, uma fita referente a cada semana. Essas fitas são armazenadas em ambiente de terceiro nível.
Todas as portas de passagem entre os níveis de acesso 3 e 4 do ambiente são monitoradas por sistema de notificação de alarmes. O sistema de notificação de alarmes utiliza 2 (dois) meios de notificação: sonoro e visual.
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.
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.

5.1.2.4Mecanismos de emergência

Mecanismos específicos foram implantados para garantir a segurança do pessoal e dos equipamentos da AC-JUS 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.
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

A AC-JUS possui sistema de fornecimento de energia sobressalente. Em caso de falta de energia, a AC-JUS funciona temporariamente utilizando no-breaks com autonomia suficiente para casos onde é necessário o acionamento do gerador de apoio, que funciona durante o tempo da falta de energia.

A área de operações segura da AC-JUS, nível 3 em diante, é conectada a uma fonte de energia padrão. Todos os componentes críticos são conectados a provisão de energia ininterrupta (UPS), prevenindo paradas anormais no caso de uma deficiência de força, de forma a atender os requisitos de disponibilidade dos sistemas da AC-JUS e seus respectivos serviços. Um sistema de aterramento está implantado.
A área de operações segura da AC-JUS, nível 3 em diante, tem um sistema de ar condicionado para controlar o calor e umidade que é independente do sistema de ar condicionado de edifício.
Todos os cabos elétricos são protegidos por tubulações ou dutos apropriados. 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.
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.
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. Qualquer modificação nessa rede é previamente documentada.
Não são admitidas instalações provisórias, fiações expostas ou diretamente conectadas às tomadas sem a utilização de conectores adequados.
O sistema de climatização atende aos requisitos de temperatura e umidade exigidos pelos equipamentos utilizados no ambiente e dispõe de filtros de poeira. Nos ambientes de nível 4, o sistema de climatização é independente e tolerante à falhas.
A temperatura dos ambientes atendidos pelo sistema de climatização é permanentemente monitorada pelo sistema de notificação de alarmes.
O sistema de ar condicionando dos ambientes de nível 4 é interno, com troca de ar realizada apenas por abertura da porta.

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

- Geradores de porte compatível;
- Geradores de reserva, do mesmo porte dos citados no nível 1;
- Sistemas de *no-breaks* redundantes;
- Sistemas redundantes de ar condicionado.

5.1.4 Exposição à água

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

Todas as instalações da AC-JUS possuem sistemas de prevenção contra incêndio.
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 sobre-aquecimento de materiais elétricos e outros materiais combustíveis presentes nas instalações.
Nas instalações da AC-JUS não é permitido fumar ou portar objetos que produzam fogo ou faísca.
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 esta fechada.
Em caso de incêndio nas instalações da AC-JUS, 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

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

5.1.7 Destruição de lixo

Documentos em papel e demais mídias não em papel que contêm elementos confidenciais da AC-JUS, informações comercialmente sensíveis ou confidenciais são eliminadas seguramente:

- No caso de mídia magnéticas:
  - Por desmagnetização e destruição completa do recurso;
- No caso de documentos em papel: pela trituração antes de ir para o lixo.
- No caso de outras mídias: pela destruição completa do recurso.

5.1.8 Instalações de segurança (*backup*) externas (*off-site*)

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 (quarenta e oito) horas.

5.2 Controles Procedimentais

5.2.1 Perfis qualificados

A separação das tarefas para funções críticas é uma prática adotada, com o intuito de evitar que um funcionário utilize indevidamente o sistema de certificação sem ser detectado. Um exemplo desta prática é que as pessoas que executam atividades de examinar registros de sistema, ou examinar *logs* de auditoria não são as mesmas pessoas envolvidas na atividade que gerou estes registros e *logs*, assegurando que as pessoas que executam estão agindo dentro das responsabilidades e dentro da política de segurança declarada.
Isto é realizado criando perfis separados e contas na estação de trabalho de serviço. Cada perfil possui uma quantia limitada de capacidade operacional. Este método permite um sistema de "verificações e equilíbrio" a ocorrer entre os vários perfis. Os seguintes perfis foram estabelecidos pela AC-JUS:

- Gerente da AC;
- Administrador de Segurança;
- Administrador de Banco de Dados;
- Administrador do Sistema de Gerenciamento de Certificados;
- Administrador do Servidor *web*;
- Administrador do Sistema Operacional;
- Administrador do Security Server;
- Administrador de AC;
- Operador;
- Segurança patrimonial;
- Apoio administrativo.

Todos os operadores do sistema de certificação 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.
Quando um funcionário se desliga da AC-JUS, suas permissões de acesso são revogadas imediatamente. Quando há mudança na posição ou função que o funcionário ocupa com relação à AC-JUS, são revistas suas permissões de acesso. Os termos de responsabilidade assinados pelo funcionário contém a descrição de todos os recursos, antes disponibilizados, que o funcionário deverá devolver à AC-JUS no ato de seu desligamento.

5.2.2 Número de pessoas necessário por tarefa

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

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

5.2.3 Identificação e autenticação para cada perfil

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

- Ser incluído em uma lista de acesso às instalações da AC-JUS;
- Ser incluído em uma lista para acesso físico ao sistema de certificação da AC-JUS;
- Receber um certificado para executar suas atividades operacionais na AC-JUS;
- Receber uma conta no sistema de certificação da AC-JUS.

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

- São diretamente atribuídos a um único operador (funcionário da AC-JUS devidamente qualificado);
- Não são compartilhados;
- São restritos às ações associadas ao perfil para o qual foram criados.

A AC-JUS 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, juntamente com procedimentos de validação dessas senhas.

5.3 Controles de Pessoal

Todos os funcionários da AC-JUS e da AR-JUS, encarregados de tarefas operacionais, tem registrado em contrato ou termo de responsabilidade:

- Os termos e as condições do perfil que ocupam;
- O compromisso de observar as normas, políticas e regras aplicáveis da AC-JUS;
- O compromisso de observar as normas, políticas e regras aplicáveis da ICP-Brasil;
- O compromisso de não divulgar informações sigilosas a que tenham acesso;
- Investigação psico-social;
- Caso servidor público, histórico de processos administrativos.

5.3.1 Antecedentes, qualificação, experiência e requisitos de idoneidade

Todo o pessoal da AC-JUS envolvido 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-JUS e na Política de Segurança da ICP-Brasil.

5.3.2 Procedimentos de Verificação de Antecedentes

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

- Verificação de antecedentes criminais;
- Verificação de situação de crédito;
- Verificação de histórico de empregos anteriores;
- Comprovação de escolaridade e de residência;
- Investigação psico-social;
- Caso servidor público, histórico de processos administrativos.

5.3.3 Requisitos de treinamento

Todo o pessoal da AC-JUS e das ARs vinculadas, envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados recebe treinamento documentado, suficiente para o domínio dos seguintes temas:

- Princípios e mecanismos de segurança da AC-JUS e das AR vinculadas;
- Sistema de certificação em uso na AC-JUS;
- Procedimentos de recuperação de desastres e de continuidade do negócio;
- Outros assuntos relativos a atividades sob sua responsabilidade.

5.3.4 Freqüência e requisitos para reciclagem técnica

Todo o pessoal da AC-JUS e das ARs 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-JUS. Treinamentos de reciclagem são realizados pela AC-JUS sempre que necessário.

5.3.5 Freqüência e seqüência de rodízios de cargos

A AC-JUS não implementa rodízio de cargos.

5.3.6 Sanções para ações não autorizadas

Na eventualidade de uma ação não autorizada, real ou suspeita, realizada por pessoa responsável por processo de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, a AC-JUS suspende o seu acesso ao sistema de certificação e toma as medidas administrativas e legais cabíveis.

5.3.7 Requisitos para contratação de pessoal

O pessoal da AC-JUS e das AC de nível imediatamente subseqüente, no exercício de atividades diretamente relacionadas com os processos de emissão, expedição,

distribuição, revogação e gerenciamento de certificados, ser contratado conforme o estabelecido na Política de Segurança da ICP Brasil.

5.3.8 Documentação disponibilizada ao pessoal

A AC-JUS disponibiliza para todo o seu pessoal, para o das AC de nível imediatamente subseqüente e para a AR vinculada :

- Esta DPC;
- A PC que implementa;
- A Política de Segurança da ICP-Brasil;
- A Política de Segurança da AC-JUS;
- Documentação de hardware e software relativa à função desempenhada;
- Documentação operacional relativa às suas atividades;
- Contratos, normas e políticas relevantes para suas atividades.

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

6. Controles Técnicos de Segurança

6.1 Geração e Instalação do Par de chaves

6.1.1 Geração do Par de Chaves

O par de chaves da AC-JUS é gerado pela própria AC-JUS, em módulo criptográfico de hardware com padrão de segurança FIPS 140-1 level 2 ou superior, utilizando algorítmo RSA para geração do par de chaves e algorítmo 3-DES para sua proteção, após o deferimento do pedido de credenciamento da mesma e a conseqüente autorização de funcionamento no âmbito da ICP-Brasil.

O par de chaves criptográficas de uma AC de nível imediatamente subseqüente ao da AC-JUS é gerado pela própria AC, após o deferimento do pedido de credenciamento e habilitação da mesma, e a conseqüente autorização de funcionamento no âmbito da ICP-Brasil. Os procedimentos específicos estão descritos na PC implementada.

As PC implementadas pela AC-JUS e pelas AC subordinadas definem o meio utilizado para armazenamento das respectivas chaves privadas, com base nos requisitos aplicáveis estabelecidos pelo documento “Requisitos Mínimos para Políticas de Certificado na ICP-Brasil”, aprovados pela Resolução no 7, de 12 de dezembro de 2001, do Comitê Gestor da ICP-Brasil.

6.1.2 Entrega da chave privada à entidade titular

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

Para a entrega de sua chave pública à AC Raiz, encarregada da emissão de seu certificado, a AC-JUS fará uso do padrão PKCS#10, em data e hora previamente estabelecidos pela AC-Raiz da ICP-Brasil.

Os procedimentos para a entrega da chave pública de um solicitante de certificado à AC-JUS estão detalhados na PC implementada.

6.1.4 Disponibilização de chave pública da AC-JUS para usuários

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

- Formato PKCS#7 (RFC 2315), que inclui toda a cadeia de certificação, no momento da disponibilização de um certificado para seu titular;
- Diretório;
- Página *web* da AC–JUS (http://www.acjus.gov.br/acjus/);
- Outros meios seguros aprovados pelo CG da ICP-Brasil.

6.1.5 Tamanhos de chave

O tamanho das chaves criptográficas associadas a certificados emitidos pela AC-JUS será de, no mínimo 2048 (dois mil e quarenta e oito) bits, conforme estabelecido pela ICP-Brasil para chaves criptográficas associadas a certificados de AC.

6.1.6 Geração de parâmetros de chaves assimétricas

Os parâmetros de geração de chaves assimétricas da AC-JUS seguem o padrão FIPS (*Federal Information Processing Standards*) 140-1[1] *level* 2 ou superior, uma vez que utilizam *hardware* criptográfico com esta certificação.

6.1.7 Verificação da qualidade dos parâmetros

A verificação dos parâmetros de geração de chave é feita de acordo com as normas estabelecidas pelo CMVP (*Cryptographic Module Validation Program*) do NIST (*National Institute of Standards and Technology*), uma vez que o *hardware* utilizado é certificado pelo NIST como FIPS 140-1 *level* 2 ou superior.

6.1.8 Geração de chave por *hardware ou software*

O processo de geração do par de chaves da AC-JUS é feito por hardware padrão FIPS (Federal Information Processing Standards) 140-1, level 3.
A PC implementada pela AC-JUS caracteriza o processo utilizado para a geração de chaves criptográficas das AC de nível imediatamente subseqüente ao seu, com base nos requisitos aplicáveis estabelecidos pelo documento “Requisitos Mínimos para Políticas de Certificado na ICP-Brasil”, aprovados pela Resolução nº 7, de 12 de dezembro de 2001, do Comitê Gestor da ICP-Brasil.

[1] FIPS 140-1 – *Federal Information Processing Standards* 140-1. Esse padrão será substituído pelo FIPS 140-2, hoje em fase de implantação por parte do National Institute of Standards and Technology.

6.1.9 Propósitos de uso de chave (conforme campo “Key usage” na X.509 v3)

A chave privada da AC-JUS é utilizada apenas para a assinatura dos certificados por ela emitidos e de suas LCR.
As chaves privadas dos titulares de certificados emitidos pela AC-JUS são utilizadas apenas para a assinatura dos certificados por ela emitidos e de suas LCR.

6.2 Proteção da Chave Privada

A chave privada da AC-JUS é gerada, armazenada e utilizada apenas em hardware criptográfico específico, classificado como FIPS 140-1 level 2, não havendo portanto tráfego da mesma em nenhum momento.

6.2.1 Padrões para módulo criptográfico

Toda a geração e armazenamento da chave da AC-JUS, e também operações de assinatura de certificados pela AC-JUS, são realizadas em um módulo de *hardware* criptográfico classificado como FIPS 140-1 Nível 3.

O padrão requerido para os módulos de geração de chaves criptográficas das AC de nível imediatamente subseqüente ao da AC-JUS é o FIPS 140-1 Nível 2.

6.2.2 Controle “n de m’ para chave privada

A chave criptográfica de ativação do componente seguro de hardware que armazena a chave privada da AC-JUS é dividida em “6” partes e distribuídas por “6” custodiantes designados pela AC-JUS (m), É necessária a presença de no mínimo “2” custodiantes (n) para a ativação do componente e a consequente utilização da chave privada.

6.2.3 Recuperação (*escrow*) de chave privada

Não é permitida, no âmbito da ICP-Brasil, a recuperação (*escrow*) de chaves privadas, das AC de nível imediatamente subseqüente.

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

A AC-JUS 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 e aprovado pelo CG da ICP-Brasil, e mantida pelo prazo de validade do certificado correspondente.
A AC-JUS não mantém cópia de segurança das chaves privadas das AC de nível imediatamente subseqüentes ao seu.
Qualquer entidade titular de certificado pode, a seu critério, manter cópia de sua própria chave privada.
A cópia de segurança deve ser armazenada, cifrada, por algoritmo simétrico como 3-DES, IDEA, SAFER+, ou outros aprovados pelo CG da ICP-Brasil, e protegida com um nível de segurança não inferior àquele definido para a chave original.

6.2.5 Arquivamento de chave privada

As chaves privadas dos titulares de certificados emitidos pela AC-JUS não são arquivadas.

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-JUS é inserida no módulo criptográfico de acordo com o estabelecido na RFC 2510.

6.2.7 Método de ativação de chave privada

A ativação da chave privada da AC-JUS é implementada por meio de cartões criptográficos, protegidos com senha, após a identificação de "2" de "6" dos *custodiantes* da chave de ativação da chave criptográfica. Os *custodiantes* da chave privada serão magistrados ou servidores do Poder Judiciário Federal indicados pelo Comitê Gestor da AC-JUS. As senhas obedecem à política de senhas estabelecida pela AC-JUS.

6.2.8 Método de desativação de chave privada

A chave privada da AC-JUS, armazenada em módulo criptográfico é desativada, quando não mais 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 "6" dos *custodiantes* da chave de ativação da chave criptográfica. As senhas obedecem à política de senhas estabelecida pela AC-JUS.

6.2.9 Método de destruição de chave privada

Além do estabelecido no item 6.2.8 desta DPC, todas as cópias de segurança da chave privada da AC–JUS e os cartões criptográficos dos custodiantes,serão destruídos pelos administradores da AC-JUS.

As mídias de armazenamento das chaves privadas serão reinicializadas de forma a não restarem nelas informações sensíveis.

6.3 Outros Aspectos do Gerenciamento do Par de Chaves

6.3.1 Arquivamento de chave pública

As chaves públicas da AC-JUS, e dos certificados por ela emitidos, são armazenadas, após a expiração dos certificados correspondentes, por no mínimo 30 (trinta) anos, na forma da legislação em vigor, para verificação de assinaturas geradas durante seu período de validade.

6.3.2 Períodos de uso para as chaves pública e privada

A chave privada da AC-JUS é utilizada apenas durante o período de validade do certificado correspondente., cujo prazo máximo é de 8 anos. A chave pública da AC-JUS 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.
Os certificados emitidos pela AC-JUS para as AC´s de nível imediatamente subseqüente ao seu terão validade de no máximo 5 anos.

6.4 Dados de ativação

6.4.1 Geração e instalação dos dados de ativação

São necessários as presenças de no mínimo dois custodiantes, com os cartões criptográficos e senha de ativação do módulo criptográfico.

6.4.2 Proteção dos dados de ativação.

Os dados de ativação são protegidos por cartões criptográficos individuais com senha, e são armazenados em ambiente de nível 6 de segurança.

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

A AC-JUS garante que a geração de seu par de chaves é realizada em ambiente *off-line,* para impedir o acesso remoto não autorizado.
Os computadores servidores, utilizados pela AC-JUS e pelas AC subordinadas, relacionados diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, implementam, entre outras, as seguintes características:

- Controle de acesso aos serviços e perfis da AC-JUS;
- Separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC-JUS;
- Acesso restrito aos bancos de dados da AC-JUS;
- Uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações;
- Geração e armazenamento de registros de auditoria da AC-JUS;
- Mecanismos internos de segurança para garantia da integridade de dados e processos críticos; e
- Mecanismos para cópias de segurança (*backup*).

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

Qualquer equipamento, ou parte deste, ao ser enviado para manutenção tem as informações sensíveis nele contidas apagadas 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 residem os equipamentos utilizados para operação da AC-JUS ou da AC subordinada, o equipamento que passou por manutenção é inspecionado. Em todo equipamento que deixar de ser utilizado em caráter permanente, são destruídas de maneira definitiva todas as informações sensíveis armazenadas, relativas à atividade da AC-JUS ou AC subseqüente. Todos esses eventos são registrados para fins de auditoria.
Qualquer equipamento incorporado à AC-JUS ou às AC subseqüente, 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 AC-JUS aplica configurações de segurança conforme recomendações do SANS INSTITUTE. Também são seguidas as recomendações de segurança do ITSEC que avaliou a plataforma da solução implementada.

6.6 Controles Técnicos do Ciclo de Vida

6.6.1 Controles de desenvolvimento de sistemas

A AC-JUS adota sistema de certificação do SERPRO (Serviço Ferderal de Processamento de Dados), desenvolvido em código aberto, todas as customizações são realizadas inicialmente em um ambiente de desenvolvimento e após a conlusão dos testes é colocado em um ambiente de homologação. Finalizando o processo de homologação das customizações, é encaminhado um pedido para a "Gerência de Mudança" que avalia e decide quanto à implementação no ambiente de produção.

6.6.2 Controle de gerenciamento de segurança

A administração de segurança de sistema é controlada pelos privilégios nomeados a contas de sistema operacional, e pelos papéis confiados descritos no item 5.2.1.

O gerenciamento de configuração, para a instalação e a contínua manutenção do sistema de certificação utilizado pela AC-JUS, envolve o teste de mudanças planejadas no Ambiente de Desenvolvimento e Homologação isolados antes de sua implantação no ambiente de Produção, incluindo as seguintes atividades:

- Instalação de novas versões ou de atualizações nos produtos que constituem a plataforma do sistema de certificação;
- Implantação ou modificação de Autoridades Certificadoras com customizações a nível de certificados, páginas web, scripts, etc.;
- Implantação de novos procedimentos operacionais relacionados com a plataforma de processamento incluindo módulos criptográficos; e
- Instalação de novos serviços na plataforma de processamento.

6.6.3 Classificação de segurança de ciclo de vida

Este item não se aplica.

6.7 Controles de Segurança de Rede

Este item não se aplica.

6.8 Controles de Engenharia do Módulo Criptográfico

O módulo criptográfico utilizado pela AC-JUS para o armazenamento de sua chave privada é certificado como FIPS (*Federal Information Processing Standards*) 140-1, *level* 3.

Ao ser gerada, a chave privada da entidade titular é gravada cifrada, por algoritmo simétrico como 3-DES, IDEA, SAFER+ ou outros aprovados pelo CG da ICP-Brasil, em hardware criptográfico aprovado pelo CG da ICP - Brasil.
O meio de armazenamento da chave privada assegura, por meios técnicos e procedimentais adequados, no mínimo, que:

- a chave privada utilizada na geração de uma assinatura é única e seu sigilo é suficientemente assegurado;
- a chave privada utilizada na geração de uma assinatura não pode, com uma segurança razoável, ser deduzida e que está protegida contra falsificações realizadas através das tecnologias atualmente disponíveis;
- a chave privada utilizada na geração de uma assinatura pode ser eficazmente protegida pelo legítimo titular contra a utilização por terceiros.

Esse meio de armazenamento não modifica os dados a serem assinados, nem impede que esses dados sejam apresentados ao signatário antes do processo de assinatura.

7. Perfis de Certificado e LCR

7.1 Perfil do Certificado

Todos os certificados emitidos pela AC-JUS estão em conformidade com o formato definido pelo padrão ITU X.509.

7.1.1 Número(s) de versão

Todos os certificados emitidos pela AC-JUS implementam a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 2459.

7.1.2 Extensões de certificados

Os certificados emitidos pela AC-JUS, sob a PC AC-JUS, obedecem às resoluções da ICP-Brasil, que define como obrigatórias as seguintes extensões para certificados de AC:

- "*Authority Key Identifier*", não crítica: o campo keyIdentifier contém o resumo SHA-1 da chave pública da AC-JUS;
- "*Subject Key Identifier*", não crítica: contém o *hash* SHA-1 da chave pública da AC titular do certificado;

- "*Key Usage*", crítica: somente os bits e keyCertSign e cRLSign são ativados;
- "*Certificate Policies*", não crítica:
  - o campo policyIdentifier contém o OID das PC que a AC titular do certificado implementa;
  - o campo policyQualifiers contém o endereço *URL* da página *web, http://www.acjus.gov.br/acjus/dpcacjus.pdf,* onde se obtém a DPC da AC-JUS;
- O "Basic Constraints", crítica: contém o campo CA=TRUE;
- "*CRL Distribution Points*", não crítica: contém o endereço *URL* da página *web, http://www.acjus.gov.br/acjus/acjus.crl,* onde se obtém a LCR da AC-JUS.

7.1.3 Identificadores de algoritmos

Os certificados emitidos pela AC-JUS são assinados com o uso do algoritmo RSA com SHA-1 como função *hash* (OID = 1.2.840.113549.1.1.5), conforme o padrão PKCS#1 (RFC 2313).

7.1.4 Formatos de nome

Para os certificados emitidos sob a PC AC-JUS, o nome da AC titular do certificado, constante do campo "*Subject*", adota o "*Distinguished Name"* (DN) do padrão ITU X.500/ISO 9594, da seguinte forma:

C= BR
O= ICP-Brasil
OU= **Conselho da Justiça Federal - CJF**
CN= nome da AC

7.1.5 Restrições de nome

As restrições aplicáveis para os nomes dos titulares de certificados emitidos pela AC-JUS são as seguintes:

- não serão utilizados sinais de acentuação, tremas ou cedilhas;
- além dos caracteres alfanuméricos, podem ser utilizados somente os seguintes
  caracteres especiais:

Caractere	Código NBR9611 (hexadecimal)
Branco	20
!	21
"	22
#	23
$	24

%	25
&	26
'	27
(	28
)	29
*	2A
+	2B
,	2C
-	2D
.	2E
/	2F
:	3A
;	3B
=	3D
?	3F
@	40
\	5C

7.1.6 OID (Object Identifier) de DPC

O Identificador de Objeto (OID) desta DPC, atribuído pela ICP-Brasil para a AC-JUS após conclusão do processo de seu credenciamento, é 2.16.76.1.1.19.

7.1.7 Uso da extensão "Policy Constraints"

Não se aplica

7.1.8 Sintaxe e semântica dos qualificadores de política

O campo policyQualifiers da extensão "Certificate Policies" contém o endereço *web* da DPC da AC-JUS, http://www.acjus.gov.br*/acjus/dpcacjus.pdf.*

7.1.9 Semântica de processamento para extensões criticas

Extensões críticas são interpretadas, no âmbito da AC-JUS, conforme a RFC 2459.

7.2 Perfil de LCR

7.2.1 Número (s) de versão

As LCR geradas pela AC-JUS implementam a versão 2 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 2459.

7.2.2 Extensões de LCR e de suas entradas

A AC-JUS adota as seguintes extensões de LCR definidas como obrigatórias pela ICP-Brasil:

- "*Authority Key Identifier*": contém o resumo SHA-1 da chave pública da AC-JUS.
- "*CRL Number*", não crítica: contém número seqüencial para cada LCR emitida.

8. Administração de Especificação

8.1 Procedimentos de mudança de especificação

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

8.2 Políticas de publicação e de notificação

A AC-JUS publica esta DPC, em sua página *web* acessível pela URL http://www.acjus.gov.br/acjus/dpcacjus.pdf. Sempre que esta DPC for atualizada será alterado o arquivo disponibilizado na *web*.

8.3 Procedimentos de aprovação

Essa DPC foi submetida à aprovação da AC-RAIZ da ICP-Brasil, durante o processo de credenciamento da AC-JUS, conforme o determinado pelo documento "Critérios e Procedimentos para Credenciamento das Entidades Integrantes da ICP-Brasil".

Política de Segurança

da

Autoridade Certificadora

do

Sistema Justiça Federal

PS AC-JUS

POLÍTICA DE SEGURANÇA DA AC-JUS

1. INTRODUÇÃO:

1.1. Este documento tem por finalidade estabelecer as diretrizes de segurança que deverão ser adotadas pela Autoridade Certificadora da Justiça Federal, AC-JUS, e suas AC´s subseqüentes e AR´s credenciadas. Tais diretrizes fundamentarão as normas e procedimentos de segurança a serem elaborados e implementados por parte de cada entidade, considerando as suas particularidades;

1.2. Para o cumprimento da finalidade supramencionada são estabelecidos os objetivos a seguir.

2. OBJETIVOS:

2.1. A Política de Segurança Geral da AC-JUS tem os seguintes objetivos específicos:

2.1.1. Definir o escopo da segurança das entidades;

2.1.2. Orientar, por meio de suas diretrizes, todas as ações de segurança das entidades, para reduzir riscos e garantir a integridade, sigilo e disponibilidade das informações dos sistemas de informação e recursos;

2.1.3. Permitir a adoção de soluções de segurança integradas;

2.1.4. Servir de referência para auditoria, apuração e avaliação de responsabilidades.

3. ABRANGÊNCIA:

3.1. A Política de Segurança abrange os seguintes aspectos:

3.1.1. Requisitos de Segurança Humana;

3.1.2. Requisitos de Segurança Física;

3.1.3. Requisitos de Segurança Lógica;

3.1.4. Requisitos de Segurança dos Recursos Criptográficos.

4. TERMINOLOGIA

As regras e diretrizes de segurança devem ser interpretadas de forma que todas as suas determinações sejam obrigatórias e cogentes.

5. CONCEITOS E DEFINIÇÕES:

5.1. Conceitos:

5.1.1. Aplicam-se os conceitos abaixo no que se refere à Política de Segurança das entidades:

5.1.1.1. **Ativo de Informação** – é o patrimônio composto por todos os dados e informações, geradas e manipuladas durante a execução dos sistemas e processos das entidades;

5.1.1.2. **Ativo de Processamento** – é o patrimônio composto por todos os elementos de *hardware* e *software* necessários para a execução dos sistemas e processos das Entidades, tanto os produzidos internamente quanto os adquiridos;

5.1.1.3. **Controle de Acesso** – são restrições ao acesso às informações de um sistema exercido pela gerência de Segurança da Informação das entidades;

5.1.1.4. **Custódia** – consiste na responsabilidade de se guardar um ativo para terceiros. Entretanto, a custódia não permite automaticamente o acesso ao ativo, nem o direito de conceder acesso a outros;

5.1.1.5. **Direito de Acesso** – é o privilégio associado a um cargo, pessoa ou processo para ter acesso a um ativo;

5.1.1.6. **Ferramentas** – é um conjunto de equipamentos, programas, procedimentos, normas e demais recursos através dos quais se aplica a Política de Segurança da Informação das entidades;

5.1.1.7. **Incidente de Segurança** – é qualquer evento ou ocorrência que promova uma ou mais ações que comprometa ou que seja uma ameaça à integridade, autenticidade, ou disponibilidade de qualquer ativo das entidades vinculadas da AC-JUS;

5.1.1.8. **Política de Segurança** – é um conjunto de diretrizes destinadas a definir a proteção adequada dos ativos produzidos pelos Sistemas de Informação das entidades;

5.1.1.9. **Proteção dos Ativos** – é o processo pelo qual os ativos devem receber classificação quanto ao grau de sensibilidade. O meio de registro de um ativo de informação deve receber a mesma classificação de proteção dada ao ativo que o contém;

5.1.1.10. **Responsabilidade** – é definida como as obrigações e os deveres da pessoa que ocupa determinada função em relação ao acervo de informações;

5.1.1.11. **Senha Fraca ou Óbvia** – é aquela onde se utilizam caracteres de fácil associação com o dono da senha, ou que seja muito simples ou pequenas, tais como: datas de aniversário, casamento, nascimento, o próprio nome, o nome de familiares, seqüências numéricas simples, palavras com significado, dentre outras.

6. REGRAS GERAIS:

6.1. Gestão de Segurança:

6.1.1. A Política de Segurança Geral da AC-JUS se aplica a todos os recursos humanos, administrativos e tecnológicos pertencentes às entidades que a compõem. A abrangência dos recursos citados refere-se tanto àqueles ligados às entidades em caráter permanente quanto temporário;

6.1.2. Esta política deve ser comunicada para todo o pessoal envolvido e largamente divulgada através das entidades, garantindo que todos tenham consciência da mesma e a pratiquem na organização;

6.1.3. Todo o pessoal deve receber as informações necessárias para cumprir adequadamente o que está determinado na política de segurança;

6.1.4. Um programa de conscientização sobre segurança da informação deverá ser implementado para assegurar que todo o pessoal seja informado sobre os potenciais riscos de segurança e exposição a que estão submetidos os sistemas e operações das entidades. Especificamente, o pessoal envolvido ou que se relaciona com os usuários deve estar informado sobre ataques típicos de engenharia social e como se proteger deles;

6.1.5. Os procedimentos deverão ser documentados e implementados para garantir que quando o pessoal contratado ou prestadores de serviços sejam transferidos,

remanejados, promovidos ou demitidos, todos os privilégios de acesso aos sistemas, informações e recursos sejam devidamente revistos, modificados ou revogados;

6.1.6. Previsão de mecanismo e repositório centralizado para ativação e manutenção de trilhas, logs e demais notificações de incidentes. Este mecanismo deverá ser incluído nas medidas a serem tomadas por um grupo encarregado de responder a este tipo de ataque, para prover uma defesa ativa e corretiva contra os mesmos;

6.1.7. Os processos de aquisição de bens e serviços, especialmente de Tecnologia da Informação – TI, devem estar em conformidade com esta Política de Segurança;

6.1.8. Esta Política de Segurança deve ser revisada e atualizada periodicamente no máximo a cada 2 (dois) anos, caso não ocorram eventos ou fatos relevantes que exijam uma revisão imediata;

6.1.9. No que se refere a segurança da informação, deve-se considerar proibido, tudo aquilo que não esteja previamente autorizado pelo responsável da área de segurança da entidade pertencente à AC-JUS;

6.2. Gerenciamento de Riscos:

O processo de gerenciamento de riscos deve ser revisto, no máximo a cada 18 (dezoito) meses, pela entidade, para prevenção contra riscos, inclusive aqueles advindos de novas tecnologias, visando a elaboração de planos de ação apropriados para proteção aos componentes ameaçados;

6.3. Inventário de ativos:

Todos os ativos das entidades vinculadas à AC-JUS devem ser inventariados, classificados, permanentemente atualizados, e possuírem gestor responsável formalmente designado;

6.4. Plano de Continuidade do Negócio:

6.4.1. Um plano de continuidade do negócio deve ser implementado e testado, pelo menos uma vez por ano, para garantir a continuidade dos serviços críticos ao negócio;

6.4.2. A AC-SJF e suas AC´s vinculadas deverão apresentar planos de gerenciamento de incidentes e de ação de resposta a incidentes a serem aprovados pela AC Raiz ou AC de nível imediatamente superior;

6.4.3. O certificado da AC deverá ser imediatamente revogado se um evento provocar a perda ou comprometimento de sua chave privada ou do seu meio de armazenamento. Nesta situação, a entidade deverá seguir os procedimentos detalhados na sua DPC;

6.4.4. Todos os incidentes deverão ser reportados à AC Raiz imediatamente, a partir do momento em que for verificada a ocorrência. Estes incidentes devem ser reportados de modo sigiloso a pessoas especialmente designadas para isso.

7. REQUISITOS DE SEGURANÇA DE PESSOAL:

7.1. Definição:

Conjunto de medidas e procedimentos de segurança, a serem observados pelos prestadores de serviço e todos os empregados, necessário à proteção dos ativos das entidades participantes da AC-JUS;

7.2. Objetivos:

7.2.1. Reduzir os riscos de erros humanos, furto, roubo, apropriação indébita, fraude ou uso não apropriado dos ativos das entidades vinculadas à AC-JUS;

7.2.2. Prevenir e neutralizar as ações sobre as pessoas que possam comprometer a segurança das entidades vinculadas à AC-JUS;

7.2.3. Orientar e capacitar todo o pessoal envolvido na realização de trabalhos diretamente relacionados às entidades vinculadas da AC-JUS, assim como o pessoal em desempenho de funções de apoio, tais como a manutenção das instalações físicas e a adoção de medidas de proteção compatíveis com a natureza da função que desempenham;

7.2.4. Orientar o processo de avaliação de todo o pessoal que trabalhe nas entidades vinculadas da AC-JUS, mesmo em caso de funções desempenhadas por prestadores de serviço;

7.3. Diretrizes:

7.3.1. O Processo de Admissão:

7.3.1.1. Devem ser adotados critérios rígidos para o processo seletivo de candidatos, com o propósito de selecionar, para os quadros das entidades vinculadas à AC-JUS, pessoas reconhecidamente idôneas e sem antecedentes que possam comprometer a segurança ou credibilidade das entidades;

7.3.1.2. Nenhuma entidade vinculada à AC-JUS admitirá estagiários no exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados;

7.3.1.3. O empregado, funcionário ou servidor assinará termo de compromisso assumindo o dever de manter sigilo, mesmo quando desligado, sobre todos os ativos de informações e de processos das entidades vinculadas à AC-JUS;

7.3.2. As Atribuições da Função:

7.3.2.1. Relacionar claramente as atribuições de cada função, de acordo com a característica das atividades desenvolvidas, a fim de determinar-se o perfil necessário do empregado ou servidor, considerando-se os seguintes itens:

7.3.2.1.1. A descrição sumária das tarefas inerentes à função;

7.3.2.1.2. As necessidades de acesso a informações sensíveis;

7.3.2.1.3. O grau de sensibilidade do setor onde a função é exercida;

7.3.2.1.4. As necessidades de contato de serviço interno e/ou externo;

7.3.2.1.5. As características de responsabilidade, decisão e iniciativa inerentes à função;

7.3.2.1.6. A qualificação técnica necessária ao desempenho da função;

7.3.3. O Levantamento de Dados Pessoais:

Deve ser elaborada pesquisa do histórico da vida pública do candidato, com o propósito de levantamento de seu perfil;

7.3.4. A Entrevista de Admissão:

7.3.4.1. Deve ser realizada por profissional qualificado, com o propósito de confirmar e/ou identificar dados não detectados ou não confirmados, durante a pesquisa para a sua admissão;

7.3.4.2. Avaliar, na entrevista inicial, as características de interesse e motivação do candidato, sendo que as informações veiculadas na entrevista do candidato só deverão ser aquelas de caráter público;

7.3.5. Avaliação Psicológica:

Deve ser realizada por profissional legalmente qualificado, com o propósito de avaliar o candidato e a existência de atributos pessoais exigidos para o cargo e/ou função a ser desempenhada;

7.3.6. O Desempenho da Função:

7.3.6.1. Acompanhar o desempenho e avaliar periodicamente os empregados ou servidores com o propósito de detectar a necessidade de atualização técnica e de segurança;

7.3.6.2. Dar aos empregados ou servidores das entidades acesso às informações, mediante o fornecimento de instruções e orientações sobre as medidas e procedimentos de segurança;

7.3.7. A Credencial de Segurança:

7.3.7.1. Identificar o empregado por meio de uma credencial, habilitando-o a ter acesso a informações sensíveis, de acordo com a classificação do grau de sigilo da informação e, conseqüentemente, com o grau de sigilo compatível ao cargo e/ou a função a ser desempenhada;

7.3.7.2. A Credencial de Segurança somente será concedida por autoridade competente, ou por ela delegada, e se fundamentará na necessidade de conhecimento técnico dos aspectos inerentes ao exercício funcional e na análise da sensibilidade do cargo e/ou função;

7.3.8. Treinamento em Segurança da Informação:

Deve ser definido um processo, pelo qual será apresentada aos empregados, servidores e prestadores de serviço a Política de Segurança da Informação, suas normas e procedimentos relativos ao trato de informações e/ou dados sigilosos, com o propósito de desenvolver e manter uma efetiva conscientização de segurança, assim como instruir o seu fiel cumprimento;

7.3.9. Acompanhamento no Desempenho da Função:

7.3.9.1. Deve ser realizado processo de avaliação de desempenho da função que documente a observação do comportamento pessoal e funcional dos empregados, a ser realizada pela chefia imediata dos mesmos;

7.3.9.2. Deverão ser motivo de registro atos, atitudes e comportamentos positivos e negativos relevantes, verificados durante o exercício profissional do empregado;

7.3.9.3. Os comportamentos incompatíveis, ou que possam gerar comprometimentos á segurança, deverão ser averiguados e comunicados à chefia imediata;

7.3.9.4. As chefias imediatas assegurarão que todos os empregados ou servidores tenham conhecimento e compreensão das normas e procedimentos de segurança em vigor;

7.3.10. O Processo de Desligamento:

7.3.10.1. O acesso de ex-empregados às instalações, quando necessário, será restrito às áreas de acesso público;

7.3.10.2. Sua credencial, identificação, crachá, uso de equipamentos, mecanismos e acessos físicos e lógicos devem ser revogados;

7.3.11. O Processo de Liberação:

O empregado ou servidor firmará, antes do desligamento, declaração de que não possui qualquer tipo de pendência junto às diversas unidades que compõem a entidade;

7.3.12. A Entrevista de Desligamento:

Deverá ser realizada entrevista de desligamento para orientar o empregado ou servidor sobre sua responsabilidade na manutenção do sigilo de dados e/ou conhecimentos sigilosos de sistemas críticos aos quais teve acesso durante sua permanência nas entidades;

7.4. Deveres:

7.4.1. Deveres dos empregados ou servidores:

7.4.1.1. Preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos recursos de processamento e informações;

7.4.1.2. Cumprir a política de segurança, sob pena de incorrer nas sanções disciplinares e legais cabíveis;

7.4.1.3. Utilizar os Sistemas de Informações das entidades e os recursos a ela relacionados somente para os fins previstos pela Gerência de Segurança;

7.4.1.4. Cumprir as regras específicas de proteção estabelecidas aos ativos de informação;

7.4.1.5. Manter o caráter sigiloso da senha de acesso aos recursos e sistemas das entidades;

7.4.1.6. Não compartilhar, sob qualquer forma, informações confidenciais com outros que não tenham a devida autorização de acesso;

7.4.1.7. Responder, por todo e qualquer acesso, aos recursos das entidades bem como pelos efeitos desses acessos efetivados através do seu código de identificação, ou outro atributo para esse fim utilizado;

7.4.1.8. Respeitar a proibição de não usar, inspecionar, copiar ou armazenar programas de computador ou qualquer outro material, em violação da legislação de propriedade intelectual pertinente;

7.4.1.9. Comunicar ao seu superior imediato o conhecimento de qualquer irregularidade ou desvio;

7.4.2. Responsabilidade das Chefias:

7.4.2.1. A responsabilidade das chefias compreende, dentre outras, as seguintes atividades:

7.4.2.1.1. Gerenciar o cumprimento da política de segurança, por parte de seus empregados ou servidores;

7.4.2.1.2. Identificar os desvios praticados e adotar as medidas corretivas apropriadas;

7.4.2.1.3. Impedir o acesso de empregados demitidos ou demissionários aos ativos de informações, utilizando-se dos mecanismos de desligamento contemplados pelo respectivo plano de desligamento do empregado;

7.4.2.1.4. Proteger, em nível físico e lógico, os ativos de informação e de processamento das entidades participantes da AC-JUS relacionados com sua área de atuação;

7.4.2.1.5. Garantir que o pessoal sob sua supervisão compreenda e desempenhe a obrigação de proteger a Informação das entidades;

7.4.2.1.6. Comunicar formalmente à unidade que efetua a concessão de privilégios a usuários de TI, quais os empregados, servidores e prestadores de serviço, sob sua supervisão, que podem acessar as informações das entidades;

7.4.2.1.7. Comunicar formalmente à unidade que efetua a concessão de privilégios aos usuários de TI, quais os empregados, servidores e prestadores de serviço demitidos ou transferidos, para exclusão no cadastro dos usuários;

7.4.2.1.8. Comunicar formalmente à unidade que efetua a concessão de privilégios a usuários de TI, aqueles que estejam respondendo a processos, sindicâncias ou que estejam licenciados, para inabilitação no cadastro dos usuários;

7.4.3. Responsabilidades Gerais:

7.4.3.1. Cada área que detém os ativos de processamento e de informação é responsável por eles, devendo prover a sua proteção de acordo com a política de classificação da informação da entidade;

7.4.3.2. Todos os ativos de informações deverão ter claramente definidos os responsáveis pelo seu uso;

7.4.3.3. Todos os ativos de processamento das entidades devem estar relacionados no plano de continuidade do negócio;

7.4.4. Responsabilidades da Gerência de Segurança:

7.4.4.1. Estabelecer as regras de proteção dos ativos das entidades vinculadas à AC-JUS;

7.4.4.2. Decidir quanto às medidas a serem tomadas no caso de violação das regras estabelecidas;

7.4.4.3. Revisar pelo menos anualmente, as regras de proteção estabelecidas;

7.4.4.4. Restringir e controlar o acesso e os privilégios de usuários remotos e externos;

7.4.4.5. Elaborar e manter atualizado o Plano de Continuidade do negócio;

7.4.4.6. Executar as regras de proteção estabelecidas pela Política de Segurança;

7.4.4.7. Detectar, identificar, registrar e comunicar a AC Raiz as violações ou tentativas de acesso não autorizadas;

7.4.4.8. Definir e aplicar, para cada usuário de TI, restrições de acesso à Rede, como horário autorizado, dias autorizados, entre outras;

7.4.4.9. Manter registros de atividades de usuários de TI (logs) por um período de tempo superior a 6 (seis) anos. Os registros devem conter a hora e a data das atividades, a identificação do usuário de TI, comandos (e seus argumentos) executados, identificação da estação local ou da estação remota que iniciou a conexão, número dos processos e condições de erro observadas (tentativas rejeitadas, erros de consistência, etc.);

7.4.4.10. Limitar o prazo de validade das contas de prestadores de serviço ao período da contratação;

7.4.4.11. Excluir as contas inativas;

7.4.4.12. Fornecer senhas de contas privilegiadas somente aos empregados que necessitem efetivamente dos privilégios, mantendo-se o devido registro e controle;

7.4.5. Responsabilidades dos prestadores de serviço:

Devem ser previstas no contrato, cláusulas que contemplem a responsabilidade dos prestadores de serviço no cumprimento desta Política de Segurança da Informação e suas normas e procedimentos;

7.5. Sanções:

Sanções previstas pela legislação vigente.

8. REQUISITOS DE SEGURANÇA DO AMBIENTE FÍSICO:

8.1. Definição:

Ambiente físico é aquele composto por todo o ativo permanente das entidades vinculadas à AC-JUS;

8.2. Diretrizes Gerais:

8.2.1. As responsabilidades pela segurança física dos sistemas das entidades deverão ser definidos e atribuídos a indivíduos claramente identificados na organização;

8.2.2. A localização das instalações e o sistema de certificação da AC-JUS e das AC subseqüentes não deverão ser publicamente identificados;

8.2.3. Sistemas de segurança para acesso físico deverão ser instalados para controlar e auditar o acesso aos sistemas de certificação;

8.2.4. Controles duplicados sobre o inventário e cartões/chaves de acesso deverão ser estabelecidos. Uma lista atualizada do pessoal que possui cartões/chaves deverá ser mantida;

8.2.5. Chaves criptográficas sob custódia do responsável deverão ser fisicamente protegidas contra acesso não autorizado, uso ou duplicação;

8.2.6. Perdas de cartões/chaves de acesso deverão ser imediatamente comunicadas ao responsável pela gerência de segurança da entidade. Ele deverá tomar as medidas apropriadas para prevenir acessos não autorizados;

8.2.7. Os sistemas de AC deverão estar localizados em área protegida ou afastada de fontes potentes de magnetismo ou interferência de rádio freqüência;

8.2.8. Recursos e instalações críticas ou sensíveis devem ser mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança e controle de acesso. Elas devem ser fisicamente protegidas de acesso não autorizado, dano, ou interferência. A proteção fornecida deve ser proporcional aos riscos identificados;

8.2.9. A entrada e saída, nestas áreas ou partes dedicadas, deverão ser automaticamente registradas com data e hora definidas e serão revisadas diariamente pelo responsável pela gerência de segurança da informação nas entidades da AC-JUS e mantidas em local adequado e sob sigilo;

8.2.10. O acesso aos componentes da infra-estrutura, atividade fundamental ao funcionamento dos sistemas das entidades, como painéis de controle de energia, comunicações e cabeamento, deverá ser restrito ao pessoal autorizado;

8.2.11. Sistemas de detecção de intrusão deverão ser utilizados para monitorar e registrar os acessos físicos aos sistemas de certificação nas horas de utilização;

8.2.12. O inventário de todo o conjunto de ativos de processamento deve ser registrado e mantido atualizado, no mínimo, mensalmente;

8.2.13. Quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, só devem ser utilizados a partir de autorização formal e mediante supervisão;

8.2.14. Nas instalações das entidades integrantes da AC-JUS, todos deverão utilizar alguma forma visível de identificação (por exemplo: crachá), e devem informar à segurança sobre a presença de qualquer pessoa não identificada ou de qualquer estranho não acompanhado;

8.2.15. Visitantes das áreas de segurança devem ser supervisionados. Suas horas de entrada e saída e o local de destino devem ser registrados. Essas pessoas devem obter acesso apenas às áreas específicas, com propósitos autorizados, e esses acessos devem seguir instruções baseadas nos requisitos de segurança da área visitada;

8.2.16. Os ambientes onde ocorrem os processos críticos das entidades integrantes da AC-JUS deverão ser monitorados, em tempo real, com as imagens registradas por meio de sistemas de CFTV;

8.2.17. Sistemas de detecção de intrusos devem ser instalados e testados regularmente de forma a cobrir os ambientes, as portas e janelas acessíveis, nos ambientes onde ocorrem processos críticos. As áreas não ocupadas devem possuir um sistema de alarme que permaneça sempre ativado.

9. REQUISITOS DE SEGURANÇA DO AMBIENTE LÓGICO:

9.1. Definição:

Ambiente lógico é composto por todo o ativo de informações das entidades;

9.2. Diretrizes gerais:

9.2.1. A informação deve ser protegida de acordo com o seu valor, sensibilidade e criticidade. Para tanto, deve ser elaborado um sistema de classificação da informação;

9.2.2. Os dados, as informações e os sistemas de informação das entidades e sob sua guarda, devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, sigilo e disponibilidade desses bens;

9.2.3. As violações de segurança devem ser registradas e esses registros devem ser analisados periodicamente para os propósitos de caráter corretivo, legal e de auditoria. Os registros devem ser protegidos e armazenados de acordo com a sua classificação;

9.2.4. Os sistemas e recursos que suportam funções críticas para operação das entidades, devem assegurar a capacidade de recuperação nos prazos e condições definidas em situações de contingência;

9.2.5. O inventário sistematizado de toda a estrutura que serve como base para manipulação, armazenamento e transmissão dos ativos de processamento, deve estar registrado e mantido atualizado em intervalos de tempo definidos pelas entidades vinculadas à AC-SJF.

9.3. Diretrizes específicas:

9.3.1. Sistemas:

9.3.1.1. As necessidades de segurança devem ser identificadas para cada etapa do ciclo de vida dos sistemas disponíveis nas entidades. A documentação dos sistemas deve ser mantida atualizada. A cópia de segurança deve ser testada e mantida atualizada;

9.3.1.2. Os sistemas devem possuir controle de acesso de modo a assegurar o uso apenas a usuários ou processos autorizados. O responsável pela

autorização ou confirmação da autorização deve ser claramente definido e registrado;

9.3.1.3. Os arquivos de *logs* devem ser criteriosamente definidos para permitir recuperação nas situações de falhas, auditoria nas situações de violações de segurança e contabilização do uso de recursos. Os *logs* devem ser periodicamente analisados, conforme definido na DPC, para identificar tendências, falhas ou usos indevidos. Os *logs* devem ser protegidos e armazenados de acordo com sua classificação;

9.3.1.4. Devem ser estabelecidas e mantidas medidas e controles de segurança para verificação crítica dos dados e configuração de sistemas e dispositivos quanto a sua precisão, consistência e integridade;

9.3.1.5. Os sistemas devem ser avaliados com relação aos aspectos de segurança (testes de vulnerabilidade) antes de serem disponibilizados para a produção. As vulnerabilidades do ambiente devem ser avaliadas periodicamente e as recomendações de segurança devem ser adotadas;

9.3.2. Máquinas servidoras:

9.3.2.1. O acesso lógico, ao ambiente ou serviços disponíveis em servidores, deve ser controlado e protegido. As autorizações devem ser revistas, confirmadas e registradas continuadamente. O responsável pela autorização ou confirmação da autorização deve ser claramente definido e registrado;

9.3.2.2. Os acessos lógicos devem ser registrados em *logs*, que devem ser analisados periodicamente. O tempo de retenção dos arquivos de *logs* e as medidas de proteção associadas devem estar precisamente definidos;

9.3.2.3. Devem ser adotados procedimentos sistematizados para monitorar a segurança do ambiente operacional, principalmente no que diz respeito à integridade dos arquivos de configuração do Sistema Operacional e de outros arquivos críticos. Os eventos devem ser armazenados em relatórios de segurança (*logs*) de modo que sua análise permita a geração de trilhas de auditoria a partir destes registros;

9.3.2.4. As máquinas devem estar sincronizadas para permitir o rastreamento de eventos.;

9.3.2.5. Proteção lógica adicional (criptografia) deve ser adotada para evitar o acesso não autorizado às informações;

9.3.2.6. A versão do Sistema Operacional, assim como outros *softwares* básicos instalados em máquinas servidoras, devem ser mantidos atualizados, em conformidade com as recomendações dos fabricantes;

9.3.2.7. Devem ser utilizados somente *softwares* autorizados pela própria entidade nos seus equipamentos. Deve ser realizado o controle da distribuição e instalação dos mesmos;

9.3.2.8. O acesso remoto a máquinas servidoras deve ser realizado adotando os mecanismos de segurança definidos para evitar ameaças à integridade e sigilo do serviço;

9.3.2.9. Os procedimentos de cópia de segurança (*backup*) e de recuperação devem estar documentados, mantidos atualizados e devem ser regularmente testados, de modo a garantir a disponibilidade das informações;

9.3.3. Redes das entidades vinculadas à AC-JUS:

9.3.3.1. O tráfego das informações no ambiente de rede deve ser protegido contra danos ou perdas, bem como acesso, uso ou exposição indevidos;
9.3.3.2. Componentes críticos da rede local devem ser mantidos em salas rotegidas e com acesso físico e lógico controlado, devendo ser protegidos contra danos, furtos, roubos e intempéries;
9.3.3.3. Devem ser adotadas as facilidades de segurança disponíveis de forma inata nos ativos de processamento da rede;
9.3.3.4. A configuração de todos os ativos de processamento deve ser averiguada quando da sua instalação inicial, para que sejam detectadas e corrigidas as vulnerabilidades inerentes à configuração padrão que se encontram nesses ativos em sua primeira ativação;
9.3.3.5. Serviços vulneráveis devem receber nível de proteção adicional;
9.3.3.6. O uso de senhas deve estar submetido a uma política específica para sua gerência e utilização;
9.3.3.7. O acesso lógico aos recursos da rede local deve ser realizado por meio de sistema de controle de acesso. O acesso deve ser concedido e mantido pela administração da rede, baseado nas responsabilidades e tarefas de cada usuário;
9.3.3.8. A utilização de qualquer mecanismo capaz de realizar testes de qualquer natureza, como por exemplo, monitoração sobre os dados, os sistemas e dispositivos que compõem a rede, só devem ser utilizado à partir de autorização formal e mediante supervisão;
9.3.3.9. A conexão com outros ambientes de rede e alterações internas na sua topologia e configuração devem ser formalmente documentadas e mantidas, de forma a permitir registro histórico, e devem ter a autorização da administração da rede e da gerência de segurança. O diagrama topológico, a configuração e o inventário dos recursos devem ser mantidos atualizados;
9.3.3.10. Devem ser definidos relatórios de segurança (*logs*) de modo a auxiliar no tratamento de desvios, recuperação de falhas, contabilização e auditoria. Os *logs* devem ser analisados periodicamente e o período de análise estabelecido deve ser o menor possível;
9.3.3.11. Devem ser adotadas proteções físicas adicionais para os recursos de rede considerados críticos;
9.3.3.12. Proteção lógica adicional deve ser adotada para evitar o acesso não-autorizado às informações;
9.3.3.13. A infra-estrutura de interligação lógica deve estar protegida contra danos mecânicos e conexão não autorizada;
9.3.3.14. A alimentação elétrica para a rede local deve ser separada da rede convencional, devendo ser observadas as recomendações dos fabricantes dos equipamentos utilizados, assim como as normas ABNT aplicáveis;
9.3.3.15. O tráfego de informações deve ser monitorado, a fim de verificar sua normalidade, assim como detectar situações anômalas do ponto de vista da segurança;
9.3.3.16. Devem ser observadas as questões envolvendo propriedade intelectual quando da cópia de software ou arquivos de outras localidades;
9.3.3.17. Informações sigilosas, corporativas ou que possam causar prejuízo às entidades devem estar protegidas e não devem ser enviadas para outras redes, sem proteção adequada;

9.3.3.18. Todo serviço de Rede não explicitamente autorizado deve ser bloqueado ou desabilitado;
9.3.3.19. Mecanismos de segurança baseados em sistemas de proteção de acesso (*firewall*) devem ser utilizados para proteger as transações entre redes externas e a rede interna da entidade;
9.3.3.20. Os registros de eventos devem ser analisados periodicamente, no menor prazo possível e em intervalos de tempo adequados;
9.3.3.21. Deve ser adotado um padrão de segurança para todos os tipos de equipamentos servidores, considerando aspectos físicos e lógicos;
9.3.3.22. Todos os recursos considerados críticos para o ambiente de rede, e que possuam mecanismos de controle de acesso, deverão fazer uso de tal controle;
9.3.3.23. A localização dos serviços baseados em sistemas de proteção de acesso (*firewall*) deve ser resultante de uma análise de riscos. No mínimo, os seguintes aspectos devem ser considerados: requisitos de segurança definidos pelo serviço, objetivo do serviço, público alvo, classificação da informação, forma de acesso, freqüência de atualização do conteúdo, forma de administração do serviço e volume de tráfego;
9.3.3.24. Ambientes de rede considerados críticos devem ser isolados de outros ambientes de rede, de modo a garantir um nível adicional de segurança;
9.3.3.25. Conexões entre as redes das entidades vinculadas à AC-JUS e redes externas deverão estar restritas somente àquelas que visem efetivar os processos;
9.3.3.26. As conexões de rede devem ser ativadas: primeiro, sistemas com função de certificação; segundo, sistemas que executam as funções de registros e repositório. Se isto não for possível, deve-se empregar controles de compensação, tais como o uso de *proxies* que deverão ser implementados para proteger os sistemas que executam a função de certificação contra possíveis ataques;
9.3.3.27. Sistemas que executam a função de certificação deverão estar isolados para minimizar a exposição contra tentativas de comprometer o sigilo, a integridade e a disponibilidade das funções de certificação;
9.3.3.28. A chave de certificação das AC deverá estar protegida de acesso desautorizado, para garantir seu sigilo e integridade;
9.3.3.29. A segurança das comunicações intra-rede e inter-rede, entre os sistemas das entidades vinculadas à AC-JUS, deverá ser garantida pelo uso de mecanismos que assegurem o sigilo e a integridade das informações trafegadas;
9.3.3.30. As ferramentas de detecção de intrusos devem ser implantadas para monitorar as redes críticas, alertando periodicamente os administradores das redes sobre as tentativas de intrusão;

9.3.4. Controle de acesso lógico (baseado em senhas):
9.3.4.1. Usuários e aplicações que necessitem ter acesso a recursos das entidades da AC-JUS devem ser identificados e autenticados;
9.3.4.2. O sistema de controle de acesso deve manter as habilitações atualizadas e registros que permitam a contabilização do uso, auditoria e recuperação nas situações de falha;

9.3.4.3. Nenhum usuário deve ser capaz de obter os direitos de acesso de outro usuário;
9.3.4.4. A informação que especifica os direitos de acesso de cada usuário ou aplicação deve ser protegida contra modificações não autorizadas;
9.3.4.5. O arquivo de senhas deve ser criptografado e ter o acesso controlado;
9.3.4.6. As autorizações devem ser definidas de acordo com a necessidade de desempenho das funções (acesso motivado) e considerando o princípio dos privilégios mínimos (ter acesso apenas aos recursos ou sistemas necessários para a execução de tarefas);
9.3.4.7. As senhas devem ser individuais, secretas, intransferíveis e ser protegidas com grau de segurança compatível com a informação associada;
9.3.4.8. O sistema de controle de acesso deve possuir mecanismos que impeçam a geração de senhas fracas ou óbvias;
9.3.4.9. As seguintes características das senhas devem estar definidas de forma adequada: conjunto de caracteres permitidos, tamanho mínimo e máximo, prazo de validade máximo, forma de troca e restrições específicas;
9.3.4.10. A distribuição de senhas aos usuários de TI (inicial ou não) deve ser feita de forma segura. A senha inicial, quando gerada pelo sistema, deve ser trocada, pelo usuário de TI, no primeiro acesso;
9.3.4.11. O sistema de controle de acesso deve permitir ao usuário alterar sua senha sempre que desejar. A troca de uma senha bloqueada só deve ser executada após a identificação positiva do usuário. A senha digitada não deve ser exibida;
9.3.4.12. Devem ser adotados critérios para bloquear ou desativar usuários de acordo com período pré-definido sem acesso e tentativas sucessivas de acesso mal sucedidas;
9.3.4.13. O sistema de controle de acesso deve solicitar nova autenticação após certo tempo de inatividade da sessão (*time-out*);
9.3.4.14. O sistema de controle de acesso deve exibir, na tela inicial, mensagem informando que o serviço só pode ser utilizado por usuários autorizados. No momento de conexão, o sistema deve exibir para o usuário informações sobre o último acesso;
9.3.4.15. O registro das atividades (*logs*) do sistema de controle de acesso deve serdefinido de modo a auxiliar no tratamento das questões de segurança, permitindo a contabilização do uso, auditoria e recuperação nas situações de falhas. Os *logs* devem ser periodicamente analisados;
9.3.4.16. Os usuários e administradores do sistema de controle de acesso devem ser formal e expressamente conscientizados de suas responsabilidades, mediante assinatura de termo de compromisso;

9.3.5. Computação pessoal:
9.3.5.1. As estações de trabalho, incluindo equipamentos portáteis ou *stand- alone* e informações devem ser protegidos contra danos ou perdas, bem como acesso, uso ou exposição indevidos;
9.3.5.2. Equipamentos que executem operações sensíveis devem receber proteção adicional, considerando os aspectos lógicos (controle de acesso e criptografia) e físicos (proteção contra furto ou roubo do equipamento ou componentes);

9.3.5.3. Devem ser adotadas medidas de segurança lógica referentes a combate a vírus, *backup*, controle de acesso e uso de software não autorizado;

9.3.5.4. As informações armazenadas em meios eletrônicos devem ser protegidas contra danos, furtos ou roubos, devendo ser adotados procedimentos de *backup*, definidos em documento específico;

9.3.5.5. Informações sigilosas, corporativas ou cuja divulgação possa causar prejuízo às entidades vinuladas à AC-JUS, só devem ser utilizadas em equipamentos das entidades onde foram geradas ou naqueles por elas autorizadas, com controles adequados;

9.3.5.6. O acesso às informações deve atender aos requisitos de segurança, considerando o ambiente e forma de uso do equipamento (uso pessoal ou coletivo);

9.3.5.7. Os usuários de TI devem utilizar apenas *softwares* licenciados pelo fabricante nos equipamentos das entidades, observadas as normas da AC-JUS e legislação de *software*;

9.3.5.8. A entidade deverá estabelecer os aspectos de controle, distribuição e instalação de *softwares* utilizados;

9.3.5.9. A impressão de documentos sigilosos deve ser feita sob supervisão do responsável. Os relatórios impressos devem ser protegidos contra perda, reprodução e uso não autorizado;

9.3.5.10. O inventário dos recursos deve ser mantido atualizado;

9.3.5.11. Os sistemas em uso devem solicitar nova autenticação após certo tempo de inatividade da sessão (*time-out*);

9.3.5.12. As mídias devem ser eliminadas de forma segura, quando não forem mais necessárias. Procedimentos formais para a eliminação segura das mídias devem ser definidos, para minimizar os riscos;

9.3.6. Combate a Vírus de Computador

Os procedimentos de combate a processos destrutivos (*vírus, cavalo-de-tróia e worms*) devem estar sistematizados e devem abranger máquinas servidoras, estações de trabalho, equipamentos portáteis e microcomputadores *stand alone*.

10. REQUISITOS DE SEGURANÇA DOS RECURSOS CRIPTOGRÁFICOS:

10.1. Requisitos Gerais para Sistema Criptográfico da AC-JUS:

10.1.1. O sistema criptográfico da AC-JUS deve ser entendido como sendo um sistema composto de documentação normativa específica de criptografia aplicada na AC-JUS, conjunto de requisitos de criptografia, projetos, métodos de implementação, módulos implementados de *hardware* e *software*, definições relativas a algoritmos criptográficos e demais algoritmos integrantes de um processo criptográfico, procedimentos adotados para gerência das chaves criptográficas, métodos adotados para testes de robustez das cifras e detecção de violações dessas;

10.1.2. Toda a documentação, referente a definição, descrição e especificação dos componentes dos sistemas criptográficos utilizados na AC-JUS, deve ser aprovada pela AC Raiz;

10.1.3. A força do sistema criptográfico deve ser periodicamente testada por entidades competentes na área de criptografia. A periodicidade a que se refere este item não deve ser superior a 2 (dois) anos;

10.1.4. Os testes necessários para satisfazer o item anterior devem estar previamente definidos em documento normativo específico e de caráter oficial aprovado pelo CG ICP-BRASIL;
10.1.5. Todo parâmetro crítico, cuja exposição indevida comprometa a segurança do sistema criptográfico da AC-JUS, deve ser armazenado cifrado;
10.1.6. Os aspectos relevantes relacionados à criptografia no âmbito da AC-JUS devem ser detalhados em documentos específicos, aprovados pela AC Raiz;

10.2. Chaves criptográficas:

10.2.1. A manipulação das chaves criptográficas utilizadas nos sistemas criptográficos da AC-JUS deverá ser restrita a um número mínimo e essencial de pessoas, assim como deve estar submetida a mecanismos de controle considerados adequados pelo CG ICP-BRASIL;
10.2.2. As pessoas, a que se refere o item anterior, deverão ser formalmente designadas pela chefia competente, conforme as funções a serem desempenhadas e o correspondente grau de privilégios, assim como terem suas responsabilidades explicitamente definidas;
10.2.3. Os algoritmos de criação e de troca das chaves criptográficas, utilizados no sistema criptográfico da AC-JUS devem ser aprovados pelo CG ICP-BRASIL;
10.2.4. Os diferentes tipos de chaves criptográficas e suas funções no sistema criptográfico da AC-JUS devem estar explicitados nas políticas de certificado específicas;

10.3. Transporte das Informações:

10.3.1. O processo de transporte de chaves criptográficas e demais parâmetros do sistema de criptografia da AC-JUS devem ter a integridade e o sigilo assegurados, por meio do emprego de soluções criptográficas específicas;
10.3.2. Deve-se adotar recursos de VPN (Virtual Private Networks – redes privadas virtuais), baseadas em criptografia, para a troca de informações sensíveis, por meio de redes públicas, entre as redes das entidades da AC-JUS que pertençam a uma mesma organização.

11. AUDITORIA:

11.1. Introdução:

11.1.1. Deverão ser realizadas auditorias periódicas nas entidades integrantes da AC-JUS, pela AC Raiz ou por prestadores de serviço por ela contratados;
11.1.2. As atividades das entidades integrantes da AC-JUS estão associadas ao conceito de confiança. O processo de auditoria periódica representa um dos instrumentos que facilita a percepção e transmissão de confiança à comunidade de usuários;

11.2. Objetivo da Auditoria:

Verificar a capacidade da AC-JUS, demais AC, AR e repositórios em atender os requisitos da ICP-BRASIL. O resultado da auditoria é um item fundamental a ser considerado no processo de credenciamento das AC para a AC-JUS, e para a ICP-BRASIL, assim como, para a manutenção da condição de credenciada;

11.3. Abrangência:

11.3.1. A auditoria deve abordar os aspectos relativos ao ambiente de operação e ciclo de vida de certificados. Os seguintes tópicos devem ser verificados:

11.3.2. Ambiente de operação:
11.3.2.1. Segurança da operação;
11.3.2.2. Segurança de pessoal;
11.3.2.3. Segurança física;
11.3.2.4. Segurança lógica;
11.3.2.5. Segurança de telecomunicações;
11.3.2.6. Segurança de recursos criptográficos;
11.3.2.7. Plano de contingência;
11.3.3. Ciclo de vida do certificado:
11.3.3.1. Solicitação;
11.3.3.2. Validação;
11.3.3.3. Emissão;
11.3.3.4. Uso;
11.3.3.5. Revogação.

11.4. Documentos de Referência:

A auditoria deve ser realizada tendo como orientação básica os atos normativos que disciplinam as atividades exercidas no âmbito da ICP-BRASIL

11.5. Identidade e qualificação do Auditor:

A auditoria da AC-JUS e das AC credenciadas atenderá aos seguintes requisitos mínimos:

11.5.1. Corpo técnico com comprovada experiência nas áreas de segurança da informação (ambientes físico e lógico), criptografia, infra-estrutura de chaves pública e sistemas críticos;
11.5.2. Experiência em serviços de auditoria dessa mesma natureza e referências de outros serviços de auditoria similares;
11.5.3. Utilização de padrões internacionais (como exemplo: ISO 17799) ou padrão similar como referência de melhores práticas e procedimentos;

11.6. O resultado da auditoria pode conter as seguintes recomendações:

11.6.1. Suspender temporariamente os serviços nas AC da AC-JUS até correção dos problemas;
11.6.2. Revogar o certificado das AC da AC-JUS;
11.6.3. Substituir / treinar pessoal;

11.7. Freqüência das Auditorias:

O processo de auditoria deve ser realizado nas seguintes situações e respectivas freqüências:

11.7.1. Credenciamento inicial – antes do credenciamento e do início de suas atividades no âmbito da AC-JUS;
11.7.2. Auditoria periódica anual – para manutenção do credenciamento;
11.7.3. Por determinação do CG ICP-BRASIL ou da AC Raiz, a qualquer tempo.

12. GERENCIAMENTO DE RISCOS:

12.1. Definição:

Processo que visa a proteção dos serviços das entidades vinculadas à da AC-JUS, por meio da eliminação, redução ou transferência dos riscos, conforme seja economicamente (e estrategicamente) mais viável. Os seguintes pontos principais devem ser identificados:

12.1.1. O que deve ser protegido;

12.1.2. Análise de riscos (Contra quem ou contra o quê deve ser protegido);
12.1.3. Avaliação de riscos (Análise da relação custo/benefício);

12.2. Fases Principais:

O gerenciamento de riscos consiste das seguintes fases principais:

12.2.1. Identificação dos recursos a serem protegidos – *hardware*, rede, *software*, dados, informações pessoais, documentação, suprimentos;
12.2.2. Identificação dos riscos (ameaças) - que podem ser naturais (tempestades, inundações), causadas por pessoas (ataques, furtos, vandalismos, erros ou negligências) ou de qualquer outro tipo (incêndios);
12.2.3. Análise dos riscos (vulnerabilidades e impactos) - identificar as vulnerabilidades e os impactos associados;
12.2.4. Avaliação dos riscos (probabilidade de ocorrência) - levantamento da probabilidade da ameaça vir a acontecer, estimando o valor do provável prejuízo. Esta avaliação pode ser feita com base em informações históricas ou em tabelas internacionais;
12.2.5. Tratamento dos riscos (medidas a serem adotadas) - maneira como lidar com as ameaças. As principais alternativas são: eliminar o risco, prevenir, limitar ou transferir as perdas ou aceitar o risco;
12.2.6. Monitoração da eficácia dos controles adotados para minimizar os riscos identificados;
12.2.7. Reavaliação periódica dos riscos em intervalos de tempo não superiores a 6 (seis) meses;

12.3. Riscos relacionados às entidades integrantes da AC-JUS:

Os riscos a serem avaliados para as entidades integrantes da AC-JUS compreendem, dentre outros, os seguintes:

Segmento	Riscos
Dados e Informação	Indisponibilidade, Interrupção (perda), interceptação, modificação, fabricação, destruição;
Pessoas	Omissão, erro, negligência, imprudência, imperícia, desídia, sabotagem perda de conhecimento;
Rede	*Hacker*, acesso desautorizado, interceptação, engenharia social, identidade forjada, reenvio de mensagem, violação de integridade, indisponibilidade ou recusa de serviço
Hardware	Indisponibilidade, interceptação (furto ou roubo), falha;
Software e sistemas	Interrupção (apagamento), interceptação, modificação, desenvolvimento, falha;
Recursos criptográficos	Ciclo de vida dos certificados, gerenciamento das chaves criptográficas; *hardware* criptográfico, algoritmos (desenvolvimento e utilização), material criptográfico;

12.4. Considerações Gerais:

12.4.1. Os riscos que não puderem ser eliminados devem ter seus controles documentados e devem ser levados ao conhecimento da AC-JUS e do CG ICP-BRASIL;

12.4.2. Um efetivo gerenciamento dos riscos permite decidir se o custo de prevenir um risco (medida de proteção) é mais alto que o custo das conseqüências do risco (impacto da perda);

12.4.3. É necessária a participação e envolvimento da alta administração das entidades;

12.5. Implementação do Gerenciamento de Riscos:

O gerenciamento de riscos nas entidades vinculada à AC-JUS pode ser conduzido de acordo com a metodologia padrão ou proprietária, desde que atendidos todos os tópicos relacionados.

13. PLANO DE CONTINUIDADE DO NEGÓCIO:

13.1. Definição:

Plano cujo objetivo é manter em funcionamento os serviços e processos críticos das entidades vinculada à AC-JUS, na eventualidade da ocorrência de desastres, atentados, falhas e intempéries;

13.2. Diretrizes Gerais:

13.2.1. Sistemas e dispositivos redundantes devem estar disponíveis para garantir a continuidade da operação dos serviços críticos de maneira oportuna;

13.2.2. Todas as AC vinculadas à AC-JUS deverão apresentar um Plano de Continuidade do Negócio que estabelecerá, no mínimo, o tratamento adequado dos seguintes eventos de segurança:

13.2.2.1. Comprometimento da chave privada das entidades;

13.2.2.2. Invasão do sistema e da rede interna da entidade;

13.2.2.3. Incidentes de segurança física e lógica;

13.2.2.4. Indisponibilidade da Infra-estrutura; e

13.2.2.5. Fraudes ocorridas no registro do usuário, na emissão, expedição, distribuição, revogação e no gerenciamento de certificados;

13.2.3. Todo pessoal envolvido com o Plano de Continuidade do Negócio deve receber um treinamento específico para poder enfrentar estes incidentes;

13.2.4. Um plano de ação de resposta a incidentes deverá ser estabelecido para todas as AC vinculadas à AC-JUS. Este plano deve prever, no mínimo, o tratamento adequado dos seguintes eventos:

13.2.4.1. Comprometimento de controle de segurança em qualquer evento referenciado no Plano de Continuidade do Negócio;

13.2.4.2. Notificação à comunidade de usuários, se for o caso;

13.2.4.3. Revogação dos certificados afetados, se for o caso;

13.2.4.4. Procedimentos para interrupção ou suspensão de serviços e investigação;

13.2.4.5. Análise e monitoramento de trilhas de auditoria; e

13.2.4.6. Relacionamento com o público e com meios de comunicação, se for o caso.