Anexo -I
Check-List

Sumário

Check-List AC-Raiz - Conformidade com DOC-ICP 01 e DOC-ICP 02

INTRODUÇÃO

Este *check-list* contêm os itens mínimos a serem verificados na auditoria de conformidade na Autoridade Certificadora Raiz e estará sujeito a ajustes por parte do ITI até o início dos trabalhos de auditoria.

A empresa contratada poderá apresentar seu próprio *check-list* desde que esse contenha todos os itens necessários para verificação da auditoria e esteja consubstanciado nos DOC-ICP-01 e DOC-ICP-02. O *check-list* apresentado pela contratada estará sujeito a aprovação do ITI.

O presente *check-list*, não esgota os processos e subprocessos existentes na AC RAIZ, devendo ser entendido apenas como um balizador ou ponto de partida para o trabalho de auditoria. Sempre caberá ao Auditor a responsabilidade pela escolha dos controles a serem auditados em conformidade com as normas da ICP Brasil.

1 - Ciclo de vida de certificados digitais

DOC-ICP-01.4.4.3.3
O prazo para a revogação de certificado de AC de nível imediatamente subseqüente ao da AC Raiz é de no máximo 2 (duas) horas e conta-se a partir do recebimento pela AC Raiz da solicitação de revogação da AC titular do certificado ou da determinação de revogação emitida pela própria AC Raiz.

DOC-ICP-01.3.1.8
A identificação de uma AC pela AC Raiz é executada por meio dos procedimentos descritos no documento CRITÉRIOS E PROCEDIMENTOS PARA CREDENCIAMENTO DAS ENTIDADES INTEGRANTES DA ICPBRASIL.

DOC-ICP-01.3.2.2
Para isto, um representante legal da AC deve preencher e assinar, em papel ou digitalmente, o formulário REVALIDAÇÃO DOS DADOS CADASTRAIS E SOLICITAÇÃO DE NOVO CERTIFICADO. Após o recebimento desse formulário, desde que a documentação esteja regularmente atualizada, a AC Raiz iniciará o processo de emissão do novo certificado.

DOC-ICP-01.3.3.1
A solicitação de novo certificado de AC após a revogação ou expiração do certificado anterior deverá ser efetivada pelo preenchimento do formulário REVALIDAÇÃO DOS DADOS CADASTRAIS E SOLICITAÇÃO DE NOVO CERTIFICADO. Este formulário deverá ser assinado por representante legalmente constituído da AC e entregue junto à AC Raiz. Após o recebimento desse formulário, desde que a documentação esteja regularmente atualizada, a AC Raiz iniciará o processo de emissão do novo certificado.

DOC-ICP-01.4.4.3.1
A solicitação de revogação do certificado à AC Raiz deve ser efetivada pelo preenchimento do formulário SOLICITAÇÃO DE REVOGAÇÃO DE CERTIFICADO DE AC. Esse formulário deverá ser assinado por seu representante legal. Quando utilizada a versão eletrônica do formulário, ele deve ser assinado digitalmente e enviado à AC Raiz. O formulário pode também ser preenchido em papel, entregue pessoalmente pelo representante à AC Raiz e assinado no ato da entrega.

DOC-ICP-01.4.4.3.2
O processo de revogação de um certificado de AC é precedido, quando for o caso, do recebimento pela AC Raiz da solicitação de revogação e termina quando uma nova LCR, contendo o certificado revogado, é emitida e publicada pela AC Raiz. Concluído esse processo, a AC Raiz informa à AC afetada a revogação do certificado.

DOC-ICP-01.4.4.3.3
O prazo para a revogação de certificado de AC de nível imediatamente subseqüente ao da AC Raiz é de no máximo 2 (duas) horas e conta-se a partir do recebimento pela AC Raiz da solicitação de revogação da AC titular do certificado ou da determinação de revogação emitida pela própria AC Raiz.

Check-List AC-Raiz - Conformidade com DOC-ICP 01 e DOC-ICP 02

DOC-ICP-01.3.4.1
O solicitante da revogação de certificado deverá ser identificado. Somente os agentes descritos no item 4.4.2 podem solicitar a revogação do certificado de uma AC de nível imediatamente subseqüente ao da AC Raiz.

DOC-ICP-01.3.4.2
O procedimento para solicitação de revogação de certificado pela AC Raiz está descrito no item 4.4.3. Solicitações de revogação de certificados devem ser registradas.

DOC-ICP-01.4.4.1.2
Um certificado deve obrigatoriamente ser revogado:
a) quando constatada emissão imprópria ou defeituosa do mesmo;
b) quando for necessária a alteração de qualquer informação constante no mesmo;
c) no caso de dissolução da AC titular do certificado; ou
d) no caso de comprometimento da chave privada da AC ou da sua mídia armazenadora.

DOC-ICP-01.4.4.2
A revogação do certificado de uma AC de nível imediatamente subseqüente ao da AC Raiz somente pode ser feita:
a) por determinação da AC Raiz;
b) por solicitação da AC titular do certificado; ou
c) por determinação judicial.

DOC-ICP-01.7.3.1
A AC Raiz implementa a sua LCR conforme a versão 2 do padrão ITU X.509.

DOC-ICP-01.7.3.2
A LCR emitida pela AC Raiz implementa as seguintes extensões previstas na RFC 3280:
a) AuthorityKeyIdentifier: contém o mesmo valor do campo “Subject Key Identifier” do certificado da AC Raiz;
b) cRLNumber: contém um número seqüencial para cada LCR emitida.

DOC-ICP-01.4.4.9
A LCR da AC Raiz é atualizada a cada 90 (noventa) dias. Em caso de revogação de certificado de AC de nível imediatamente ao seu, a AC Raiz emite nova LCR no prazo previsto no item 4.4.3 e notifica todas as ACs de nível imediatamente subseqüente ao seu.

DOC-ICP-01.4.4.10
Todos os certificados das ACs de nível imediatamente subseqüente ao da AC Raiz devem ter a validade verificada, na LCR da AC Raiz, antes de serem utilizados. Também deve ser verificada a autenticidade da LCR da AC Raiz, por meio da verificação da assinatura da AC Raiz e do período de validade da LCR.

DOC-ICP-01.4.4.11
Não serão aceitos pedidos de revogação on-line ao sistema de certificação da AC Raiz. A única forma de consulta on-line de status de certificado é a realizada por meio da LCR.

DOC-ICP-01.4.4.13
Informações de revogação de certificado de AC de nível imediatamente subseqüente ao da AC Raiz também podem ser divulgadas por meio de sua publicação no Diário Oficial da União ou na página web da AC Raiz.

DOC-ICP-01.4.2.4
A AC Raiz entrega o certificado emitido, em formato definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL, para o representante legal da AC credenciada presente à cerimônia.

DOC-ICP-01.6.1.4.1
A entrega do certificado da AC Raiz para as ACs de nível imediatamente subseqüente ao seu é feita no momento da disponibilização do certificado da AC, utilizando-se para isto o formato definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL.

DOC-ICP-01.4.1.2
A AC deve encaminhar a solicitação de seu certificado à AC Raiz por meio de seus representantes legais, utilizando o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL.

DOC-ICP-01.6.1.5
O tamanho das chaves criptográficas assimétricas da AC Raiz e das ACs de nível imediatamente subseqüente ao seu encontra-se definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL.

DOC-ICP-01.7.3.1 - O certificado da AC Raiz é assinado com o uso do algoritmo definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL.

DOC-ICP-01.7.2.3
O certificado de AC de nível subseqüente ao da AC Raiz é assinado com o uso de algoritmo definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL.

DOC-ICP-01.6.1.1.1
O par de chaves criptográficas da AC Raiz é gerado pela própria AC Raiz, em hardware específico, conforme o detalhado em 6.1.8.

DOC-ICP-01.6.1.6
Os parâmetros de geração de chaves assimétricas da AC Raiz adotam o padrão definido no documento PADRÕES E ALGORIOS CRIPTOGRÁFICOS DA ICP-BRASIL.

DOC-ICP-01.6.1.7
Os parâmetros são verificados de acordo com as normas referenciadas no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL.

DOC-ICP-01.6.1.8
A AC Raiz utiliza um componente seguro de hardware para a geração de seu par de

chaves, de seu certificado, dos certificados das ACs de nível imediatamente subseqüente ao seu e para a geração e assinatura de sua LCR. O componente seguro de hardware utiliza um mecanismo de detecção de violação.

DOC-ICP-01.6.1.9 - A chave privada da AC Raiz é utilizada apenas para a assinatura de seu próprio certificado, dos certificados das ACs de nível imediatamente subseqüente ao seu e de sua LCR.

DOC-ICP-01.6.2.1
O módulo criptográfico da AC Raiz adota o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL.

DOC-ICP-01.6.2.3
Não é permitida, no âmbito da ICP-Brasil, a custódia (escrow) das chaves privadas da AC Raiz ou das Acs de nível imediatamente subseqüente.

DOC-ICP-01.6.2.4.1
A AC Raiz 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 mantida pelo prazo de validade do certificado correspondente.

DOC-ICP-01.6.2.4.2
A AC Raiz não mantém cópia de segurança das chaves privadas das ACs de nível imediatamente subseqüente ao seu.

DOC-ICP-01.6.2.6
A chave privada da AC Raiz é inserida no módulo criptográfico de acordo com o estabelecido na RFC 2510.

DOC-ICP-01.6.2.7
A ativação da chave privada da AC Raiz é implementada por meio do módulo criptográfico, após identificação dos operadores responsáveis. Esta identificação é realizada por meio de senha e de dispositivo de controle de acesso em hardware (token).

DOC-ICP-01.6.2.8
Quando a chave privada da AC Raiz for desativada, em decorrência de expiração ou revogação, esta deve ser eliminada da memória do módulo criptográfico. Qualquer espaço em disco, onde a chave eventualmente estivesse armazenada, deve ser sobrescrito.

DOC-ICP-01.6.2.9
Além do estabelecido no item 6.2.8, todas as cópias de segurança da chave privada da AC-Raiz devem ser destruídas, como também todos os discos rígidos, tokens, módulos criptográficos e qualquer mídia de armazenamento que as tenham hospedado por algum período.

DOC-ICP-01.6.3.1
As chaves públicas da AC Raiz e das ACs de nível imediatamente subseqüente ao seu são armazenadas permanentemente, após a expiração dos certificados correspondentes, para verificação de assinaturas geradas durante seu prazo de validade.

DOC-ICP-01.6.3.2
A chave privada da AC Raiz é utilizada apenas durante o período de validade do certificado correspondente. A chave pública da AC Raiz 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.

DOC-ICP-01.6.4.1
Os dados de ativação da chave privada da AC Raiz são únicos e aleatórios, instalados fisicamente em dispositivos de controle de acesso em hardware (token).

DOC-ICP-01.6.4.2
Os dados de ativação da chave privada da AC Raiz são protegidos contra uso não autorizado por meio de mecanismo de criptografia e de controle de acesso físico.

DOC-ICP-01.6.8
O módulo criptográfico utilizado para armazenamento da chave privada da AC Raiz está em conformidade com o padrão definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL.

DOC-ICP-01.7.1
O formato de todos os certificados emitidos pela AC Raiz está em conformidade com o padrão ITU X.509 ou ISO/IEC 9594. O certificado da AC Raiz é o único certificado auto-assinado da ICP-Brasil, e possui validade de 13 (treze) anos, podendo este prazo ser revisto de acordo com as definições estabelecidas pelo CG da ICP-Brasil.

DOC-ICP-01.2.8
A chave privada de assinatura digital de cada AC credenciada é gerada e mantida pela própria AC, que deve assegurar seu sigilo. A divulgação ou utilização indevida da chave privada de assinatura pela AC é de sua inteira responsabilidade.

DOC-ICP-01.6.1.1.2
O par de chaves criptográficas de uma AC de nível imediatamente subseqüente ao da AC Raiz é gerado pela própria AC, após o deferimento do seu pedido de credenciamento e a conseqüente autorização de funcionamento no âmbito da ICP-Brasil.

DOC-ICP-01.6.1.1.3
O algoritmo a ser utilizado para as chaves criptográficas da AC Raiz está definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL.

DOC-ICP-01.6.1.3.1
A AC de nível imediatamente subseqüente ao da AC Raiz entrega à AC Raiz cópia de sua chave pública, em formato definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICPBRASIL.

DOC-ICP-01.6.1.3.2
Essa entrega é feita por representante legalmente constituído da AC, em cerimônia específica, em data e hora previamente estabelecidas pela AC Raiz. Todos os eventos ocorridos nessa cerimônia são registrados para fins de auditoria.

DOC-ICP-01.6.5.1.1
A geração do par de chaves da AC Raiz e dos certificados das ACs de nível imediatamente subseqüente ao seu deve ser realizada num ambiente off-line, para impedir o acesso remoto não autorizado. As informações utilizadas nesses procedimentos devem ser mantidas no ambiente off-line, com acesso restrito.

DOC-ICP-01.7.1.1
O certificado da AC Raiz implementa a versão 3 de certificado do padrão ITU X.509.

DOC-ICP-01.7.1.2
O certificado da AC Raiz implementa as seguintes extensões previstas na versão 3 do padrão ITU X.509:
a) basicConstraints: contém o campo cA=True. O campo pathLenConstraint não é utilizado.
b) keyUsage: contém apenas os bits keyCertSign(5) e cRLSign(6) ligados. Os demais bits estão desligados.
c) cRLDistributionPoints: contém o endereço na Web onde se obtém a LCR correspondente ao certificado:
i) para certificados emitidos até 29.07.2008: http://acraiz.icpbrasil.gov.br/LCRacraiz.crl ;
ii) para certificados a partir de 29.07.2008: http://acraiz.icpbrasil.gov.br/LCRacraizv1.crl.
d) Certificate Policies: especifica o Object Identifier (OID) da DPC da AC Raiz e o atributo id-qt-cps com o endereço na Web dessa DPC (http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf).
e) SubjectKeyIdentifier: contém o hash da chave pública da AC Raiz.

DOC-ICP-01.7.1.3
O certificado da AC Raiz é assinado com o uso do algoritmo definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICP-BRASIL.

DOC-ICP-01.7.1.4 - Os nomes do titular e do emissor do certificado da AC Raiz, constantes do campo “Distinguished Name” (DN), são os mesmos e seguem o padrão ITU X.500/ISO 9594, como abaixo descrito:
a) para certificado emitido em 30.11.2001:
C = BR
O = ICP-Brasil
OU = Instituto Nacional de Tecnologia da Informacao - ITI
CN = Autoridade Certificadora Raiz Brasileira
b) para certificado emitido em 29.07.2008:
C = BR
O = ICP-Brasil
OU = Instituto Nacional de Tecnologia da Informacao - ITI
CN = Autoridade Certificadora Raiz Brasileira v1

2 - Credenciamento da AC

DOC-ICP-01.2.1.1
Constituem obrigações da AC Raiz:
a) a geração e o gerenciamento do seu par de chaves criptográficas;
b) a emissão e distribuição do seu certificado digital;
c) a emissão, a expedição e a distribuição de certificados de AC de nível imediatamente subseqüente ao seu;
d) a publicação de certificados por ela emitidos;
e) a revogação de certificados por ela emitidos;
f) a emissão, o gerenciamento e a publicação de sua Lista de Certificados Revogados – LCR;
g) a fiscalização e a auditoria das ACs, das Autoridades de Carimbo do Tempo (ACTs), das ARs e dos Prestadores de Serviço de Suporte (PSS) habilitados em conformidade com os critérios estabelecidos pelo Comitê Gestor da ICP-Brasil (CG da ICP-Brasil);
h) a implementação de acordos de certificação cruzada, conforme as diretrizes estabelecidas pelo CG da ICP-Brasil;
i) adotar medidas de segurança e controle, previstas na DPC e na POLÍTICA DE SEGURANÇA DA ICP-BRASIL, envolvendo seus processos, procedimentos e atividades;
j) manter os processos, procedimentos e atividades em conformidade com a legislação vigente e com as normas, práticas e regras estabelecidas pelo CG da ICP-Brasil;
k) manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada; e
l) manter e testar regularmente seu Plano de Continuidade de Negócio (PCN).

DOC-ICP-01.5.3.6
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 Raiz suspende o seu acesso ao sistema de certificação e toma as medidas administrativas e legais cabíveis.

DOC-ICP-02.3
A PS abrange os seguintes aspectos:
a)Requisitos de Segurança Humana;
b)Requisitos de Segurança Física;
c)Requisitos de Segurança Lógica;
d)Requisitos de Segurança dos Recursos Criptográficos.

DOC-ICP-02.6.1.2
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.

DOC-ICP-02.9.3.3.6
O uso de senhas deve estar submetido a uma política específica para sua gerência e utilização.

DOC-ICP-01.5.3.1
Todo o pessoal da AC Raiz em atividades diretamente relacionadas com os processos de

emissão, expedição, distribuição, revogação e gerenciamento de certificados é admitido conforme o estabelecido na PS da ICP-Brasil.

DOC-ICP-01.5.3.8
A AC Raiz disponibiliza para todo o seu pessoal:
a) sua DPC;
b) a PS da ICP-Brasil;
c) documentação operacional relativa a suas atividades;
d) contratos, normas e políticas relevantes para suas atividades.

DOC-ICP-01.6.2
A chave privada da AC Raiz é armazenada de forma cifrada no mesmo componente seguro de hardware utilizado para sua geração. O acesso a esse componente é controlado por meio de chave criptográfica de ativação.

DOC-ICP-01.6.2.2
A chave criptográfica de ativação do componente seguro de hardware que armazena a chave privada da AC Raiz é dividida em 5 (cinco) partes e distribuída entre 5 (cinco) pessoas designadas pela AC Raiz. É necessária a presença de apenas 3 (três) dessas 5 (cinco) pessoas para a ativação do componente e a conseqüente utilização da chave privada da AC Raiz.

DOC-ICP-01.6.2.3
Não é permitida, no âmbito da ICP-Brasil, a custódia (escrow) das chaves privadas da AC Raiz ou das Acs de nível imediatamente subseqüente.

DOC-ICP-01.6.2.4.1
A AC Raiz 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 mantida pelo prazo de validade do certificado correspondente.

DOC-ICP-01.6.2.4.2
A AC Raiz não mantém cópia de segurança das chaves privadas das ACs de nível imediatamente subseqüente ao seu.

3 - Equipe Capacitada e habilitada

DOC-ICP-02.7.3.5.1
Acompanhar o desempenho e avaliar periodicamente os empregados ou servidores com o propósito de detectar a necessidade de atualização técnica e de segurança.

DOC-ICP-02.7.3.5.2
Dar aos empregados ou servidores das entidades acesso às informações, mediante o fornecimento de instruções e orientações sobre as medidas e procedimentos de segurança.

DOC-ICP-02.7.3.8.1
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.

DOC-ICP-02.7.3.8.2
Deverão ser motivo de registro atos, atitudes e comportamentos positivos e negativos relevantes, verificados durante o exercício profissional do empregado.

DOC-ICP-02.7.3.8.3
Os comportamentos incompatíveis, ou que possam gerar comprometimentos à segurança, deverão ser averiguados e comunicados à chefia imediata.

DOC-ICP-02.7.3.8.4
As chefias imediatas assegurarão que todos os empregados ou servidores tenham conhecimento e compreensão das normas e procedimentos de segurança em vigor.

DOC-ICP-02.6.1.3
Todo o pessoal deve receber as informações necessárias para cumprir adequadamente o que está determinado na PS.

DOC-ICP-02.6.1.4
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. Especialmente, o pessoal envolvido ou que se relaciona com os usuários deve estar treinado sobre ataques típicos de engenharia social, como proceder e como se proteger deles.

DOC-ICP-02.7.3.7
Deve ser definido um processo pelo qual será apresentada aos empregados, servidores e prestadores de serviço esta PS e as 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.

DOC-ICP-01.5.2.1.1
A AC Raiz garante a separação das tarefas para funções críticas, com o intuito de evitar

que um empregado de má fé utilize o sistema de certificação sem ser detectado. As ações de cada empregado estão limitadas de acordo com seu perfil.

DOC-ICP-01.5.2.1.2
A AC Raiz estabelece um mínimo de 3 (três) perfis distintos para sua operação, distinguindo as operações do dia-a-dia do sistema, o gerenciamento e auditoria dessas operações, bem como o gerenciamento de mudanças substanciais no sistema. A divisão de responsabilidades entre os três perfis é a seguinte:

DOC-ICP-01.5.2.1.3 - Gerente de Configurações:
a) configuração e manutenção do hardware e do software da AC Raiz;
b) início e término dos serviços da AC Raiz;

DOC-ICP-01.5.2.1.4 - Gerente de Segurança:
a) gerenciamento dos operadores da AC Raiz;
b) implementação das políticas de segurança da AC Raiz;
c) verificação dos registros de auditoria;
d) verificação do cumprimento desta DPC;

DOC-ICP-01.5.2.1.5 - Administrador do Sistema:
a) gerenciamento dos processos de iniciação dos usuários internos à AC Raiz;
b) emissão, expedição, distribuição, revogação e gerenciamento de certificados;
c) distribuição de cartões (tokens), quando for o caso.

DOC-ICP-01.5.2.1.6
Somente os empregados responsáveis por tarefas descritas para o Gerente de Configurações e o Administrador do Sistema têm acesso ao software e ao hardware do sistema de certificação da AC Raiz.

DOC-ICP-01.5.2.2.1
Controle multiusuário, via o uso de segredo compartilhado, é requerido para a geração e a utilização da chave privada da AC Raiz, conforme o descrito no DOC-ICP-01.6.2.2.

DOC-ICP-01.5.2.2.2
Todas as tarefas executadas no ambiente onde está localizado o equipamento de certificação da AC Raiz necessitam da presença de no mínimo 2 (dois) empregados da AC Raiz. As demais tarefas da AC Raiz podem ser executadas por um único empregado.

DOC-ICP-01.5.2.3.1
Todo empregado da AC Raiz tem sua identidade e perfil verificados antes de:
a) ser incluído em uma lista de acesso às instalações da AC Raiz;
b) ser incluído em uma lista para acesso físico ao sistema de certificação da AC Raiz;
c) receber um certificado para executar suas atividades operacionais na AC Raiz;
d) receber uma conta no sistema de certificação da AC Raiz.

DOC-ICP-01.5.2.3.2
Os certificados, contas e senhas utilizados para identificação e autenticação dos empregados devem:

a) ser diretamente atribuídos a um único empregado;
b) não permitir compartilhamento;
c) ser restritos às ações associadas ao perfil para o qual foram criados.

DOC-ICP-01.5.3.3
Todo o pessoal da AC Raiz em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados recebe treinamento suficiente para o domínio dos seguintes temas:
a) princípios e mecanismos de segurança da AC Raiz;
b) software de certificação em uso na AC Raiz;
c) atividades sob sua responsabilidade; e
d) procedimentos de recuperação de desastres e de continuidade do negócio.

DOC-ICP-01.5.3.4
Todo o pessoal da AC Raiz em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados manter-se-á atualizado sobre eventuais mudanças tecnológicas no sistema de certificação da AC Raiz. Treinamentos de reciclagem são realizados pela AC Raiz sempre que houver a necessidade.

DOC-ICP-02.10.2.1
Os processos que envolvem as chaves criptográficas utilizadas nos sistemas criptográficos da ICPBrasil deverão ser executados por um número mínimo e essencial de pessoas, assim como devem estar submetidos a mecanismos de controle considerados adequados pelo CG ICP-Brasil.

DOC-ICP-02.10.2.2
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.

DOC-ICP-02.13.2.3
Todo pessoal envolvido com o PCN deve receber um treinamento específico para poder enfrentar estes incidentes.

DOC-ICP-02.6.3
Todos os ativos das entidades integrantes da ICP-Brasil devem ser inventariados, classificados, permanentemente atualizados pela própria entidade, e possuírem gestor responsável formalmente designado.

DOC-ICP-02.7.3.1
Devem ser adotados critérios rígidos para o processo seletivo de candidatos, com o propósito de selecionar, para os quadros das entidades integrantes da ICP-Brasil, pessoas reconhecidamente idôneas e sem antecedentes que possam comprometer a segurança ou credibilidade das entidades.

DOC-ICP-02.7.3.2
Nenhuma entidade participante da ICP-Brasil admitirá estagiários no exercício de

atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados.

DOC-ICP-02.7.3.3
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 integrantes da ICP-Brasil.

DOC-ICP-02.7.3.6.1
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.

DOC-ICP-02.7.3.6.2
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.

DOC-ICP-02.7.3.6.3
Será de um ano o prazo de validade máximo de concessão a um indivíduo de uma credencial de segurança. Este prazo poderá ser prorrogado por igual período, quantas vezes for necessário, por ato da Autoridade Outorgante, enquanto exigir a necessidade do serviço.

DOC-ICP-02.7.4.1
São deveres dos empregados ou servidores:
a)preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos recursos de processamento de informações;
b)cumprir a PS, sob pena de incorrer nas sanções disciplinares e legais cabíveis;
c)utilizar os Sistemas de Informações das entidades e os recursos a ela relacionados somente para os fins previstos pela Gerência de Segurança;
d)cumprir as regras específicas de proteção estabelecidas aos ativos de informação;
e)manter o caráter sigiloso da senha de acesso aos recursos e sistemas das entidades;
f)não compartilhar, sob qualquer forma, informações confidenciais com outros que não tenham a devida autorização de acesso;
g)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;
h)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;
i)comunicar ao seu superior imediato o conhecimento de qualquer irregularidade ou desvio.

DOC-ICP-02.7.4.2
São responsabilidades das chefias:
a)gerenciar o cumprimento da PS, por parte de seus empregados ou servidores;

b)identificar os desvios praticados e adotar as medidas corretivas apropriadas;
c)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;
d)proteger, em nível físico e lógico, os ativos de informação e de processamento das entidades participantes da ICP-Brasil relacionados com sua área de atuação;
e)garantir que o pessoal sob sua supervisão compreenda e desempenhe a obrigação de proteger a Informação das entidades;
f)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;
g)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;
h)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.

DOC-ICP-02.7.4.3
São responsabilidades gerais:
a)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;
b)todos os ativos de informações deverão ter claramente definidos os responsáveis pelo seu uso;
c)todos os ativos de processamento das entidades devem estar relacionados no PCN.

DOC-ICP-02.7.4.4
São responsabilidades das Gerências de Segurança:
a)estabelecer as regras de proteção dos ativos das entidades participantes da ICP-Brasil;
b)decidir quanto às medidas a serem tomadas no caso de violação das regras estabelecidas;
c)revisar pelo menos anualmente, as regras de proteção estabelecidas;
d)restringir e controlar o acesso e os privilégios de usuários remotos e externos;
e)elaborar e manter atualizado o PCN;
f)executar as regras de proteção estabelecidas pela PS;
g)detectar, identificar, registrar e comunicar à AC Raiz as violações ou tentativas de acesso não autorizadas;
h)definir e aplicar, para cada usuário de Tecnologia da Informação - TI, restrições de acesso à Rede, como horário autorizado, dias autorizados, entre outras;
i)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.);
j)limitar o prazo de validade das contas de prestadores de serviço ao período da contratação;

k)excluir as contas inativas;
l)fornecer senhas de contas privilegiadas somente aos empregados que necessitem efetivamente dos privilégios, mantendo-se o devido registro e controle.

DOC-ICP-02.7.4.5
Devem ser previstas no contrato cláusulas que contemplem a responsabilidade dos prestadores de serviço no cumprimento desta PS e suas normas e procedimentos.

DOC-ICP-02.8.2.1
As responsabilidades pela segurança física dos sistemas das entidades deverão ser definidos e atribuídos a indivíduos claramente identificados na organização.

DOC-ICP-02.9.3.4.16
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.

DOC-ICP-02.7.3.1.2
Nenhuma entidade participante da ICP-Brasil admitirá estagiários no exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados.

DOC-ICP-02.7.3.4.1
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.

DOC-ICP-02.7.3.4.2
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.

DOC-ICP-01.5.3
Todos os empregados da AC Raiz que executam tarefas operacionais têm registrado em contrato ou termo de responsabilidade:
a) os termos e as condições do perfil que ocupam;
b) o compromisso de não divulgar informações sigilosas a que têm acesso.

DOC-ICP-01.5.3.1
Todo o pessoal da AC Raiz 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 ICP-Brasil.

DOC-ICP-01.5.3.7
O pessoal da AC Raiz no exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é contratado conforme o estabelecido na Política de Segurança da ICP-Brasil.

DOC-ICP-02.7.3.9.1
O acesso de ex-empregados às instalações, quando necessário, será restrito às áreas de acesso público.

DOC-ICP-02.7.3.9.2
Sua credencial, identificação, crachá, uso de equipamentos, mecanismos e acessos físicos e lógicos devem ser revogados.

DOC-ICP-02.7.3.10
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, devendo-se checar junto à unidade de Recursos Humanos e quantas mais unidades forem necessárias a veracidade das informações.

DOC-ICP-02.7.3.11
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.

DOC-ICP-02.6.1.5
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.

DOC-ICP-01.5.3.6
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 Raiz suspende o seu acesso ao sistema de certificação e toma as medidas administrativas e legais cabíveis.

DOC-ICP-01.4.5.1.3
Todos os registros de auditoria, eletrônicos ou manuais, devem conter a data e a hora do evento e a identidade do usuário que o causou. A AC Raiz também coleta e consolida, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo sistema de certificação, tais como:
a) registros de acessos físicos;
b) manutenção e mudanças na configuração dos seus sistemas
c) mudanças de pessoal;
d) relatórios de discrepância e comprometimento;
e) registros de destruição de mídia contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuário.

4 - Segurança Física

DOC-ICP-01.5.1.3.2
A área tem um sistema de ar condicionado tolerante a falhas que controla calor e umidade, independente do sistema de ar condicionado do edifício onde está localizado.

DOC-ICP-02.9.3.3.14
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.

DOC-ICP-01.5.1.3.1
A sala-cofre da AC Raiz, além de conectada à rede elétrica, dispõe dos seguintes recursos, que permitem sua operação ininterrupta, mesmo em caso de interrupção no fornecimento de energia:
a) gerador de porte compatível;
b) gerador de reserva;
c) sistema de no-breaks;
d) sistema de aterramento e proteção a descargas atmosféricas;
e) iluminação de emergência.

DOC-ICP-01.6.5.1.1
A geração do par de chaves da AC Raiz e dos certificados das ACs de nível imediatamente subsequente ao seu deve ser realizada num ambiente off-line, para impedir o acesso remoto não autorizado. As informações utilizadas nesses procedimentos devem ser mantidas no ambiente off-line, com acesso restrito.

DOC-ICP-01.6.5.1.2
Cada computador servidor da AC Raiz diretamente relacionado com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados possui as seguintes características:
a) controle de acesso aos serviços e perfis da AC Raiz;
b) clara separação das tarefas e atribuições relacionadas a cada perfil da AC Raiz;
c) uso de criptografia para segurança de base de dados;
d) geração e armazenamento de registros de auditoria da AC Raiz;
e) mecanismos internos de segurança para garantia da integridade de dados e processos críticos; e
f) mecanismos para cópias de segurança (backup).

DOC-ICP-01.6.5.1.3
Essas características são implementadas pelo sistema operacional ou por meio da combinação deste com o software de certificação e mecanismos de segurança física.

DOC-ICP-01.6.7
O computador servidor da AC Raiz que hospeda o sistema de certificação opera off-line, fisicamente desconectado de qualquer rede.

DOC-ICP-01.5.1.5.1
A sala-cofre possui sistema para detecção antecipada de fumaça através de partículas iônicas e sistema de extinção de incêndio por gás.

DOC-ICP-01.5.1.5.2
Em caso de incêndio nas instalações da AC Raiz, o aumento da temperatura interna, dentro da sala-cofre, não deverá exceder 50 (cinqüenta) graus Celsius e a sala deverá suportar essa condição por menos 1 (uma) hora.

DOC-ICP-02.8.2.2
A localização das instalações e o sistema de certificação da AC Raiz e das ACs não deverão ser publicamente identificados.

DOC-ICP-02.8.2.3
Sistemas de segurança para acesso físico deverão ser instalados para controlar e auditar o acesso aos sistemas de certificação.

DOC-ICP-02.8.2.4
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.

DOC-ICP-02.8.2.5
Chaves criptográficas sob custódia do responsável deverão ser fisicamente protegidas contra acesso não autorizado, uso ou duplicação.

DOC-ICP-02.8.2.6
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.

DOC-ICP-02.8.2.7
Os sistemas de AC e de ACT deverão estar localizados em área protegida ou afastada de fontes potentes de magnetismo ou interferência de rádio freqüência.

DOC-ICP-02.8.2.8
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.

DOC-ICP-02.8.2.9
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 ICP-Brasil e mantidas em local adequado e sob sigilo.

DOC-ICP-02.8.2.10
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.

DOC-ICP-02.8.2.11
Sistemas de detecção de intrusão deverão ser utilizados para monitorar e registrar os acessos físicos aos sistemas de certificação nas horas de utilização.

DOC-ICP-02.8.2.13
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.

DOC-ICP-02.8.2.14
Nas instalações das entidades integrantes da ICP-Brasil, 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.

DOC-ICP-02.8.2.15
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.

DOC-ICP-02.8.2.16
Os ambientes onde ocorrem os processos críticos das entidades integrantes da ICP-Brasil deverão ser monitorados, em tempo real, com as imagens registradas por meio de sistemas de Circuito Fechado de Televisão - CFTV.

DOC-ICP-02.8.2.17
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.

DOC-ICP-02.9.3.3.2
Componentes críticos da rede local devem ser mantidos em salas protegidas e com acesso físico e lógico controlado, devendo ser protegidos contra danos, furtos, roubos e intempéries.

DOC-ICP-02.9.3.3.11
Devem ser adotadas proteções físicas adicionais para os recursos de rede considerados críticos.

DOC-ICP-02.9.3.3.13
A infra-estrutura de interligação lógica deve estar protegida contra danos mecânicos e

conexão não autorizada.

DOC-ICP-02.9.3.3.27
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.

DOC-ICP-02.9.3.3.28
A chave de certificação das ACs deverá estar protegida de acesso desautorizado, para garantir seu sigilo e integridade.

DOC-ICP-02.9.3.5.2
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).

DOC-ICP-01.4.5.1.2
A AC Raiz registra em arquivos de auditoria todos os eventos relacionados à segurança do sistema de certificação. Dentre outros, os seguintes eventos devem obrigatoriamente estar incluídos no arquivo de auditoria:
a) iniciação e desligamento do sistema de certificação;
b) tentativas de criar, remover, definir senhas ou mudar os privilégios de sistema dos operadores da AC Raiz;
c) mudanças na configuração da AC Raiz e/ou nas suas chaves;
d) mudanças nas políticas de criação de certificados;
e) tentativas de acesso (login) e de saída do sistema (logoff);
f) tentativas não-autorizadas de acesso aos arquivos de sistema;
g) geração de chaves próprias da AC Raiz;
h) emissão e revogação de certificados;
i) geração de LCR;
j) tentativas de iniciar, remover, habilitar e desabilitar usuários, e de atualizar e recuperar suas chaves; e
k) operações falhas de escrita e leitura no diretório de certificados e da LCR.

DOC-ICP-01.5.1.1
A AC Raiz da ICP-Brasil, para a execução dos seus serviços ligados ao ciclo de vida do certificado, utiliza instalações homologadas pelo CG da ICP-Brasil.

DOC-ICP-01.5.1.2.1
O acesso físico às dependências da AC Raiz onde são realizadas as atividades de AC Raiz é gerenciado e controlado internamente conforme o previsto na Política de Segurança da ICP-Brasil. 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.

DOC-ICP-01.5.1.2.2
O sistema de certificação da AC Raiz está situado em uma sala-cofre, localizada nas suas instalações. Segurança patrimonial e controles de segurança biométricos restringem o

acesso aos equipamentos da sala-cofre.

DOC-ICP-01.5.2.3.1
Todo empregado da AC Raiz tem sua identidade e perfil verificados antes de:
a) ser incluído em uma lista de acesso às instalações da AC Raiz;
b) ser incluído em uma lista para acesso físico ao sistema de certificação da AC Raiz;
c) receber um certificado para executar suas atividades operacionais na AC Raiz;
d) receber uma conta no sistema de certificação da AC Raiz.

DOC-ICP-01.5.1.4
A sala-cofre da AC Raiz é construída na forma de uma célula estanque, inteiriça, imune a infiltrações e inundações.

5 - Segurança Lógica

DOC-ICP-02.9.3.1.5
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.

DOC-ICP-02.9.3.3.1
O tráfego das informações no ambiente de rede deve ser protegido contra danos ou perdas, bem como acesso, uso ou exposição indevidos, incluindo-se o “Efeito Tempest”.

DOC-ICP-02.9.3.3.19
Mecanismos de segurança baseados em sistemas de proteção de acesso () devem ser utilizados para proteger as transações entre redes externas e a rede interna da entidade.

DOC-ICP-02.9.3.3.27
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.

DOC-ICP-02.9.3.3.3
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.

DOC-ICP-02.9.3.3.4
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.

DOC-ICP-02.9.3.5.12
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.

DOC-ICP-02.9.3.5.3
Devem ser adotadas medidas de segurança lógica referentes a combate a vírus, backup , controle de acesso e uso de software não autorizado.

DOC-ICP-02.9.3.6
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.

DOC-ICP-01.4.5.1.2
A AC Raiz registra em arquivos de auditoria todos os eventos relacionados à segurança

do sistema de certificação. Dentre outros, os seguintes eventos devem obrigatoriamente estar incluídos no arquivo de auditoria:
a) iniciação e desligamento do sistema de certificação;
b) tentativas de criar, remover, definir senhas ou mudar os privilégios de sistema dos operadores da AC Raiz;
c) mudanças na configuração da AC Raiz e/ou nas suas chaves;
d) mudanças nas políticas de criação de certificados;
e) tentativas de acesso (login) e de saída do sistema (logoff);
f) tentativas não-autorizadas de acesso aos arquivos de sistema;
g) geração de chaves próprias da AC Raiz;
h) emissão e revogação de certificados;
i) geração de LCR;
j) tentativas de iniciar, remover, habilitar e desabilitar usuários, e de atualizar e recuperar suas chaves; e
k) operações falhas de escrita e leitura no diretório de certificados e da LCR.

DOC-ICP-01.5.1.1
A AC Raiz da ICP-Brasil, para a execução dos seus serviços ligados ao ciclo de vida do certificado, utiliza instalações homologadas pelo CG da ICP-Brasil.

DOC-ICP-01.6.2.6
A chave privada da AC Raiz é inserida no módulo criptográfico de acordo com o estabelecido na RFC 2510.

DOC-ICP-01.6.5.1.2
Cada computador servidor da AC Raiz diretamente relacionado com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados possui as seguintes características:
a) controle de acesso aos serviços e perfis da AC Raiz;
b) clara separação das tarefas e atribuições relacionadas a cada perfil da AC Raiz;
c) uso de criptografia para segurança de base de dados;
d) geração e armazenamento de registros de auditoria da AC Raiz;
e) mecanismos internos de segurança para garantia da integridade de dados e processos críticos;
f) mecanismos para cópias de segurança (backup).

DOC-ICP-02.6.1.6
Previsão de mecanismo e repositório centralizado para ativação e manutenção de trilhas, 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.

DOC-ICP-02.9.2.3
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.

DOC-ICP-02.9.3.1.3

Os arquivos de logs 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 ou DPCT, para identificar tendências, falhas ou usos indevidos. Os logs devem ser protegidos e armazenados de acordo com sua classificação.

DOC-ICP-02.9.3.2.2
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.

DOC-ICP-02.9.3.2.3
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.

DOC-ICP-02.9.3.3.10
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.

DOC-ICP-02.9.3.3.20
Os registros de eventos devem ser analisados periodicamente, no menor prazo possível e em intervalos de tempo adequados.

DOC-ICP-02.9.3.4.15
O registro das atividades () do sistema de controle de acesso deve ser definido 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.

DOC-ICP-01.4.5.1.3 - Tipos de eventos registrados
A AC responsável pela DPC deverá também registrar, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo seu sistema de certificação, tais como:
a) registros de acessos físicos;
b) manutenção e mudanças na configuração de seus sistemas;
c) mudanças de pessoal e de perfis qualificados;
d) relatórios de discrepância e comprometimento; e
e) registros de destruição de mídias de armazenamento contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuários.

DOC-ICP-01.4.5.2.1
A AC Raiz garante que seus registros de auditoria são analisados mensalmente, sempre que houver utilização de seu sistema de certificação (equipamento off-line, que permanece desligado grande parte do tempo) ou em caso de suspeita de

comprometimento da segurança.

DOC-ICP-01.4.5.2.2
Todos os eventos significativos são explicados em relatório de auditoria de registros. Tal análise envolve uma inspeção breve de todos os registros, verificando que não foram alterados, seguida de uma investigação mais detalhada de quaisquer alertas ou irregularidades nos mesmos. Todas as ações tomadas em decorrência dessa análise são documentadas.

DOC-ICP-01.4.5.3
A AC Raiz mantém em suas próprias instalações os seus registros de auditoria por pelo menos 2 (dois) meses e, subseqüentemente, os armazena da maneira descrita no item 4.6.

DOC-ICP-01.4.5.4
O sistema de registro de eventos de auditoria inclui mecanismos para proteger os arquivos de auditoria contra leitura não autorizada, modificação e remoção. Informações manuais de auditoria também são protegidas contra a leitura não autorizada, modificação e remoção.

DOC-ICP-01.4.5.5
Os registros de eventos e sumários de auditoria do equipamento off-line utilizado pela AC Raiz têm cópias de segurança mensais ou sempre que houver alguma utilização desse equipamento.

DOC-ICP-01.4.5.7
Quando um evento é registrado pelo conjunto de sistemas de auditoria, nenhuma notificação é enviada à pessoa, organização, dispositivo ou aplicação que causou o evento.

DOC-ICP-01.4.5.8
Os eventos que representem possível vulnerabilidade, detectados na análise mensal dos registros de auditoria, são analisados detalhadamente e, dependendo de sua gravidade, são registrados em separado. Como decorrência, ações corretivas são implementadas e registradas para fins de auditoria.

DOC-ICP-01.4.6.1
Informações de auditoria detalhadas no item 4.5.1 e os processos de credenciamento de AC de nível imediatamente subseqüente ao da AC Raiz.

DOC-ICP-01.4.6.2
A documentação relativa aos eventos relacionados no item anterior são retidos pelo seguinte período:
a) certificados de assinatura digital e respectivas LCR deverão ser retidos permanentemente, para fins de consulta histórica;
b) as cópias dos processos de credenciamento de AC por no mínimo, por 30 (trinta) anos a contar da data de expiração ou revogação do certificado; e
c) as demais informações, inclusive arquivos de auditoria, deverão ser retidas por, no

mínimo, 6 (seis) anos.

DOC-ICP-01.6.7

O computador servidor da AC Raiz que hospeda o sistema de certificação opera off-line, fisicamente desconectado de qualquer rede.

DOC-ICP-02.9.3.2.9

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

DOC-ICP-01.4.6.4.1

Uma segunda cópia de todo o material descrito no item 4.6.1 é armazenada em loca externo à AC Raiz, recebendo o mesmo tipo de proteção utilizada por ela.

DOC-ICP-01.4.6.4.2

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

DOC-ICP-01.4.6.4.3

A AC Raiz verifica a integridade das cópias de segurança a cada 6 (seis) meses.

DOC-ICP-01.4.8.1

Procedimentos descritos no PCN (Plano de Continuidade de Negócio) da AC Raiz.

DOC-ICP-01.5.1.6

Para garantir a segurança de mídia armazenada, a AC Raiz dispõe de ambientes específicos que garantem que as mídias neles armazenadas não sofram nenhum tipo de dano gerado por fatores externos.

DOC-ICP-01.6.3.1

As chaves públicas da AC Raiz e das ACs de nível imediatamente subseqüente ao seu são armazenadas permanentemente, após a expiração dos certificados correspondentes, para verificação de assinaturas geradas durante seu prazo de validade.

DOC-ICP-02.9.3.3.16

Devem ser observadas as questões envolvendo propriedade intelectual quando da cópia de software ou arquivos de outras localidades.

DOC-ICP-02.6.1.5

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.

DOC-ICP-02.9.3.1.2

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.

DOC-ICP-02.9.3.2.1
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.

DOC-ICP-02.9.3.2.5
Proteção lógica adicional (criptografia) deve ser adotada para evitar o acesso não-autorizado às informações.

DOC-ICP-02.9.3.2.8
O acesso remoto a máquinas servidoras deve ser realizado adotando os mecanismos de segurança pré-definidos para evitar ameaças à integridade e sigilo do serviço.

DOC-ICP-02.9.3.3.12
Proteção lógica adicional deve ser adotada para evitar o acesso não-autorizado às informações.

DOC-ICP-02.9.3.3.18
Todo serviço de rede não explicitamente autorizado deve ser bloqueado ou desabilitado.

DOC-ICP-02.9.3.3.2
Componentes críticos da rede local devem ser mantidos em salas protegidas e com acesso físico e lógico controlado, devendo ser protegidos contra danos, furtos, roubos e intempéries.

DOC-ICP-02.9.3.3.22
Todos os recursos considerados críticos para o ambiente de rede, e que possuam mecanismos de controle de acesso, deverão fazer uso de tal controle.

DOC-ICP-02.9.3.3.28
A chave de certificação das ACs deverá estar protegida de acesso desautorizado, para garantir seu sigilo e integridade.

DOC-ICP-02.9.3.3.7
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.

DOC-ICP-02.9.3.4.1
Usuários e aplicações que necessitem ter acesso a recursos das entidades da ICP-Brasil devem ser identificados e autenticados.

DOC-ICP-02.9.3.4.10
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.

DOC-ICP-02.9.3.4.11
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.

DOC-ICP-02.9.3.4.12
Devem ser adotados critérios para bloquear ou desativar usuários de acordo com período pré-definido sem acesso e tentativas sucessivas de acesso mal sucedidas.

DOC-ICP-02.9.3.4.13
O sistema de controle de acesso deve solicitar nova autenticação após certo tempo de inatividade da sessão (out).

DOC-ICP-02.9.3.4.14
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.

DOC-ICP-02.9.3.4.2
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.

DOC-ICP-02.9.3.4.3
Nenhum usuário deve ser capaz de obter os direitos de acesso de outro usuário.

DOC-ICP-02.9.3.4.4
A informação que especifica os direitos de acesso de cada usuário ou aplicação deve ser protegida contra modificações não autorizadas.

DOC-ICP-02.9.3.4.5
O arquivo de senhas deve ser criptografado e ter o acesso controlado.

DOC-ICP-02.9.3.4.6
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).

DOC-ICP-02.9.3.4.7
As senhas devem ser individuais, secretas, intransferíveis e ser protegidas com grau de segurança compatível com a informação associada.

DOC-ICP-02.9.3.4.8
O sistema de controle de acesso deve possuir mecanismos que impeçam a geração de senhas fracas ou óbvias.

DOC-ICP-02.9.3.4.9
As seguintes características das senhas devem estar definidas de forma adequada:

conjunto de caracteres permitidos, tamanho mínimo e máximo, prazo de validade máxima, forma de troca e restrições específicas.

DOC-ICP-02.9.3.5.1
As estações de trabalho, incluindo equipamentos portáteis ou alone, e informações devem ser protegidos contra danos ou perdas, bem como acesso, uso ou exposição indevidos.

DOC-ICP-02.9.3.5.2
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).

DOC-ICP-01..1.5
São disponibilizados no repositório da AC Raiz, logo após sua emissão, os certificados por ela emitidos e sua LCR.

DOC-ICP-01.2.6.3.1
Não há qualquer restrição ao acesso para consulta a esta DPC, aos certificados emitidos e à LCR da AC Raiz.

DOC-ICP-01.2.6.3.2
São utilizados controles de acesso apropriados para restringir a possibilidade de escrita ou modificação dessas informações a pessoal autorizado.

DOC-ICP-01.2.6.4
O repositório da AC Raiz está disponível para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

DOC-ICP-01.5.1.2.2
O sistema de certificação da AC Raiz está situado em uma sala-cofre, localizada nas suas instalações. Segurança patrimonial e controles de segurança biométricos restringem o acesso aos equipamentos da sala-cofre.

DOC-ICP-01.5.2.2.2
Todas as tarefas executadas no ambiente onde está localizado o equipamento de certificação da AC Raiz necessitam da presença de no mínimo 2 (dois) empregados da AC Raiz. As demais tarefas da AC Raiz podem ser executadas por um único empregado.

DOC-ICP-01. 5.2.3.1
Todo empregado da AC Raiz tem sua identidade e perfil verificados antes de:
a) ser incluído em uma lista de acesso às instalações da AC Raiz;
b) ser incluído em uma lista para acesso físico ao sistema de certificação da AC Raiz;
c) receber um certificado para executar suas atividades operacionais na AC Raiz;
d) receber uma conta no sistema de certificação da AC Raiz.

DOC-ICP-01.5.2.3.2
Os certificados, contas e senhas utilizados para identificação e autenticação dos

empregados devem:
a) ser diretamente atribuídos a um único empregado;
b) não permitir compartilhamento;
c) ser restritos às ações associadas ao perfil para o qual foram criados.

DOC-ICP-01.5.3.6
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 Raiz suspende o seu acesso ao sistema de certificação e toma as medidas administrativas e legais cabíveis.

DOC-ICP-01. 6.5.1.2
Cada computador servidor da AC Raiz diretamente relacionado com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados possui as seguintes características:
a) controle de acesso aos serviços e perfis da AC Raiz;
b) clara separação das tarefas e atribuições relacionadas a cada perfil da AC Raiz;
c) uso de criptografia para segurança de base de dados;
d) geração e armazenamento de registros de auditoria da AC Raiz;
e) mecanismos internos de segurança para garantia da integridade de dados e processos críticos; e
f) mecanismos para cópias de segurança (backup).

DOC-ICP-01.6.6.2
Uma metodologia formal de gerenciamento de configuração é usada para instalação e contínua manutenção do sistema de certificação da AC Raiz. O software de certificação da AC Raiz é instalado pelo próprio fabricante. Novas versões desse software somente serão instaladas após comunicação do fabricante e testes em ambiente de homologação da AC Raiz.

DOC-ICP-02.13.2.4
Um plano de ação de resposta a incidentes deverá ser estabelecido para todas as ACs integrantes da ICP-Brasil. Este plano deve prever, no mínimo, o tratamento adequado dos seguintes eventos:
comprometimento de controle de segurança em qualquer evento referenciado no PCN;
notificação à comunidade de usuários, se for o caso;
revogação dos certificados afetados, se for o caso;
procedimentos para interrupção ou suspensão de serviços e investigação;
análise e monitoramento de trilhas de auditoria; e
relacionamento com o público e com meios de comunicação, se for o caso.

DOC-ICP-02.9.3.3.9
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.

DOC-ICP-02.9.3.3.15
O tráfego de informações deve ser monitorado, a fim de verificar sua normalidade, assim como detectar situações anômalas do ponto de vista da segurança.

DOC-ICP-02.9.3.3.23
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.

DOC-ICP-02.9.3.3.24
Ambientes de rede considerados críticos devem ser isolados de outros ambientes de rede, de modo a garantir um nível adicional de segurança.

DOC-ICP-02.9.3.3.25
Conexões entre as redes das entidades da ICP-Brasil e redes externas deverão estar restritas somente àquelas que visem efetivar os processos.

DOC-ICP-02.9.3.3.26
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.

DOC-ICP-02.9.3.3.29
A segurança das comunicações intra-rede e inter-rede, entre os sistemas das entidades da ICP-Brasil, deverá ser garantida pelo uso de mecanismos que assegurem o sigilo e a integridade das informações trafegadas.

DOC-ICP-02.9.3.3.30
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.

DOC-ICP-01.5.1.2.1
O acesso físico às dependências da AC Raiz onde são realizadas as atividades de AC Raiz é gerenciado e controlado internamente conforme o previsto na Política de Segurança da ICP-Brasil. 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.

DOC-ICP-01.5.1.7
Todos os documentos em papel com informações sensíveis são destruídos antes de ir para o lixo. Todos os dispositivos eletrônicos não mais utilizáveis, que tenham sido anteriormente utilizados no armazenamento de informações sensíveis, são fisicamente destruídos.

DOC-ICP-01.6.2.2
A chave criptográfica de ativação do componente seguro de hardware que armazena a chave privada da AC Raiz é dividida em 5 (cinco) partes e distribuída entre 5 (cinco) pessoas designadas pela AC Raiz. É necessária a presença de apenas 3 (três) dessas 5 (cinco) pessoas para a ativação do componente e a conseqüente utilização da chave privada da AC Raiz.

DOC-ICP-01.6.2.4.1
A AC Raiz 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 mantida pelo prazo de validade do certificado correspondente.

DOC-ICP-01.6.2.4.2
A AC Raiz não mantém cópia de segurança das chaves privadas das ACs de nível imediatamente subseqüente ao seu.

DOC-ICP-01.6.2.7
A ativação da chave privada da AC Raiz é implementada por meio do módulo criptográfico, após identificação dos operadores responsáveis. Esta identificação é realizada por meio de senha e de dispositivo de controle de acesso em hardware (token).

DOC-ICP-01.6.2.8
Quando a chave privada da AC Raiz for desativada, em decorrência de expiração ou revogação, esta deve ser eliminada da memória do módulo criptográfico. Qualquer espaço em disco, onde a chave eventualmente estivesse armazenada, deve ser sobrescrito.

DOC-ICP-01.6.2.9
Além do estabelecido no item 6.2.8, todas as cópias de segurança da chave privada da AC-Raiz devem ser destruídas, como também todos os discos rígidos, tokens, módulos criptográficos e qualquer mídia de armazenamento que as tenham hospedado por algum período.

DOC-ICP-01.6.3.2
A chave privada da AC Raiz é utilizada apenas durante o período de validade do certificado correspondente. A chave pública da AC Raiz 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.

DOC-ICP-01.6.4.2
Os dados de ativação da chave privada da AC Raiz são protegidos contra uso não autorizado por meio de mecanismo de criptografia e de controle de acesso físico.

DOC-ICP-01.6.5.1.1
A geração do par de chaves da AC Raiz e dos certificados das ACs de nível imediatamente subseqüente ao seu deve ser realizada num ambiente off-line, para

impedir o acesso remoto não autorizado. As informações utilizadas nesses procedimentos devem ser mantidas no ambiente off-line, com acesso restrito.

6 - Manter PSC – Prestador de Serviço de Certificação

DOC-ICP-02.11.3
Deverão ser realizadas auditorias periódicas nas entidades integrantes da ICP-Brasil, pela AC Raiz ou por terceiros por ele autorizados, conforme o disposto no documento CRITÉRIOS E PROCEDIMENTOS PARA REALIZAÇÃO DE AUDITORIAS NAS ENTIDADES INTEGRANTES DA ICP-BRASIL. Esse documento trata do objetivo, freqüência e abrangência das auditorias, da identidade e qualificação do auditor e demais temas correlacionados.

DOC-ICP-01.2.7.4
As entidades integrantes da ICP-Brasil sofrem auditoria prévia, para fins de credenciamento, e auditorias anuais, para fins de manutenção de credenciamento, conforme disposto no documento citado no parágrafo anterior.

DOC-ICP-01.4.9
No caso de extinção da AC Raiz, devem ser tomadas, no mínimo, as seguintes providências:
a) notificação de todas as entidades integrantes da ICP-Brasil;
b) manutenção da operação da AC Raiz pelo período mínimo de 1 (um) ano após a notificação de sua extinção, salvo em casos de sucessão;
c) armazenamento dos dados da AC Raiz pelo período previsto na legislação.

DOC-ICP-01.1.3.2
A atividade de identificação e cadastramento das ACs de nível imediatamente subseqüente ao da AC Raiz será realizada junto com o processo de credenciamento, não havendo Autoridades de Registro (AR) no âmbito da AC Raiz.

DOC-ICP-01.1.3.3
A AC Raiz contrata o SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS (SERPRO) como prestador de serviços de suporte para disponibilização de infra-estrutura física e lógica e de recursos humanos especializados.

7 - Manter repositório

DOC-ICP-01.2.1.5
São disponibilizados no repositório da AC Raiz, logo após sua emissão, os certificados por ela emitidos e sua LCR.

DOC-ICP-01.2.6.1.1
O certificado da AC Raiz, sua LCR e os certificados das ACs de nível imediatamente subseqüente ao seu são publicados na página Web da AC Raiz http://acraiz.icpbrasil.gov.br, obedecendo às regras e os critérios estabelecidos nesta DPC.

DOC-ICP-01.2.6.1.2
A lista das Autoridades Certificadoras que integram a ICP-Brasil também é encontrada na página Web da AC Raiz.

DOC-ICP-01.2.6.1.3
A disponibilidade das informações publicadas pela AC Raiz em sua página Web, tais como certificados, sua LCR, sua DPC, entre outras, é de 99,99% (noventa e nove inteiros e noventa e nove décimos por cento) do tempo, 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

DOC-ICP-01.2.6.1.4
A AC Raiz inclui nos certificados emitidos a identificação da sua página web.

DOC-ICP-01.2.6.4
O repositório da AC Raiz está disponível para consulta durante 24 (vinte e quatro) horas por dia, 7 (sete) dias por semana.

DOC-ICP-01.2.6.2
Certificados são publicados imediatamente após sua emissão. A publicação de LCR se dá conforme o item 4.4.9.

DOC-ICP-01.4.4.3.2
O processo de revogação de um certificado de AC é precedido, quando for o caso, do recebimento pela AC Raiz da solicitação de revogação e termina quando uma nova LCR, contendo o certificado revogado, é emitida e publicada pela AC Raiz. Concluído esse processo, a AC Raiz informa à AC afetada a revogação do certificado.

DOC-ICP-01.4.7.2
Expirado o certificado de uma AC de nível imediatamente subseqüente ao seu, a AC Raiz remove imediatamente esse certificado do diretório e de sua página Web, mantendo-o armazenado permanentemente para efeito de consulta histórica.

DOC-ICP-01.7.1.2
O certificado da AC Raiz implementa as seguintes extensões previstas na versão 3 do padrão ITU X.509:
a) basicConstraints: contém o campo cA=True. O campo pathLenConstraint não é

utilizado.
b) keyUsage: contém apenas os bits keyCertSign(5) e cRLSign(6) ligados. Os demais bits estão desligados.
c) cRLDistributionPoints: contém o endereço na *Web* onde se obtém a LCR correspondente ao certificado:
i) para certificados emitidos até 29.07.2008: http://acraiz.icpbrasil.gov.br/LCRacraiz.crl ;
ii) para certificados a partir de 29.07.2008: http://acraiz.icpbrasil.gov.br/LCRacraizv1.crl.
d) Certificate Policies: especifica o Object Identifier (OID) da DPC da AC Raiz e o atributo id-qt-cps com o endereço na Web dessa DPC (http://acraiz.icpbrasil.gov.br/DPCacraiz.pdf).
e) SubjectKeyIdentifier: contém o hash da chave pública da AC Raiz.

8 - Segurança da Informação

DOC-ICP-02.6.3
Todos os ativos das entidades integrantes da ICP-Brasil devem ser inventariados, classificados, permanentemente atualizados pela própria entidade, e possuírem gestor responsável formalmente designado

DOC-ICP-02.8.2.12
O inventário de todo o conjunto de ativos de processamento deve ser registrado e mantido atualizado, no mínimo, mensalmente.

DOC-ICP-02.9.2.5
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 participantes da ICP-Brasil.

DOC-ICP-02.9.3.5.10
O inventário dos recursos deve ser mantido atualizado.

DOC-ICP-01.4.5.6
O sistema de coleta de dados de auditoria interno à AC Raiz é uma combinação de processos automatizados e manuais, executada por seu pessoal operacional ou por seus sistemas.

DOC-ICP-01.4.6.6
Todos os sistemas de coleta de dados de arquivo utilizados pela AC Raiz em seus procedimentos operacionais são internos.

DOC-ICP-02.12.1
Processo que visa a proteção dos serviços das entidades integrantes da ICP-Brasil, por meio da eliminação, redução ou transferência dos riscos, conforme seja economicamente (e estrategicamente) mais viável. Os seguintes pontos principais devem ser identificados:
a)o que deve ser protegido;
b)análise de riscos (contra quem ou contra o quê deve ser protegido);
c)avaliação de riscos (análise da relação custo/benefício).

DOC-ICP-02.12.2
O gerenciamento de riscos consiste das seguintes fases principais:
a)identificação dos recursos a serem protegidos – hardware, rede, software, dados, informações pessoais, documentação, suprimentos;
b)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);
c)análise dos riscos (vulnerabilidades e impactos) - identificar as vulnerabilidades e os impactos associados;
d)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;
e)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;
f)monitoração da eficácia dos controles adotados para minimizar os riscos identificados;
g)reavaliação periódica dos riscos em intervalos de tempo não superiores a 6 (seis) meses;

DOC-ICP-02.12.3
Os riscos a serem avaliados para as entidades integrantes da ICP-Brasil compreendem, dentre outros, os seguintes:

Segmentos	***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
Sofware 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.

DOC-ICP-02.12.4.1
Os riscos que não puderem ser eliminados devem ter seus controles documentados e devem ser levados ao conhecimento da AC Raiz.

DOC-ICP-02.12.4.1.2
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).

DOC-ICP-02.12.4.1.3
É necessária a participação e o envolvimento da alta administração das entidades.

DOC-ICP-02.12.5
O gerenciamento de riscos nas entidades da ICP-Brasil pode ser conduzido de acordo com a metodologia padrão ou proprietária, desde que atendidos todos os tópicos relacionados.

DOC-ICP-02.13.2.2
Todas as ACs e ACTs integrantes da ICP-Brasil deverão apresentar um PCN que estabelecerá, no mínimo, o tratamento adequado dos seguintes eventos de segurança:
a)comprometimento da chave privada das entidades;
b)invasão do sistema e da rede interna da entidade;
c)incidentes de segurança física e lógica;
d)indisponibilidade da Infra-estrutura; e
e)fraudes ocorridas no registro do usuário, na emissão, expedição, distribuição, revogação e no gerenciamento de certificados.

DOC-ICP-02.6.2
O processo de gerenciamento de riscos deve ser revisto, no máximo a cada 18 (dezoito) meses, pela
própria entidade, para prevenção contra riscos, inclusive àqueles advindos de novas tecnologias, visando a elaboração de planos de ação apropriados para proteção aos componentes ameaçados.

DOC-ICP-02.6.4.1
Um Plano de Continuidade do Negócio – PCN deve ser implementado e testado, pelo menos uma vez por ano, para garantir a continuidade dos serviços críticos ao negócio.

DOC-ICP-02.6.4.2
Todas as ACs 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.

DOC-ICP-02.6.4.3
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.

DOC-ICP-02.6.4.4
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.

DOC-ICP-01.4.5.8
Os eventos que representem possível vulnerabilidade, detectados na análise mensal dos registros de auditoria, são analisados detalhadamente e, dependendo de sua gravidade, são registrados em separado. Como decorrência, ações corretivas são implementadas e registradas para fins de auditoria.

DOC-ICP-01.4.9.1
No caso de extinção da AC Raiz, devem ser tomadas, no mínimo, as seguintes providências:
a) notificação de todas as entidades integrantes da ICP-Brasil;
b) manutenção da operação da AC Raiz pelo período mínimo de 1 (um) ano após a

notificação de sua extinção, salvo em casos de sucessão;
c) armazenamento dos dados da AC Raiz pelo período previsto na legislação.

DOC-ICP-01.5.3.8
A AC Raiz disponibiliza para todo o seu pessoal:
a) sua DPC;
b) a PS da ICP-Brasil;
c) documentação operacional relativa a suas atividades;
d) contratos, normas e políticas relevantes para suas atividades.

DOC-ICP-02.9.2.1
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.

DOC-ICP-02.9.3.3.9
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.

DOC-ICP-02.9.3.5.9
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.

DOC-ICP-01.4.5.1.2
A AC Raiz registra em arquivos de auditoria todos os eventos relacionados à segurança do sistema de certificação. Dentre outros, os seguintes eventos devem obrigatoriamente estar incluídos no arquivo de auditoria:
a) iniciação e desligamento do sistema de certificação;
b) tentativas de criar, remover, definir senhas ou mudar os privilégios de sistema dos operadores da AC Raiz;
c) mudanças na configuração da AC Raiz e/ou nas suas chaves;
d) mudanças nas políticas de criação de certificados;
e) tentativas de acesso (login) e de saída do sistema (logoff);
f) tentativas não-autorizadas de acesso aos arquivos de sistema;
g) geração de chaves próprias da AC Raiz;
h) emissão e revogação de certificados;
i) geração de LCR;
j) tentativas de iniciar, remover, habilitar e desabilitar usuários, e de atualizar e recuperar suas chaves;
k) operações falhas de escrita e leitura no diretório de certificados e da LCR.

DOC-ICP-01.4.5.4
O sistema de registro de eventos de auditoria inclui mecanismos para proteger os arquivos de auditoria contra leitura não autorizada, modificação e remoção. Informações manuais de auditoria também são protegidas contra a leitura não autorizada, modificação

e remoção.

DOC-ICP-01.4.6.1
Informações de auditoria detalhadas no DOC-ICP-01.4.5.1 e os processos de credenciamento de AC de nível imediatamente subseqüente ao da AC Raiz.

DOC-ICP-01.4.6.2
A documentação relativa aos eventos relacionados no item anterior são retidos pelo seguinte período:
a) certificados de assinatura digital e respectivas LCR deverão ser retidos permanentemente, para fins de consulta histórica;
b) as cópias dos processos de credenciamento de AC por no mínimo, por 30 (trinta) anos a contar da data de expiração ou revogação do certificado; e
c) as demais informações, inclusive arquivos de auditoria, deverão ser retidas por, no mínimo, 6 (seis) anos.

DOC-ICP-01.4.6.3
Todos os arquivos são protegidos e armazenados fisicamente com os mesmos requisitos de segurança que os de sua instalação.

DOC-ICP-01.4.6.4.1
Uma segunda cópia de todo o material descrito no item 4.6.1 é armazenada em local externo à AC Raiz, recebendo o mesmo tipo de proteção utilizada por ela.

DOC-ICP-01.4.6.4.2
Essas cópias seguem os períodos de retenção definidos para os registros dos quais são cópias de segurança.

DOC-ICP-01.4.6.4.3
A AC Raiz verifica a integridade das cópias de segurança a cada 6 (seis) meses.

DOC-ICP-01.5.1.7
Todos os documentos em papel com informações sensíveis são destruídos antes de ir para o lixo. Todos os dispositivos eletrônicos não mais utilizáveis, que tenham sido anteriormente utilizados no armazenamento de informações sensíveis, são fisicamente destruídos.

9 - Sistemas Aplicativos

DOC-ICP-02.9.3.1.1
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.

DOC-ICP-02.9.3.1.5
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.

DOC-ICP-02.9.3.5.11
Os sistemas em uso devem solicitar nova autenticação após certo tempo de inatividade da sessão (time-out).

DOC-ICP-01.6.1.3.1
A AC de nível imediatamente subseqüente ao da AC Raiz entrega à AC Raiz cópia de sua chave pública, em formato definido no documento PADRÕES E ALGORITMOS CRIPTOGRÁFICOS DA ICPBRASIL.

DOC-ICP-01.6.1.3.2
Essa entrega é feita por representante legalmente constituído da AC, em cerimônia específica, em data e hora previamente estabelecidas pela AC Raiz. Todos os eventos ocorridos nessa cerimônia são registrados para fins de auditoria.

DOC-ICP-01.4.4.3.2
O processo de revogação de um certificado de AC é precedido, quando for o caso, do recebimento pela AC Raiz da solicitação de revogação e termina quando uma nova LCR, contendo o certificado revogado, é emitida e publicada pela AC Raiz. Concluído esse processo, a AC Raiz informa à AC afetada a revogação do certificado.

DOC-ICP-01.4.5.1.2
A AC Raiz registra em arquivos de auditoria todos os eventos relacionados à segurança do sistema de certificação. Dentre outros, os seguintes eventos devem obrigatoriamente estar incluídos no arquivo de auditoria:
a) iniciação e desligamento do sistema de certificação;
b) tentativas de criar, remover, definir senhas ou mudar os privilégios de sistema dos operadores da AC Raiz;
c) mudanças na configuração da AC Raiz e/ou nas suas chaves;
d) mudanças nas políticas de criação de certificados;
e) tentativas de acesso (login) e de saída do sistema (logoff);
f) tentativas não-autorizadas de acesso aos arquivos de sistema;
g) geração de chaves próprias da AC Raiz;
h) emissão e revogação de certificados;
i) geração de LCR;
j) tentativas de iniciar, remover, habilitar e desabilitar usuários, e de atualizar e recuperar

suas chaves;
k) operações falhas de escrita e leitura no diretório de certificados e da LCR.

DOC-ICP-02.9.3.1.5
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.

DOC-ICP-01.4.4.1.2
Um certificado deve obrigatoriamente ser revogado:
a) quando constatada emissão imprópria ou defeituosa do mesmo;
b) quando for necessária a alteração de qualquer informação constante no mesmo;
c) no caso de dissolução da AC titular do certificado; ou
d) no caso de comprometimento da chave privada da AC ou da sua mídia armazenadora.

DOC-ICP-01.4.5.7
Quando um evento é registrado pelo conjunto de sistemas de auditoria, nenhuma notificação é enviada à pessoa, organização, dispositivo ou aplicação que causou o evento.

DOC-ICP-01.6.2.2
A chave criptográfica de ativação do componente seguro de hardware que armazena a chave privada da AC Raiz é dividida em 5 (cinco) partes e distribuída entre 5 (cinco) pessoas designadas pela AC Raiz. É necessária a presença de apenas 3 (três) dessas 5 (cinco) pessoas para a ativação do componente e a conseqüente utilização da chave privada da AC Raiz.

DOC-ICP-01.6.4.1
Os dados de ativação da chave privada da AC Raiz são únicos e aleatórios, instalados fisicamente em dispositivos de controle de acesso em hardware (token).

DOC-ICP-01.6.5.1.1
A geração do par de chaves da AC Raiz e dos certificados das ACs de nível imediatamente subseqüente ao seu deve ser realizada num ambiente off-line, para impedir o acesso remoto não autorizado. As informações utilizadas nesses procedimentos devem ser mantidas no ambiente off-line, com acesso restrito.

DOC-ICP-01.6.5.1.2
Cada computador servidor da AC Raiz diretamente relacionado com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados possui as seguintes características:
a) controle de acesso aos serviços e perfis da AC Raiz;
b) clara separação das tarefas e atribuições relacionadas a cada perfil da AC Raiz;
c) uso de criptografia para segurança de base de dados;
d) geração e armazenamento de registros de auditoria da AC Raiz;
e) mecanismos internos de segurança para garantia da integridade de dados e processos críticos;

f) mecanismos para cópias de segurança (backup).

DOC-ICP-01.6.6.1
A AC Raiz utiliza um software projetado e desenvolvido por meio de uma metodologia formal rigorosa, específica para ambientes de segurança crítica.

DOC-ICP-01.6.6.2
Uma metodologia formal de gerenciamento de configuração é usada para instalação e contínua manutenção do sistema de certificação da AC Raiz. O software de certificação da AC Raiz é instalado pelo próprio fabricante. Novas versões desse software somente serão instaladas após comunicação do fabricante e testes em ambiente de homologação da AC Raiz.

DOC-ICP-02.9.3.1.4
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.

DOC-ICP-02.9.3.2.3
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.

DOC-ICP-02.9.3.2.4
As máquinas devem estar sincronizadas para permitir o rastreamento de eventos.

DOC-ICP-02.9.3.2.4
O sistema de registro de eventos de auditoria inclui mecanismos para proteger os arquivos de auditoria contra leitura não autorizada, modificação e remoção. Informações manuais de auditoria também são protegidas contra a leitura não autorizada, modificação e remoção.

DOC-ICP-02.9.3.2.6
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.

DOC-ICP-02.9.3.2.7
Devem ser utilizados somente softwares autorizados pela própria entidade nos seus equipamentos. Deve ser realizado o controle da distribuição e instalação dos mesmos.

DOC-ICP-02.9.3.3.3
Devem ser adotadas as facilidades de segurança disponíveis de forma inata nos ativos de processamento da rede.

DOC-ICP-02.9.3.3.4

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.

DOC-ICP-02.9.3.5.8
A entidade deverá estabelecer os aspectos de controle, distribuição e instalação de softwares utilizados.

DOC-ICP-01.6.5.1.1
A geração do par de chaves da AC Raiz e dos certificados das ACs de nível imediatamente subseqüente ao seu deve ser realizada num ambiente off-line, para impedir o acesso remoto não autorizado. As informações utilizadas nesses procedimentos devem ser mantidas no ambiente off-line, com acesso restrito.

DOC-ICP-01.6.5.1.3
Essas características são implementadas pelo sistema operacional ou por meio da combinação deste com o software de certificação e mecanismos de segurança física.

DOC-ICP-01.6.7
O computador servidor da AC Raiz que hospeda o sistema de certificação opera off-line, fisicamente desconectado de qualquer rede.

DOC-ICP-01.4.5.1.3
Todos os registros de auditoria, eletrônicos ou manuais, devem conter a data e a hora do evento e a identidade do usuário que o causou. A AC Raiz também coleta e consolida, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo sistema de certificação, tais como:
a) registros de acessos físicos;
b) manutenção e mudanças na configuração dos seus sistemas;
c) mudanças de pessoal;
d) relatórios de discrepância e comprometimento;
e) registros de destruição de mídia contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuário.

DOC-ICP-02.10.3.1
O processo de transporte de chaves criptográficas e demais parâmetros do sistema de criptografia da ICP-Brasil devem ter a integridade e o sigilo assegurados, por meio do emprego de soluções criptográficas específicas.

DOC-ICP-02.9.3.3.17
Informações sigilosas, corporativas ou que possam causar prejuízo às entidades devem estar protegidas e não devem ser enviadas para outras redes, sem proteção adequada.

DOC-ICP-02.9.3.5.4
As informações armazenadas em meios eletrônicos devem ser protegidas contra danos, furtos ou roubos, devendo ser adotados procedimentos de backup, definidos em documento específico.

DOC-ICP-02.9.3.5.5
Informações sigilosas, corporativas ou cuja divulgação possa causar prejuízo às entidades da ICP-Brasil, só devem ser utilizadas em equipamentos das entidades onde foram geradas ou naqueles por elas autorizadas, com controles adequados.

DOC-ICP-01.4.5.3
A AC Raiz mantém em suas próprias instalações os seus registros de auditoria por pelo menos 2 (dois) meses e, subseqüentemente, os armazena da maneira descrita no DOC-ICP-01.4.6.

DOC-ICP-01.4.5.4
O sistema de registro de eventos de auditoria inclui mecanismos para proteger os arquivos de auditoria contra leitura não autorizada, modificação e remoção. Informações manuais de auditoria também são protegidas contra a leitura não autorizada, modificação e remoção.

DOC-ICP-01.4.5.8
Os eventos que representem possível vulnerabilidade, detectados na análise mensal dos registros de auditoria, são analisados detalhadamente e, dependendo de sua gravidade, são registrados em separado. Como decorrência, ações corretivas são implementadas e registradas para fins de auditoria.

DOC-ICP-01.4.6.2
A documentação relativa aos eventos relacionados no item anterior são retidos pelo seguinte período:
a) certificados de assinatura digital e respectivas LCR deverão ser retidos permanentemente, para fins de consulta histórica;
b) as cópias dos processos de credenciamento de AC por no mínimo, por 30 (trinta) anos a contar da data de expiração ou revogação do certificado; e
c) as demais informações, inclusive arquivos de auditoria, deverão ser retidas por, no mínimo, 6 (seis) anos.

DOC-ICP-01.4.6.5
Informações de data e hora nos registros baseiam-se na hora oficial internacional, Coordinated Universal Time – UTC e obedecem ao formato YYYYMMDDHHMMSSZ incluindo segundos mesmo que o número de segundos seja zero.

10 - Sítio de Contingência

DOC-ICP-02.10.3.1
O processo de transporte de chaves criptográficas e demais parâmetros do sistema de criptografia da ICP-Brasil devem ter a integridade e o sigilo assegurados, por meio do emprego de soluções criptográficas específicas.

DOC-ICP-02.10.3.2
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 ICP-Brasil que pertençam a uma mesma organização.

DOC-ICP-01.4.6.4.1
Uma segunda cópia de todo o material descrito no item 4.6.1 é armazenada em local externo à AC Raiz, recebendo o mesmo tipo de proteção utilizada por ela.

DOC-ICP-01.4.6.4.2
Essas cópias seguem os períodos de retenção definidos para os registros dos quais são cópias de segurança.

DOC-ICP-01.4.6.4.3
A AC Raiz verifica a integridade das cópias de segurança a cada 6 (seis) meses.

DOC-ICP-02.13.2.1
Sistemas e dispositivos redundantes devem estar disponíveis para garantir a continuidade da operação dos serviços críticos de maneira oportuna.

DOC-ICP-01.5.1.8
A AC Raiz possui instalação de backup que atende aos mesmos requisitos de segurança da instalação principal. Sua localização é tal que, em caso de sinistro que torne inoperante a instalação principal, a instalação de backup não é atingida e pode se tornar totalmente operacional, em condições idênticas em, no máximo, 48 (quarenta e oito) horas.