Rede Nacional de Ensino e Pesquisa

Requisitos Mínimos para a Política de Certificados e Boas Práticas de Certificação da ICPEDU

Versão 2.0RC5 – 4 de abril de 2011

Sumário

Sobre este documento

Este documento estabelece os requisitos mínimos de observância obrigatória pelas Autoridades Certificadoras (AC) integrantes da Infra-estrutura de Chaves Públicas para Ensino e Pesquisa (ICPEDU) na elaboração de suas Políticas de Certificados, e sugere melhores práticas para gerenciamento do ciclo de vida dos certificados da ICPEDU para suportar a confecção de uma Declaração de Práticas de Certificação condizente.

A ICPEDU é um esforço da RNP que tem como objetivo principal incentivar a implantação de soluções de certificação digital nas instituições parceiras. Possui uma infra-estrutura hierárquica na qual os primeiros dois níveis consistem de uma AC raiz e dois tipos de ACs credenciadas, subordinadas a esta: ACs de serviços e ACs Institucionais.

Todas as instituições que desejem fazer parte da ICPEDU devem escrever uma Política de Certificados e uma Declaração de Práticas de Certificação e submetê-la para aprovação do Comitê Gestor.

Uma Política de Certificados (PC) é um conjunto de diretivas que define a aplicabilidade de um certificado a uma comunidade em particular e/ou classe de aplicação com requisitos de segurança em comum. O principal objetivo de uma PC é prover informações suficientes para que uma entidade confiante seja capaz de decidir se um certificado e o relacionamento que ele representa são confiáveis e apropriados para um uso em particular.

Uma Declaração de Práticas de Certificação (DPC) é a descrição das atividades (práticas) exercidas por uma Autoridade Certificadora para oferecer o serviço de gerenciamento do ciclo de vida de um certificado, isto é, sua emissão, revogação, renovação, re-emissão de chaves e publicação das informações relacionadas a estas. O objetivo de uma DPC é informar às partes confiantes das práticas empregadas na implementação da PC e na emissão de certificados.

A responsabilidade pela elaboração e manutenção deste documento de requisitos mínimos é da Autoridade de Gerência de Políticas da ICPEDU.

Escopo deste Documento

As provisões aqui descritas afetam diretamente as operações da AC Raiz da ICPEDU e suas ACs intermediárias, além das ACs de serviços. Ainda que não esteja no escopo deste documento estipular requisitos para ACs subordinadas às ACs intermediárias da ICPEDU, estas devem garantir diretamente, por meio de texto de suas DPCs, que as primeiras sigam as melhores práticas da ICPEDU.

As determinações deste documento objetivam estabelecer um grau de segurança mínimo para que uma AC da ICPEDU possa operar de forma confiável. Entretanto, ACs Institucionais (AC-UFSC e AC-UFMG, por exemplo) e ACs de Serviço (como a AC-Grades e a AC-SSL, por exemplo) possuem diferentes necessidades de segurança e confiabilidade. ACs Institucionais, por exemplo, devem levar em conta danos à imagem da instituição responsável durante a escolha dos controles de segurança apropriados à sua operação e, portanto, seu nível de confiabilidade deve ser o maior possível.

É necessário ressaltar que as sugestões de melhores práticas compreendem as atividades não só para atender aos requisitos mínimos das políticas de certificado da ICPEDU, mas também para contemplar padrões de segurança reconhecidos internacionalmente. As provisões aqui sugeridas podem ser adaptadas para melhor se adequar à realidade da instituição responsável.

Relação entre Política de Certificados e Declaração de Práticas de Certificação

Apesar de abordarem os mesmos temas e formarem um conjunto de informações de grande interesse para as entidades participantes da ICP em termos de confiança, os documentos se diferenciam em seus objetivos. Enquanto a PC determina os requisitos e padrões relacionados aos diversos tópicos abordados, a DPC estabelece o que deve ser feito pelos participantes para que estejam de acordo com esses padrões.

Em termos gerais, uma PC determina O QUE os participantes devem fazer; a DPC, por outro lado, determina COMO os participantes devem agir e implementar controles.

Organização do documento

Este documento está organizado em seções de acordo com àquelas especificadas no RFC 3647 [RFC3647], arcabouço seguido pela maioria dos documentos recentes de PC/DPC. Para facilitar o acompanhamento do RFC 3647, cada seção correspondente deste documento possui cinco componentes:

- **Descrição:** Descreve a proposta da seção de forma geral e que deve ser escrita nas PC/DPCs das ACs Credenciadas.
- **Requisitos mínimos:** Descreve as exigências nas políticas de certificado da Autoridade Certificadora para sua participação na ICPEDU.
- **Melhores práticas:** Descreve as melhores práticas de certificação, no âmbito da ICPEDU, para atingir os requisitos mínimos impostos pela PC e pela Política de Segurança da ICPEDU, a fim de dar apoio na confecção da DPC instruindo a operação da AC.
- **Exemplos de Texto:** Este subitem tem o intuito a apresentar ao leitor *uma idéia* de que deve ser escrito na seção correspondente da PC/DPC.

Lembre que cada AC é diferente, devida sua função e/ou implantação, alguns textos podem ser especificas uma particular tipo de AC então verifica se aplica no seu caso.

- **Auditoria:** [Por enquanto, apenas incluída em algumas seções] A **verificação** dos requisitos necessários pode acontecer em três tempos: a) durante a revisão da DPC (chamado aqui como uma auditoria pré-aprovação); durante a auditoria *on-site* feita antes a emissão do certificado da AC (que se chama auditoria pré-emissão); e/ou também durante a operação da AC, por exemplo, na auditoria interna anual da AC ou uma auditoria externa solicitada pela AGP (ambas neste documento identificadas como uma auditoria operacional).

Este texto está em conformidade não só com a Política de Segurança (PS) da ICPEDU, mas com diversos arcabouços e normas técnicas de segurança da informação, das quais trechos foram inseridos com o intuito de ajudar o leitor a compreender as seções. Os excertos em fonte `courier azul` foram retirados do RFC 3647 do Internet Engineering Task Force [RFC3647] enquanto os escritos em fonte `courier verde` foram retirados da norma ISO/IEC 17799:2005 [ISO17799]. Outros documentos, como o NIST SP 800-53 [NIST80053], são referenciados no próprio texto. Os trechos em *itálico* foram retirados de DPCs de Autoridades Certificadoras da ICPEDU, e podem ser usados como exemplos de texto.

O embasamento em PCs e DPCs já aprovadas é permitido e encorajado. Todavia, é importante salientar que as particularidades existentes em cada entidade devem ser consideradas no momento do desenvolvimento da política e na determinação da prática.

Os capítulos que seguem tratam das seções que devem, obrigatoriamente, estarem presentes nos documentos de PC e DPC da ICPEDU.

Avaliação de PC/DPCs

O Comitê Gestor (CG) da ICPEDU é o responsável pela aprovação da criação de uma AC diretamente subordinada à AC Raiz da ICPEDU. Esta aprovação depende, em parte, de um parecer favorável da Autoridade de Gerência de Políticas (AGP) com respeito aos documentos de PC e de DPC da AC solicitante. A AGP tem que irá verificar a conformidade da PC com os requisitos mínimos estabelecidos neste documento, e se as práticas na DPC atendem as políticas da PC.

Os avaliadores consideram as particularidades de uso e as necessidades de cada Instituição. Portanto, uma PC é dita em conformidade com os requisitos mínimos se suas provisões puderem ser consideradas equivalentes aos requerimentos de todas as seções indicadas neste documento.

Considerações Gerais

Os documentos de PC e DPC devem seguir o formato descrito no RFC 3647.

A AC Raiz e todas as ACs intermediárias devem sempre estar em conformidade com este documento de Requisitos Mínimos. Estas entidades têm **6 meses** para se adaptar a qualquer alteração feita neste documento, contados a partir de sua data de publicação da versão aprovada pela AGP.

Identificação do documento

Este documento é chamado *Requisitos Mínimos para as Políticas de Certificado e Boas Práticas de Certificação da ICPEDU,* comumente referida como "os Requisitos Mínimos da ICPEDU".

Titulo:	*Requisitos Mínimos para as Políticas de Certificado e Boas Práticas de Certificação da ICPEDU*
Versão:	Versão 2.0. RC5
Data:	4 de abril de 2011.
Aprovado:	??de 2011.
Expiração:	Este documento é válido até sua substituição por uma versão mais nova aprovada pela AGP.
ASN.1 OID:	O seguinte Object Identifier (OID) único identifica este documento:

1.3.6.1.4.1.15996.2.1.10.3.1.2.0

1.3.6.1.4.1	Prefixo para IANA private enterprises iso(1).org(3).dod(6).internet(1).private(4).enterprise(1)
15996	Identificador registrado pela RNP
2	ICPEDU
1	
10	AGP
3	Documentos
1	Requisitos Mínimos
2.0	Número de versão e subversão do documento

Lista de Alterações

No final deste documento, tem uma seção que descreve as alterações feitas nas seções deste documento, em relação das versões anteriores, inclusivo a grau de mudança em termos de política ou prática. Ainda mais, inclui uma lista de assuntos que estarão consideradas para versões futuras deste documento.

1. Introdução

O capítulo deve identificar e introduzir as entidades envolvidas, o escopo da atuação da Autoridade Certificadora, e aplicabilidade dos certificados emitidos no âmbito da ICP.

This component identifies and introduces the set of provisions, and indicates the types of entities and applications for which the document (either the CP or the CPS being written) is targeted.

1.1 Visão Geral

This subcomponent provides a general introduction to the document being written. This subcomponent can also be used to provide a synopsis of the PKI to which the CP or CPS applies. For example, it may set out different levels of assurance provided by certificates within the PKI. Depending on the complexity and scope of the particular PKI, a diagrammatic representation of the PKI might be useful here.

Descrição: Fornece uma introdução ao documento de PC/DPC e uma prévia sobre sua ICP, os tipos de certificados que oferece, seu propósito e seus participantes.

Requisitos mínimos: A subseção deve apresentar o documento, seu conteúdo e objetivos, além da conformidade com padrões existentes.

Sendo uma AC subordinada à AC-Raíz da ICPEDU, deve ser mencionar quem é a Rede Nacional de Ensino e Pesquisa (RNP), o que é a Infra-estrutura de Chaves Públicas para Pesquisa e Ensino (ICPEDU), e qual é o papel da AC intermediaria descrito na PC/DPC nesse contexto - se é **uma AC Institucional** ou **uma AC de Serviços**. A instituição que a AC intermediária representa, e sua localização, devem ser informadas nessa seção, além de outras informações relevantes sobre sua natureza.

Também deve apresentar para quem ou para qual finalidade se destinam os certificados. Qual é a entidade (departamento/setor) que seria responsável para a operação da AC? Qual é sua relação com a instituição e quais são suas responsabilidades dentro a instituição.

Melhores práticas: É importante que os documentos introduzam e descrevam claramente a natureza da ICP e seu propósito. A RFC 3647 sugere que "dependendo da complexidade e escopo de uma ICP em particular, uma representação por meio de diagrama pode ser útil" [RFC3647].

Exemplos de texto: de identificação da RNP e do serviço ICPEDU:

"A Rede Nacional de Pesquisa e Ensino (RNP) foi criada em 1989 pelo Ministério da Ciência e Tecnologia (MCT) com o objetivo de construir uma infra-estrutura de rede Internet nacional para a comunidade acadêmica. Uma das iniciativas atuais é a implantação de um serviço nacional de chaves publicas para seus usuários, chamado a Infra-estrutura de Chaves Publicas Educacional (ICPEDU)".

"O funcionamento da ICPEDU é determinado pelo Comitê Gestor (CG). A âncora de confiança da ICPEDU é a AC Raiz operada pelo Grupo de Operação da Autoridade Certificadora (GOPAC), que fica sob a responsabilidade da RNP. Subordinados à AC Raiz podem operar duas classes de autoridades certificadoras intermediárias: ACs Institucionais e ACs de Serviços. As autoridades certificadoras internas são aquelas criadas e operadas pelo GOPAC. As autoridades certificadoras externas são aquelas de responsabilidade das organizações parceiras, podendo ou não ser operadas pelo GOPAC".

Exemplos de texto: de identificação da AC e da instituição responsável:

*"A AC de Grades é uma **AC de Serviços externa**, operada pelo Instituto de Computação (IC) da Universidade Federal Fluminense (UFF) em nome da RNP.(...) Sob os cuidados do IC-UFF, o SGCLab é responsável pela manutenção e operação da Autoridade Certificadora de Grades da ICPEDU (daqui em diante conhecido como AC Grades). O principal objetivo da AC Grades é emitir certificados para autoridades certificadoras que apoiar atividades de pesquisa brasileira em e-Science e grades computacionais, como por exemplo a UFF Brazilian Grid CA do International Grid Trust Federation.".*

"A AC UFSC é a autoridade certificadora de nível mais alto no âmbito da UFSC e tem seu certificado digital assinado pela autoridade certificadora raiz da ICPEDU. A AC UFSC emite certificados digitais exclusivamente para autoridades certificadoras vinculadas a UFSC."

Exemplos de texto: da conformidade com padrões existentes.:

"Esta DPC foi elaborada de acordo com a RFC 3647 [RFC3647] e estabelece requisitos para a emissão e gerenciamento de certificados digitais em conformidade com os Requisitos Mínimos para a Política de Certificados e os Melhores Práticas de Certificação da ICPEDU [ReqMins2010] ".

Auditoria: Pré-aprovação.

1.2 Nome do Documento e Identificação

```
This subcomponent provides any applicable names or other identifiers,
including ASN.1 object identifiers, for the document. An example of
such a document name would be the US Federal Government Policy for
Secure E-mail.
```

Descrição: Apresenta o título do documento e outros identificadores relevantes. A principal forma de identificação de documentos é através de um identificador de objetos (OID). O OID é um conjunto único de números, organizados de forma hierárquica, que identifica atributos e objetos, incluindo diversos componentes em certificados X.509, como a política de certificação sob a qual o certificado foi emitido. Mais informações sobre OIDs podem ser encontradas no FAQ em http://www.oid-info.com/faq.htm.

Em um primeiro momento, deve-se verificar se sua instituição já tem um OID alocado para ela (o site http://www.oid-info.com/basic-search.htm pode fornecer essa informação, a partir do nome da instituição). Alternativamente, a lista da

IANA na pagina http://www.iana.org/assignments/enterprise-numbers pode ser utilizada (sendo necessário fazer uma busca no texto).

Caso a instituição já possua um OID, deve-se entrar em contato com a pessoa indicada na pesquisa. Este é o responsável pela gerência dos sub-arcos da Instituição, e deverá alocar um subconjunto de OIDs para ser usado e gerenciado no contexto da AC.

Caso a instituição não esteja cadastrada, é possível obter um OID da *Internet Assigned Numbers Authority* (IANA), umas das entidades responsáveis por manter e alocar códigos únicos para registros de entidades. Para solicitar o reconhecimento da sua instituição, basta preencher o formulário na pagina http://pen.iana.org/pen/PenApplication.page.

Requisitos mínimos: O título deve ser claro e definir objetivamente o documento a que se refere. Esta seção deve apresentar o título do documento, a versão atual e seu OID. Em casos de mudanças significativas em um documento, o OID do documento deverá ser alterado. A versão e data do documento devem mudar com cada versão publica do documento, especialmente durante sua revisão. Em adição, as mudanças devem ser anotadas na seção de modificações no final da PC/DPC.

Melhores práticas: Além dos dados obrigatórios para identificar o documento, a PC/DPC pode apresentar também a entidade responsável pela sua avaliação e a data de sua aprovação. Uma tabela explicativa sobre os campos do identificador de objetos (OID) pode ser útil.

Exemplos de texto:

"Esta DPC é chamada DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DA AC UFSC e comumente referida como "DPC da AC UFSC". O identificador de objeto (OID) desta DPC é 1.3.6.1.4.1.7687.3.1.1"

"Titulo:	*Política de Certificados e Declaração de Práticas de Certificação da UFF Brazilian Grid CA*
Versão:	*Versão 1.0.*
Data:	*10 de Junho de 2006.*
Aprovado:	*Por TAGPMA em 19 de Julho de 2006.*
Expiração:	*Este documento é válido até uma futura notificação.*
ASN.1 OID:	*O seguinte Object Identifier (OID) único identifica este PC/DPC: 1.3.6.1.4.1.24839.2.1.10.3.1.1.0*

1.3.6.1.4.1	*Prefixo para IANA private enterprises iso(1).org(3).dod(6).internet(1).private(4).enterprise(1)*
24839	*Identificador registrado da UFF*
2	*Centro Tecnológico*
1	*Instituto de Computação*
10	*Autoridades Certificadoras*
3	*UFF BrGrid CA*
1	*PC/DPC*
1.0	*Número de versão do PC/DPC"*

Auditoria: Pré-aprovação – o identificador institucional deve ser confirmado no registro do emissor de OIDs (por exemplo, no exemplo acima, seria IANA – acessa o site http://www.iana.org/assignments/enterprise-numbers.).

1.3 Participantes da ICP

This subcomponent describes the identity or types of entities that fill the roles of participants within a PKI.

1.3.1 Autoridades Certificadoras

The entities that issue certificates. A CA is the issuing CA with respect to the certificates it issues and is the subject CA with respect to the CA certificate issued to it. CAs may be organized in a hierarchy in which an organization's CA issues certificates to CAs operated by subordinate organizations, such as a branch, division, or department within a larger organization.

Descrição: Identifica a Autoridade Certificadora da ICPEDU que implementa a PC.

Requisitos mínimos: A subseção deve identificar claramente a AC, sua posição na hierarquia da ICPEDU, se já não foi explicado em seção 1.1, e a quem se destinam os certificados emitidos.

Melhores práticas: É necessário estar claro para a entidade confiante quem cumprirá o papel de AC na ICP.

Exemplos de texto:

"A UFF BrGrid CA e subordinada a AC Grades que é uma AC de Serviços de ICPEDU. Todos os certificados serão emitidos somente sob versões do PC/DPC aprovadas pelo TAGPMA e devem ser assinados pela UFF BrGrid CA. A UFF BrGrid CA não emite certificados para Autoridades Certificados subordinadas".

"A AC UFSC é uma AC Institucional que visa exclusivamente emitir certificados digitais para autoridades certificadoras imediatamente subordinadas a ela e para ARs de sua confiança".

Auditoria: Pré-aprovação (verifique que esta seção está consistente com o resta da PC/DPC) e operacional.

1.3.2 Autoridades de Registro

The entities that establish enrollment procedures for end-user certificate applicants, perform identification and authentication of certificate applicants, initiate or pass along revocation requests for certificates, and approve applications for renewal or re-keying certificates on behalf of a CA. Subordinate organizations within a larger organization can act as RAs for the CA serving the entire organization, but RAs may also be external to the CA.

Descrição: Identifica as Autoridades de Registro (AR) relacionadas à AC da ICPEDU que implementa a PC.

Requisitos mínimos: A subseção deve identificar claramente as ARs responsáveis pelos processos de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes. As ACs da ICPEDU não podem assumir o papel de AR simultaneamente. Uma AR principal (aquela responsável por receber todas as solicitações de certificado caso não haja nenhuma AR específica para atendê-las) deve ser indicada.

Melhores práticas: A necessidade de diversas ARs vinculadas à uma determinada AC deve ser cuidadosamente estudada. Em alguns modelos, uma única AR principal pode ser suficiente para receber as solicitações relacionadas ao ciclo de vida do certificado. Poderia ser escrito que novas ARs podem vir a ser instaladas, conforme as necessidades da AC. Estas ARs têm a obrigação de cumprir os requisitos relevantes desta DPC.

Exemplos de texto:

"A UFF BrGrid CA não assume o papel de Autoridade de Registro (AR). A autenticação de entidades-finais é delegada a ARs que serão instaladas conforme a necessidade de suportar atividades de pesquisa acadêmica pelo país. A lista de ARs atualmente ativas para a UFF BrGrid CA está disponível no site da AC cujo URL esta indicado em Seção 2.1.

Autoridades de Registro devem ser operadas por organizações relacionadas com a comunidade acadêmica brasileira. ARs devem assinar um contrato de concordância com a UFF BrGrid CA onde assumem a obrigação de seguir os procedimentos impostos por esta PC/DPC e pela UFF BrGrid CA para a operação e autenticação de requisições de certificados. As ARs devem operar com equipes compostas por membros com dedicação integral de suas respectivas organizações.

A AR no Instituto de Computação da UFF será a principal Autoridade de Registro catch-all para a UFF BrGrid CA".

Auditoria: Operacional.

1.3.3 Titulares dos Certificados

Examples of subscribers who receive certificates from a CA include employees of an organization with its own CA, banking or brokerage customers, organizations hosting e-commerce sites, organizations participating in a business-to-business exchange, and members of the public receiving certificates from a CA issuing certificates to the public at large.

Descrição: Caracteriza as entidades que poderão possuir certificados emitidos pela AC ou são autorizados a controlar a chave privada de um dispositivo, aplicação ou função.

Requisitos mínimos: As entidades a quem se destinam os certificados emitidos pela AC segundo a PC devem ser claramente definidas nessa subseção.

Melhores práticas: Deve estar claro quem é permitido obter certificados da AC em questão. Pode ser necessário documentar os possíveis titulares de certificados, usando exemplos para facilitar a compreensão.

Exemplos de texto:

No caso de AC que só emite certificados para ACs subordinadas: *"Os titulares dos certificados são as autoridades certificadoras e autoridades de registro subordinadas à AC UFSC".*

No caso de uma AC que emite certificados para entidades finais:
"Os titulares dos certificados são de um dos seguintes tipos:

a) *Empregados, pesquisadores e estudantes relacionados às organizações educacionais e de pesquisa brasileiras; ou,*
b) *Sistemas e serviços computacionais relacionados às organizações educacionais e de pesquisa brasileiras;*

Auditoria: Operacional.

1.3.4 Entidades Confiantes

Examples of relying parties include employees of an organization having its own CA who receive digitally signed e-mails from other employees, persons buying goods and services from e-commerce sites, organizations participating in a business-to-business exchange who receive bids or orders from other participating organizations, and individuals and organizations doing business with subscribers who have received their certificates from a CA issuing certificates to the public. Relying parties may or may not also be subscribers within a given PKI.

Descrição: Caracteriza as entidades que confiarão nos certificados emitidos pela AC para os usos autorizados.

Requisitos mínimos: As entidades que confiarão nos certificados emitidos pela AC devem ser citadas e claramente definidas nesta subseção.

Melhores práticas: Deve estar claro quem pode confiar nos certificados emitidos, podendo utilizá-los para os fins expressos na PC.

Exemplos de texto:

"Entidades confiantes podem ser:

a) *Pessoas físicas recebendo e-mails assinados, acessando recursos ou serviços computacionais;*
b) *Recursos nos quais os donos de certificados iniciam sessões ou enviam processos ou tarefas;*
c) *Serviços utilizados por donos de um certificado."*

"Pessoas físicas ou sistemas vinculados ao sistema acadêmico e de pesquisa brasileiros".

1.3.5 Outros Participantes

Such as certificate manufacturing authorities, providers of repository services, and other entities providing PKI-related services.

Descrição: Caracteriza outras entidades (como provedores de serviço de repositório, por exemplo) que participem da ICP.

Requisitos mínimos: Não estipulado.

Melhores práticas: Caso seja aplicável, os provedores de serviço relacionados à ICP devem ser definidos.

Exemplos de texto:

*"A UFF BrGrid CA disponibiliza uma âncora de confiança em pelo menos um repositório independente e confiável, atualmente o **TACAR** (**T**ERENA **A**cademic **CA** **R**epository), conforme indicado pela TAGPMA, através dos métodos especificados nas políticas dos respectivos repositórios de confiança."*

1.4 Uso do Certificado

This subcomponent contains:

* A list or the types of applications for which the issued certificates are suitable, such as electronic mail, retail transactions, contracts, and a travel order, and/or
* A list or the types of applications for which use of the issued certificates is prohibited.

In the case of a CP or CPS describing different levels of assurance, this subcomponent can describe applications or types of applications that are appropriate or inappropriate for the different levels of assurance.

1.4.1 Aplicações apropriadas para os certificados

Descrição: Relaciona usos para os quais os certificados emitidos sob a PC são adequados.

Requisitos mínimos: A subseção deve conter uma descrição geral da aplicabilidade dos certificados emitidos pela AC.

A chave privada da AC deve ser usada somente para emitir outros certificados e assinar sua LCR. A chave pública relacionada só deve ser usada para verificar certificados que reivindicam ser emitidos pela AC em questão.

O par de chaves da AR deve ser usados somente pelo Gerente da AR para atividades relacionadas a AR, nunca para atividades de natureza pessoal. Neste caso, deve ser usado um certificado de entidade final.

Melhores práticas: A subseção deve permitir ao leitor conhecer os usos permitidos dos certificados emitidos pela AC. Portanto devem ser claramente definidos.

Exemplos de texto:

"Os certificados emitidos pela AC UFSC têm como objetivo único identificar as ACs e ARs credenciadas pela AC UFSC."

(...) O certificado de entidade final pode ser usado para qualquer aplicação apropriada para certificados X.509 (...), em particular:

a) Autenticação de usuários, hosts e serviços;
b) Autenticação e criptografia de comunicações;
c) Autenticação de e-mails assinados;
d) Autenticação de objetos assinados.

"O certificado da AC LNCC deve ser usado somente para emitir outros certificados, assinar a LCR da AC LNCC e para checar certificados que reivindicam ser emitidos pela AC LNCC.

O certificado da AR LNCC deve ser utilizado somente por seus administradores e operadores para atividades relacionadas à AR LNCC.

Os certificados emitidos pela AC LNCC podem ser utilizados para prover integridade, confidencialidade e autenticação de mensagens eletrônicas e nas comunicações via redes de computadores. Exemplos de aplicações:

- *Assinatura de documentos eletrônicos;*
- *E-mail seguro com o protocolo S/MIME;*
- *Aplicações cliente-servidor com suporte aos protocolos SSL e TLS;*
- *Identificação, autenticação e delegação de privilégios em grades computacionais."*

Auditoria: Pré-aprovação (está em conformidade com Seção 1) e Operacional.

1.4.2 Aplicações proibidas para os certificados

Descrição: Relaciona as aplicações para as quais existam restrições ou proibições para o uso dos certificados emitidos sob a PC.

Requisitos mínimos: A subseção deve conter uma descrição geral das aplicações restritas ou proibidas dos certificados emitidos pela AC.

Certificados emitidos por Autoridades Certificadoras participantes da ICPEDU são válidos apenas no contexto acadêmico de pesquisa e atividades educacionais e qualquer outro uso é estritamente proibido.

Melhores práticas: A subseção deve permitir ao leitor conhecer os usos não permitidos dos certificados emitidos pela AC. Portanto devem ser claramente definidos. É interessante salientar que os certificados emitidos por ACs da ICPEDU não reivindicam valor probante.

Exemplos de texto:

"Qualquer uso não estipulado na Subseção 1.4.1 deve ser considerado impróprio e proibido."

"Certificados emitidos pela UFF BrGrid CA não reivindicam valor legal, bem como a posse de um certificado emitido pela UFF BrGrid CA não implica no acesso automático de qualquer tipo de recurso computacional".

Auditoria: Operacional.

1.5 Dados para Contato

This subcomponent includes the name and mailing address of the organization that is responsible for the drafting, registering, maintaining, and updating of this CP or CPS. It also includes the name, electronic mail address, telephone number, and fax number of a contact person. As an alternative to naming an actual person, the document may name a title or role, an e-mail alias, and other generalized contact information. In some cases, the organization may state that its contact person, alone or in combination with others, is available to answer questions about the document.

Moreover, when a formal or informal policy authority is responsible for determining whether a CA should be allowed to operate within or interoperate with a PKI, it may wish to approve the CPS of the CA as being suitable for the policy authority's CP. If so, this subcomponent can include the name or title, electronic mail address (or alias), telephone number, fax number, and other generalized information of the entity in charge of making such a determination. Finally, in this case, this subcomponent also includes the procedures by which this determination is made.

1.5.1 Entidade responsável por este documento

Descrição: Identifica a entidade responsável pela elaboração e manutenção da PC e da DPC.

Requisitos mínimos: Devem ser informados dados consistentes sobre a organização que está divulgando o regulamento presente neste e em qualquer outro documento da ICP. As seguintes informações devem estar presentes:

- Nome da entidade
- Endereço para correspondência
- E-mail

Melhores práticas: Esta informação é necessária para que se saiba a quem atribuir o documento, facilitando citações ao mesmo. Também possibilita ao leitor um canal para sanar dúvidas relacionadas à interpretação deste documento.

Exemplos de texto:

AC de Grades da ICPEDU
Instituto de Computação,
Universidade Federal Fluminense,
Rua Passos da Pátria, 156 – São Domingos,
CEP 24210-240 Niterói, RJ,
Brasil.

E-mail: ac-grades@ic.uff.br
BrGrid CA servidor web URL: http://ac-grades.ic.uff.br

Auditoria: Pré-aprovação (email e endereço web se fornecido), pré-emissão (endereço) e Operacional.

1.5.2 Ponto de Contato

Descrição: Identifica uma pessoa responsável para tratar de questões relativas à PC/DPC e demais informações sobre este documento ou a AC.

Requisitos mínimos: Uma pessoa deve ser indicada para servir de ponto de contato da AC responsável. Deve ser informado, no mínimo:

- Função do contato (Gerente da AC, Gerente de Políticas, etc.)
- Endereço para correspondência
- Telefone
- E-mail

Melhores práticas: É interessante para a AC manter um ponto de contato que possa receber críticas e sugestões sobre as PC e a DPC. É de grande valia se esta pessoa for um dos responsáveis diretos pela administração da AC ou de quaisquer dos documentos citados.

Exemplos de texto:

Gerente da AC de Grades,
Instituto de Computação,
Universidade Federal Fluminense,
Rua Passos da Pátria, 156 – São Domingos,
CEP 24210-240 Niterói, RJ,
Brasil.

E-mail: gerente-acgrades@ic.uff.br
Telefone: 021 26295640

Auditoria: Pré-aprovação (email), pré-emissão (endereço e telefone) e Operacional.

1.5.3 Responsável por determinar a adequabilidade da DPC às Políticas

Descrição: Identifica os responsáveis por avaliar se as práticas determinadas na DPC estão de acordo com o estabelecido pela PC.

Requisitos mínimos: Identificar os responsáveis para esta tarefa.

Melhores práticas: A manutenção da adequabilidade da DPC às políticas determinadas é uma atividade importante para a operação da AC. Além de garantir que a prática esteja sempre de acordo com os estabelecido na PC (e, consequentemente, com os Requisitos Mínimos da ICPEDU), o processo permite a identificação de possíveis atualizações nas políticas, tornando-as mais apropriadas à realidade da AC. O item pode conter, por exemplo, dados de contato (como e-mail, telefone, etc.) e os procedimentos utilizados para determinar essa adequabilidade.

Exemplos de texto:

"O gestor da UFF BrGrid CA (ver Sessão 1.5.2) é responsável por determinar uma DPC condizente com a política".

Auditoria: Pré-aprovação.

1.5.4 Procedimentos de aprovação da PC

Descrição: Identifica os responsáveis pela análise e aprovação do documento.

Requisitos mínimos: A subseção deve informar que a PC é analisada pela Autoridade de Gerência de Política (AGP) e aprovada pelo Comitê Gestor (CG) da ICPEDU.

Melhores práticas: A informação sobre quem aprova a política é importante para garantir a confiabilidade na AC. Se o interessado confia na entidade que aprova o documento, essa confiança é transferida para o documento aprovado por ela.

Exemplos de texto:

"Esta DPC é analisada pela Autoridade de Gerência de Políticas (AGP) e aprovada pelo Comitê Gestor (CG) da ICPEDU".

1.6 Definições e Acrônimos

This subcomponent contains a list of definitions for defined terms used within the document, as well as a list of acronyms in the document and their meanings.

Descrição: Esta seção identifica siglas, abreviações e termos usados no documento.

Requisitos mínimos: Não estipulado.

Melhores práticas: A subseção deve deixar claro que as palavras-chave: “DEVE”, “NÃO DEVE”, “REQUERIDO”, “RECOMENDADO”, “PODE”, “OPCIONAL” no documento devem ser interpretadas como na RFC 2119. Essas palavras devem ser capitalizadas no texto.

Para facilitar a compreensão, siglas e abreviações podem ser dispostas em formato de tabela. Para fins de padronização da documentação da ICPEDU, sugere-se uma formatação semelhante àquela utilizada na seção 1.6 da DPC da AC Raiz.

2. Responsabilidades referentes a publicações e repositórios

A seção aborda a responsabilidade da Autoridade Certificadora no que diz respeito à divulgação das informações necessárias (como os certificados emitidos, as PCs e DPCs) e gerência dos repositórios onde ficam disponíveis.

2.1 Repositórios

An identification of the entity or entities that operate repositories within the PKI, such as a CA, certificate manufacturing authority, or independent repository service provider.

Descrição: Identifica o(s) repositório(s) onde as informações divulgadas pela AC serão disponibilizadas.

Requisitos mínimos: A subseção deve indicar um endereço web onde serão disponibilizadas pela AC informações consideradas públicas, incluindo repositórios independentes.

Melhores práticas: A AC deve disponibilizar um site seguro, com alta disponibilidade, que possibilite autenticação SSL e possua um certificado SSL emitido por uma entidade comercial confiável ou pela AC-SSL de ICPEDU. Algumas informações devem estar disponíveis também sem autenticação ou conexão segura, como o certificado da AC e a LCR mais atual. Caso um repositório público independente (como o TACAR[1], por exemplo) seja utilizado, uma breve explicação seguida de um ponteiro para o *website* do mesmo pode ser inserido.

Auditoria: Pré-aprovação (servidor de web deve ser registrado no DNS), pré-emissão (deve ser operacional e no ar) e Operacional (disponibilidade seria monitorada pelo AGP).

2.2 Publicação de informações

The responsibility of a PKI participant to publish information regarding its practices, certificates, and the current status of such certificates, which may include the responsibilities of making the CP or CPS publicly available using various mechanisms and of identifying components, subcomponents, and elements of such documents that exist but are not made publicly available, for instance, security controls, clearance procedures, or trade secret information due to their sensitivity.

Descrição: Define as informações a serem publicadas pela AC.

Requisitos mínimos: Os repositórios da AC devem conter, no mínimo:

[1] **T**ERENA **A**cademic **CA R**epository (TACAR): http://www.tacar.org/

- O certificado da AC, em formatos apropriados;
- Todos os certificados emitidos pela AC, ou informações sobre cada um deles;
- Versão atual da Lista de Certificados Revogados (LCR);
- Versão atual e anteriores aprovadas das PCs e DPCs da AC;

Melhores práticas: O repositório deve prover aos participantes da ICP as informações necessárias para verificar a validade e confiabilidade dos certificados emitidos pela AC. Para tanto, outras informações além das citadas anteriormente podem ser disponibilizadas como, por exemplo, o certificado da AC-Raiz. Algumas ACs podem não achar necessário publicar sua PC por completo, tornando público apenas trechos que achar mais conveniente.

Exemplos de texto:

O repositório contém as seguintes informações:

- *Certificados emitidos pela AC UFSC;*
- *Versão atual e anteriores da lista de certificados revogados (LCR) da AC UFSC;*
- *Versão atual e anteriores das PCs e DPCs da AC UFSC.*

A UFF BrGrid CA opera um repositório on-line seguro que contêm:

a) O certificado raiz da UFF BrGrid CA, em formatos apropriados, e todos os anteriores necessários para checar certificados válidos existentes;
b) Informação para validar a integridade do certificado raiz;
c) Todos os certificados emitidos pela BrGrid CA;
d) URLs versões em texto, DER e PEM da lista de certificados revogados da UFF BrGrid CA (Lista de Certificados Revogados);
e) A atual e todas as versões anteriores aprovadas do PC/DPC;
f) Um contato de e-mail para duvidas, falhas e reportar incidentes;
g) Um endereço postal;
h) Assim como qualquer outra informação julgada relevante ao serviço da UFF BrGrid CA.

Auditoria: Pré-emissão e Operacional.

2.3 Frequência de publicação

When information must be published and the frequency of publication.

Descrição: Informa a freqüência de publicação das informações citadas na subseção anterior.

Requisitos mínimos: O repositório mantido pela AC deve ser atualizado imediatamente sempre que:

- Um certificado for emitido;
- Quando houver atualizações na Lista de Certificados Revogados (LCR), seja por expiração da mesma ou revogação de algum certificado válido por qualquer motivo.

Alterações aprovadas na PC ou DPC devem ser publicadas antes de implantação.

Melhores práticas: Como o repositório deve ser mantido com informações sempre consistentes, deve-se buscar o menor tempo possível entre alguma mudança e sua atualização no mesmo. Certificados e LCRs, por exemplo, devem ser publicados no repositório assim que são emitidos.

Auditoria: Operacional.

2.4 Controles de acesso aos repositórios

`Access control on published information objects including CPs, CPS, certificates, certificate status, and CRLs.`

Descrição: Descreve quais controles de acesso são implementados sobre informações publicadas no repositório.

Requisitos mínimos: Informações consideradas públicas devem ser acessadas de forma anônima apenas para consulta. O acesso a elas deve ser monitorado a fim de evitar quaisquer atividades não autorizadas. Deve especifica o nível de disponibilidade e qualidade de serviço que devem ser esperado por as partes confiantes. Um esforço deve ser feito para que as informações no repositório sejam disponíveis para o maior tempo possível senão sempre.

Melhores práticas: As informações dos repositórios devem estar disponíveis para as entidades confiantes e titulares de certificado sempre que precisarem fazer uma consulta, idealmente 24 horas por dia, sete dias por semana. Sua integridade, portanto, deve ser preservada para que a confiança seja mantida.

Exemplos de texto:

“Todas as informações do repositório são públicas e podem ser acessadas de forma anônima”.

“A UFF BrGrid CA implementou medidas de segurança física e lógica para evitar que pessoas não-autorizadas adicionem, excluam ou modifiquem os dados no repositório. Algumas informações específicas são consideradas públicas e podem ser acessadas apenas para leitura, sem restrições. Atualmente, a UFF BrGrid CA não impõe nenhum controle de acesso a este PC/DPC, seu certificado, certificados emitidos ou LCRs. Entretanto, se o uso errado destes dados for evidente, controles de acesso serão decretados para proteger os titulares dos certificados.

O repositório on-line é mantido com os melhores esforços e está disponível 24 horas por dia, 7 dias por semana, sujeito a manutenção agendada. Fora do período de 09:00-17:00 (hora local), Segunda a Sexta, pode rodar sem acompanhamento”.

Auditoria: Operacional.

3. Identificação e Autenticação

A seção aborda os nomes presentes no certificado, além dos métodos para validar a identidade de uma entidade antes da emissão do certificado.

This component describes the procedures used to authenticate the identity and/or other attributes of an end-user certificate applicant to a CA or RA prior to certificate issuance. In addition, the component sets forth the procedures for authenticating the identity and the criteria for accepting applicants of entities seeking to become CAs, RAs, or other entities operating in or interoperating with a PKI. It also describes how parties requesting re-key or revocation are authenticated. This component also addresses naming practices, including the recognition of trademark rights in certain names.

3.1 Estrutura de Nomes

This subcomponent includes the following elements regarding naming and identification of the subscribers.

3.1.1 Tipos de nomes

Types of names assigned to the subject, such as X.500 distinguished names; RFC-822 names; and X.400 names.

Descrição: Descreve a estrutura de nomes admitidos para identificar os titulares de certificados emitidos sob a PC.

Requisitos mínimos: Os nomes usados no certificado devem seguir a padrão X.500 e ser apropriados para a aplicação na qual serão usados.

Melhores práticas: Não estipulado.

Auditoria: Operacional.

3.1.2 Necessidade de que nomes sejam significativos

Whether names have to be meaningful or not.

Descrição: Define a necessidade de que os nomes que identifiquem is titulares de certificado sejam significativos, ou seja, que possibilitem determinar a identidade da pessoa ou organização a que se referem. Também impõe restrições para o conteúdo destes nomes.

Requisitos mínimos: Os nomes especificados nos campos *common name* (CN), *organization name* (O) e *organizational unit* (OU) precisam ser relacionados (ou ao menos expressar uma associação razoável) ao nome real e organização do titular de certificado.

Porém não são admitidos caracteres especiais ou de acentuação no campo *distinguished name* (DN) – ver subseção 7.1.4.

Melhores práticas: Para certificados pessoais, o CN deve ser obtido a partir do nome legal da pessoa, conforme apresentado em um documento de identidade oficial emitido pelo governo (ex.: passaporte, carteira de identidade ou carteira nacional de habilitação) – ver também subseção 3.1.3. Titulares de certificado devem escolher uma representação do seu nome dentro do grupo de caracteres permitidos.

Para certificados de recursos (máquinas) ou serviços, o CN deve ser o nome completo do recurso que consta no *Domain Name Server* (DNS).

Auditoria: Operacional.

3.1.3 Anonimato dos titulares de certificado

Whether or not subscribers can be anonymous or pseudonymous, and if they can, what names are assigned to or can be used by anonymous subscribers.

Descrição: Descreve se a autoridade certificadora irá ou não emitir certificados com suporte ao anonimato.

Requisitos mínimos: As ACs da ICPEDU não devem emitir certificados com suporte ao anonimato.

Melhores práticas: Não estipulado.

Auditoria: Operacional.

3.1.4 Regras para interpretação dos diversos formatos de nomes

Rules for interpreting various name forms, such as the X.500 standard and RFC-822;

Descrição: A palavra “nome” no titulo refere o *Distinguished Name* ou DN do certificado. Este subseção descreve, quando aplicáveis, as regras para interpretação das vários campos do DN admitidas pela PC.

Requisitos mínimos: O DN de certificados emitido pela AC deve consistir de uma parte fixa e uma parte variável. A parte fixa deve ser única no contexto da ICPEDU. O formato deve ser em conformidade com subseção 7.1.4.

Melhores práticas: Caso a AC emita certificados com formatos de nomes específicos (seja por força da lei, contrato ou aplicação em especial), o formato utilizado deve ser especificado claramente na PC.

Múltiplas instâncias do atributo *organization* (O) podem ser usadas em um mesmo DN. A maior parte dos softwares deve tratar corretamente essa representação, e combinar os atributos na ordem apropriada. Além disso, múltiplas instancias do atributo *commonName* podem ser usadas. Note, entretanto, que a representação visual de ambos seguindo esse formato pode não ser completa em muitos navegadores, e usualmente apenas o primeiro ou

o último destes é mostrado ao usuário. Isso afeta apenas a representação visual. [OGFGridCertProfile]

Auditoria: Operacional.

3.1.5 Unicidade dos nomes

`Whether names have to be unique.`

Descrição: Informa se os nomes admitidos pela AC são únicos ou não.

Requisitos mínimos: Os identificadores *Distinguished Name* (DN) devem ser únicos para cada titular de certificado no âmbito da AC emitente. Todo DN deve ser relacionado a uma, e apenas uma, entidade final durante todo o tempo de vida da AC. Titulares não devem compartilhar certificados. Com a exceção de certificados de *hosts*, não podem ser emitido certificados que utilizam *wildcards* nos seus DNs.

Melhores práticas: Certificados devem pertencer a apenas um indivíduo ou recurso. Deve ser informado claramente que o campo DN do certificado é único. Podem ser apresentados critérios usados para definir a unicidade de um nome e o tratamento para evitar duplicidades.

Exemplos de texto:

"O Distinguished Name (DN) em cada certificado emitido pela UFF BrGrid CA DEVE ser único. Nesta política da PC/DPC, dois nomes são considerados idênticos se eles diferem exclusivamente em letras maiúsculas e minúsculas, pontuação ou espaços em branco; Portanto, estes não DEVEM ser usados para diferenciar nomes. (...) Em casos onde o nome pessoal não é suficiente para diferenciar dois certificados, números serão adicionados ao final do Common Name (CN)".

Todos os titulares serão identificados de forma única durante todo o ciclo de vida da UFF BrGrid CA, e não apenas pelo período de validade do certificado."

Auditoria: Operacional.

3.1.6 Reconhecimento, autenticação e papel de marcas registradas

Descrição: Estabelece como é executada a confirmação de autenticidade de marcas registradas.

Requisitos mínimos: Não estipulado.

Melhores práticas: A fim de minimizar o risco de conflitos pela utilização de marcas registradas em certificados, a PC pode impor a não violação de direitos autorais por parte da entidade solicitante. Para tanto, AC pode utilizar regulamentos internos ou a legislação vigente para tratar, reconhecer e confirmar a autenticidade de marcas registradas.

Exemplos de texto:

"A AC UFSC respeitará as marcas registradas e direitos autorais vigentes, de acordo com as regras do Departamento de Propriedade Intelectual da UFSC".

3.2 Validação Inicial da Identidade

This subcomponent contains the following elements for the identification and authentication procedures for the initial registration for each subject type (CA, RA, subscriber, or other participant).

3.2.1 Método para prova de posse da chave privada

If and how the subject must prove possession of the companion private key for the public key being registered, for example, a digital signature in the certificate request message.

Descrição: Estabelece os procedimentos executados pela AC responsável ou pela AR a ela vinculadas para confirmar que a entidade solicitante possui a chave privada correspondente à chave pública a qual está sendo solicitado o certificado digital.

Requisitos mínimos: A AC deve descrever o método utilizado para comprovar a posse da chave privado pelo solicitante.

Melhores práticas: O método escolhido pela AC deve levar em conta o risco da assinatura de um certificado para a pessoa errada e estar de acordo com a legislação vigente, se aplicável. O método mais comum de validação de posse da chave privada é através da verificação da assinatura na requisição do certificado através da chave pública do solicitante.

Exemplos de texto:

"A posse de uma chave privada por parte do solicitante é considerada provada quando:

1. *A assinatura digital da requisição de assinatura de certificado puder ser verificada usando a chave pública do solicitante; e*
2. *O PIN, informado no momento da geração das chaves, puder ser verificado durante o encontro com a Autoridade de Registro."*

"O requerente deverá apresentar à AC UFSC um arquivo de requisição de certificado assinado usando a chave privada que faz par à chave pública sendo apresentada. Esta assinatura consiste na prova de posse da chave privada."

Auditoria: Operacional.

3.2.2 Autenticação da identidade organizacional

Identification and authentication requirements for organizational identity of subscriber or participant (CA; RA; subscriber (in the case of certificates issued to organizations or devices controlled by an organization), or other participant), for example, consulting the

database of a service that identifies organizations or inspecting an organization's articles of incorporation.

Descrição: Deve estabelecer os procedimentos empregados para a confirmação da existência da entidade solicitante e seu direito para fazer tal pedido, além da associação de um solicitante com sua respectiva instituição.

Requisitos mínimos: Somente instituições parceiras de RNP podem solicitar a criação de uma AC institucional no âmbito de ICPEDU.

No caso de uma solicitação de um certificado de uma AC intermediária, primeiro, deve ser verificada se a unidade organizacional que pretende operar a AC realmente existe e se tem direto para fazer tal solicitação. Depois a relação entre o solicitante e sua unidade organizacional deve ser confirmada mediante apresentação de um documento oficial ou em papel timbrado assinado pelo representante legal da unidade organizacional. Uma verificação de quem seria representante legal da unidade organizacional deve ser feita.

No caso de uma solicitação de um certificado pessoal, a relação entre o solicitante e a organização que vai aparecer no certificado sendo solicitado deve ser confirmada pela AR e o método utilizado para tal deve ser descrito.

Melhores práticas: Verificar a identidade organizacional garante que o nome presente no certificado corresponde a uma organização real (permitindo manter consistente a informação existente no certificado) e evita que um requerente não autorizado torne-se titular de um certificado (prevenindo fraudes em nome da organização em questão). Portanto, determinar os procedimentos de validação da relação entre um requerente e uma organização os riscos envolvendo qualquer transação que utilize o certificado.

Exemplos de texto:

"O relacionamento entre o titular e a organização ou unidade mencionada no nome deve ser provada através de um cartão de identificação da organização, um documento legalmente aceito ou um documento oficial da organização em papel timbrado e assinado por um representante oficial da organização. Em caso de dúvida, a AR pode seguir qualquer conjunto de passos necessários para questionar o relacionamento do credenciado com a organização. Opcionalmente, a requisição pode ser autorizada eletronicamente através da assinatura digital de um representante oficial da organização de posse de um certificado válido emitido pela UFF BrGrid CA".

"O requerente deverá apresentar um documento do representante legal da unidade organizacional designando-o como responsável pela AC".

Auditoria: Pré-aprovação (no caso de ACs Institucionais, feita durante a autenticação da instituição) e Operacional.

3.2.3 Autenticação da identidade individual

Identification and authentication requirements for an individual subscriber or a person acting on behalf of an organizational subscriber or participant (CA, RA, in the case of certificates issued

to organizations or devices controlled by an organization, the subscriber, or other participant), including:

a) Type of documentation and/or number of identification credentials required;

b) How a CA or RA authenticates the identity of the organization or individual based on the documentation or credentials provided;

c) If the individual must personally present to the authenticating CA or RA;

d) How an individual as an organizational person is authenticated, such as by reference to duly signed authorization documents or a corporate identification badge.

Descrição: Deve estabelecer os procedimentos empregados para a confirmação da identidade de um indivíduo em particular a pessoa fazendo a solicitação.

Requisitos mínimos: A confirmação de identidade de um requerente deve ser realizada mediante a presença física do mesmo, com base em documento de identificação legalmente aceito com foto. Uma prova de relacionamento com a organização que será especificada no *Distinguished Name* (DN) do certificado também deve ser apresentada. Em casos especiais (como a impossibilidade de um encontro presencial devido à distância geográfica), o processo equivalente pode ser adotado, por exemplo, a validação pode ser feita através de videoconferência. Sendo assim, uma cópia autenticada do documento deve ser enviada antes do agendamento da reunião.

As cópias de todos os documentos necessários no processo de autenticação devem ser arquivadas pela AC ou AR.

Melhores práticas: Validar a identidade do requerente permite garantir que o certificado não está sendo emitido para alguém tentando se passar por outra pessoa.

Exemplos de documentos de identificação legalmente válidos são:

- Carteira Nacional de Habilitação;
- Carteira de trabalho;
- Passaporte válido;

Auditoria: Operacional.

3.2.4 Dados dos titulares de certificado que não são verificados

List of subscriber information that is not verified (called "nonverified subscriber information") during the initial registration.

Descrição: Estabelece quais os dados dos titulares de certificados coletados não são ou não devem ser verificados pela AC ou AR no momento do registro.

Requisitos mínimos: Quando aplicável, a AC ou AR deve informar que dados dos titulares de certificado não são verificados pela AC ou AR no momento do registro.

Melhores práticas: O critério de validação e sua aplicação dependem do risco, grau de sensibilidade e das conseqüências das aplicações dos certificados que as contêm. Depois de decidido o processo de validação que será utilizado, a política deverá estabelecer claramente quais dados não são verificados para que a AC ou AR não sejam responsabilizada pela inconsistência desses dados no certificado.

Exemplos de texto:

"O e-mail de contato, número de telefone e endereço do solicitante podem não ser verificados."

"Apenas o nome do requerente e o vínculo institucional são validados. Os demais dados recebidos não são verificados."

3.2.5 Validação de autoridade

Validation of authority involves a determination of whether a person has specific rights, entitlements, or permissions, including the permission to act on behalf of an organization to obtain a certificate.

Descrição: Estabelece os métodos que devem ser utilizados pela AC ou AR para validar a permissão de pessoas ao agir em nome de outros como, por exemplo, organizações ou departamentos.

Requisitos mínimos: Descreve o processo de validação. Por exemplo, uma declaração assinada por um representante legal da organização reconhecido pela AC ou AR, ou equivalente, é suficiente para validação da autoridade.

Melhores práticas: Pode haver diferentes tipos de validação de autoridade, variando de acordo com a organização e aplicabilidade do certificado. Para fortalecer o processo de validação, a assinatura da declaração enviada pelo representante legal pode ter firma reconhecida em cartório.

Auditoria: Operacional.

3.2.6 Critérios para interoperabilidade

In the case of applications by a CA wishing to operate within, or interoperate with, a PKI, this subcomponent contains the criteria by which a PKI, CA, or policy authority determines whether or not the CA is suitable for such operations or interoperation. Such interoperation may include cross-certification, unilateral certification, or other forms of interoperation.

Descrição: Estabelece os critérios para determinar se uma AC externa a ICPEDU está apta para cooperar em uma determinada aplicação.

Requisitos mínimos: Ainda não definida pelo CG da ICPEDU.

Melhores práticas: Não se aplica.

3.3 Identificação e Autenticação para Requisição de Substituição de Chaves

This subcomponent addresses the following elements for the identification and authentication procedures for re-key for each subject type (CA, RA, subscriber, and other participants).

3.3.1 Identificação e autenticação para troca de chaves de rotina

Identification and authentication requirements for routine re-key, such as a re-key request that contains the new key and is signed using the current valid key.

Descrição: Estabelece o processo de identificação do solicitante exigido para a geração do novo par de chaves e de seu respectivo certificado.

Requisitos mínimos: A solicitação de um certificado para um novo par de chaves pode ser aceito pela AC se for assinada digitalmente utilizando a chave privada relacionada ao certificado válido do solicitante. Em outros casos, o processo de identificação para um novo certificado deve ser seguido.

Melhores práticas: A troca do par de chaves não é encorajada, mas sim uma nova solicitação de certificado. Contudo, caso ocorra, é necessário verificar a continuação do relacionamento do solicitante com a entidade indicada no certificado.

Exemplos de texto:

"Toda requisição de certificado é tratada como uma nova requisição. Desta forma não é permitida a simples substituição da chave".

"(...) Embora a prova de relacionamento seja necessária, o processo de substituição de chaves não requer a verificação de identidade por parte da AR e, portanto, não requer presença física do credenciado. Se a prova de relacionamento ocorrer através de documentos de papel, eles devem ser enviados a AR por carta registrada".

Auditoria: Operacional.

3.3.2 Identificação e autenticação para troca de chaves após revogação

Identification and authentication requirements for re-key after certificate revocation. One example is the use of the same process as the initial identity validation.

Descrição: Estabelece o processo de identificação do solicitante exigido para a geração do novo par de chaves após a revogação do respectivo certificado.

Requisitos mínimos: A AC deve estabelecer que os mesmos processos de identificação e autenticação de solicitação de um novo certificado devem ser exigidos.

Melhores práticas: Não é aceita a troca de chaves depois da revogação.

Auditoria: Operacional.

3.4 Identificação e Autenticação para Requisição de Revogação

This subcomponent describes the identification and authentication procedures for a revocation request by each subject type (CA, RA, subscriber, and other participant). Examples include a revocation request digitally signed with the private key whose companion public key needs to be revoked, and a digitally signed request by the RA.

Descrição: Estabelece o processo de identificação do solicitante exigido para a revogação de um certificado. Possíveis solicitantes devem ser listadas em Seção 4.9.2.

Requisitos mínimos: A AC deve determinar quem pode solicitar a revogação do certificado e qual o processo de autenticação utilizado, bem como estabelecer um processo de registro dessas solicitações.

Melhores práticas: No caso de certificados de AC, apenas o representante legal da entidade relacionada deve solicitar a revogação. Nos demais casos, os donos do certificado podem fazê-lo a AR ou diretamente a AC.

Enquanto o mesmo processo de autenticação para solicitação de novos certificados pode ser adotado, é comum emitir uma senha de revogação junto com a emissão do certificado.

Auditoria: Operacional.

4. Requisitos Operacionais do Ciclo de Vida do Certificado

A seção estabelece os procedimentos adotados pela AC para gerenciar o ciclo de vida dos certificados, de sua solicitação até expiração ou revogação.

This component is used to specify requirements imposed upon issuing CA, subject CAs, RAs, subscribers, or other participants with respect to the life-cycle of a certificate.

Within each subcomponent, separate consideration may need to be given to subject CAs, RAs, subscribers, and other participants.

4.1 Procedimentos do requerente para solicitar o certificado

This subcomponent is used to address the following requirements regarding subject certificate application: Who can submit a certificate application, such as a certificate subject or the RA; and Enrollment process used by subjects to submit certificate applications and responsibilities in connection with this process.

An example of this process is where the subject generates the key pair and sends a certificate request to the RA. The RA validates and signs the request and sends it to the CA. A CA or RA may have the responsibility of establishing an enrollment process in order to receive certificate applications. Likewise, certificate applicants may have the responsibility of providing accurate information on their certificate applications.

4.1.1 Quem pode submeter uma solicitação de certificado

Descrição: Descreve quem está autorizado a submeter uma solicitação de certificado.

Requisitos mínimos: A AC deve estabelecer quem pode solicitar os certificados emitidos sob a PC, bem como as restrições impostas aos pedidos. Se a AC permitir que pessoas solicitem certificados em nome de outras entidades (no caso de uma máquina ou serviço, por exemplo), a PC deve especificar também quem é responsável por autorizar esse tipo de solicitação.

Melhores práticas: Os certificados pessoais são normalmente solicitados pelo próprio titular do certificado. Outros certificados só podem ser solicitados com autorização do representante legal da unidade organizacional a qual está vinculado.

Exemplos de texto:

As entidades titulares de certificado podem ser dos seguintes tipos:

a) Empregados, pesquisadores e estudantes afiliados com as organizações acima;
b) Sistemas computacionais (hosts) pertencentes a organizações acima ou administrados por elas; e

c) *Serviços fornecidos por um host administrado por uma das organizações acima.*

"Qualquer servidor docente e técnico administrativo da UFSC devidamente autorizado pelo representante legal da unidade organizacional a qual está vinculado".

Auditoria: Operacional.

4.1.2 Processo de solicitação e responsabilidades

Descrição: Descreve todos os requisitos e procedimentos operacionais estabelecidos para as solicitações de emissão de certificado.

Requisitos mínimos: A PC deve prever a utilização de algum tipo de interface para envio da requisição de um certificado e descrever os procedimentos a serem tomados pela parte solicitante para efetuar a requisição e submetê-la à AR correspondente.

O solicitante é responsável pela veracidade das informações fornecidas para identificação, autenticação e geração do certificado. Caso o par de chaves seja gerado pelo solicitante, é de sua responsabilidade garantir que a chave privada seja gerada utilizando algoritmo criptográfico e tamanho apropriados, de acordo com os requisitos da ICPEDU.

Melhores práticas: Os procedimentos para solicitação de certificados devem levar em conta medidas de segurança para evitar erros e acessos não-autorizados. Tais medidas devem ser consideradas em todo o processo, do momento da geração do par de chaves até a transmissão da requisição.

Auditoria: Pré-aprovação (verifica que o texto esta consistente com seções 3.2.2, 3.2.3 e 3.2.4), Operacional.

4.2 Processamento da solicitação pela AR

This subcomponent is used to describe the procedure for processing certificate applications. For example, the issuing CA and RA may perform identification and authentication procedures to validate the certificate application. Following such steps, the CA or RA will either approve or reject the certificate application, perhaps upon the application of certain criteria. Finally, this subcomponent sets a time limit during which a CA and/or RA must act on and process a certificate application.

4.2.1 Realização das funções de identificação e autenticação

Descrição: Descreve os procedimentos operacionais para validar a identidade de quem faz as solicitações de certificados. Esta tarefa é a mais importante do processo de emissão de um certificado, visto que a aprovação ou rejeição de um pedido de certificado depende diretamente da confirmação das informações providas.

Requisitos mínimos: A AR responsável por receber a solicitação deve aplicar procedimentos para verificação da identidade do requerente utilizando um mecanismo seguro e confiável. A AR deve, no mínimo, estabelecer procedimentos que permitam verificar a posse da chave privada correspondente à chave pública da requisição de certificado (ver seção 3.2.1), a relação do solicitante com sua organização, sua identidade pessoal e todas as informações que serão presente no certificado.

Melhores práticas: A AR pode deve medir o tempo necessário para executar as tarefas de identificação e autenticação dos usuários, e estabelecer um período no qual consegue processar as solicitações. As verificações podem ser feitas através da verificação de assinatura do pedido de certificado (no caso da posse da chave privada) ou da utilização de um cartório (como no caso de documentos legalmente aceitos, como RG)

Exemplos de texto:

"Se a solicitação de certificado for recebida por e-mail, a AR deve verificar a assinatura digital da solicitação de assinatura de certificado".

"A identificação e autenticação do requerente serão realizadas pessoalmente nas instalações da AC UFSC".

Auditoria: Operacional.

4.2.2 Aprovação ou rejeição das solicitações

Descrição: Descreve os procedimentos operacionais para a aprovação ou rejeição das solicitações de certificados.

Requisitos mínimos: A AC deve informar os critérios para aprovação e rejeição de solicitações, bem como as ações tomadas em cada caso. Devem ser mantidos registros sobre a aprovação ou rejeição de solicitações.

Melhores práticas: A aprovação da solicitação está intimamente ligada ao sucesso na validação da identidade do solicitante e da posse da chave privada relacionada à chave pública que acompanha o pedido. Outros critérios, como a adequação da solicitação a PC também pode ser usada como critério para aprovar ou rejeitar requisições de certificados, por exemplo, um campo incorreto no DN ou chaves geradas usando um algoritmo criptográfico inaceitável. No caso de rejeição, deve indicar se uma nova solicitação deverá ser feito ou se haverá um prazo de adequação.

Exemplos de texto:

"Para aprovação da solicitação, a AC solicitante deve estar em conformidade com a Política de Segurança e com as diretrizes expressas no Documento de Requisitos Mínimos da ICPEDU. As políticas adotadas para o estabelecimento desta conformidade devem estar descritas na sua PC".

"Se a autenticação da informação se mostrar inexata, ou a parte requisitante não for capaz de atender os requisitos dentro de 10 (dez) dias úteis após o recebimento da solicitação pela AR, o pedido deve ser recusado".

Auditoria: Operacional.

4.2.3 Tempo para processamento das solicitações

Descrição: Estabelece o prazo máximo para processamento de solicitações.

Requisitos mínimos: Não estipulado.

Melhores práticas: A AC deve levar em conta diversos fatores ao estabelecer um prazo para o processamento das solicitações. Exemplos que devem ser considerados:

- Questões contratuais;
- Se os procedimentos de verificação são feitos de forma manual ou automática;
- O número de pessoas envolvidas em cada tarefa;
- A complexidade da atividade, etc.

4.3 Processamento da solicitação pela AC

4.3.1 Ações da AC durante a emissão de certificado

Describes the actions performed by the CA during the issuance of the certificate, for example a procedure whereby the CA validates the RA signature and RA authority and generates a certificate.

Descrição: Descreve os requisitos e procedimentos operacionais estabelecidos pela AC para a emissão do certificado.

Requisitos mínimos: Apenas solicitações assinadas pela AR e devidamente verificadas pela AC devem ser processadas.

Melhores práticas: Não estipulado.

Auditoria: Operacional.

4.3.2 Notificação da emissão do certificado pela AC para o solicitante

Describes the notification mechanisms, if any, used by the CA to notify the subscriber of the issuance of the certificate; an example is a procedure under which the CA e-mails the certificate to the subscriber or the RA or e-mails information permitting the subscriber to download the certificate from a web site.

Descrição: Descreve os requisitos e procedimentos operacionais estabelecidos pela AC para notificar o solicitante da emissão do certificado.

Requisitos mínimos: Não estipulado.

Melhores práticas: A AC pode estabelecer um processo automatizado de comunicação da emissão do certificado. Isso possibilitaria ao solicitante verificar a exatidão das informações presentes no certificado e notificar a AC para que sejam tomadas as medidas cabíveis.

4.4 Aceitação do Certificado

4.4.1 Conduta que constitui a aceitação do certificado

The conduct of an applicant that will be deemed to constitute acceptance of the certificate. Such conduct may include affirmative steps to indicate acceptance, actions implying acceptance, or a failure to object to the certificate or its content. For instance, acceptance may be deemed to occur if the CA does not receive any notice from the subscriber within a certain time period; a subscriber may send a signed message accepting the certificate; or a subscriber may send a signed message rejecting the certificate where the message includes the reason for rejection and identifies the fields in the certificate that are incorrect or incomplete.

Descrição: Descreve os requisitos e procedimentos operacionais referentes à aceitação do certificado emitido.

Requisitos mínimos: Não estipulado.

Melhores práticas: A PC deve garantir a aceitação do certificado por parte do titular ou pessoa responsável pelo mesmo (no caso de equipamentos ou aplicações, por exemplo) provendo um mecanismo onde o titular deve explicitamente aceitar o certificado. A AC pode permitir que os usuários sejam capazes de revisar o conteúdo do certificado antes de sua assinatura através de uma interface apropriada, agilizando o processo de aceitação. Além disso, a usabilidade do certificado deve ser verificada juntamente com a chave privada de posse da parte solicitante como, por exemplo, assinando um arquivo arbitrário com a chave privada e verificando a assinatura digital com o certificado.

4.4.2 Publicação do certificado pela AC

Publication of the certificate by the CA. For example, the CA may post the certificate to an X.500 or LDAP repository.

Descrição: Descreve os requisitos e procedimentos operacionais referentes à publicação do certificado emitido.

Requisitos mínimos: A PC deve garantir que os certificados serão publicados assim que emitidos.

Melhores práticas: Os certificados emitidos devem ser automaticamente disponibilizados numa interface web ou diretório LDAP.

Exemplos de texto:

"Os certificados serão publicados tão logo que sejam emitidos".

Auditoria: Operacional.

4.4.3 Notificação da emissão do certificado pela AC para outras entidades

Notification of certificate issuance by the CA to other entities. As an example, the CA may send the certificate to the RA.

Descrição: Estabelece se haverá notificação de outras entidades sobre a emissão do certificado.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

Exemplos de texto:

"Nenhuma outra entidade será notificada após a emissão de um certificado alem do solicitante".

4.5 Utilização de pares de chaves e de certificados

This subcomponent is used to describe the responsibilities relating to the use of keys and certificates.

4.5.1 Responsabilidade pela utilização das chaves privadas e dos certificados por parte dos titulares

Subscriber responsibilities relating to use of the subscriber's private key and certificate. For example, the subscriber may be required to use a private key and certificate only for appropriate applications as set forth in the CP and in consistency with applicable certificate content (e.g., key usage field). Use of a private key and certificate are subject to the terms of the subscriber agreement, the use of a private key is permitted only after the subscriber has accepted the corresponding certificate, or the subscriber must discontinue use of the private key following the expiration or revocation of the certificate.

Descrição: Estabelece as responsabilidades do titular do certificado pela utilização das chaves privadas e dos certificados.

Requisitos mínimos: A PC não deve permitir os certificados emitidos pela AC credenciada sejam utilizados para quaisquer fins senão o estipulado por esta, e

definir que sua responsabilidade de uso e manutenção é exclusivamente do usuário.

Em caso de comprometimento da chave privada, o titular, ou responsável pelo certificado, deve informar imediatamente a AC que emitiu o certificado ou sua AR.

Melhores práticas: O uso do certificado deve ser permitido apenas após a assinatura do Termo de Concordância. Certificados emitidos pela AC credenciada devem ser usados apenas para os fins permitidos na PC, e qualquer outro proibido. Quando um certificado for revogado ou expirar, a chave privada associada não deverá mais ser utilizada. Os usos para os quais os certificados emitidos são permitidos devem constar no campo *key usage* do certificado.

Exemplos de texto:

"O titular de certificado deve proteger sua chave privada contra uso não autorizado".

"Certificados emitidos pela AC de Grades e suas chaves privadas associadas devem ser usadas unicamente de acordo com as condições permitidas definidas na Seção 1.4. Qualquer outro uso é estritamente proibido. Certificados devem ser usados unicamente de acordo com o conteúdo indicado no campo key usage do certificado. Quando um certificado é revogado ou expirado, sua chave privada associada não deve mais ser usada".

"É responsabilidade unicamente do usuário a manutenção da sua chave privada, que só deve ser utilizada para os fins descritos nesta PC/DPC."

4.5.2 Responsabilidade pela utilização das chaves públicas e dos certificados por parte das entidades confiantes

Relying party responsibilities relating to the use of a subscriber's public key and certificate. For instance, a relying party may be obligated to rely on certificates only for appropriate applications as set forth in the CP and in consistency with applicable certificate content (e.g., key usage field), successfully perform public key operations as a condition of relying on a certificate, assume responsibility to check the status of a certificate using one of the required or permitted mechanisms set forth in the CP/CPS (see Section 4.9 below), and assent to the terms of the applicable relying party agreement as a condition of relying on the certificate.

Descrição: Estabelece as responsabilidades da entidade confiante pela utilização das chaves públicas e dos certificados.

Requisitos mínimos: A PC deve estabelecer que seja de responsabilidade das entidades confiantes verificarem a validade e uso apropriado do certificado de acordo com o PC sob o qual foi emitido.

Melhores práticas: Devem ser estabelecidos critérios para que as entidades confiantes possam definir se devem ou não confiar em um certificado. A

responsabilidade pela aceitação de um certificado é exclusivamente da entidade confiante.

Exemplos de texto:

"Um usuário do certificado deverá, ao ser apresentado a um certificado emitido pela AC de Grades, verificar:

a) sua validade
- *Verificando se confia na AC que emitiu o certificado;*
- *Verificando se o certificado não expirou;*
- *Consultando a ultima versão da LCR da AC de Grades no momento de utilização do certificado.*

b) o uso apropriado do certificado como descrito na PC sob qual foi emitido (identificado pelo OID no próprio certificado) e o uso das chaves inclusas no certificado, através do campo Key Usage".

"As entidades confiantes devem:
- *Estar cientes das informações presentes neste documento;*
- *Verificar a LCR mais recente antes de aceitar um certificado como sendo válido;*
- *Observar as políticas estabelecidas para o certificado".*

4.6 Reemissão de certificados por troca do prazo de validade

This subcomponent is used to describe the following elements related to certificate renewal. Certificate renewal means the issuance of a new certificate to the subscriber without changing the subscriber or other participant's public key or any other information in the certificate.

4.6.1 Circunstância para renovação de certificados

Circumstances under which certificate renewal takes place, such as where the certificate life has expired, but the policy permits the same key pair to be reused;

Descrição: Estabelece as circunstâncias sob as quais uma renovação deve ser solicitada, quando aplicável.

Requisitos mínimos: Se aplicável, a PC deve estabelecer que só seja permitido renovar um certificado se suas informações não sofrerem alterações e a respectiva unidade organizacional continuar vinculada à organização. Também deve ser estabelecido um limite de renovações para um mesmo par de chaves. Solicitação de renovação para certificados expirados não é permitida. A posse da chave privada deve ser verificada antes da re-emissão.

Melhores práticas: Devido à exposição das chaves decorrente de sua utilização por um longo período de tempo, é importante encorajar os usuários a seguir os procedimentos de troca de chaves ao invés da renovação do certificado. As credenciais só devem ser renovadas se as chaves são guardadas em um dispositivo de hardware seguro e não devem ser renovadas

por mais de cinco anos consecutivos sem uma revalidação da identidade do titular.

Exemplos de texto:

"A UFF BrGrid CA pode optar por rejeitar a renovação por motivos de segurança, a fim de evitar riscos derivados da exposição de chaves privadas por um longo período de tempo. Em qualquer caso, certificados não serão renovados por mais de cinco anos consecutivos sem que haja uma verificação da identidade".

Auditoria: Operacional.

4.6.2 Quem pode solicitar renovação

Who may request certificate renewal, for instance, the subscriber, RA, or the CA may automatically renew an end-user subscriber certificate;

Descrição: Estabelece quem está autorizado a solicitar a renovação de um certificado, se aplicável.

Requisitos mínimos: A renovação do certificado deve, se aplicável, ser solicitada pelo seu responsável (titulares no caso de certificados pessoais ou gerentes no caso de certificados de AC, por exemplo).

Melhores práticas: Certificados não devem ser renovados automaticamente pela AC e nenhum pedido de renovação deve ser feito automaticamente pela AR, e os indivíduos autorizados a solicitar renovação devem estar claramente definidos.

Exemplos de texto:

"Qualquer servidor docente e técnico administrativo da UFMG devidamente autorizado pelo representante legal da unidade organizacional a qual está vinculado".

"O dono do certificado pode solicitar a renovação de um certificado antes que este expire, usando a interface web segura ou enviando um e-mail assinado com a chave privada associada ao certificado cuja renovação é solicitada a AR apropriada".

Auditoria: Operacional.

4.6.3 Processamento de solicitações de renovação

A CA or RA's procedures to process renewal requests to issue the new certificate, for example, the use of a token, such as a password, to re-authenticate the subscriber, or procedures that are the same as the initial certificate issuance;

Descrição: Estabelece as medidas que AC e AR devem tomar para validar e responder pedidos de renovação, quando aplicável.

Requisitos mínimos: Os procedimentos devem ser equivalentes aqueles seguidos para a emissão do primeiro certificado do titular.

Melhores práticas: Ainda não definido.

Auditoria: Operacional.

4.6.4 Notificação de nova emissão de certificado para o titular

Descrição: Estabelece se a AC deve ou não comunicar o titular do certificado sobre a renovação.

Requisitos mínimos: Os procedimentos devem ser equivalentes aqueles seguidos para a emissão do primeiro certificado do titular.

Melhores práticas: Ainda não definido.

Auditoria: Operacional.

4.6.5 Conduta que constitui aceitação de um certificado renovado

Descrição: Estabelece a conduta de um titular de certificado que caracterize a aceitação de um certificado.

Requisitos mínimos: Não estipulado.

Melhores práticas: Apesar de ser um processo diferente da solicitação inicial de um certificado, pode ser apropriado utiliza os mesmo procedimentos, como descritos em seção 4.4.1 onde o solicitante deve indicar sua aceitação dentro um prazo estabelecido para confirmar o recebimento do certificado.

4.6.6 Publicação do certificado renovado pela AC

Descrição: Especifica os locais de publicação dos certificados renovados.

Requisitos mínimos: A AC deve publicar os certificados renovados em seu repositório público, assim como os outros certificados emitidos.

Melhores práticas: Ainda não definido.

Auditoria: Operacional.

4.6.7 Notificação pela AC da emissão de um certificado para outras entidades

Descrição: Estabelece se a AC deve ou não comunicar outras entidades (AR e partes confiantes, por exemplo) sobre a renovação.

Requisitos mínimos: Não estipulado.

Melhores práticas: Nenhuma ação além da publicação do certificado emitido no repositório precisa ser tomada. Entretanto, uma entidade pode solicitar que seja notificada quando um certificado for emitido, fornecendo uma justificativa razoável. Com, por exemplo:

a) Um administrador de rede pode solicitar que seja notificado sempre que um certificado for emitido para um recurso sobre sua responsabilidade;
b) O coordenador de uma determinada Unidade Organizacional pode solicitar que seja notificado caso algum certificado seja emitido para sua OU.

4.7 Reemissão de certificados por troca de chaves

This subcomponent is used to describe the following elements related to a subscriber or other participant generating a new key pair and applying for the issuance of a new certificate that certifies the new public key.

4.7.1 Circunstâncias para substituição das chaves criptográficas

Circumstances under which certificate re-key can or must take place, such as after a certificate is revoked for reasons of key compromise or after a certificate has expired and the usage period of the key pair has also expired.

Descrição: Estabelece as circunstâncias sob as quais as chaves criptográficas devem ser trocadas, quando aplicável. Este é método preferido para re-emissão de certificados de entidades finais, onde o DN é mantido. No caso de ACs intermediarias novos certificados devem ser solicitados (isto é, gerando uma nova solicitação). Os DNs são modificados para diferençar entre as duas instancias da AC (a antiga e a nova).

Requisitos mínimos: A PC deve estabelecer que não seja permitida a substituição de chaves de um certificado não valido (i.e. expirado ou revogado). Nesse caso, procedimentos para solicitação de um novo certificado devem ser seguidos.

Melhores práticas: Sempre que não for mais possível garantir a veracidade das informações no certificado (mudança de sobrenome, organização ou unidade organizacional do titular, por exemplo), a troca do par de chaves não deve ser permitida.

Auditoria: Operacional.

4.7.2 Quem pode solicitar a certificação de uma nova chave pública

Who may request certificate re-key, for example, the subscriber.

Descrição: Estabelece, quando aplicável, quem está autorizado a solicitar a troca de chaves de um certificado.

Requisitos mínimos: O pedido de certificação de uma nova chave pública deve ser solicito pelo seu responsável (titulares no caso de certificados pessoais ou gerentes no caso de certificados de AC, por exemplo).

Melhores práticas: O pedido de certificação de uma nova chave pública deve ser solicito pelo seu responsável, utilizando a chave privada ainda válida.

Auditoria: Operacional.

4.7.3 Processamento de solicitações de substituição de certificados

A CA or RA's procedures to process re-keying requests to issue the new certificate, such as procedures that are the same as the initial certificate issuance.

Descrição: Estabelece as medidas tomadas por AC ou AR para processar solicitações de substituição de certificados.

Requisitos mínimos: A existência e validade do certificado devem ser verificadas durante o processamento da solicitação. A solicitação deve ser autenticada e o solicitante deve ser identificado de forma apropriada. No mínimo, o conteúdo do certificado relacionado ao solicitante deve ser verificado.

Melhores práticas: Recomenda-se seguir os mesmos procedimentos definidos na seção 3.2, ou que a solicitação seja assinada com o certificado ainda valido do solicitante, a fim de garantir que o solicitante realmente é o titular do certificado cuja troca de par de chaves está sendo solicitada.

Auditoria: Operacional.

4.7.4 Notificação de nova emissão de certificado para o titular

Descrição: Estabelece se a AC deve ou não comunicar o titular sobre a emissão do novo certificado.

Requisitos mínimos: Não estipulado.

Melhores práticas: Nenhuma ação além da publicação do certificado emitido no repositório precisa ser tomada. Entretanto, uma entidade pode solicitar que seja notificada caso certificados sejam emitidos, fornecendo uma justificativa razoável. Com, por exemplo:

a) Um administrador de rede pode solicitar que seja notificado sempre que um certificado for emitido para um recurso sobre sua responsabilidade;
b) O responsável de uma determinada Unidade Organizacional (OU) pode solicitar que seja notificado caso algum certificado seja emitido para sua OU.

4.7.5 Conduta para a aceitação de um novo certificado

Descrição: Estabelece a conduta de um titular de certificado que caracterize a aceitação de um novo certificado.

Requisitos mínimos: Não estipulado.

Melhores práticas: Ainda não definido.

4.7.6 Publicação do novo certificado

Descrição: Especifica os locais de publicação dos novos certificados.

Requisitos mínimos: A AC deve publicar os certificados com a troca de chave em seu repositório público, assim como os outros certificados emitidos.

Melhores práticas: Ainda não definido.

Auditoria: Operacional.

4.7.7 Notificação pela AC da emissão de um certificado para outras entidades

Descrição: Estabelece se a AC deve ou não comunicar outras entidades (AR e partes confiantes, por exemplo) sobre a emissão do novo certificado.

Requisitos mínimos: Não estipulado

Melhores práticas: Ainda não definido.

4.8 Reemissão de certificados por troca de dados

This subcomponent is used to describe the following elements related to the issuance of a new certificate due to changes in the information in the certificate other than the subscriber public key.

4.8.1 Circunstâncias para modificação de certificados

Circumstances under which certificate modification can take place, such as name change, role change, reorganization resulting in a change in the DN.

Descrição: Estabelece as circunstâncias sob um certificado pode ser modificado.

Requisitos mínimos: Não é permitida a modificação de certificados.

Melhores práticas: A modificação de certificados deve ser evitada. Caso seja necessário alterar qualquer dado contido nos mesmos, deve-se fazer uma nova solicitação para que as informações sejam validadas novamente.

Auditoria: Operacional.

4.8.2 Quem pode solicitar a modificação de um certificado

A CA or RA's procedures to process modification requests to issue the new certificate, such as procedures that are the same as the initial certificate issuance.

Descrição: Estabelece, quando aplicável, quem está autorizado a solicitar a modificação de um certificado.

Requisitos mínimos: Não se aplica, pois não é permitida a modificação de certificados.

Melhores práticas: Não se aplica.

4.8.3 Processamento de solicitações de modificação de certificados

Descrição: Estabelece as medidas tomadas por AC ou AR para processar solicitações de modificação de certificados.

Requisitos mínimos: Não se aplica.

Melhores práticas: Ainda não definido.

4.8.4 Notificação de nova emissão de certificado para o titular

Descrição: Estabelece se a AC deve ou não comunicar o titular sobre a emissão do novo certificado.

Requisitos mínimos: Não se aplica.

Melhores práticas: Ainda não definido.

4.8.5 Conduta para a aceitação de um novo certificado modificado

Descrição: Estabelece a conduta de um titular de certificado que caracterize a aceitação de um novo certificado modificado.

Requisitos mínimos: Não se aplica.

Melhores práticas: Ainda não definido.

4.8.6 Publicação do certificado pela AC

Descrição: Especifica os locais de publicação de certificados modificados.

Requisitos mínimos: Não se aplica.

Melhores práticas: Ainda não definido.

4.8.7 Notificação pela AC da emissão de um certificado para outras entidades

Descrição: Estabelece se a AC deve ou não comunicar outras entidades (AR e partes confiantes, por exemplo) sobre a emissão do novo certificado.

Requisitos mínimos: Não se aplica.

Melhores práticas: Ainda não definido.

4.9 Revogação e Suspensão

4.9.1 Circunstâncias para revogação de certificados

Circumstances under which a certificate may be suspended and circumstances under which it must be revoked, for instance, in cases of subscriber employment termination, loss of cryptographic token, or suspected compromise of the private key.

Descrição: Estabelece as circunstâncias sob um certificado deve ser revogado.

Requisitos mínimos: Um certificado deve ser revogado obrigatoriamente quando:

a) for constatado o não cumprimento da PC;
b) for constatada a emissão imprópria ou defeituosa;
c) as informações que ele contém estão incorretas;
d) o titular de certificado não deseja mais ser vinculado à AC;
e) houver dissolução da AC que emitiu o certificado; ou
f) houver comprometimento da chave privada ou da sua mídia armazenadora.

Em caso de comprometimento da chave privada de uma AC, todos os certificados emitidos por ela devem ser imediatamente revogados.

Melhores práticas: Um certificado pode ser revogado a qualquer momento, caso suas informações estejam incorretas ou sob suspeita de comprometimento, ou por solicitação do responsável. Em caso de comprometimento da chave privada da AC, todos os certificados por ela emitidos devem ser imediatamente revogados. Deve ser mantido um registro de revogações, contendo o motivo da revogação (obrigatória ou solicitada) e a identificação de quem solicitou a revogação.

Auditoria: Operacional.

4.9.2 Quem pode solicitar revogação

Who can request the revocation of the participant's certificate, for example, the subscriber, RA, or CA in the case of an end-user subscriber certificate.

Descrição: Estabelece quem está autorizado a solicitar a revogação de um certificado.

Requisitos mínimos: Uma solicitação de revogação pode ser feita por:

a) determinação do CG ICPEDU;
b) determinação da AC que emitiu o certificado;
c) solicitação de uma AR relacionada à AC que emitiu o certificado;
d) solicitação de uma entidade confiante;
e) solicitação do responsável pelo certificado (titulares em caso de certificados pessoais ou alguém que represente responsabilidade pela máquina ou serviço certificado);
f) determinação da instituição hospedeira; ou
g) determinação judicial;

Melhores práticas: As ACs devem determinar políticas e práticas que estabeleçam uma conexão entre quem pode solicitar a revogação com as circunstâncias em que ela pode ocorrer.

4.9.3 Processamento de solicitações de revogação

Procedures used for certificate revocation request, such as a digitally signed message from the RA, a digitally signed message from the subscriber, or a phone call from the RA.

Descrição: Estabelece as medidas tomadas por AC ou AR para processar solicitações de revogação de certificados.

Requisitos mínimos: Antes de revogar um certificado, a AC ou AR deve autenticar a fonte da solicitação de acordo com os procedimentos usados para o registro inicial. Em casos emergenciais, a revogação pode ser iniciada por comunicação oral. As AC devem manter registro de todas as solicitações.

Melhores práticas: A AC ou AR deve estabelecer um canal de comunicação para envio de solicitações de revogação (um e-mail assinado com a chave privada do certificado, caso não esteja comprometida, por exemplo). As AC podem revogar certificados sem confirmação a respeito de prova de comprometimento ou não comprimento da PC, mas ainda assim deve manter registro das ações.

Exemplos de texto:

“A solicitação de revogação deve ser feita na página web da AC LNCC após autenticação com usuário e senha”.

"Antes de revogar um certificado, a AC de Grades deve autenticar a fonte da solicitação de acordo com os procedimentos usados para o registro inicial. A AC de Grades tentará sempre notificar o titular antes de revogar o certificado".

Auditoria: Operacional.

4.9.4 Prazo para solicitação de revogação

The grace period available to the subscriber, within which the subscriber must make a revocation request;

Descrição: Estabelece um prazo para solicitação de revogação caso ocorra qualquer circunstância definida no item 4.9.1.

Requisitos mínimos: Um prazo apropriado deve ser estabelecido.

Melhores práticas: Caso seja necessário uma revogação, o titular de certificado deve fazê-lo o mais breve possível. Recomenda-se que sejam definidos diferentes prazos para cada tipo de certificado emitido (certificados de AC, de AR, recursos, pessoas, etc.) de acordo com a demanda.

Auditoria: Operacional.

4.9.5 Prazo para a AC processar a solicitação de revogação

Descrição: Estabelece um prazo para AC processar uma solicitação de revogação.

Requisitos mínimos: Uma solicitação de revogação deve ser processada no prazo máximo de 1 (um) dia útil.

Melhores práticas: Não se aplica.

4.9.6 Requisitos para verificação de revogação por entidades confiantes

The mechanisms, if any, that a relying party may use or must use in order to check the status of certificates on which they wish to rely;

Descrição: Estabelece mecanismos que devem ser usados pelas entidades confiantes a fim de verificar o status de certificados e determinar se são confiáveis.

Requisitos mínimos: Todos os certificados de nível imediatamente subseqüente ao da AC devem ter a validade verificada na LCR mais recente emitida por esta antes de serem utilizados. Também deve ser confirmada a autenticidade da LCR, através da verificação da assinatura da AC e do período de validade.

Melhores práticas: As AC podem também optar por outro modo de comunicação da revogação dos certificados, variando conforme sua aplicação. Estes procedimentos dependem fortemente da necessidade da AC de disseminar direta e rapidamente a notificação entre as entidades confiantes.

Auditoria: Pré-emissão e Operacional.

4.9.7 Frequência de emissão de LCRs

`If a CRL mechanism is used, the issuance frequency;`

Descrição: Estabelece a freqüência na qual uma nova Lista de Certificados Revogados (LCR) deve ser emitida.

Requisitos mínimos: A AC deve emitir uma nova LCR, no mínimo, sempre que houver revogação de certificado. Uma nova LCR deve ser emitida e publicada antes do tempo determinado na LCR vigente. O período de validade de LCRs de ACs que emite certificados para entidades finais não deve ser mais de 35 dias.

Melhores práticas: As LCRs provem informações sobre status dos certificados. A freqüência de emissão deve ser documentada. A LCR nova deve ser emitida pelo menos dois dias antes da expiração da LCR atual. E em casos onde a geração da LCR requer intervenção humana este tempo deve ser maior, for exemplo, sete dias. Por exemplo, LCRs poderia ter uma validade de 35 dias, mas porem serem emitidas cada 28 dias. O objetivo é sempre garantir que existe uma LCR valida ainda em caso de imprevistos que podem atrasar a emissão da nova LCR.

Auditoria: Operacional (a LCR seria monitorada em tempo real pela AGP).

4.9.8 Latência máxima para LCRs

`If a CRL mechanism is used, maximum latency between the generation of CRLs and posting of the CRLs to the repository (in other words, the maximum amount of processing- and communication-related delays in posting CRLs to the repository after the CRLs are generated);`

Descrição: Estabelece o tempo máximo entre a geração de uma LCR e sua publicação no repositório da AC.

Requisitos mínimos: A latência máxima deve ser de, no máximo, 30 minutos.

Melhores práticas: É desejável que o tempo entre a emissão e a publicação de uma LCR seja o menor possível. Portanto, ela deve ser publicada imediatamente após sua emissão, sem atraso.

Auditoria: Operacional.

4.9.9 Mecanismos para verificação on-line do status de certificados

`On-line revocation/status checking availability, for instance, OCSP and a web site to which status inquiries can be submitted;`

Descrição: Estabelece, se aplicável, um mecanismo on-line que permita a verificação do status do certificado.

Requisitos mínimos: Não estipulado.

Melhores práticas: Ainda não definido.

4.9.10 Obrigações da entidade confiante de verificar on-line o status de certificados

`Requirements on relying parties to perform on-line revocation/status checks;`

Descrição: Define as obrigações das entidades confiantes quanto à verificação on-line do status de certificados

Requisitos mínimos: Ainda não definido.

Melhores práticas: Ainda não definido.

4.9.11 Outras formas de comunicação de revogação

Descrição: Estabelece formas alternativas de comunicação de revogação.

Requisitos mínimos: Não estipulado.

Melhores práticas: Ainda não definido.

4.9.12 Procedimentos adicionais no caso de comprometimento da chave privada

`Any variations of the above stipulations for which suspension or revocation is the result of private key compromise (as opposed to other reasons for suspension or revocation).`

Descrição: Estabelece procedimentos específicos para revogações em caso de comprometimento de chave privada.

Requisitos mínimos: Não estipulado.

Melhores práticas: Ainda não definido.

4.9.13 Circunstâncias para suspensão de certificados

`Circumstances under which a certificate may be suspended.`

Descrição: Estabelece as circunstâncias sob um certificado pode ser suspenso.

Requisitos mínimos: Certificados não devem ser suspensos sob nenhuma hipótese.

Melhores práticas: Caso haja necessidade de suspensão de um certificado, este deve ser revogado e o processo de solicitação de um novo certificado deve ser seguido.

4.9.14 Quem pode solicitar suspensão

Who can request the suspension of a certificate, for example, the subscriber, human resources personnel, a supervisor of the subscriber, or the RA in the case of an end-user subscriber certificate.

Descrição: Estabelece quem está autorizado a solicitar a suspensão de um certificado.

Requisitos mínimos: Não se aplica.

Melhores práticas: Não se aplica.

4.9.15 Processamento de solicitações de suspensão

Descrição: Estabelece as medidas tomadas por AC ou AR para processar solicitações de suspensão de certificados.

Requisitos mínimos: Não se aplica.

Melhores práticas: Caso haja necessidade de suspensão de um certificado, este deve ser revogado e o processo de solicitação de um novo certificado deve ser seguido.

4.9.16 Limites para o período de suspensão

Descrição: Define um período máximo de suspensão de certificados.

Requisitos mínimos: Não se aplica.

Melhores práticas: Ainda não definido.

4.10 Serviços de status de certificado

This subcomponent addresses the certificate status checking services available to the relying parties.

4.10.1 Características operacionais

`The operational characteristics of certificate status checking services.`

Descrição: Estabelece as características do serviço de verificação do status de certificados.

Requisitos mínimos: Não estipulado.

Melhores práticas: Devem ser descritas as principais características do serviço escolhido para prover às entidades confiantes informações suficientes para a verificação do status de um certificado. Caso essa informação seja disponibilizada através de LCRs, por exemplo, deve-se citar onde é possível encontrá-la.

Exemplos de texto:

"*A AC Grades deve guardar em um repositório público e disponibilizar através do web site:*

a) O certificado da AC (e a cadeia de certificação até a AC raiz);
b) todos os certificados válidos; e
c) A LCR mais recente".

"A AC LNCC disponibiliza a última LCR emitida no seu sítio web."

4.10.2 Disponibilidade do serviço

`The availability of such services, and any applicable policies on unavailability.`

Descrição: Define a disponibilidade do serviço e sob que circunstâncias ele pode se tornar indisponível.

Requisitos mínimos: Devem ser tomadas medidas para que os serviços de verificação de status sejam mantidos disponíveis continuamente, mesmo durante por manutenções programadas.

Melhores práticas: Falhas de disponibilidade são inevitáveis, mas todo esforço razoável deve ser feito para minimizar o tempo de indisponibilidade.

Exemplos de texto:

"A LCR estará disponível no repositório da AC que oferece o serviço continuamente mesmo durante por manutenções programadas exceto por falhas for do controle da AC."

Auditoria: Operacional (a LCR seria monitorado pela AGP).

4.10.3 Características operacionais

`Any optional features of such services.`

Descrição: Define quaisquer características opcionais dos serviços de verificação de status de certificado.

Requisitos mínimos: Não estipulado.

Melhores práticas: Ainda não definido.

4.11 Encerramento do vínculo com a AC

This subcomponent addresses procedures used by the subscriber to end subscription to the CA services, including the revocation of certificates at the end of subscription (which may differ, depending on whether the end of subscription was due to the expiration of the certificate or termination of the service).

Descrição: Estabelece os procedimentos que caracterizam o encerramento do vínculo do titular com a AC.

Requisitos mínimos: O vínculo é encerrado quando ocorre expiração ou revogação de um certificado.

Melhores práticas: Ainda não definido.

4.12 Custódia e recuperação de chaves

This subcomponent contains the following elements to identify the policies and practices relating to the escrowing, and/or recovery of private keys where private key escrow services are available (through the CA or other trusted third parties).

4.12.1 Políticas e práticas para custódia e recuperação de chaves

Identification of the document containing private key escrow and recovery policies and practices or a listing of such policies and practices.

Descrição: Define um documento ou estabelece políticas e práticas para custódia e recuperação de chaves.

Requisitos mínimos: Não deve ser permitida a custódia das chaves privadas das entidades participantes da ICPEDU.

Melhores práticas: Tendo em vista que a chave privada deve estar sempre de posse (isto é, de controle de acesso/uso) unicamente do titular do certificado ou organização responsável pelo certificado, não deve ser oferecido nenhum serviço de custódia de chaves por **terceiros**. Entendemos que o termo *key escrow* significa que uma terceira parte (por ser autorizada) teria direito de usar a chave privada. Este conceito é diferente da guardar da chave privada onde é permitido que, por exemplo, a chave privado de uma AC ser guardado em um HSM junto com as chaves de outras AC se acesso a cada chave privada seja controlado unicamente do titular do certificado ou organização responsável pelo

certificado. O local físico da HSM não necessariamente teria que ser nas dependências da organização responsável para a AC.

4.12.2 Políticas e práticas para custódia e recuperação de chaves de sessão

Identification of the document containing session key encapsulation and recovery policies and practices or a listing of such policies and practices.

Descrição: Define um documento ou estabelece políticas e práticas para custódia e recuperação de chaves de sessão.

Requisitos mínimos: Não estipulado.

Melhores práticas: Ver seção 4.12.1.

5. Controles operacionais, gerenciais e de instalações físicas

A seção estabelece os controles operacionais, de segurança de pessoal e de segurança física usados para prover confiabilidade nas operações da ICP para seus participantes.

This component describes non-technical security controls (that is, physical, procedural, and personnel controls) used by the issuing CA to securely perform the functions of key generation, subject authentication, certificate issuance, certificate revocation, auditing, and archiving.

This component can also be used to define non-technical security controls on repositories, subject CAs, RAs, subscribers, and other participants. The non-technical security controls for the subject CAs, RAs, subscribers, and other participants could be the same, similar, or very different.

These non-technical security controls are critical to trusting the certificates since lack of security may compromise CA operations resulting for example, in the creation of certificates or CRLs with erroneous information or compromising the CA private key.

Within each subcomponent, separate consideration will, in general, need to be given to each entity type, that is, the issuing CA, repository, subject CAs, RAs, subscribers, and other participants.

5.1 Controles de Segurança Física

In this subcomponent, the physical controls on the facility housing the entity systems are described.

5.1.1 Localização e construção das instalações físicas

Site location and construction, such as the construction requirements for high-security zones and the use of locked rooms, cages, safes, and cabinets;

Descrição: Define a localização do ambiente que abriga os sistemas da AC, bem como os requisitos de segurança da construção.

Requisitos mínimos: A AC deve estar localizada em um ambiente sem janelas (ou com janelas que possam ser mantidas seguras), protegido ou afastado de fontes potentes de magnetismo ou interferência de rádio freqüência e de acesso restrito apenas ao pessoal autorizado.

Melhores práticas: O ambiente de operação da AC deve ser uma sala possível de ser trancada, protegida contra acessos não autorizados, possuir mecanismos de controle de acesso (como alarmes e travas, por exemplo) e mantida separada de áreas utilizadas por terceiros para processamento de informações. Proteção externa para portas e janelas deve ser considerada, especialmente as de fácil acesso.

Auditoria: Pré-emissão (visita ao local) e Operacional.

5.1.2 Acesso físico

Physical access, i.e., mechanisms to control access from one area of the facility to another or access into high-security zones, such as locating CA operations in a secure computer room monitored by guards or security alarms and requiring movement from zone to zone to be accomplished using a token, biometric readers, and/or access control lists.

Descrição: Define os mecanismos de controle de acesso ao ambiente que abriga a AC.

Requisitos mínimos: O ambiente de operação da AC deve ser protegido por controles apropriados que garantam acesso apenas ao pessoal autorizado. Sistemas de segurança para acesso físico devem ser estabelecidos para controlar e possibilitar auditoria o acesso aos sistemas de certificação e às chaves criptográficas, que devem ser protegidas contra acesso, uso ou duplicação não autorizadas.

Melhores práticas: Devem ser implantados controles de autenticação (biometria, senhas, cartões), e uma trilha de auditoria deve ser mantida e revisada freqüentemente.

Visitantes devem ter seu acesso previamente autorizado, e a data e hora de entrada e saída registradas. Os direitos de acesso a áreas restritas devem ser revistos constantemente. Em [ISO17799] é estabelecido que locais de carga e descarga devam ficar preferencialmente, isolados da área de operação da AC.

Exemplos de texto:

"A AC opera em um ambiente controlado com acesso restrito ao pessoal da BrGrid CA e aos administradores de sistema do IC-UFF. Acesso de terceiros só é permitido sob supervisão do pessoal autorizado da AC. Todos os acessos são registrados".

"O acesso físico às dependências da AC UFSC é gerenciado e controlado conforme a Política de Segurança da AC UFSC, que prevê a utilização de chaves, senhas, cartões, identificações biométricas ou outros dispositivos para controle de acesso. O acesso físico é monitorado, assegurando que apenas pessoas autorizadas participem das atividades pertinentes".

Auditoria: Pré-emissão e Operacional.

5.1.3 Energia e refrigeração

Descrição: Estabelece as medidas tomadas para manutenção da energia e da temperatura ideal no local de operação da AC.

Requisitos mínimos: O ambiente que abriga os equipamentos deve dispor de recursos que os protejam de falhas de energia e de um sistema de ar condicionado que o mantenha em temperatura ideal.

Melhores práticas: O fornecimento de energia que alimenta os equipamentos e a temperatura do ambiente que os abriga deve estar de acordo com as especificações dos fabricantes. Os sistemas de suporte a energia e refrigeração devem ser inspecionados freqüentemente, conforme definido pelo responsável local ou fabricante do equipamento, para garantir seu perfeito funcionamento e reduzir o risco de falha. Um sistema de contingência deve ser considerado a fim de reduzir a possibilidade de indisponibilidade do serviço.

Auditoria: Pré-emissão e Operacional.

5.1.4 Exposição à água

Descrição: Define as medidas tomadas para evitar a exposição dos sistemas a enchentes e alagamentos.

Requisitos mínimos: Os sistemas devem ser mantidos em instalações que os proteja de inundações, goteiras e outras ameaças provenientes da água.

Melhores práticas: Ao estabelecer um plano para reduzir riscos relacionados à água, devem-se levar em conta quaisquer ameaças apresentadas por instalações vizinhas (inundações em andares superiores, vazamentos em salas próximas).

Exemplos de texto:

"Dada à localização das dependências do Instituto de Computação, inundações não são esperadas. O Instituto de Computação está situado no terceiro andar, e os recursos computacionais da AC Grades são mantidos longe de janelas e tubulações de aqua, portanto não há expectativas de exposição à água".

"A Sala Cofre foi construída para ser completamente a prova d'água".

"A sala cofre se encontra em local protegido de inundações e vazamento internos de água."

Auditoria: Pré-emissão e Operacional.

5.1.5 Prevenção e proteção contra incêndio

Descrição: Define as medidas tomadas para evitar a exposição dos sistemas incêndios.

Requisitos mínimos: Sistemas de detecção e controle de incêndio, como detectores de fumaça e extintores devem ser mantidos de forma a possibilitar

sua ativação caso seja necessário. Material inflamável deve ser mantido a uma distância segura do ambiente de operação.

Melhores práticas: Equipamentos apropriados de combate a incêndios devem ser disponibilizados segundo as normas da brigada de incêndio local. Devem ser empregados sistemas que possibilitem ativação e notificação automáticas de incêndio e um grupo emergencial para respostas de eventos envolvendo fogo.

Auditoria: Pré-emissão e Operacional.

5.1.6 Armazenamento de mídia

Media storage, for example, requires the storage of backup media in a separate location that is physically secure and protected from fire and water damage.

Descrição: Define os requisitos para prevenção contra acesso, modificação, remoção e destruição não autorizados à mídia armazenada.

Requisitos mínimos: Toda mídia sensível deve ser armazenada em local seguro e apropriado de acordo com as especificações do fabricante, acessível apenas ao pessoal autorizado. Sua entrada, saída e utilização devem ser registradas a fim de manter uma trilha de auditoria.

Melhores práticas: Informação cujo tempo de armazenamento necessário é maior que a vida útil da mídia (de acordo com as especificações do fabricante) deve ser armazenada também em outros locais para evitar perda de informação proveniente da degradação da mídia [ISO17799].

Exemplos de texto:

"Cópias de backup de informações relacionadas à AC, mantidas em CD ou DVD e são armazenadas em um cofre trancado acessível apenas ao pessoal autorizado".

"O CPD do LNCC possui armários para armazenamento de mídia acessíveis somente pelo pessoal da Coordenação de Sistemas e Redes".

Auditoria: Pré-emissão e Operacional.

5.1.7 Descarte de lixo

Descrição: Define os requisitos para descarte de informações sensíveis e dispositivos eletrônicos que são não mais necessários.

Requisitos mínimos: Dispositivos (incluindo mídias de armazenamento) e documentos contendo informação sensível devem ser totalmente destruídos fisicamente antes do descarte.

Melhores práticas: Métodos apropriados de remoção e formatação devem ser utilizados a fim de deixar a informação inutilizada por pessoal não autorizado, mesmo antes da destruição. Devem ser adotados procedimentos formais de descarte de lixo, de acordo com o grau de confidencialidade da informação, a fim de minimizar o risco de exposição. Ferramentas anti-forense, por exemplo, podem ser utilizadas para apagar discos rígidos que contenham informações críticas.

Exemplos de texto:

"Toda mídia eletrônica, papel, memória e qualquer outro meio que possa conter informação considerada confidencial pela AC UFSC é armazenada em local apropriado (anexo a Sala Cofre) e posteriormente destruído".

"Material contendo informação potencialmente confidencial e dados que devem ser protegidos (dados relevantes como chaves privadas ou passphrases, ou dados pessoais) são descartados de forma a garantir que a informação não seja obtida ou re-utilizada".

Auditoria: Operacional.

5.1.8 Cópias de segurança em outras instalações

Descrição: Define os requisitos para cópias de segurança em outras instalações, como sua freqüência e considerações de segurança por não estar presente no ambiente principal.

Requisitos mínimos: Cópias de segurança das informações e software devem ser feitas e testadas regularmente, para serem mantidas em um ambiente externo. Os mesmos requisitos de segurança da instalação principal devem ser atendidos nas instalações externas que abrigam as cópias de segurança.

Melhores práticas: A localização do ambiente que guarda as cópias de segurança mantidas externamente deve ser tal que não seja atingida em caso de sinistro que torne inoperante a instalação principal, e possibilite a recuperação de desastre o mais rápido possível. Essas cópias devem ser revistas e testadas periodicamente para garantir que estão seguindo os requisitos do plano de continuidade de negócio. A opção de cifrar informações deve ser considerada, dependendo do seu grau de confidencialidade.

Auditoria: Pré-emissão e Operacional.

5.2 Procedimentos de Controle

In this subcomponent, requirements for recognizing trusted roles are described, together with the responsibilities for each role. Examples of trusted roles include system administrators, security officers, and system auditors.

5.2.1 Papéis de Confiança

Descrição: Descrever os perfis dos funcionários, e as respectivas responsabilidades, com o intuito de evitar que um funcionário de má fé utilize o sistema sem ser detectado.

Requisitos mínimos: O pessoal envolvido nas atividades da AC institucional deve passar por um processo seletivo e de verificação de antecedentes. Devem ser relacionadas e documentadas claramente as atribuições de cada função, de acordo com a característica das atividades envolvidas, a fim de determinar-se o perfil necessário do empregado ou servidor, considerando-se os seguintes itens:

a) A descrição sumária das tarefas inerentes à função;
b) As necessidades de acesso a informações sensíveis;
c) O grau de sensibilidade do setor onde a função é exercida;
d) As necessidades de contato de serviço interno e/ou externo;
e) As características de responsabilidade, decisão e iniciativas inerentes à função;
f) A qualificação técnica necessária ao desempenho da função.

Melhores práticas: Indivíduos que assumam papéis cuja função possa comprometer as chaves devem ser confiáveis. As atribuições de cada papel deverão ser claramente definidas e comunicadas à pessoa que irá assumir a função, e garante que o indivíduo será responsabilizado pelas ações tomadas.

Funcionários de terceiros que estejam relacionados com tarefas que suportam o gerenciamento do ciclo de vida dos certificados também devem ser claramente comunicados sobre suas responsabilidades.

Exemplos de texto:

"***Gerente*** *Servidor técnico administrativo designado pelo reitor da UFSC para ser o responsável pela AC UFSC, que formará os grupos de administradores, operadores e auditores. Ele também é responsável pela aprovação dos relatórios da AC UFSC. Adicionalmente, depois de ter recebido os relatórios de auditorias, ele é responsável por encaminhar estes relatórios ao CG da ICPEDU".*

*"**Administrador** O administrador é responsável pela instalação, configuração, backup e manutenção dos equipamentos e software de gestão do ciclo de vida do certificado digital. Também define as políticas e cria ACs, além de definir ou trocar os grupos de operadores e auditores. Adicionalmente, é responsável pelos relatórios de operação da AC UFSC";*

*"**Operador** Os operadores são os responsáveis pelo uso da chave privada da AC UFSC para a emissão de LCRs e de certificados digitais de ACs";*

*"**Auditor** O auditor é responsável pela auditoria do ciclo de vida do certificado digital, das chaves criptográficas e de todas as operações AC UFSC".*

Auditoria: Pré-emissão e Operacional.

5.2.2 Número de pessoas necessárias por tarefa

For each task identified, the number of individuals required to perform the task (n out m rule) should be stated for each role. Identification and authentication requirements for each role may also be defined.

Descrição: Especificar o número de pessoas necessárias para executar as tarefas listadas, caso sejam necessários controles de multiusuário.

Requisitos mínimos: Não estipulado.

Melhores práticas: A AC deve garantir a separação das tarefas para funções críticas, e se necessário adotar controle multiusuário, com o intuito de evitar que um funcionário de má fé utilize o sistema de certificação sem ser detectado.
.

5.2.3 Identificação e autenticação para cada papel

This component also includes the separation of duties in terms of the roles that cannot be performed by the same individuals.

Descrição: Especificar os controles necessários para identificar e autenticar os indivíduos na atuação de seus papéis.

Requisitos mínimos: Todos os indivíduos devem ser identificados de forma única e autenticados para exercer cada papel. A autenticação deve se dar por meio de senhas, *tokens*, biometria ou, em caso de autenticação múltipla, uma combinação destes fatores [NIST800-53]. Compartilhamento de identificadores só é permitido para fins específicos (como a utilização da chave privada da AC pelos operadores para assinar certificados aprovados).

Melhores práticas: Indivíduos que exerçam funções fundamentais para operação da AC ou AR devem ser funcionários da instituição responsável por sua administração. Devem ser adotados procedimentos de autenticação múltipla para papéis envolvidos no gerenciamento do ciclo de vida do certificado. Todos os procedimentos de autenticação devem ser documentados e registros de sucesso ou falha durante este processo devem ser armazenados.

Auditoria: Pré-emissão e Operacional.

5.2.4 Papéis que requerem separação de responsabilidade

Descrição: Especifica papéis que não podem ser exercidos simultaneamente pelo mesmo indivíduo.

Requisitos mínimos: As pessoas que exercem papéis de gerente, administrador e operador não devem assumir o papel de auditor.

Melhores práticas: A separação de responsabilidade deve ser adotada para reduzir os riscos de modificação não autorizada de conteúdos confidenciais e devem ser tomados cuidados específicos para que ninguém seja capaz de acessar ou modificar informações sem autorização e detecção.

Auditoria: Pré-emissão e Operacional.

5.3 Controle de Pessoal

Neste item deve ser especificado que os funcionários, empregados ou servidores que exercem tarefas operacionais devem assinar um termo de responsabilidade assumindo o dever de manter o sigilo, mesmo quando desligado, sobre todos os ativos de informações e de processos das entidades integrantes da ICPEDU. Também deve ser especificado como será esse termo.

5.3.1 Requisitos de qualificação, experiência e conformidade com obrigações governamentais

Qualifications, experience, and clearances that personnel must have as a condition of filling trusted roles or other important roles. Examples include credentials, job experiences, and official government clearances that candidates for these positions must have before being hired.

Descrição: Especifica os requisitos para contratação de pessoal.

Requisitos mínimos: Somente funcionários da própria Instituição responsável, ou terceiras contratadas pela instituição especificamente para este fim (ver seção 5.3.7), devem ser admitidos no exercício de atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados da AC Institucional.

Melhores práticas: Devem ser adotados critérios rígidos para o processo seletivo de candidatos, com o propósito de selecionar, para os quadros das entidades integrantes da ICPEDU, pessoas reconhecidamente idôneas e sem antecedentes que possam comprometer a segurança ou credibilidade das entidades [AGP07].

Exemplos de texto:

“O pessoal envolvido na operação da AC UFSC é pertencente ao quadro de Servidores Técnico-Administrativos da UFSC. Estes são escolhidos de acordo com a sua qualificação, experiência e respeito ao regulamento da UFSC”.

Auditoria: Pré-emissão e Operacional.

5.3.2 Procedimentos de verificação de antecedentes

Background checks and clearance procedures that are required in

connection with the hiring of personnel filling trusted roles or perhaps other important roles; such roles may require a check of their criminal records, references, and additional clearances that a participant undertakes after a decision has been made to hire a particular person;

Descrição: Descreve os procedimentos seguidos para verificar os antecedentes antes da contratação de um funcionário.

Requisitos mínimos: Os procedimentos internos de verificação de antecedentes de cada instituição devem ser seguidos.

Melhores práticas: Deve considerar a elaboração de uma pesquisa do histórico de vida pública do candidato para papéis de confiança, de acordo com a legislação institucional e nacional vigente, com o propósito de levantamento de seu perfil. A legislação trabalhista deve ser levada em conta no decorrer do processo de pesquisa de antecedentes dos candidatos que devem ser informados sobre esta pesquisa previamente [ISO17799]. Dados que podem ser verificados, se permitido:

a) Curriculum vitae do candidato;
b) Confirmação de qualificação acadêmica e profissional;
c) Verificação de validade do documento de identificação apresentado.

Auditoria: Pré-emissão e Operacional.

5.3.3 Requisitos de treinamento

Training requirements and training procedures for each role following the hiring of personnel.

Descrição: Estabelece o processo de treinamento pelo qual o pessoal deverá passar.

Requisitos mínimos: Uma política de treinamento deve ser formalmente definida e documentada, além de revisada periodicamente para que seja mantida em conformidade com a política de segurança e os requisitos de operação do software que suporte as atividades de administração do ciclo de vida dos certificados.

Melhores práticas: O programa de treinamento deve ser baseado nos requisitos de segurança da instituição e da ICPEDU, e nas instruções de operação do software e hardware que suportam as atividades da AC e AR. O treinamento deve ser dado antes de autorizar o acesso ao sistema para executar a tarefa designada.

Auditoria: Pré-emissão e Operacional.

5.3.4 Requisitos de freqüência de treinamento

Any retraining period and retraining procedures for each role after completion of initial training.

Descrição: Estabelece a freqüência na qual deve haver um novo treinamento.

Requisitos mínimos: Um novo treinamento deve ser efetuado a cada mudança nos procedimentos ou na plataforma computacional.

Melhores práticas: O pessoal de operação da AC e AR deve ser treinado nos procedimentos descritos na PC/DPC com freqüência de um ano, ou sempre que surgirem alterações significativas.

Auditoria: Operacional.

5.3.5 Freqüência e seqüência para revezamento de trabalho

`Frequency and sequence for job rotation among various roles.`

Descrição: Estabelece a freqüência de revezamento no exercício de papéis.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

5.3.6 Sanções para ações não autorizadas

`Sanctions against personnel for unauthorized actions, unauthorized use of authority, and unauthorized use of entity systems for the purpose of imposing accountability on a participant's personnel.`

Descrição: Estabelece e descreve as medidas que podem ser tomadas caso haja alguma ação não autorizada.

Requisitos mínimos: Caso seja constatada uma ação não autorizada, esta deve ser avaliada e, se julgado necessário, sanções apropriadas previstas na legislação vigente, no regulamento interno da instituição responsável pela AC ou na PC/DPC devem ser aplicadas.

A PC/DPC deve deixar claro que ações podem ser tomadas quando há ocorrência de ações não autorizadas.

Melhores práticas: Deve ser estabelecido um processo disciplinar formal para o tratamento de pessoal suspeito de tomar uma ação não autorizada. As sanções devem levar em conta “fatores como a natureza e gravidade da ação e seu impacto no negócio, se é ou não uma primeira ou repetida ofensa, se o violador foi ou não treinado apropriadamente, legislação relevante, contratos de negócio e outros fatores conforme a necessidade” [ISO17799].

Exemplos de texto:

“O acesso de um indivíduo envolvido na operação da AC será imediatamente revogado quando for verificada a ocorrência de uma ação não autorizada e todas as medidas administrativas cabíveis serão tomadas pela entidade responsável.”

Auditoria: Operacional.

5.3.7 Requisitos para prestadores de serviços independentes

Controls on personnel that are independent contractors rather than employees of the entity; examples include: Bonding requirements on contract personnel; Contractual requirements including indemnification for damages due to the actions of the contractor personnel; Auditing and monitoring of contractor personnel; and other controls on contracting personnel.

Descrição: Estabelece e descreve os controles sobre pessoal externo ao quadro de empregados da instituição na prestação de serviço para a mesma.

Requisitos mínimos: Devem ser previstas no contrato cláusulas que contemplem a responsabilidade dos prestadores de serviço no cumprimento da Política de Segurança, da PC/DPC, suas normas e procedimentos. As ações de terceiros devem ser monitoradas a fim de verificar a conformidade das operações com essas cláusulas.

Melhores práticas: A instituição deverá garantir que as ações dos prestadores de serviço estão de acordo com o estabelecido na política de segurança, exigindo relatórios e registros das operações. Auditorias devem ser conduzidas regularmente para monitorar e revisar as operações dos prestadores de serviço.

Auditoria: Pré-emissão (verificar se os procedimentos e mecanismos foram implementados) e Operacional.

5.3.8 Documentação fornecida aos funcionários

Documentation to be supplied to personnel during initial training, retraining, or otherwise.

Descrição: Estabelece quais documentos serão fornecidos ao pessoal responsável pela operação da AC ou AR.

Requisitos mínimos: Deve ser disponibilizado para o pessoal envolvido na operação da AC, mas não somente:

a) Sua PC/DPC e a PS da instituição;
b) Documentação operacional relativa à sua atividade;
c) Contratos normas e políticas relevantes para suas atividades.

Melhores práticas: A documentação disponível para pessoal autorizado deve incluir [NIST800-53]:

a) Guias de usuário e administrador (contendo informações de instalação, configuração e operação) dos sistemas;
b) Documentação do fabricante, se disponível, descrevendo a arquitetura e implementação dos controles de segurança empregados nos sistemas suficientemente detalhado para permitir análise e teste dos mesmos.

Auditoria: Pré-emissão e Operacional.

5.4 Sistemas de auditoria e procedimentos para registro de eventos

This subcomponent is used to describe event logging and audit systems, implemented for the purpose of maintaining a secure environment.

5.4.1 Tipos de eventos registrados

Types of events recorded, such as certificate lifecycle operations, attempts to access the system, and requests made to the system.

Descrição: Especifica que eventos serão registrados para compor a trilha de auditoria.

Requisitos mínimos: Devem ser registrados eventos relacionados às atividades dos usuários, exceções e eventos de segurança da informação. No mínimo o sucesso ou falha dos seguintes eventos devem ser registrados (mas não limitado a estes), com data e hora:

a) Acessos físicos;
b) Inicialização e desligamento do sistema;
c) Login e logout;
d) Uso do SGCI e do HSM, tais como:
    i. **Erro:** Quando ocorre um erro na execução de um comando;
    ii. **Verbose:** Mensagens durante a execução de todas as operações no HSM;
    iii. **Warning:** Mensagens de aviso enviadas aos clientes conectados;
    iv. **Connection:** Quando as conexões são iniciadas e finalizas;
    v. **Commands:** Todos os comandos que são enviados ao HSM;
    vi. **Answer:** Todas as mensagens de resposta (finalização da execução de um comando) a um comando;
    vii. **Logs Gerais:** Por exemplo: opções selecionadas na configuração inicial do sistema;
    viii. Iniciação e desligamento do sistema de certificação;
    ix. Tentativas de criar, remover, definir senhas ou mudar os privilégios de sistema dos administradores, operadores e auditores;
    x. Mudanças na configuração da AC ou da chave privada de assinatura;
    xi. Mudanças nas políticas de criação de certificados;
    xii. Geração de chaves;
    xiii. Emissão e revogação de certificados;
    xiv. Geração de LCR.
e) Registros de destruição de mídia;
f) Ativação ou desativação dos registros automáticos de auditoria.

Melhores práticas: As instituições devem observar a conformidade com a legislação aplicável ao monitoramento das atividades. É recomendado concentrar os registros de auditoria em um servidor central que permita uma

análise modular (de cada componente individualmente) e global do sistema, através de uma trilha de auditoria baseada em tempo. Os registros de eventos auditáveis devem ser periodicamente analisados.

Auditoria: Operacional.

5.4.2 Freqüência de análise dos registros de auditoria

Frequency with which audit logs are processed or archived, for example, weekly, following an alarm or anomalous event, or when ever the audit log is n% full.

Descrição: Especifica a freqüência na qual os registros de auditoria são analisados em busca de um evento suspeito e então arquivados.

Requisitos mínimos: Os registros devem ser analisados mensalmente.

Melhores práticas: Os registros de auditoria devem ser analisados pelo menos mensalmente ou no caso de suspeita de uma brecha de segurança.

Auditoria: Operacional.

5.4.3 Período de arquivamento de registros de auditoria

Period for which audit logs are kept.

Descrição: Especifica o período de arquivamento dos registros de auditoria.

Requisitos mínimos: Os registros de auditoria deverão ser guardados no mínimo por 5 (cinco) anos.

Melhores práticas: Não estipulado.

Auditoria: Operacional.

5.4.4 Proteção de registros de eventos

Who can view audit logs, for example only the audit administrator. Protection against modification of audit logs, for instance a requirement that no one may modify or delete the audit records or that only an audit administrator may delete an audit file as part of rotating the audit file; and protection against deletion of audit logs.

Descrição: Especifica e descreve os controles impostos às atividades relacionadas à administração dos registros de auditoria, como acesso e modificação, por exemplo.

Requisitos mínimos: Os registros devem ser acessíveis apenas pelo grupo de auditores e administradores. Devem ser estabelecidos controles para evitar mudanças não autorizadas, como alterações ou remoções, e estes devem ser documentados na PC/DPC. O sistema deve informar se houver falha no

registro de uma ocorrência ou se o espaço ocupado pelos registros de auditoria estiver próximo do limite máximo estipulado.

Melhores práticas: Um sistema de contingência, no qual a cópia de certos eventos para outros arquivos é feita no momento do registro, pode ser adotado. Para controlar o crescimento do volume de registros, deve ser considerada a utilização de sistemas de racionalização ou ferramentas de auditoria.

Auditoria: Pré-emissão (verificar se os procedimentos e mecanismos foram implementados) e Operacional.

5.4.5 Procedimentos para cópias de segurança de registros de eventos

Descrição: Especifica os procedimentos para cópias de segurança de registros de eventos.

Requisitos mínimos: Cópias de segurança dos registros de eventos devem ser feitas periodicamente e revisadas com freqüência. Os procedimentos de cópia devem ser documentados para facilitar o processo de auditoria e implementação.

Melhores práticas: Devem ser feitas cópias com freqüência no mínimo mensal. Os arquivos copiados devem ser cifrados e sua integridade deve ser verificada periodicamente.

Exemplos:

"As cópias de segurança dos registros de eventos são armazenados de forma cifrada em mídia eletrônica removível. A integridade das cópias de segurança é verificada anualmente".

Auditoria: Pré-emissão (verificar se os procedimentos e mecanismos foram implementados) e Operacional.

5.4.6 Sistema de recolhimento de registros de eventos (interno ou externo)

Whether the audit log accumulation system is internal or external to the entity.

Descrição: Especifica se o sistema de recolhimento de registros de eventos é interno (ou seja, pertence à instituição) ou externo (está fora das dependências da instituição).

Requisitos mínimos: Não estipulado.

Melhores práticas: os sistemas de eventos para auditoria utilizados devem ser internos para que se possa ter maior controle sobre os mesmos.

5.4.7 Notificação do sujeito causador do evento

Whether the subject who caused an audit event to occur is notified of the audit action.

Descrição: Especifica se o causador de um evento será ou não notificado sobre a auditoria

Requisitos mínimos: Não estipulado.

Melhores práticas: Pode ser interessante informar ao causador do evento sobre sua conduta, a fim de que ele cesse a má prática e evite uma nova ocorrência. Por outro lado, em caso de eventos hostis, a notificação pode dificultar o rastreamento do atacante.

5.4.8 Avaliação de vulnerabilidades

Vulnerability assessments, for example, where audit data is run through a tool that identifies potential attempts to breach the security of the system.

Descrição: Especifica como será feita a avaliação de vulnerabilidades nos sistemas. Vulnerabilidades é o termo aplicado para determinar pontos fracos que possibilitem o comprometimento de um sistema. Essas fraquezas podem ser resultantes de diversos fatores, incluindo senhas fracas, bugs no software utilizado e pessoal mal treinado.

Requisitos mínimos: Avaliações de vulnerabilidades devem ser feitas mensalmente (e sempre que forem identificadas ou reportadas vulnerabilidades que afetem ou possam afetar os sistemas) e as medidas cabíveis para minimizar o risco associado a elas devem ser tomadas.

Melhores práticas: As instituições devem utilizar programas específicos de varredura que permitam atualizar a lista de vulnerabilidades a serem pesquisadas, sua gravidade, e os componentes que estão vulneráveis. As ações necessárias para minimizar o risco associado aos problemas encontrados devem ser tomadas no menor tempo possível.

O pessoal responsável pela segurança das operações da AC deve acompanhar os informes de segurança dos produtos que suportam o gerenciamento do ciclo de vida dos certificados, a fim de mantê-los sempre atualizados.

Exemplos:

"Todos os registros serão analisados sob a ótica de possíveis vulnerabilidades na plataforma computacional que hospeda o sistema de gerenciamento de certificados digitais e as chaves criptográficas da AC além da plataforma hospedeira do seu repositório. Também serão analisados os registros do ambiente seguro."

Auditoria: Operacional.

5.5 Arquivamento de Registros

This subcomponent is used to describe general records archival (or records retention) policies.

5.5.1 Tipos de registros armazenados

Types of records that are archived, for example, all audit data, certificate application information, and documentation supporting certificate applications.

Descrição: Especifica que registros serão arquivados, isto é, retidos em local separado para posterior auditoria, se necessário.

Requisitos mínimos: Os registros de eventos devem ser arquivados.

Melhores práticas: Devem ser mantidos, mas não limitados a estes:

a) Registros de mudanças, programadas ou não, no software, hardware ou procedimentos de operação dos sistemas;
b) Listas de Certificados Revogados;
c) Certificados emitidos;
d) Solicitações de certificados
e) Solicitações de revogações
f) Mudanças na PC/DPC (*changelog*)

Auditoria: Operacional.

5.5.2 Período de retenção dos registros arquivados

Descrição: Especifica por quanto tempo os registros arquivados serão retidos.

Requisitos mínimos: Os registros devem ser guardados por no mínimo 5 (cinco) anos em mídia não volátil.

Melhores práticas: Não estipulado.

Auditoria: Operacional.

5.5.3 Proteção dos registros armazenados

Who can view the archive, for example, a requirement that only the audit administrator may view the archive; Protection against modification of the archive, such as securely storing the data on a write once medium; Protection against deletion of the archive; Protection against the deterioration of the media on which the archive is stored, such as a requirement for data to be migrated periodically to fresh media; and protection against obsolescence of hardware, operating systems, and other software, by, for example, retaining as part of the archive the hardware, operating systems, and/or other software in order to permit access to and use of archived records over time.

Descrição: Especifica os controles impostos as atividades relacionadas aos registros arquivados.

Requisitos mínimos: Os registros armazenados devem ser acessíveis apenas pelo grupo de auditores e administradores e guardados em mídia não volátil e de escrita uma vez só (*write once/read only*). Devem ser estabelecidos controles para evitar mudanças não autorizadas, como destruição ou remoção das mídias do local que as abriga.

Melhores práticas: Vide 5.4.4.

Auditoria: Pré-emissão (verificar se os procedimentos e mecanismos foram implementados) e Operacional.

5.5.4 Procedimentos para cópias dos registros armazenados

Descrição: Especifica os procedimentos para cópias de segurança dos registros arquivados.

Requisitos mínimos: Cópias de segurança dos registros arquivados devem ser feitas periodicamente e revisadas com freqüência. Os procedimentos de cópia devem ser e documentados para facilitar o processo de auditoria e implementação.

Melhores práticas: Devem ser feitas cópias com freqüência no mínimo mensal. Os arquivos copiados devem ser cifrados e sua integridade deve ser verificada periodicamente.

Auditoria: Pré-emissão (verificar se os procedimentos e mecanismos foram implementados) e Operacional.

5.5.5 Requisitos para datação dos registros armazenados

Descrição: Especifica os requisitos para manter uma linha do tempo a partir da data e hora dos registros armazenados.

Requisitos mínimos: Todos os registros devem conter informações de data e hora.

Melhores práticas: Não estipulado.

Auditoria: Operacional.

5.5.6 Sistema de recolhimento de registros arquivados (interno ou externo)

Whether the archive collection system is internal or external.

Descrição: Especifica se o sistema de recolhimento de registros arquivados é interno (ou seja, pertence à instituição) ou externo (está fora das dependências da instituição).

Requisitos mínimos: Não estipulado.

Melhores práticas: Recomenda-se que seja interno.

5.5.7 Procedimentos para obtenção e verificação dos registros armazenados

Procedures to obtain and verify archive information, such as a requirement that two separate copies of the archive data be kept under the control of two persons, and that the two copies be compared in order to ensure that the archive information is accurate.

Descrição: Especifica os procedimentos para obter e verificar os registros arquivados.

Requisitos mínimos: Não estipulado.

Melhores práticas: Informações do arquivo só devem ser obtidas mediante aprovação do gerente da AC. A integridade das informações do arquivo de registro pode ser verificada através da comparação do resumo criptográfico deste, publicado (e guardado em local seguro) a cada modificação. Uma outra abordagem é guardar duas ou mais cópias, que deverão ser comparadas a fim de confirmar a veracidade do registro.

5.6 Nova Chave Pública para a AC

This subcomponent describes the procedures to provide a new public key to a CA's users following a re-key by the CA. These procedures may be the same as the procedure for providing the current key. Also, the new key may be certified in a certificate signed using the old key.

Descrição: Especifica os procedimentos para divulgação da chave pública da AC para as entidades confiantes após o processo de troca de chaves. A AC não pode assinar certificados com validade maior do que seu o próprio certificado. Portanto, o certificado da AC deve ser renovado antes de sua data de expiração, e seu par de chaves deve ser trocado. *O ponto de atualização da AC* é definido como a última data em que a chave atual deve ser utilizada para assinar solicitações para assinaturas de certificados (*Certificate Signing Requests* – CSRs). Supondo que a maior período de validade de um certificado emitido por esta AC é de 10 dias, o *ponto de atualização da AC* é a data correspondente a 10 dias antes da expiração do certificado atual da AC.

Requisitos mínimos: Certificados da AC não serão renovados; nesse caso, um novo par de chaves será gerado. Um novo par de chaves para uma AC Institucional deve ser gerado no mínimo 1 (um) mês antes do ponto de atualização da AC, de acordo com os processos e cerimônias já definidos. O

certificado assinado pela AC Raiz com a nova chave pública deve ser divulgado para às entidades confiantes de forma segura.

Melhores práticas: O certificado que contém a chave pública anterior deve ser mantido para que a assinatura nos certificados previamente emitidos possa ser verificada, até que todos estes certificados expirem, e para a geração de LCRs.

5.7 Comprometimento e Recuperação de Desastre

This subcomponent describes requirements relating to notification and recovery procedures in the event of compromise or disaster. Each of the following may need to be addressed separately.

5.7.1 Procedimentos para tratamento de incidentes e comprometimentos

Identification or listing of the applicable incident and compromise reporting and handling procedures.

Descrição: Descreve os procedimentos para relatar e tratar incidentes e comprometimentos, inclusive da chave privada da AC.

Requisitos mínimos: Deve ser estabelecida uma política formal e documentada de tratamento de incidentes em conformidade com a legislação vigente. Os procedimentos de tratamento de incidentes devem incluir desde a comunicação de eventos de segurança até a resposta ao receber um informe destes eventos. O Centro de Atendimento a Incidentes de Segurança (CAIS) da RNP deve ser notificado em caso de incidentes.

Melhores práticas: A instituição deve adotar mecanismos automáticos para suportar o processo de monitoramento e tratamento de incidentes [NIST800-53]. Responsabilidades devem ser atribuídas para garantir uma resposta rápida e eficaz.

Alguns tópicos, retirados de [ISO17799], devem ser considerados ao desenvolver os procedimentos de tratamento de incidentes de segurança:

a) procedures should be established to handle different types of information security incident, including:
   1) information system failures and loss of service;
   2) malicious code (see 10.4.1);
   3) denial of service;
   4) errors resulting from incomplete or inaccurate business data;
   5) breaches of confidentiality and integrity;
   6) misuse of information systems.

b) in addition to normal contingency plans (see 14.1.3), the procedures should also cover (see also 13.2.2):
   1) analysis and identification of the cause of the incident;
   2) containment;
   3) planning and implementation of corrective action to prevent recurrence, if necessary;
   4) communication with those affected by or involved with recovery from the incident;
   5) reporting the action to the appropriate authority;

c) audit trails and similar evidence should be collected (see 13.2.3) and secured, as appropriate, for:
   1) internal problem analysis;
   2) use as forensic evidence in relation to a potential breach of contract breach or regulatory requirement or in the event of civil or criminal proceedings, e.g. under computer misuse or data protection legislation;
   3) negotiating for compensation from software and service suppliers;

d) action to recover from security breaches and correct system failures should be carefully and formally controlled; the procedures should ensure that:
   1) only clearly identified and authorized personnel are allowed access to live systems and data (see also 6.2 for external access);
   2) all emergency actions taken are documented in detail;
   3) emergency action is reported to management and reviewed in an orderly manner;
   4) the integrity of business systems and controls is confirmed with minimal delay.

Auditoria: Pré-emissão (verificar se os procedimentos e mecanismos foram implementados) e Operacional.

5.7.2 Procedimentos em caso de comprometimento de recursos computacionais, software e/ou dados

The recovery procedures used if computing resources, software, and/or data are corrupted or suspected to be corrupted. These procedures describe how a secure environment is re-established, which certificates are revoked, whether the entity key is revoked, how the new entity public key is provided to the users, and how the subjects are re-certified.

Descrição: Especifica os procedimentos a ser seguidos em caso de comprometimento de recursos que suportam a operação da AC ou AR.

Requisitos mínimos: Descreve os procedimentos estabelecidos ou, em caso de informação sigilosa, apontar para um documento interna. Pelo menos o gerente da AC e AR deve ser ciente dos procedimentos respectivos.

Melhores práticas: Não estipulado.

Auditoria: Pré-emissão (verificar se os procedimentos e mecanismos foram implementados) e Operacional.

5.7.3 Procedimentos para o comprometimento de chave privada de entidade

The recovery procedures used if the entity key is compromised. These procedures describe how a secure environment is re-established, how the new entity public key is provided to the users, and how the subjects are re-certified.

Descrição: Especifica os procedimentos de recuperação a serem tomados no caso do comprometimento da chave privada da entidade.

Requisitos mínimos: Em caso de comprometimento da chave privada da entidade, a chave pública e certificado correspondente devem ser revogados imediatamente e as entidades confiantes notificadas. Em caso de comprometimento da chave privada da AC, o CG da ICPEDU e os titulares de certificados devem ser notificados imediatamente.

Melhores práticas: Ainda não definido.

Auditoria: Operacional.

5.7.4 Procedimentos para continuidade de negócio após desastre

The entity's capabilities to ensure business continuity following a natural or other disaster. Such capabilities may include the availability of a remote hot-site at which operations may be recovered. They may also include procedures for securing its facility during the period of time following a natural or other disaster and before a secure environment is re-established, either at the original site or at a remote site. For example, procedures to protect against theft of sensitive materials from an earthquake-damaged site.

Descrição: Especifica resumidamente os procedimentos definidos no plano de continuidade de negócios aplicáveis.

Requisitos mínimos: A instituição (que opera a AC) deve definir procedimentos e mecanismos que permitam a continuidade da operação após um desastre, retornando o serviço da AC a um estado estável e considerado seguro. Em geral, instituições consideram o plano confidencial; nesse caso, detalhes não devem parecer na PC/DPC, sendo suficiente uma referencia ao documento institucional apropriado.

Melhores práticas: Deve estar claro na PC/DPC que um plano existe (porém que não é divulgado publicamente). Por exemplo, deve ser possível restabelecer as operações da AC, usando os backups que guardados de forma segura em local diferente do ambiente que hospeda a AC. A instituição deve incluir a total recuperação do sistema como parte do seu plano de contingência. Os processos devem:

a) Identificar dos processos de negócio críticos;
b) Identificar os ativos envolvidos nos processos de negócio críticos;
c) Identificar o impacto causado pela indisponibilidade dos ativos no negócio;
d) Identificar e considerar a implementação de controles preventivos adicionais;
e) Garantir a segurança do pessoal e a proteção do ambiente de processamento de informações e da propriedade da instituição;
f) Formular e documentar planos de continuidade de negócio que estabeleçam requisitos de segurança da informação de acordo com a estratégia da instituição;
g) Testes e atualizações regulares, entre outros.

Outros elementos a serem considerados no momento da confecção do Plano de Continuidade de Negócios podem ser encontrados em [ISO17799].

Auditoria: Pré-emissão (verificar se os procedimentos e mecanismos foram implementados) e Operacional.

5.8 Finalização da AC ou AR

This subcomponent describes requirements relating to procedures for termination and termination notification of a CA or RA, including the identity of the custodian of CA and RA archival records.

Descrição: Descreve as providências tomadas quando houver finalização da AC ou uma de suas ARs.

Requisitos mínimos: Ao encerrar suas operações, a AC deverá:

a) Notificar o CG da ICPEDU
b) Notificar as ARs credenciadas;
c) Notificar titulares de certificados e entidades confiantes;
d) Notificar contatos de segurança relevantes;
e) Revogar todos os certificados validos emitidos;
f) Emitir e publicar pelo menos um LCR final válida até a data original de expiração do certificado da AC;
g) Destruir qualquer cópia das chaves privadas;
h) Arquivar os registros de forma segura, indicando o responsável pela sua custódia.

Melhores práticas: Uma notificação de finalização da AC deve ser enviada aos interessados pelo menos 1 (um) ano antes da total parada de suas operações. Durante esse período a AC não deverá emitir certificados, apenas LCRs. Essa prática permitirá os titulares possam permanecer utilizando seus certificados até a finalização efetiva da AC. Passado esse período, o certificado da AC deverá ser revogado e os interessados novamente notificados da terminação.

Os registros devem ser mantidos pela entidade responsável para futuras revisões e auditorias, por um período de 5 (cinco) anos.

Exemplo:

"No caso de extinção da AC Raiz, devem ser tomadas, no mínimo, as seguintes providências:

a) notificação de todas as entidades integrantes da ICPEDU;
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. Após este período, seu certificado deve ser revogado;
c) armazenamento dos dados da AC Raiz pelo período previsto nesta DPC".

Auditoria: Operacional.

6. Controles Técnicos de Segurança

A seção trata dos controles técnicos de segurança abordados pela ICP no que tange a criação do par de chaves, algoritmos criptográficos, tamanho e proteção das chaves, por exemplo.

This component is used to define the security measures taken by the issuing CA to protect its cryptographic keys and activation data (e.g., PINs, passwords, or manually-held key shares). This component may also be used to impose constraints on repositories, subject CAs, subscribers, and other participants to protect their private keys, activation data for their private keys, and critical security parameters. Secure key management is critical to ensure that all secret and private keys and activation data are protected and used only by authorized personnel.

This component also describes other technical security controls used by the issuing CA to perform securely the functions of key generation, user authentication, certificate registration, certificate revocation, auditing, and archiving. Technical controls include life-cycle security controls (including software development environment security, trusted software development methodology) and operational security controls.

This component can also be used to define other technical security controls on repositories, subject CAs, RAs, subscribers, and other participants.

6.1 Geração e Instalação do Par de Chaves

Key pair generation and installation need to be considered for the issuing CA, repositories, subject CAs, RAs, and subscribers.

6.1.1 Geração do par de chaves

Who generates the entity public, private key pair? Possibilities include the subscriber, RA, or CA. Also, how is the key generation performed? Is the key generation performed by hardware or software?

Descrição: Estabelece quem será responsável pela geração do par de chaves da entidade que solicita um certificado e como a atividade é realizada.

Requisitos mínimos: O par de chaves deve ser gerado pela entidade solicitante em um ambiente seguro, utilizando software e hardware apropriados. A AC deverá informar qual procedimento seria/foi utilizado para gerar o seu par de chaves, que deve ser feito apenas pelo gerente da AC. As ACs credenciadas devem gerar suas chaves em um módulo de hardware seguro (Hardware Security Module, HSM) aprovado pela ICPEDU.

Melhores práticas: A geração do par de chaves deve ocorrer sempre nos sistemas da entidade solicitante, de acordo com as melhores práticas de segurança. Antes da escolha do sistema gerador do par de chaves, devem ser considerados fatores como sua capacidade de gerar chaves de forma correta e aleatoriedade.

Auditoria: Pré-emissão (verificar os procedimentos) e Operacional.

6.1.2 Fornecimento de chave privada ao titular

How is the private key provided securely to the entity? Possibilities include a situation where the entity has generated it and therefore already has it, handing the entity the private key physically, mailing a token containing the private key securely, or delivering it in an SSL session.

Descrição: Estabelece os métodos utilizados para que a chave privada seja entregue de forma segura ao titular do certificado.

Requisitos mínimos: Não se aplica, uma vez que a chave privada do titular deve ser gerada pelo próprio em seu sistema.

Melhores práticas: Não estipulado.

6.1.3 Entrega da chave pública à Autoridade Certificadora

How is the entity's public key provided securely to the certification authority? Some possibilities are in an online SSL session or in a message signed by the RA.

Descrição: Estabelece os métodos utilizados para que a chave pública de um certificado seja entregue de forma segura à Autoridade Certificadora.

Requisitos mínimos: A chave pública deve ser entregue à AC pessoalmente, em uma mensagem assinada por uma de suas ARs credenciadas, ou através de uma transmissão segura após o processo de autenticação e identificação do titular.

Melhores práticas: As instituições devem estabelecer mecanismos seguros de entrega das chaves públicas apropriadas, que impeçam interceptação e modificação não autorizada. Uma conexão SSL, por exemplo, pode ser estabelecida entre a AC e a AR credenciada a fim de enviar a chave pública do titular através de uma conexão cifrada segura.

Auditoria: Operacional.

6.1.4 Divulgação da chave pública da AC às partes confiantes

In the case of issuing CAs, how is the CA's public key provided securely to potential relying parties? Possibilities include handing the public key to the relying party securely in person, physically mailing a copy securely to the relying party, or delivering it in a SSL session.

Descrição: Estabelece e descreve os métodos utilizados para que a chave pública da AC seja disponibilizada de forma segura para as entidades confiantes.

Requisitos mínimos: O certificado da AC deve ser publicado pelo menos:

a) No repositório público da AC;
b) No site da AC.

Informação suficiente deve ser disponibilizada para verificar a autenticidade do certificado publicado. O certificado da AC Raiz da ICPEDU deve ser publicado em um repositório confiável de certificados Raiz como, por exemplo, TACAR (TERENA Academic CA Repository).

Melhores práticas: Podem ser utilizadas diversas formas de distribuição da chave pública da AC. O certificado da AC contendo sua chave pública pode ser divulgado em um site que possibilite autenticação usando SSL, a fim de permitir que a entidade confiante verifique se está de fato tendo acesso ao certificado da AC requisitada, e não de um atacante. O certificado SSL do servidor deve ser de confiança do usuário, emitido preferencialmente por uma AC da ICPEDU. É de inteira responsabilidade do usuário confiar em um certificado emitido por uma AC que não faça parte da ICPEDU.

Auditoria: Operacional.

6.1.5 Tamanho das chaves

`What are the key sizes? Examples include a 1,024 bit RSA modulus and a 1,024 bit DSA large prime.`

Descrição: Estabelece o tamanho mínimo das chaves geradas.

Requisitos mínimos: O tamanho das chaves das AC deve ser no mínimo *RSA 2048-bit modulus* ou *ECC P256 modulus*. Ver [ICPEDU06]

Melhores práticas: Em geral, quanto maior a chave, mais forte será a criptografia ou assinatura digital resultante. Por outro lado, chaves maiores demoram mais tempo para serem geradas e podem ocorrer problemas de compatibilidade com os softwares existentes dada suas incapacidades de processar chaves de certos tamanhos.

Para certificados de duração muito longa, recomenda-se usar chaves grandes a fim de mantê-la mais resistente aos avanços tecnológicos da criptoanálise.

6.1.6 Geração dos parâmetros de chave pública e verificação de qualidade

`Who generates the public key parameters, and is the quality of the parameters checked during key generation?`

Descrição: Estabelece quem é responsável pela geração dos parâmetros da chave pública e os procedimentos de verificação de sua qualidade durante este processo.

Requisitos mínimos: Ver [ICPEDU06]

Melhores práticas: A qualidade dos parâmetros de geração das chaves afeta diretamente a segurança de uma ICP e, portanto, a geração de parâmetros incorretos pode por em risco sua confiabilidade. Padrões internacionais como FIPS 140 e FIPS 189 devem ser levados em consideração e a verificação de qualidade deve ser baseada nas necessidades de segurança da ICP. Controles de qualidade devem ser adequadamente documentados e periodicamente revisados.

Auditoria: Operacional.

6.1.7 Propósito de uso de chaves

For what purposes may the key be used, or for what purposes should usage of the key be restricted? For X.509 certificates, these purposes should map to the key usage flags in X.509 Version 3 certificates.

Descrição: Estabelece para que propósitos as chaves possam ser usadas ou são restritos.

Requisitos mínimos: A chave privada da AC só deve ser utilizada para assinar certificados e LCRs. Certificados de AR só devem ser utilizados para atividades requeridas ao trabalho de uma AR.

Melhores práticas: As chaves devem ser utilizadas conforme o conteúdo do campo *key usage*, caso esteja presente, e devem ser documentados.

Auditoria: Operacional.

6.2 Proteção de Chaves Privadas e Controles Tecnológicos de módulos Criptográficos

Requirements for private key protection and cryptographic modules need to be considered for the issuing CA, repositories, subject CAs, RAs, and subscribers.

6.2.1 Padrões e controles de módulos criptográficos

What standards, if any, are required for the cryptographic module used to generate the keys? A cryptographic module can be composed of hardware, software, firmware, or any combination of them. For example, are the keys certified by the infrastructure required to be generated using modules compliant with the US FIPS 140-1? If so, what is the required FIPS 140-1 level of the module? Are there any other engineering or other controls relating to a cryptographic module, such as the identification of the cryptographic module boundary, input/output, roles and services, finite state machine, physical security, software security, operating system security, algorithm compliance, electromagnetic compatibility, and self tests.

Descrição: Estabelece os padrões e controles requeridos para os módulos criptográficos.

Requisitos mínimos: Ver [ICPEDU06]

Melhores práticas: Alguns fatores devem ser considerados ao adquirir um módulo criptográfico:

- O módulo criptográfico deve operar de forma a não permitir observação externa de qualquer evento interno;
- O algoritmo criptográfico utilizado;
- A escolha das varáveis utilizadas no algoritmo criptográfico (tamanho das chaves, por exemplo);
- O módulo criptográfico deve ser protegido contra violações físicas e lojas, como trava de segurança a prova de arrombamentos, por exemplo;
- O módulo deve ter sido testado e aprovado em diversos testes de falha de ambiente (como flutuações de temperatura e voltagem fora dos padrões de operação);
- O módulo autentica usuários a cada importação, exportação e ativação de chaves;

Módulos criptográficos que atendem as exigências do padrão FIPS 140-2, nível 3 atendem as exigências citadas. Informações que existam fora do módulo criptográfico necessitam de proteção adicional.

6.2.2 Número de operadores para o Controle da Chave Privada

`Is the private key under n out of m multi-person control? If yes, provide n and m (two person control is a special case of n out of m, where n = m = 2)?`

Descrição: Estabelece o número mínimo de operadores para liberar a chave privada da AC. Esse tipo de abordagem reforça a segurança ao impor a necessidade de múltiplos operadores, requerendo um conjunto de *n* em um universo de *m* pessoas para liberar o acesso à chave privada.

Requisitos mínimos: Deve ser estipulado um número mínimo (*n*) e máximo (*m*) de operadores para o controle da chave privada da AC.

Melhores práticas: Esse tipo de controle possibilita reduzir o risco de mau uso da chave e acesso não autorizado, por tanto a escolha do número mínimo de operadores deve considerar os riscos de comprometimento da chave privada da AC. A política e os métodos de partilha do controle da chave privada devem ser explicitamente documentados para facilitar a operação da AC pelo pessoal responsável.

Auditoria: Pré-emissão (verificar se os procedimentos foram estabelecidos) e Operacional.

6.2.3 Custódia de chaves privadas

`Is the private key escrowed? If so, who is the escrow agent, what`

form is the key escrowed in (examples include plaintext, encrypted, split key), and what are the security controls on the escrow system?

Descrição: Estabelece quem é responsável pela custódia das chaves privadas como é feita e os controles de segurança envolvidos, se aplicável. Nesse tipo de abordagem, a chave privada é mantida sob custódia de um agente de custódia, permitindo que uma mensagem cifrada pela chave pública correspondente possa ser decifrada por uma terceira parte autorizada, sob circunstâncias especiais.

Requisitos mínimos: Não deve ser permitida a custódia de chave privada das entidades participantes da ICPEDU.

Melhores práticas: Apesar de possibilitar que um titular de certificado tenha acesso novamente a sua chave privada caso ela seja destruída de alguma forma, os riscos envolvendo a exposição da chave privada decorrentes de sua custódia por um agente de custódia devem ser fortemente considerados. Legislação local, a real necessidade de transferir a custódia da chave privada para um agente e a compatibilidade do software usado pelo usuário com o módulo deve ser verificada.

6.2.4 Cópias de segurança de chaves privadas

Is the private key backed up? If so, who is the backup agent, what form is the key backed up in (examples include plaintext, encrypted, split key), and what are the security controls on the backup system?

Descrição: Estabelece como e com qual freqüência é feita a cópia de segurança da chave privada da AC, AR e entidades finais, se aplicável.

Requisitos mínimos: A cópia da chave privada das AC deve ser registrada e mantida em um HSM de backup, guardado em um cofre/ambiente seguro. O processo de backup só deve ser feito mediante autorização formal do gerente da AC e ser supervisionado por participantes do grupo de administradores e auditores. Cópias de segurança para ARs e entidades finais devem ser consideradas conforme a necessidade da instituição.

Melhores práticas: A cópia de segurança da chave privada da AC ou AR permite que as operações de emissão e revogação de certificados/LCRs prossigam em caso de desastre. Manter uma cópia de segurança da chave privada da AC é vital para a continuidade do serviço, dado o alto risco ocasionado por sua corrupção, por exemplo. Os dados de ativação (como smartcards e senhas) do HSM de backup, a cópia da chave de backup e o próprio HSM de backup não devem ser guardadas no mesmo local.

Auditoria: Pré-emissão (verificar o ambiente e instalação de equipamento) e Operacional.

6.2.5 Arquivamento de chaves privadas

Is the private key archived? If so, who is the archival agent, what form is the key archived in (examples include plaintext, encrypted, split key), and what are the security controls on the archival system?

Descrição: Estabelece como é feito o arquivamento da cópia da chave privada, isto é, seu armazenamento por um período de tempo longo, se aplicável.

Requisitos mínimos: As cópias de segurança da chave privada devem ser mantidas cifradas e seu acesso deve ser controlado.

Melhores práticas: Um dos riscos associados ao armazenamento da chave privada da AC por um período de tempo muito longo reside no fato de que esta chave pode ser utilizada para assinar um documento mesmo após a troca de chaves da AC. Este seria considerado válido por softwares que não tivessem sido devidamente atualizados com a nova chave pública da AC. Portanto, o descarte dessa cópia deve constar nos procedimentos de descarte de mídia após uma troca de chaves. É recomendado que a cópia da chave privada de uma AC credenciada deve seja arquivada em um HSM.

Auditoria: Pré-emissão (verificar se tem a infraestrutura disponível) e Operacional.

6.2.6 Transferência de chaves privadas de/para módulos criptográficos

Under what circumstances, if any, can a private key be transferred into or from a cryptographic module? Who is permitted to perform such a transfer operation? In what form is the private key during the transfer (i.e., plaintext, encrypted, or split key)?

Descrição: Estabelece as circunstâncias nas quais a chave privada pode ser transferida de ou para um módulo criptográfico, e descreve os procedimentos envolvidos na tarefa.

Requisitos mínimos: A chave privada só deve ser transferida (recuperação ou cópia de segurança) do módulo criptográfico sob supervisão do administrador da AC com a finalidade de criar uma cópia de segurança e deve ser mantida cifrada durante o processo.

Melhores práticas: A transferência de chaves privadas de/para módulos criptográficos é uma atividade crítica, dado o risco de comprometimento decorrente da modificação, troca ou divulgação da chave privada. Deve ser escolhido um método de transferência que minimize esse risco. Caso o módulo criptográfico de destino esteja localizado nas dependências da AC, as seguintes medidas devem ser consideradas:

- uma lista de pessoas autorizadas a transportar a mídia deve ser estabelecida;

- a mídia deve ser guardada em um pacote que evite danos físicos durante o transporte, como exposição ao calor, umidade e campo eletromagnético;
- utilizar empacotamento que permita verificar qualquer tentativa de violação.

Auditoria: Operacional.

6.2.7 Armazenamento de chaves privadas em módulos criptográficos

How is the private key stored in the module (i.e., plaintext, encrypted, or split key)?

Descrição: Estabelece como as chaves privadas devem estar armazenadas nos módulos criptográficos.

Requisitos mínimos: A chave privada deve ser armazenada cifrada na memória permanente/não volátil do módulo criptográfico.

Melhores práticas: A chave privada deve ser armazenada cifrada na memória dos módulos criptográficos, e seu acesso deve ser controlado e registrado.

6.2.8 Método para ativação de chaves privadas

Who can activate (use) the private key? What actions must be performed to activate the private key (e.g., login, power on, supply PIN, insert token/key, automatic, etc.)? Once the key is activated, is the key active for an indefinite period, active for one time, or active for a defined time period?

Descrição: Estabelece quem pode ativar as chaves privadas, que ações devem ser tomadas para a ativação e o período em que a chave pode ficar ativa.

Requisitos mínimos: O método de ativação da chave privada da AC deve ser claramente definido. Para realizar a operação, deve ser necessária a autorização do grupo de operadores do hardware criptográfico.

Melhores práticas: O método para ativação da chave privada pode variar de acordo com o participante na ICP. Os operadores do HSM das ACs da ICPEDU devem, através de seus smartcards e senhas pessoais, liberar a chave privada da AC para 100 (cem) usos. Após o uso, a chave deve ser descarregada da memória. O número de vezes que a chave foi usada num procedimento deve ser explicado no relatório do cerimonial de execução do procedimento.

Auditoria: Pré-emissão (verificar se os procedimentos e mecanismos foram implementados) e Operacional.

6.2.9 Método para desativação de chaves privadas

Who can deactivate the private key and how? Examples of methods of deactivating private keys include logging out, turning the power off, removing the token/key, automatic deactivation, and time expiration.

Descrição: Estabelece quem pode e como desativar as chaves privadas e que ações devem ser tomadas para a desativação.

Requisitos mínimos: O método de desativação da chave privada da AC deve ser claramente definido.

Melhores práticas: O método escolhido para desativação da chave privada deve considerar estratégias que previnam tentativas de recuperação da chave após a utilização. Apagar ou sobrescrever a memória do dispositivo que abrigou a chave é uma das estratégias possíveis.

Quando o hardware criptográfico for desligado ou o número máximo de usos especificado na seção anterior for atingido, a chave privada deve ser automaticamente desativada.

6.2.10 Método para destruição de chaves privadas

Who can destroy the private key and how? Examples of methods of destroying private keys include token surrender, token destruction, and overwriting the key.

Descrição: Estabelece quem pode destruir as chaves privadas, que ações devem ser tomadas para efetuar a tarefa.

Requisitos mínimos: O dispositivo contendo a chave privada da AC Raiz deve ser destruído de forma segura e que impossibilite reutilização posterior. As demais ACs podem simplesmente apagar as chaves do HSM, ou seja, reiniciá-lo. A atividade deve ser registrada.

Melhores práticas: Se necessário, os dispositivos, incluindo qualquer HSM de backup, contendo chaves privadas devem ser destruídos por pessoal autorizado através de incineração ou trituração, por exemplo, e a atividade registrada. O método de destruição da chave privada escolhido deve considerar também fatores externos a ICP, como a legislação vigente e normas relacionadas.

Auditoria: Operacional.

6.2.11 Avaliação requerida de módulos criptográficos

Provide the capabilities of the cryptographic module in the following areas: identification of the cryptographic module boundary, input/output, roles and services, finite state machine, physical security, software security, operating system security, algorithm compliance, electromagnetic compatibility, and self tests. Capability may be expressed through reference to compliance with a standard such as U.S. FIPS 140-1, associated level, and rating.

Descrição: Provê características sobre módulos criptográficos a serem utilizados.

Requisitos mínimos: Vide [ICPEDU06].

Melhores práticas: A seção pode listar diversas características que devem ser consideradas na escolha de um módulo criptográfico. Deve ser considerada a utilização de uma fonte já consolidada a fim de validar a avaliação.

6.3 Outros Aspectos do Gerenciamento de Chaves

Other aspects of key management need to be considered for the issuing CA, repositories, subject CAs, RAs, subscribers, and other participants.

6.3.1 Armazenamento de chaves públicas

Is the public key archived? If so, who is the archival agent and what are the security controls on the archival system? Also, what software and hardware need to be preserved as part of the archive to permit use of the public key over time? Note: this subcomponent is not limited to requiring or describing the use of digital signatures with archival data, but rather can address integrity controls other than digital signatures when an archive requires tamper protection. Digital signatures do not provide tamper protection or protect the integrity of data; they merely verify data integrity. Moreover, the archival period may be greater than the cryptanalysis period for the public key needed to verify any digital signature applied to archival data.

Descrição: Estabelece se as chaves públicas dos participantes da ICP devem ou não ser arquivadas e que controles são utilizados para mantê-las seguras.

Requisitos mínimos: As chaves públicas da AC e todos os certificados emitidos por ela devem ser armazenados no formato PEM em mídia digital e/ou impressas em papel para pelo menos cinco anos depois da expiração do certificado.

Melhores práticas: O armazenamento da chave pública das entidades pode ser útil para verificar a assinatura digital em um documento após seu certificado ser removido do repositório da AC. Portanto, é necessário avaliar a necessidade de manter as chaves públicas dos participantes da ICP em mídia digital a fim de manter a propriedade de não-repúdio do serviço sempre disponível.

Auditoria: Operacional.

6.3.2 Períodos operacionais de certificados e períodos de utilização de pares de chaves

What is the operational period of the certificates issued to the

subscriber. What are the usage periods, or active lifetimes, for the subscriber's key pair?

Descrição: Estabelece os períodos operacionais dos certificados emitidos pela AC e os tempos de vida das par de chaves correspondentes.

Requisitos mínimos: A AC deve especificar os períodos de validade de seu certificado e dos demais certificados emitidos por ela. Certificados de entidades finais devem ter uma validade máxima de 1 a 3 anos. A chave privada da AC deverá ser utilizada apenas durante o período de validade do certificado correspondente. Certificados de ACs baseados em chaves de 2048-bit RSA modulus devem expirar antes de 2031.

Melhores práticas: Para entidades finais, o período de utilização do par de chaves deve ser o mesmo da validade do certificado. Para estes, recomenda-se um período de aproximadamente 1 (um) ano, dada a maior exposição da chave privada.

Um tempo razoável para certificados de ACs depende da função da AC solicitante. O mais longo o tempo de validade o maior seria o risco. Porem o mais curto o tempo de validade, maior seria o numero de renovações e então a necessidade de mais trabalho de gerencia. É uma questão de risco versus custo.

Entretanto, a chave pública da AC deverá estar disponível por tempo indeterminado, para verificação de assinaturas geradas durante o período de validade do certificado correspondente.

Auditoria: Operacional.

6.4 Dados de Ativação

Activation data refers to data values other than whole private keys that are required to operate private keys or cryptographic modules containing private keys, such as a PIN, passphrase, or portions of a private key used in a key-splitting scheme. Protection of activation data prevents unauthorized use of the private key, and potentially needs to be considered for the issuing CA, subject CAs, RAs, and subscribers. Such consideration potentially needs to address the entire life-cycle of the activation data from generation through archival and destruction. For each of the entity types (issuing CA, repository, subject CA, RA, subscriber, and other participants), all of the questions listed in 6.1 through 6.3 potentially need to be answered with respect to activation data rather than with respect to keys.

6.4.1 Geração e instalação dos dados de ativação

Descrição: Estabelece os dados de ativação usados para ativar as chaves privadas, bem como seus métodos de geração e instalação.

Requisitos mínimos: A AC deve fornecer o suporte necessário para geração e instalação dos dados de ativação da chave privada de seus titulares. Os dados

de ativação da chave privada da AC devem ser gerados durante sua cerimônia de criação.

Melhores práticas: A AC deve garantir que os dados de ativação são gerados em um ambiente seguro, e instalados no sistema de forma a minimizar o risco de exposição. Dependendo do nível de segurança no qual a chave deve ser mantida, o uso de mais de uma forma de autenticação é recomendado (ex.: smartcard).

Auditoria: Pré-emissão (verificar se os procedimentos e mecanismos foram implementados) e Operacional.

6.4.2 Proteção dos dados de ativação

Descrição: Estabelece os procedimentos para proteção dos dados de ativação das chaves privadas.

Requisitos mínimos: A AC deve estabelecer controles que permitam verificar se os dados de ativação foram gerados corretamente e que após a geração e a instalação eles não estão corrompidos. Os dados de ativação (smartcards e PINs) devem ser armazenados em envelopes lacrados e guardados no cofre da AC.

Melhores práticas: Não estipulado.

Auditoria: Pré-emissão (verificar se os procedimentos e mecanismos foram implementados) e Operacional.

6.4.3 Outros aspectos de dados de ativação

Descrição: Estabelece outros aspectos sobre os dados de ativação.

Requisitos mínimos: Não se aplica.

Melhores práticas: Não se aplica.

6.5 Controles de Segurança computacional

This subcomponent is used to describe computer security controls such as: use of the trusted computing base concept, discretionary access control, labels, mandatory access controls, object re-use, audit, identification and authentication, trusted path, security testing, and penetration testing. Product assurance may also be addressed.

A computer security rating for computer systems may be required. The rating could be based, for example, on the Trusted System Evaluation Criteria (TCSEC), Canadian Trusted Products Evaluation Criteria, European Information Technology Security Evaluation Criteria (ITSEC), or the Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408:1999. This subcomponent can also address requirements

for product evaluation analysis, testing, profiling, product certification, and/or product accreditation related activity undertaken.

6.5.1 Requisitos técnicos específicos de segurança computacional

Descrição: Estabelece controles sobre plataformas e aplicações específicas.

Requisitos mínimos: Ver [AGP07]. Só a equipe da AC deve ter acesso aos recursos da AC.

Melhores práticas: Diversas abordagens podem ser escolhidas para esta seção, podendo abranger desde todos os controles de segurança ou apenas apontar para outros documentos que os contenham. Essa escolha deve ser motivada pelas necessidades da AC e da instituição, de acordo com suas políticas de segurança.

Uma metodologia formal de gerenciamento de configuração deve ser utilizada para instalação e contínua manutenção do sistema de certificação da AC. Novas versões desse sistema somente serão instaladas após testes em ambiente de homologação apropriado.

Controles de acesso devem ser implementados nos sistemas que gerenciam o ciclo de vida dos certificados. Outros controles devem ser implementados para proteger o ambiente contra malware e para definir práticas de manipulação de mídia.

Auditoria: Pré-emissão (verificar se os procedimentos e mecanismos foram implementados) e Operacional.

6.5.2 Classificação de segurança computacional

Descrição: Estabelece índices de segurança independentes para avaliação de sistemas relacionados às operações da AC.

Requisitos mínimos: Não estipulado.

Melhores práticas: A classificação os sistemas de acordo com índices pré-determinados deve considerar o tipo de avaliação que será feita futuramente e a real necessidade da instituição de estabelecer esse tipo de controle, bem como a confiabilidade dos certificados. Certificados que não necessitam de alta confiabilidade, podem não valer o esforço de implementar esse tipo de índice, enquanto certificados cuja confiabilidade seja crítica podem ter sua segurança fortalecida ao impor a utilização de software endossado pela AC.

6.6 Controles técnicos de ciclo de vida

This subcomponent addresses system development controls and security management controls.

System development controls include development environment security, development personnel security, configuration management security during product maintenance, software engineering practices, software development methodology, modularity, layering, use of failsafe design and implementation techniques (e.g., defensive programming) and development facility security.

Security management controls include execution of tools and procedures to ensure that the operational systems and networks adhere to configured security. These tools and procedures include checking the integrity of the security software, firmware, and hardware to ensure their correct operation.

This subcomponent can also address life-cycle security ratings based, for example, on the Trusted Software Development Methodology (TSDM) level IV and V, independent life-cycle security controls audit, and the Software Engineering Institute's Capability Maturity Model (SEI-CMM).

6.6.1 Controles de desenvolvimento de sistemas

Descrição: Estabelece controles sobre o desenvolvimento dos sistemas utilizados para o gerenciamento do ciclo de vida dos certificados.

Requisitos mínimos: A AC deve utilizar um sistema de gerenciamento de certificados digitais e um módulo criptográfico elaborados sob uma metodologia de desenvolvimento reconhecida internacionalmente.

Melhores práticas: Os controles sobre o software utilizado na AC devem levar em conta fatores como a segurança no ambiente de desenvolvimento, do pessoal envolvido, técnicas de implementação e tolerância às falhas, gerência de configuração, metodologia utilizada entre outras práticas de engenharia de software.

Auditoria: Pré-emissão (verificar se os procedimentos e o funcionamento do sistema) e Operacional.

6.6.2 Controles do gerenciamento de segurança

Descrição: Estabelece controles usados para garantir que os sistemas estão operando corretamente e de forma consistente com a configuração desejada.

Requisitos mínimos: Deve ser identificado quem será responsável por verificar se os requisitos apresentados na seção 6.5.1 são atendidos.

Melhores práticas: A escolha dos controles de gerenciamento de segurança deve ser feita de acordo com o contexto da AC e da instituição.

Auditoria: Pré-emissão (identificação do responsável) e Operacional.

6.6.3 Controles de segurança de ciclo de vida

Descrição: Estabelece controles usados para garantir que os sistemas estão operando corretamente e de forma consistente com a configuração desejada.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

6.7 Controles para a Segurança da Rede de Comunicações

This subcomponent addresses network security related controls, including firewalls.

Descrição: Estabelece controles sobre a rede de comunicações, especialmente sobre aquelas usadas pela AC e AR.

Requisitos mínimos: A máquina hospedeira do sistema de gerenciamento da AC Raiz deve operar off-line, fisicamente desconectada de qualquer rede. As outras AC podem operar online. Em ambos as casos, o ambiente de rede que hospedar a AC deverá ser operado e controlado de acordo com todas as características de segurança consideradas boas práticas e estabelecidas na política de segurança da ICPEDU, a fim de manter segura toda informação em trânsito.

Melhores práticas: Proteger a rede que conecta os sistemas de suporte às atividades da AC, especialmente àquelas relacionadas ao serviço de certificação, é um processo crítico. Recomenda-se o estabelecimento controles de segurança na rede, tais como:

- Firewalls e outros controles que para proteger a integridade da rede de intrusões;
- Autenticação suficiente forte que permita estabelecer uma comunicação segura entre as entidades apropriadas, como ACs e ARs e mecanismos que garantam a integridade dos dados transmitidos;
- Controles de acesso contra uso não autorizado das informações;
- Mecanismos de previnam contra ameaças à disponibilidade do serviço, como ataques de negaça de serviço.

Os controles que a AC deseja impor aos participantes da ICP devem ser claramente documentados e expostos na PC/DPC e devem considerar também requisitos legais ou normativos.

Auditoria: Pré-emissão (verificar se os procedimentos e mecanismos foram implementados) e Operacional.

6.8 Carimbo do Tempo

This subcomponent addresses requirements or practices relating to the use of timestamps on various data. It may also discuss whether or not the time-stamping application must use a trusted time source.

Descrição: Estabelece os requisitos relacionados ao uso de carimbo do tempo. Carimbo. Carimbos do tempo são utilizados para determinar a existência de um objeto a partir de certo momento, sem que haja a possibilidade de seu dono retroceder a data do carimbo do tempo.

Requisitos mínimos: A data e hora dos eventos e dados dos sistemas computacionais on-line que precisarem ser datados deverão ser obtidas a partir de um relógio sincronizado pelo protocolo NTP a uma fonte de tempo confiável. Os relógios dos sistemas computacionais off-line e do módulo criptográfico deverão ser atualizados sempre que iniciados.

Melhores práticas: A precisão do relógio deve ser definida na PC/DPC e sua calibragem com a fonte de tempo deve ser regularmente verificada, a fim de manter a sincronia entre ambos. O relógio, bem como a fonte de tempo, deve ser mantido seguros contra ameaças (como choques elétricos e alteração por pessoal não autorizado) que alterem o relógio de forma que não possa ser detectada, comprometendo a manutenção da precisão imposta na PC/DPC.

Ajustes manuais no relógio devem ser registrados. Caso a fonte de tempo esteja fora da precisão determinada, então carimbos de tempo não devem ser emitidos.

Auditoria: Operacional.

7. Perfis dos Certificados, LCR e OCSP

A seção define o conteúdo e formato de certificados e LCRs, tratando de que campos estão presentes, como devem ser preenchidos e interpretados.

This component is used to specify the certificate format and, if CRLs and/or OCSP are used, the CRL and/or OCSP format. This includes information on profiles, versions, and extensions used.

7.1 Perfil dos Certificados

This subcomponent addresses such topics as the following (potentially by reference to a separate profile definition, such as the one defined in IETF PKIX RFC 3280):

7.1.1 Versão

Descrição: Define a versão dos certificados emitidos pela AC.

Requisitos mínimos: Todos os certificados emitidos pela AC deverão implementar a versão 3 de certificado definida no padrão X. 509, de acordo com o perfil estabelecido em [RFC5280].

Melhores práticas: Não estipulado.

Auditoria: Operacional.

7.1.2 Extensões

Descrição: Define as extensões utilizadas nos certificados emitidos pela AC.

Requisitos mínimos: Os certificados de autoridades certificadoras devem utilizar as seguintes extensões:

- A extensão *basicConstraints*, marcada como crítica e definida como “CA:TRUE”;
- A extensão *keyUsage*, marcada como crítica e definida apenas como *keyCertSign* e *crlSign*;
- A extensão *subjectKeyIdentifier,* definido com o *hash* da chave pública da AC solicitante, e gerado em conformidade com [ICPEDU06].
- A extensão *authorityKeyIdentifier,* definido com o *hash* da chave pública da AC emissora do certificado, e gerado em conformidade com [ICPEDU06].

Certificados para entidades finais devem utilizar as seguintes extensões:

- A extensão *basicConstraints*, definida como “CA:FALSE”;
- A extensão *keyUsage*, definida apenas alguma combinação de *digitalSignature*, *nonRepudiation*, *keyEncipherment* e *dataEncipherment* dependendo no uso pretendido do certificado;
- A extensão *subjectKeyIdentifier,* definido com o *hash* da chave pública do solicitante;

- A extensão *authorityKeyIdentifier,* definido com o *hash* da chave pública da AC emissora do certificado, e gerado em conformidade com [ICPEDU06].

Certificados para recursos de rede ou serviços devem utilizar as seguintes extensões:

- A extensão *basicConstraints*, definida como "CA:FALSE";
- A extensão *keyUsage*, definida apenas alguma combinação de *digitalSignature*, *keyEncipherment* e *dataEncipherment* dependendo no objetivo da emissão do certificado;
- A extensão *subjectKeyIdentifier,* definido com o *hash* da chave pública do recurso ou serviço.
- A extensão *authorityKeyIdentifier,* definido com o *hash* da chave pública da AC emissora do certificado, e gerado em conformidade com [ICPEDU06].

Em todos os certificados, a extensão *cRLDistributionPoints* deve ser presente e definida com, pelo menos, uma URL da LCR da AC emissor no formato binário (DER).

Os certificados de entidades finais devem utilizar extensão *certificatePolicies*, com o OID da PC sob a qual o certificado foi emitido.

Melhores práticas: As extensões *basicConstraints* e *keyUsage* citadas anteriormente devem ser marcadas como críticas (CRITICAL). Não é recomendada a utilização das extensões *certificatePolicies e extendedKeyUsage* em certificados de ACs.

Auditoria: Operacional.

7.1.3 Identificadores de objeto dos algoritmos

Descrição: Define os OIDs dos algoritmos criptográficos.

Requisitos mínimos: Neste item deve ser informado o OIDs dos algoritmos criptográficos. MD2, MD4 e MD5 não são mais aceitáveis.

Melhores práticas: Os OIDs dos algoritmos utilizados para definir certificados digitais são:

Função	Nome	OID
Função hash	Id-sha1	1.3.14.3.2.26
	Id-sha256	2.16.840.1.101.3.4.2.1
	Id-sha512	2.16.840.1.101.3.4.2.3
Criptografia	rsaEncryption	1.2.840.113549.1.1.1
Assinatura	sha1WithRSAEncryption	1.2.840.113549.1.1.5
	sha2WithRSAEncryption	1.2.840.113549.1.1.13

Tabela 1 OID dos algoritmos utilizados

Auditoria: Pré-emissão (verificar a configuração do sistema) e Operacional.

7.1.4 Formato dos nomes

Descrição: Define formato do *Distinguished Name* (DN) dos certificados emitidos pela AC.

Requisitos mínimos: Não são admitidos caracteres especiais ou de acentuação nos campos do DN. Todos os componentes do DN devem estar em conformidade com [RFC4630] e codificados como "*PrintableString*" de acordo com [RFC1778] e [RFC2252] ou, se "*UTF8String"* for usado para codificação, as componentes do DN não deve conter caracteres que não possam ser expressos em ASCII 7 bits, pois estes caracteres possuem representações inconsistentes.

As tabelas a seguir mostram os valores dos campos do DN.

Campo	Conteúdo	Mandatório
C	BR	Sim.
O	ICPEDU	Sim.
O	Nome da Instituição que opera a AC	Sim.
OU	Nome da unidade organizacional pertencente à Instituição que opera a AC	Sim.
L	Localidade	Não.
ST	Unidade de Federação	Não.
CN	Nome da AC ("AC + espaço + sigla da instituição ou serviço)".	Sim.

Tabela 2 Formato do DN para certificados de AC Institucional

Campo	Conteúdo	Mandatório
C	BR	Sim.
O	ICPEDU	Sim.
O	Nome da Instituição que responsável pela AR	Sim.
L	Localidade	Não.
ST	Unidade de Federação	Não.
CN	Nome da AR ("AR + espaço + sigla da instituição ou serviço)".	Sim.

Tabela 3 Formato do DN para certificados de AR

Melhores práticas: Não estipulado.

Auditoria: Operacional.

7.1.5 Restrições para nomes

Descrição: Define as restrições aplicáveis para nomes de titulares de certificados.

Requisitos mínimos: Não devem ser utilizados sinais de acentuação, tremas ou cedilhas. Além dos caracteres alfanuméricos e espaço em branco, poderão ser utilizados somente os símbolos:

Símbolo	Descrição	Código NBR9611 (hexadecimal)
	Espaço em branco	20
	! Ponto de exclamação	21
“	Aspas	22
#	Cerquila	23
$	Dólar	24
%	Percentual	25
&	E comercial	26
‘	Apóstrofo	27
(	Abre parênteses	28
)	Fecha parênteses	29
*	Asterisco	2A
+	Mais	2B
,	Vírgula	2C
-	menos	2D
.	Ponto	2E
/	Barra	2F
:	Dois pontos	3A
;	Ponto e vírgula	3B
=	Igual	3D
?	Ponto de interrogação	3F
@	Arroba	40
\	Barra invertida	5C

Tabela 4 Outros símbolos permitidos

Melhores práticas: Não estipulado.

Auditoria: Operacional.

7.1.6 Identificador de objeto da PC

Descrição: Apresenta o OID da PC que constará no certificado se a AC emite certificados para entidades finais.

Requisitos mínimos: Se apropriado, a seção deverá apresentar o(s) OID(s) da PC atual ou outras políticas que podem estar presente no certificado.

Melhores práticas: O texto pode apenas fazer referência a seção 1.2.

7.1.7 Uso da extensão *Policy Constraints*

Descrição: Define o uso da extensão *Policy Constraints* pela AC, e as limitações impostas por ela.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

7.1.8 Sintaxe e semântica dos qualificadores de política

Descrição: Define se a AC utiliza os qualificadores de política com a extensão *certificate policies* para transportar informações e define que informações são transportadas.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

7.1.9 Semântica de Processamento para a extensão crítica Certificate Policies

Descrição: Define se a AC marca como crítica a extensão *certificate policies* ou requer que uma AC subordinada o faça.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

7.2 Perfil da LCR

This subcomponent addresses such topics as the following (potentially by reference to a separate profile definition, such as the one defined in IETF PKIX RFC 3280).

7.2.1 Versão

Descrição: Define a versão de LCR emitida pela AC.

Requisitos mínimos: Todas as LCRs emitidas pela AC deverão implementar a versão 2 de listas de certificados revogados definida no padrão X.509, de

acordo com o perfil estabelecido em [RFC5280]. A LCR deve conter os seguintes campos:

- **Version:** v2
- **Signature Algorithm:** Conforme definido em [PadrõesCriptográficos]
- **Issuer:** DN da AC
- **thisUpdate:** Data de emissão da LCR
- **nextUpdate:** Data da emissão da próxima LCR
- **revokedCertificates:** Número de série e data de revogação de todos os certificados revogados (pelo menos que ainda não expiraram)

Melhores práticas: Não estipulado.

Auditoria: Operacional.

7.2.2 Extensões da LCR e de entradas da LCR

CRL and CRL entry extensions populated and their criticality.

Descrição: Descreve as extensões de LCR utilizadas e sua criticidade.

Requisitos mínimos: A LCR deve conter as extensões *AuthorityKeyIdentifier*, com o mesmo valor do *SubjectKeyIdentifier* da AC e marcada como crítico e cRLNumber, que contém um número seqüencial para cada LCR emitida.

Melhores práticas: Não estipulado.

Auditoria: Operacional.

7.3 Perfil da OCSP

This subcomponent addresses the following topics potentially by reference to a separate profile definition, such as the IETF RFC 2560 profile.

7.3.1 Versão

Descrição: Define a versão da OCSP disponível para verificar o status dos certificados.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

7.3.2 Extensões OCSP

Descrição: Define as extensões usadas pela OCSP.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

8. Auditoria de conformidade e outras avaliações

A seção das considerações envolvendo auditoria e outras avaliações periódicas dos participantes da ICP a fim de determinar se as entidades estão em conformidade com os controles impostos pela PC/DPC, PS e demais critérios determinados pelo CG da ICPEDU.

The list of topics covered by the assessment and/or the assessment methodology used to perform the assessment; examples include WebTrust for CAs and SAS 70.

8.1 Frequência ou circunstâncias das avaliações

Frequency of compliance audit or other assessment for each entity that must be assessed pursuant to a CP or CPS, or the circumstances that will trigger an assessment; possibilities include an annual audit, pre-operational assessment as a condition of allowing an entity to be operational, or investigation following a possible or actual compromise of security.

Descrição: Estabelece a freqüência das auditorias de conformidade ou outras avaliações, que podem ou não ser motivadas por alguma causa especial a ser relacionada na seção.

Requisitos mínimos: Os gerentes das ACs devem conduzir avaliações periódicas, com freqüência mínima de 1 (um) ano a fim de garantir que os procedimentos de segurança estão sendo corretamente seguidos e sua conformidade com os requisitos de segurança.

Melhores práticas: A freqüência das avaliações deve considerar fatores como a legislação vigente, normas internas da instituição e questões contratuais. Quando maior for o nível de confiança da AC, menor o período entre as avaliações, mas sempre levando em conta seu objetivo final.

Auditoria: Operacional.

8.2 Identidade e qualificações do avaliador

The identity and/or qualifications of the personnel performing the audit or other assessment.

Descrição: Estabelece quem pode conduzir as avaliações.

Requisitos mínimos: As avaliações devem ser conduzidas apenas por pessoal reconhecidamente qualificado e autorizado, ou sob sua supervisão. No caso de uma auditoria externa, os avaliadores serão indicados pelo Comitê Gestor da ICPEDU, respeitando critérios de qualificação tais como proficiência em infra-estruturas de chaves públicas, segurança de sistemas e da informação e experiência em processos de auditoria.

Melhores práticas: Se aplicável, as qualificações dos auditores selecionados deve considerar a legislação local e questões contratuais, e devem constar na PC/DPC ou outro documento relevante da AC. Os avaliadores devem possuir conhecimento e treinamento adequados em ferramentas e técnicas de análise de segurança de sistemas e da informação, infra-estruturas de chaves públicas.

Auditoria: Operacional.

8.3 Relação entre o avaliador e a entidade avaliada

The relationship between the assessor and the entity being assessed, including the degree of independence of the assessor.

Descrição: Estabelece a relação do avaliador com a entidade avaliada e sua autonomia.

Requisitos mínimos: Os avaliadores devem ser externos à estrutura administrativa e operacional da AC.

Melhores práticas: Permitir que os responsáveis pelas ACs e ARs avaliem seus próprios sistemas causaria um provável conflito de interesses, além de limitar a visão do avaliador apenas à deficiências previamente conhecidas. Por esses motivos, a contratação de um avaliador externo se torna necessária para elevar o nível de confiança das ACs credenciadas.

Auditoria: Operacional.

8.4 Tópicos cobertos na avaliação

Descrição: Estabelece os requisitos que serão avaliados.

Requisitos mínimos: A avaliação deverá abranger no mínimo a conformidade entre a PC/DPC, as políticas da ICPEDU e as operações da AC.

Melhores práticas: Auditorias e avaliações devem ser feitas utilizando critérios abrangendo os controles de gerenciamento do ambiente, das chaves e do ciclo de vida dos certificados da entidade avaliada. A relevância e eficácia dos controles devem ser avaliadas de acordo com as definições impostas na PC/DPC, na PS, e nas regras determinadas pela ICPEDU.

O processo de auditoria envolve, tipicamente, entrevistas com o gerente da AC ou AR e o pessoal envolvido na operação do serviço de gerenciamento de certificados, observação dos controles estabelecidos e procedimentos relacionados e revisão dos documentos de PC/DPC e PS. O escopo da avaliação deve ser condizente com os requisitos impostos pela AGP da ICPEDU e pela legislação vigente.

As avaliações devem ser cuidadosamente planejadas para que não afetem o serviço de certificação oferecido pela AC. As seguintes recomendações devem ser observadas:

a) As verificações devem ser limitadas a acesso apenas para leitura aos dados e software;
b) Outros acessos que não sejam apenas para leitura devem ser permitidos apenas em cópias isoladas dos arquivos do sistema, que devem ser apagados após o fim da auditoria ou passar pelo processo de proteção apropriado se houver obrigação de mantê-los para documentação;
c) Os recursos necessários para efetuar as avaliações devem ser explicitamente identificados e disponibilizados;
d) Todo acesso deve ser monitorado e registrado para produzir uma trilha referência;
e) Todos os procedimentos, requisitos e responsabilidades devem ser documentados.

Outras recomendações podem ser encontradas em [ISO17799].

Auditoria: Operacional.

8.5 Ações tomadas resultantes de deficiências

Actions taken as a result of deficiencies found during the assessment; examples include a temporary suspension of operations until deficiencies are corrected, revocation of certificates issued to the assessed entity, changes in personnel, triggering special investigations or more frequent subsequent compliance assessments, and claims for damages against the assessed entity.

Descrição: Estabelece as ações tomadas quando alguma não-conformidade é encontrada após uma avaliação.

Requisitos mínimos: O gerente da AC deverá estabelecer e manter um plano de ação para corrigir qualquer não-conformidade encontrada durante as avaliações e encaminhar um relatório para o CG da ICPEDU descrevendo as medidas tomadas.

Melhores práticas: Os gerentes da AC devem, ao encontrar uma não-conformidade [ISO17799]:

a) determinar as causas da não-conformidade;
b) avaliar a necessidade de medidas para garantir que a não-conformidade não ocorrerá novamente;
c) determinar e implementar as medidas corretivas apropriadas;
d) revisar as medidas corretivas tomadas.

As medidas tomadas devem considerar os custos envolvidos no processo e, por esse motivo, não é recomendada a tomada de medidas extremas, como encerramento das atividades, por exemplo. As ações apropriadas devem levar em conta a cultura da instituição que administra a AC e o nível de confiança da AC.

As atualizações no plano de ação devem ser freqüentes e baseadas nas descobertas de avaliações nos controles de segurança, análises de impacto na segurança e monitoramento contínuo das atividades [NIST80053].

Auditoria: Operacional.

8.6 Comunicação dos resultados

Who is entitled to see results of an assessment (e.g., assessed entity, other participants, the general public), who provides them (e.g., the assessor or the assessed entity), and how they are communicated.

Descrição: Estabelece quem terá acesso aos resultados das avaliações, e como serão divulgados.

Requisitos mínimos: O gerente da AC deverá encaminhar os resultados de avaliações e um relatório com medidas tomadas para corrigir as não-conformidades encontradas para o CG da ICPEDU.

Melhores práticas: Os gerentes de ACs são incentivados a divulgar publicamente partes do relatório que não comprometam a segurança do serviço de certificação, a fim de declarar publicamente seu nível de confiança. Os resultados comunicados devem estar em conformidade com a lei aplicável e os requisitos impostos pelo CG da ICPEDU.

Em caso de auditoria interna (isto é, comandada pela própria AC), o gerente da AC deverá fornecer ao avaliador externo uma cópia do relatório final.

Auditoria: Operacional.

.

9. Aspectos Legais e Assuntos Gerais

A seção aborda assuntos diversos relacionados a provisões legais, taxas a serem cobradas pelos serviços oferecidos. O foco está nos aspectos legais e do negócio, portanto menos técnico que as demais seções.

This component covers general business and legal matters. Sections 9.1 and 9.2 of the framework discuss the business issues of fees to be charged for various services and the financial responsibility of participants to maintain resources for ongoing operations and for paying judgments or settlements in response to claims asserted against them. The remaining sections are generally concerned with legal topics.

Starting with Section 9.3 of the framework, the ordering of topics is the same as or similar to the ordering of topics in a typical software licensing agreement or other technology agreement. Consequently, this framework may not only be used for CPs and CPSs, but also associated PKI-related agreements, especially subscriber agreements, and relying party agreements. This ordering is intended help lawyers review CPs, CPSs, and other documents adhering to this framework.

With respect to many of the legal subcomponents within this component, a CP or CPS drafter may choose to include in the document terms and conditions that apply directly to subscribers or relying parties. For instance, a CP or CPS may set forth limitations of liability that apply to subscribers and relying parties. The inclusion of terms and conditions is likely to be appropriate where the CP or CPS is itself a contract or part of a contract.

In other cases, however, the CP or CPS is not a contract or part of a contract; instead, it is configured so that its terms and conditions are applied to the parties by separate documents, which may include associated agreements, such as subscriber or relying party agreements. In that event, a CP drafter may write a CP so as to require that certain legal terms and conditions appear (or not appear) in such associated agreements. For example, a CP might include a subcomponent stating that a certain limitation of liability term must appear in a CA's subscriber and relying party agreements. Another example is a CP that contains a subcomponent prohibiting the use of a subscriber or relying party agreement containing a limitation upon CA liability inconsistent with the provisions of the CP. A CPS drafter may use legal subcomponents to disclose that certain terms and conditions appear in associated subscriber, relying party, or other agreements in use by the CA. A CPS might explain, for instance, that the CA writing it uses an associated subscriber or relying party agreement that applies a particular provision for limiting liability.

9.1 Taxas

This subcomponent contains any applicable provisions regarding fees charged by CAs, repositories, or RAs.

9.1.1 Taxas de emissão e renovação de certificados

Descrição: Estabelece uma taxa pela prestação dos serviços de emissão e renovação de certificados.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

9.1.2 Taxas para acesso aos certificados

Descrição: Estabelece uma taxa para utilização dos certificados pelas entidades confiantes.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

9.1.3 Taxas revogação ou informações de estado

Descrição: Estabelece uma taxa pela prestação dos serviços de revogação ou informação de estados dos certificados.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

9.1.4 Outras taxas

Fees for other services such as providing access to the relevant CP or CPS.

Descrição: Estabelece uma taxa pela prestação de serviços não definidos anteriormente.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

9.1.5 Política de reembolso

Descrição: Estabelece uma política de reembolso das taxas pagas pela prestação de serviços.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

9.2 Responsabilidade Financeira

This subcomponent contains requirements or disclosures relating to the resources available to CAs, RAs, and other participants providing certification services to support performance of their operational PKI responsibilities, and to remain solvent and pay damages in the event they are liable to pay a judgment or settlement in connection with a claim arising out of such operations.

Descrição: Estabelece responsabilidades e/ou requisitos relacionados ao suporte financeiro do serviço de certificação digital (operações da AC e da AR, serviços de repositório, etc.) e no caso de ações indevidas que resultem em algum tipo de dado.

Requisitos mínimos: Não estipulado.

Melhores práticas: Nenhuma responsabilidade financeira é assumida, seja no que diz respeito ao serviço de certificação digital ou a má utilização dos certificados emitidos sob a PC em questão.

9.2.1 Cobertura de Seguro

A statement that the participant maintains a certain amount of insurance coverage for its liabilities to other participants.

Descrição: Estabelece a cobertura de seguro de um participante sobre os riscos de suas responsabilidades.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

9.2.2 Outros ativos

A statement that a participant has access to other resources to support operations and pay damages for potential liability, which may be couched in terms of a minimum level of assets necessary to operate and cover contingencies that might occur within a PKI, where examples include assets on the balance sheet of an organization, a surety bond, a letter of credit, and a right under an agreement to an indemnity under certain circumstances.

Descrição: Estabelece outros ativos nos quais o participante tem acesso para suportar as operações de ICP e arca com as despesas causadas por danos de sua responsabilidade.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

9.2.3 Cobertura de Seguro ou garantia para entidades finais

A statement that a participant has a program that offers first-party insurance or warranty protection to other participants in connection with their use of the PKI.

Descrição: Estabelece a cobertura de seguro de terceiros envolvidos na participação de uma entidade na ICP.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

9.3 Informações confidenciais

This subcomponent contains provisions relating to the treatment of confidential business information that participants may communicate to each other, such as business plans, sales information, trade secrets, and information received from a third party under a nondisclosure agreement.

9.3.1 Escopo de informações confidenciais

The scope of what is considered confidential information.

Descrição: Define que informações são consideradas confidenciais

Requisitos mínimos: No mínimo, as seguintes informações devem ser consideradas confidenciais:

a) informações relativas a solicitações de certificados;
b) registros de trilhas de auditoria;
c) relatórios de auditoria;
d) planos de contingência e planos de recuperação de desastre; e
e) medidas de segurança relativas:
    I. à operação de hardware e software da ICPEDU; e
    II. aos serviços de certificação.

Melhores práticas: As informações citadas anteriormente são consideradas privadas e devem ser estabelecidos controles de segurança apropriados para guardá-las e protegê-las de acesso não autorizado.

9.3.2 Informações fora do escopo de informações confidenciais

The types of information that are considered to be outside the scope of confidential information.

Descrição: Define que informações não são consideradas confidenciais.

Requisitos mínimos: São consideradas informações não confidenciais:

a) certificados das ACs;
b) lista de certificados revogados; e
c) versões publicas de PCs, DPCs e Políticas de Segurança (PS).

Melhores práticas: Não estipulado.

9.3.3 Responsabilidade de proteção de informações confidenciais

The responsibilities of participants that receive confidential information to secure it from compromise, and refrain from using it or disclosing it to third parties.

Descrição: Define responsáveis pela guarda e proteção de informações consideradas confidenciais.

Requisitos mínimos: A AC deve proteger contra acesso não autorizado as informações classificadas como confidenciais.

Melhores práticas: Não estipulado.

Auditoria: Pré-emissão (verificar se os procedimentos e mecanismos foram implementados) e Operacional.

9.4 Privacidade das Informações Pessoais

This subcomponent relates to the protection that participants, particularly CAs, RAs, and repositories, may be required to afford to personally identifiable private information of certificate applicants, subscribers, and other participants. Specifically, this subcomponent addresses the following, to the extent pertinent under applicable law.

9.4.1 Plano de Privacidade

`The designation and disclosure of the applicable privacy plan that applies to a participant's activities, if required by applicable law or policy.`

Descrição: Define o plano de privacidade aplicável às atividades dos participantes.

Requisitos mínimos: Não estipulado.

Melhores práticas: Caso a AC opte por - ou necessite - criar e adotar um plano de privacidade, esta deve observar a legislação apropriada, regulamento interno da instituição ou contratos, buscando estar conforme com quaisquer requisitos legais e contratuais. A AC pode também considerar padrões internacionais, a fim de atender a expectativa dos titulares em relação à confiabilidade dos certificados.

9.4.2 Informação tratada como privada

`Information that is considered private within the PKI.`

Descrição: Define que informações são tratadas como privadas.

Requisitos mínimos: No mínimo, toda informação provida pelo titular de certificado para verificar sua identidade deve ser tratada como privada, com exceção da informação presente no certificado, e deve ser mantida com o mesmo nível de segurança de qualquer informação confidencial.
.
Melhores práticas: A AC deve estabelecer um plano de privacidade baseado na legislação institucional ou local vigente, nos padrões de segurança atualmente disponíveis ou qualquer outro requisito contratual. O comprometimento de informações privadas pode causar danos à imagem da instituição que administra a AC e prejuízos financeiros ocasionados por ações judiciais.

Auditoria: Pré-emissão (verificar se os procedimentos e mecanismos foram implementados) e Operacional.

9.4.3 Informação não considerada privada

`Information that is not considered private within the PKI.`

Descrição: Define que informações não são tratadas como privadas.

Requisitos mínimos: Qualquer informação que componha o certificado, LCRs ou cuja divulgação seja previamente autorizada pelo proprietário não é considerada privada.

Melhores práticas: Mesmo em informações não consideradas privadas devem ser aplicados controles de segurança suficientes para manter sua integridade.

9.4.4 Responsabilidade de proteção de informação privada

Any responsibility of participants that receive private information to secure it, and refrain from using it and from disclosing it to third parties.

Descrição: Estabelece a responsabilidade pela proteção de informações que são tratadas como privadas.

Requisitos mínimos: A AC é responsável pela proteção de qualquer informação considerada privada.

Melhores práticas: Vide 9.4.2.

9.4.5 Aviso e consentimento para o uso de informação privada

Any requirements as to notices to, or consent from individuals regarding use or disclosure of private information.

Descrição: Estabelece os requisitos para determinar o consentimento do uso de uma informação privada por parte do dono.

Requisitos mínimos: O usuário deve consentir formalmente, por escrito, antes a utilização e/ou divulgação de qualquer informação considerada como privada.

Melhores práticas: Ainda não definido.

9.4.6 Circunstâncias para revelação de informações confidenciais em processos judiciais e administrativos

Any circumstances under which a participant is entitled or required to disclose private information pursuant to judicial, administrative process in a private or governmental proceeding, or in any legal proceeding.

Descrição: Define as circunstâncias nas quais é requerida ao participante a divulgação de informações consideradas privadas para atender processos administrativos.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

9.4.7 Outras Circunstâncias para revelação de informações

Descrição: Define outras circunstâncias nas quais é requerida ao participante a divulgação de informações consideradas privadas.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

9.5 Direitos de Propriedade Intelectual

This subcomponent addresses the intellectual property rights, such as copyright, patent, trademarks, or trade secrets, that certain participants may have or claim in a CP, CPS, certificates, names, and keys, or are the subject of a license to or from participants.

Descrição: Estabelece os direitos de propriedade intelectual sobre vários aspectos, como certificados, PCs, DPCs, nomes, bancos de dados, entre outros.

Requisitos mínimos: Não estipulado.

Melhores práticas: Sugere-se à AC adotar um sistema de gestão de licenças para gestão compartilhada de informações, como o Creative Commons. Neste é possível escolher que condições se aplicam aos objetos, permitindo desde a distribuição apenas para uso não comercial, distribuição desde que o autor seja notificado, até uma combinação destes.

9.6 Representações e Garantias

This subcomponent can include representations and warranties of various entities that are being made pursuant to the CP or CPS. For example, a CPS that serves as a contract might contain a CA's warranty that information contained in the certificate is accurate. Alternatively, a CPS might contain a less extensive warranty to the effect that the information in the certificate is true to the best of the CA's knowledge after performing certain identity authentication procedures with due diligence. This subcomponent can also include requirements that representations and warranties appear in certain agreements, such as subscriber or relying party agreements. For instance, a CP may contain a requirement that all CAs utilize a subscriber agreement, and that a subscriber agreement must contain a warranty by the CA that information in the certificate is accurate. Participants that may make representations and warranties include CAs, RAs, subscribers, relying parties, and other participants.

9.6.1 Garantias de AC

Descrição: Estabelece as garantias oferecidas pela AC na prestação do serviço de certificação.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

9.6.2 Garantias de AR

Descrição: Estabelece as garantias oferecidas pela AR na prestação do serviço de autenticação.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

9.6.3 Garantias de titulares de certificado

Descrição: Estabelece as garantias oferecidas pelos titulares na utilização de certificados.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

9.6.4 Garantias de entidades confiantes

Descrição: Estabelece as garantias oferecidas pelas entidades confiantes na utilização de certificados.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

9.6.5 Garantias de outros participantes

Descrição: Estabelece as garantias oferecidas por outros participantes da ICP.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

9.7 Renúncia das Garantias

This subcomponent can include disclaimers of express warranties that may otherwise be deemed to exist in an agreement, and disclaimers of implied warranties that may otherwise be imposed by applicable law, such as warranties of merchantability or fitness for a particular purpose. The CP or CPS may directly impose such disclaimers, or the CP or CPS may contain a requirement that disclaimers appear in associated agreements, such as subscriber or relying party agreements.

Descrição: O conteúdo é composto por renúncias de garantias que possam existir no documento ou impostar pela lei aplicável, por exemplo.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

9.8 Limitações das Responsabilidades

This subcomponent can include limitations of liability in a CP or CPS or limitations that appear or must appear in an agreement associated with the CP or CPS, such as a subscriber or relying party agreement. These limitations may fall into one of two categories: limitations on the elements of damages recoverable and limitations on the amount of damages recoverable, also known as liability caps. Often, contracts contain clauses preventing the recovery of elements of damages such as incidental and consequential damages, and sometimes punitive damages. Frequently, contracts contain clauses that limit the possible recovery of one party or the other to an amount certain or to an amount corresponding to a benchmark, such as the amount a vendor was paid under the contract.

Descrição: Descreve limitações de responsabilidades atreladas aos acordos de aceitação por parte dos usuários e entidades confiantes, por exemplo.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

9.9 Indenização

This subcomponent includes provisions by which one party makes a second party whole for losses or damage incurred by the second party, typically arising out of the first party's conduct. They may appear in a CP, CPS, or agreement. For example, a CP may require that subscriber agreements contain a term under which a subscriber is responsible for indemnifying a CA for losses the CA sustains arising out of a subscriber's fraudulent misrepresentations on the certificate application under which the CA issued the subscriber an inaccurate certificate. Similarly, a CPS may say that a CA uses a relying party agreement, under which relying parties are responsible for indemnifying a CA for losses the CA sustains arising out of use of a certificate without properly checking revocation information or use of a certificate for purposes beyond what the CA permits.

Descrição: Estabelece indenizações decorrentes de conduta de uma entidade que cause dano à outra.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

9.10 Finalização

This subcomponent can include the time period in which a CP or a CPS remains in force and the circumstances under which the document, portions of the document, or its applicability to a particular participant can be terminated. In addition or alternatively, the CP or CPS may include requirements that certain term and termination clauses appear in agreements, such as subscriber or relying party agreements.

9.10.1 Prazo de validade

The term of a document or agreement, that is, when the document becomes effective and when it expires if it is not terminated earlier.

Descrição: Estabelece o período de validade das provisões do documento.

Requisitos mínimos: Os documentos de PC e DPC passam a ter validade a partir de sua publicação, que só pode ocorrer após a sua aprovação pelo CG da ICPEDU, sem data de expiração.

Melhores práticas: As ACs devem revisar constantemente as provisões de suas PCs e DPCs, para que estejam de acordo com os requisitos operacionais da ICPEDU e de qualquer outra legislação vigente. Estas revisões devem acontecer quando é publicada uma nova versão dos Requisitos Mínimos da ICPEDU (isto é uma nova versão deste documento) ou num período máximo de 1 (um) ano, o que estabeleceria este período com um prazo de validade razoável para os documentos.

9.10.2 Finalização

Termination provisions stating circumstances under which the document, certain portions of it, or its application to a particular participant ceases to remain in effect.

Descrição: Estabelece o prazo em que o documento ou parte dele deixa de ter efeito.

Requisitos mínimos: As provisões de PCs e DPCs são válidas até que uma nova versão seja publicada ou que sejam revogadas por determinação explícita da AC imediatamente superior ou do Comitê Gestor da ICPEDU.

Melhores práticas: Não estipulado.

9.10.3 Efeitos de finalização e provisões remanescentes

Any consequences of termination of the document. For example, certain provisions of an agreement may survive its termination and remain in force. Examples include acknowledgements of intellectual property rights and confidentiality provisions. Also, termination may trigger a responsibility of parties to return confidential information to the party that disclosed it.

Descrição: Descreve as conseqüências da terminação de validade do documento.

Requisitos mínimos: Não estipulado.

Melhores práticas: O texto deve permanecer por um tempo mínimo de 1 (um) ano após o último certificado assinado sob o mesmo expirar ou ser revogado.

9.11 Notificações Individuais e Comunicações com Participantes

This subcomponent discusses the way in which one participant can or must communicate with another participant on a one-to-one basis in order for such communications to be legally effective. For example, an RA may wish to inform the CA that it wishes to terminate its agreement with the CA. This subcomponent is different from publication and repository functions, because unlike individual communications described in this subcomponent, publication and posting to a repository are for the purpose of communicating to a wide audience of recipients, such as all relying parties. This subcomponent may establish mechanisms for communication and indicate the contact information to be used to route such communications, such as digitally signed e-mail notices to a specified address, followed by a signed e-mail acknowledgement of receipt.

Descrição: Estabelece a forma de comunicação entre os participantes para que seja legalmente efetiva.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

9.12 Emendas

It will occasionally be necessary to amend a CP or CPS. Some of these changes will not materially reduce the assurance that a CP or its implementation provides, and will be judged by the policy administrator to have an insignificant effect on the acceptability of certificates. Such changes to a CP or CPS need not require a change in the CP OID or the CPS pointer (URL). On the other hand, some changes to a specification will materially change the acceptability of certificates for specific purposes, and these changes may require corresponding changes to the CP OID or CPS pointer qualifier (URL).

9.12.1 Procedimento para emendas

The procedures by which the CP or CPS and/or other documents must, may be, or are amended.

Descrição: Estabelece os procedimentos tomados quando necessárias emendas nos documentos.

Requisitos mínimos: Emendas (isto é, alterações nas políticas e práticas que causem algum impacto nas operações e na confiança da AC) nos documentos de PC e DPC devem ser encaminhadas ao Comitê Gestor da ICPEDU para aprovação antes de sua publicação. Alterações menores, como correções meramente ortográficas, não são consideradas emendas.

Melhores práticas: Registros das alterações devem ser mantidos no próprio documento para facilitar o acompanhamento do mesmo. As alterações também devem ser sinalizadas de forma a direcionar os usuários para prováveis mudanças.

9.12.2 Período e mecanismo de notificação

In the case of CP or CPS amendments, change procedures may include a notification mechanism to provide notice of proposed amendments to affected parties, such as subscribers and relying parties, a comment period, a mechanism by which comments are received, reviewed and incorporated into the document, and a mechanism by which amendments become final and effective.

Descrição: Estabelece os mecanismos utilizados para notificar os interessados caso haja emendas no documento.

Requisitos mínimos: O surgimento de novas versões dos documentos de PC e DPC devem ser devidamente noticiados no repositório da AC.

Melhores práticas: A AC pode divulgar os documentos (ou trechos relevantes) de PC e DPC para comentários públicos previamente a sua aprovação.

9.12.3 Circunstâncias nas quais o identificador de objeto deve ser modificado

The circumstances under which amendments to the CP or CPS would require a change in CP OID or CPS pointer (URL).

Descrição: Circunstâncias nas quais as emendas acarretam na mudança do identificador de objeto do documento.

Requisitos mínimos: Sempre que surgirem novas versões o identificador de objeto deve ser modificado.

Melhores práticas: Não estipulado.

Auditoria: Operacional.

9.13 Procedimentos para Resolução de Disputas

This subcomponent discusses procedures utilized to resolve disputes arising out of the CP, CPS, and/or agreements. Examples of such procedures include requirements that disputes be resolved in a certain forum or by alternative dispute resolution mechanisms.

Descrição: Determina os procedimentos utilizados para resolver disputas envolvendo as provisões dos documentos da ICP.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

9.14 Leis Governamentais

This subcomponent sets forth a statement that the law of a certain jurisdiction governs the interpretation and enforcement of the subject CP or CPS or agreements.

Descrição: Estabelece que as atividades da AC devam estar conformes com a legislação vigente no país.

Requisitos mínimos: A AC deve respeitar a legislação vigente no país.

Melhores práticas: Não estipulado.

9.15 Conformidade com as leis aplicáveis

This subcomponent relates to stated requirements that participants comply with applicable law, for example, laws relating to cryptographic hardware and software that may be subject to the export control laws of a given jurisdiction. The CP or CPS could purport to impose such requirements or may require that such provisions appear in other agreements.

Descrição: Estabelece provisões para garantir a conformidade das atividades da AC com a legislação vigente no país.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

9.16 Provisões Diversas

This subcomponent contains miscellaneous provisions, sometimes called "boilerplate provisions," in contracts. The clauses covered in this subcomponent may appear in a CP, CPS, or agreements.

9.16.1 Concordância completa

An entire agreement clause, which typically identifies the document or documents comprising the entire agreement between the parties and states that such agreements supersede all prior and contemporaneous written or oral understandings relating to the same subject matter.

Descrição: Estabelece a concordância completa entre as partes cobertas no documento.

Requisitos mínimos: Não estipulado.

Melhores práticas: Nesta provisão, a AC deve determinar que os documentos de PC e DPC sobreponham qualquer acordo prévio entre as partes.

9.16.2 Delegação de direitos e obrigações

An assignment clause, which may act to limit the ability of a party in

an agreement, assigning its rights under the agreement to another party (such as the right to receive a stream of payments in the future) or limiting the ability of a party to delegate its obligations under the agreement.

Descrição: Estabelece os limites de delegação de direitos e obrigações das entidades participantes.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

9.16.3 Acordo entre as partes em caso de revogação de cláusula pela justiça

A severability clause, which sets forth the intentions of the parties in the event that a court or other tribunal determines that a clause within an agreement is, for some reason, invalid or unenforceable, and whose purpose is frequently to prevent the unenforceability of one clause from causing the whole agreement to be unenforceable.

Descrição: Estabelece um acordo entre as partes definindo que a revogação de uma cláusula não afete a validade de todo documento.

Requisitos mínimos: Não estipulado.

Melhores práticas: A PC ou DPC deve determinar que, caso uma cláusula do documento se torne inválida por conflitar com a legislação vigente ou for invalidada por um tribunal, esta cláusula será revogada e substituída por outro conforme com as disposições legais sem, no entanto, invalidar todo o documento.

9.16.4 Responsabilidades relacionadas a encargos jurídicos

An enforcement clause, which may state that a party prevailing in any dispute arising out of an agreement is entitled to attorneys' fees as part of its recovery, or may state that a party's waiver of one breach of contract does not constitute a continuing waiver or a future waiver of other breaches of contract.

Descrição: Estabelece quem será responsável por arcar com as despesas relacionadas aos encargos jurídicos.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

9.16.5 Força maior

9.16.5 Força Maior

A force majeure clause, commonly used to excuse the performance of one

or more parties to an agreement due to an event outside the reasonable control of the affected party or parties. Typically, the duration of the excused performance is commensurate with the duration of the delay caused by the event. The clause may also provide for the termination of the agreement under specified circumstances and conditions. Events considered to constitute a "force majeure" may include so-called "Acts of God," wars, terrorism, strikes, natural disasters, failures of suppliers or vendors to perform, or failures of the Internet or other infrastructure. Force majeure clauses should be drafted so as to be consistent with other portions of the framework and applicable service level agreements. For instance, responsibilities and capabilities for business continuity and disaster recovery may place some events within the reasonable control of the parties, such as an obligation to maintain backup electrical power in the face of power outages.

Descrição: Estabelece como serão tratados eventos fora do controle da AC.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

9.17 Outras Provisões

This subcomponent is a "catchall" location where additional responsibilities and terms can be imposed on PKI participants that do not neatly fit within one of the other components or subcomponents of the framework. CP and CPS writers can place any provision within this subcomponent that is not covered by another subcomponent.

Descrição: Estabelece termos e responsabilidades gerais que não se enquadrem em nenhuma das seções anteriores.

Requisitos mínimos: Não estipulado.

Melhores práticas: Não estipulado.

10. Prolog

Descrição: Incluir seções relevantes como referencias, e anexos referenciados no texto.

Requisitos mínimos: Deveria ter uma seção que indica quais seções foram modificadas em relação à versão anterior do documento.

Melhores práticas: Não estipulado.

Referências

[COBIT] IT Governance Institute*, Control Objectives for Information and related Technology*, CobIT 4.1, 2007.

[FIPS1402] National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules*, FIPS 140-2, Março 2001 http://.

[ICPEDU06] Comitê Técnico de Políticas da ICPEDU, *Padrões e Algoritmos Criptográficos da ICPEDU,* 2005.

[ISO17799] Joint Technical Comitee ISO/IEC JTC 1, *Information technology*, Subcomittee SC 27*, IT Security techniques*, Information techniques – Security techniques – *Code of practice for information security management (2nd edition)*, ISO/IEC 17799:2005, Fevereiro 2005.

[ISO27001] Joint Technical Comitee ISO/IEC JTC 1, *Information technology*, Subcomittee SC 27*, IT Security techniques*, Information technology – Security techniques – Information Security management systems – Requirements, ISO/IEC 27001:2006, Abril 2006.

[OGF08] D. Groep, M. Helm, J. Jensen, M. Sova, S. Rea, R. Karlsen-Masur, U. Epting, M. Jones, *Grid Certificate Profile*, Janeiro 2008.

[NIST80053] R. Ross, S. Katzke, A. Johnson, M. Swanson, G. Stoneburner, G. Rogers, *Recommended Security Controls for Federal Information Systems*, NIST Special Publication 800-53 Revision 2 Dezembro 2007.

[RFC3628] D. Pinkas, N. Pope, J. Ross, *Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework*, RFC 3628, Novembro 2003. http://www.ietf.org/rfc/rfc3628.txt

[RFC3647] S. Chokani, W. Ford, R. Sabett and S.Wu, *Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework*, RFC 3647, Novembro 2003. http://www.ietf.org/rfc/rfc3647.txt

[RFC4630] R. Housley, S. Santesson, *Update to DirectoryString Processing in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revogation List (CRL) Profile*, RFC 4630, Agosto 2006. http://www.ietf.org/rfc/rfc4630.txt

[RFC5280] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk, *Internet X.509 Infrastructure Certificate and Certificate Revogation List (CRL) Profile*, RFC 5280, Novembro 2003. http://www.ietf.org/rfc/rfc5280.txt

Controle de Alterações

Nesta seção apresenta um histórico das modificações principais feitas neste documento de uma versão para a próxima. Cada versão deste documento seria identificada por dois números, o primeiro é o número de versão, o segundo o número de subversão. Mudanças na política causarão o numero de versão a ser incrementado enquanto a subversão mudará com a inclusão de outras mudanças inclusivas das práticas. Uma versão pode ser seguida por a sigla RC (de *Release Candidate*) e um número que significa que esta versão ainda não foi finalizada e esta sendo sujeito algumas pequenas modificações.

Versão 2.0RC5, 4 de abril de 2011

Alem de correções ortográficas e texto para melhor o entendimento, foram feitos as seguintes modificações:

Seção	Descrição da Mudança	Classificação	Impacto	Autor
Considerações gerais	Incluída a seção intitulada Identificação do documento	Editoração	Baixa	Vinod Rebello
2.2/2.4	Mudou o Requisito em 2.2 de alta disponibilidade de informações no repositório para 2.4	Política	Alta	Vinod Rebello
2.3	Correção: Repositório deve ser atualizado imediatamente depois o certificado foi emitido	Política	Alta	Vinod Rebello
4.1.2	Acrescentou na seção de auditoria a verificação que a seção esta consistente com outras antes a aprovação do documento	Auditoria	Alta	Vinod Rebello
4.2.2	Opções em caso de rejeição	Praticas	Baixa	Lucas Martins
4.7.3	Requisitos Mínimos corrigidos.	Política	Alta	Vinod Rebello
5.5.3	Requisitos Mínimos corrigidos.	Política	Alta	Vinod Rebello
6.2.10	Incluir HSM de backup	Praticas	Alta	
7.1.2	Requisitos Mínimos corrigidos.	Política	Alta	Vinod Rebello
7.1.3	SHA-2 incluido	Praticas	Alta	Vinod Rebello
7.1.4	Tabela corrigida (S -> ST).	Política	Baixa	Vinod Rebello
7.1.6	Requisitos Mínimos corrigidos.	Política	Baixa	Vinod Rebello
9.4	Removida a restrição que a seção só aplica se AC a emitir certificados para entidades finais.	Política	Alta	Lucas Martins
9.10.1	A PC/DPC deve ser revisada depois da emissão de um novo documento de Requisitos Mínimos.	Praticas	Alta	Vinod Rebello

Versão 2.0RC4, 23 de Setembro de 2010

O titulo do documento foi modificado para *Requisitos Mínimos para as Políticas de Certificado e Boas Práticas de Certificação*. O texto em geral tem sofrido bastantes alterações na tentativa de deixar as questões mais claras. Foram acrescentados também exemplos de textos para seções correspondentes (ainda faltam bons exemplos). Foi acrescentado um item sobre

auditoria em cada seção. Tais alterações não estão identificadas na tabela seguinte, só as mudanças significativas são apresentadas.

Seção	Descrição da Mudança	Classificação	Impacto	Autor
Considerações gerais	Mudança no período de tempo máximo para adequar os critérios de uma nova versão do documento de Requisitos Mínimos.	Política	Alta	Vinod Rebello
1.1	Deve ser identificada a entidade que vai operar a AC e sua relação com e função dentro a instituição	Política	Alta	
1.2	Acrescentado onde podem ser encontradas informações sobre OIDs e onde um pode ser requerido.	Informação		
1.2	Quando deve ter mudanças no OID da PC/DPC.	Política	Alta	
1.3.2	Múltiplos ARs	Prática	Baixa	Lucas Martins
1.4.1	Definição de usos permitidos das chaves	Política	Alta	
1.5.3	Seção que faltava inserido: *Responsável por determinar a adequabilidade da DPC às políticas.*	Política	Baixa	
1.5.4.	Antiga seção 1.5.3: *Procedimentos de aprovação da PC*	Informação		
2.1	Inclusão de uso de repositórios independentes e só for utilizado, informações sobre os mesmos também devem ser disponibilizadas.	Prática	Baixa	
2.4	Informações públicas devem ser acessadas anonimamente apenas para consultas, o acesso a elas deve monitorado. Informações no repositório devem estar mantidas sempre disponíveis.	Política e Prática novas	Alta	
3.1.5	Permitir *wildcards* em certificados de hosts.	Política	Baixa	
3.2.3	Permitir verificação remota por videoconferência em casos uma impossibilidade de encontro presencial	Política	Baixa	
4.1.2	Acrescentada as responsabilidades do solicitante quanto a veracidade das informações fornecidas e quanto a geração de suas chaves.	Política	Baixa	
4.2.1	Necessidade de verificar todas as informações que vão estar no certificado.	Política	Alta	
4.2.2	A AC deve informar os critérios para aprovação ou rejeição de solicitações, bem como as	Política	Baixa	

	ações tomadas para processá-las cada tipo de pedido.			
4.2.3	A AC deve levar em conta diversos fatores ao estabelecer um prazo para o processamento das solicitações.	Prática nova	Baixa	
4.5.1	O titular deve informar imediatamente à AC emissora caso sua chave privada seja comprometida.	Política	Alta	
4.6.1	Permitir renovação se as chaves foram geradas originalmente num dispositivo de hardware seguro. Necessário verificar o posse da chave privada cada renovação.	Política e Práticas novas	Baixa	
4.6.3	Os procedimentos para renovação devem ser equivalentes aos seguidos para emissão do primeiro certificado.	Política nova	Alta	
4.6.4	Utilizar procedimentos parecidos com uma solicitação nova	Política e Práticas novas	Baixa	
4.6.5	Utilizar procedimentos parecidos com aqueles descritos na seção 4.4.1.	Prática	Baixa	
4.6.6	A AC deve publicar os certificados renovados em seu repositório público, assim como os outros emitidos.	Política nova	Alta	
4.6.7	Além da publicação do certificado no repositório, uma entidade pode solicitar notificação da emissão de certificados	Prática	Baixa	
4.7.1	Será permitida renovação por troca de chaves se é possível garantir a veracidade das informações e o certificado ainda não expirou.	Política e Práticas novas	Alta	
4.7.3	Foi criada políticas e praticas apropriada. Teria a necessidade de verificar a existência certificado valido. A solicitação deve ser autenticada e o solicitante deve ser identificado de forma apropriada. Recomenda-se seguir os mesmos procedimentos definidos na seção 3.2.	Política e Prática novas	Alta	
4.7.4	Nenhuma ação precisa ser tomada além da publicação do certificado no repositório. Entretanto, uma entidade pode solicitar notificação caso haja uma justificativa razoável.	Práticas Novas	Baixa	
4.9.2	Acrescidas novas entidades que podem solicitar revogação.	Política estendida	Alta	

4.9.4	Um prazo apropriado deve ser estabelecido para revogação. O titular do certificado deve solicitar revogação o mais breve possível caso seja necessária.	Política e Prática novas	Alta	
4.9.7	Esclarecimento sobre a freqüência de emissão da CRL. Acrescentadas novas políticas para emissão de uma nova LCR.	Políticas estendidas e Práticas novas	Alta	
4.10.2	Antigas melhores práticas passaram a ser a nova política. Falhas de indisponibilidade são inevitáveis, mas todo esforço razoável deve ser feito para minimizar o tempo de indisponibilidade.	Política e Prática novas	Baixa	
4.12.1	Não seria permitido a custodio da chave privada das ACs.da ICPEDU	Política nova e esclarecimento da Prática	Baixa	
5.2.1	Foi removido a requisito que o pessoal da AC deve ser do quadro de funcionários da instituição.	Política modificada	Alta	
5.2.2	A AC deve garantir a separação das tarefas para funções críticas e, se necessário, adotar controle multiusuário.	Prática nova	Alta	
5.3.1	Não somente funcionários da própria instituição, agora funcionários de terceiras podem ser contratados.	Política modificada	Baixa	
5.4.2	A prática passou ser o requisito.	Política nova	Alta	
5.5.1	Solicitações de certificados e revogações e changelogs devem ser arquivadas também.	Prática estendida	Baixa	
5.6	*Descrição:* A AC não pode assinar certificados com validade maior que a sua própria, portanto, seu próprio certificado deve ser renovado antes de sua expiração, numa data chamada de ponto de atualização.	Esclarecimentos		
5.6	*Req. Mín.*: Um novo par de chaves para a AC deve ser gerado no mínimo a um mês do ponto de atualização e o certificado assinado com a nova chave pública deve ser divulgada de forma segura para as entidades confiantes.	Política nova	Alta	
5.6	O certificado anterior deve ser mantido ate sua expiração, dentre outros motivos, para a geração de LCR.	Prática nova	Alta	
5.7.2	Descrever os procedimentos			

	para casos de comprometimento de recursos, se forem sigilosos, apontar um documentos internos.	Política nova	Alta	
6.1.4	Informação suficiente deve ser disponibilizada para verificar a autenticidade do certificado publicado.	Política estendida	Baixa	
6.1.5	O tamanho mínimo das chaves da AC deve ser RSA 2048-bit módulos ou ECC P256 módulos.	Política estendida	Alta	
6.2.7	A chave privada deve ser armazenada cifrada na memória não volátil do módulo criptográfico.	Esclarecimento		
6.2.9	Não será mais necessária a autorização do grupo de operadores do hardware criptográfico para desativação.	Política	Baixa	
6.2.10	Inclui uma referencia aos HSM de backup e necessidade de ser a chave de backup também removida.	Esclarecimento		
6.3.2	Certificados de ACs baseadas em chaves 2048bit-RSA devem expirar antes de 2031.	Política	Baixa	
6.3.2	Para entidades finais, o período de utilização das chaves deve ser o mesmo da validade do certificado e para estes, é recomendado um período de 1 ano por maiores riscos de exposição das chaves. Para ACs, o tempo depende da função da AC, por isso deve-se avaliar risco versus custo, pois um período mais longo seria mais tempo para exposição das chaves e períodos mais curtos requer mais renovações e maior trabalho para gerenciar.	Prática		
6.5.1	Só a equipe da AC pode ter acesso aos recursos da AC.	Política	Alta	
7.1.2	Campos dos certificados	Esclarecimento		
7.1.3	Algoritmos MD2, MD4 e MD5 não são mais aceitáveis.	Política	Alta	
7.1.6	A seção pode apenas fazer referência a seção 1.2.	Prática		
7.2.1	LCR deve ser versão 2.			
9.2	Nenhuma responsabilidade financeira é assumida, seja no que diz respeito ao serviço de certificação digital ou a má utilização dos certificados emitidos sob a PC em questão.	Prática		

Versão 1.0 RC2, 12 de Setembro de 2008

Inicial versão do documento *Requisitos Mínimos para política de certificados e melhores práticas de certificação da ICPEDU*.

Assuntos sob Consideração para Versões Futuros deste Documento

Versão 2.0

Para finalizar esta versão precisamos:

- Resolver as referencias a Comitê Gestor de ICPEDU – não existe deste março 2011;
- Definir e incluir um OID.

Versão 3.0

- Vai precisar adequar o documento com os requisitos de Webtrust ou outro conjunto de requisitos aceitável para permitir que o certificado da AC Raiz de ICPEDU seja aceito pelos principais Browsers Web.

Pendências:

Os subitens sobre Auditoria

- Discutir com CAIS as opções para os campos de Auditoria de cada seção.
- Como as auditorias serão afetadas pelos requisitos de Webtrust?

Estrutura do documento

- Melhorias e inclusão de mais exemplos de texto.
- Considerar a divisão em documentos separados para cada tipo de AC (perfis de autenticação).
- Definição formal do espaço de nomes das ACs.
- IPR, documentos devem ter uma licença *creative commons*? DPCs devem referencia outro PC/DPCs de onde textos foram copiados