Declaração de Práticas de Certificação da Autoridade Certificadora da UFSC

Universidade Federal de Santa Catarina

5 de maio de 2009

Sumário

Lista de Figuras

Lista de Tabelas

Resumo

Contém da declaração de práticas de certificação da AC-UFSC.

Capítulo 1

Introdução

1.1 Visão Geral

Este documento apresenta a Declaração de Práticas de Certificação (DPC) da Autoridade Certificadora da Universidade Federal de Santa Catarina (AC UFSC) na ICPEDU.

A ICPEDU é uma iniciativa da RNP que visa a implantação de um serviço nacional de chaves publicas para seus usuários, chamado a Infraestrutura de Chaves Publicas Educacional. 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 infraestrutura de rede Internet nacional para a comunidade acadêmica. 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 AGP.
Neste documento são descritas as políticas para emissão de certificados assim como as práticas e controles operacionais empregadas pela AC UFSC na execução dos seus serviços. 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 é uma AC Institucional e emite certificados digitais exclusivamente para autoridades certificadoras e autoridades de registros vinculadas à UFSC. Esta DPC estabelece os requisitos mínimos para a emissão e gerenciamento destes certificados digitais.

A UFSC está localizada na cidade de Florianópolis, Estado de Santa Catarina, com área total de 18.081.543 m^2. Em 2009 mantém 62 cursos de graduação, 48 de mestrado e 33 de doutorado, distribuidos em 11 centros de ensino contabilizando mais de 35.000 alunos. Conta com 1552 professores e 2987 técnicos administrativos.

Esta DPC foi elaborada conforme a RFC 3647 [**?**].

1.2 Nome do Documento e Identificação

Esta PC/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 PC/DPC é 1.3.6.1.4.1.7687.3.1.1.1

1.3 Participantes

Os participantes da AC UFSC são:

1.3.1 Autoridades certificadoras

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 é uma AC Institucional e emite certificados digitais exclusivamente para autoridades certificadoras e autoridades de registros vinculadas à UFSC.

1.3.2 Autoridades de registro

A atividades de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais e de identificação de seus solicitantes das AC subordinadas à AC UFSC é realizada pela AR da AC UFSC.

1.3.3 Titulares dos certificados

Os titulares dos certificados são as autoridades certificadoras e autoridades de registro subordinadas à AC UFSC.

1.3.4 Entidades confiantes

Pessoas físicas ou jurídicas ou sistemas vinculados ao sistema acadêmico e de pesquisa brasileira.

1.3.5 Outros participantes

Não se aplica.

1.4 Uso do Certificado

1.4.1 Aplicações apropriadas para os certificados

Os certificados emitidos pela AC UFSC têm como objetivo único identificar as ACs e ARs da AC UFSC. O certificado da AC UFSC podem ser utilizados para prover integridade, confidencialidade e autenticação para aplicação científicas não comerciais para certificados X.509, em particular:

- Autenticação de usuários, hosts e serviços;
- Autenticação e criptografia de comunicações;
- Autenticação de e-mails e objetos assinados.
- Identificação, autenticação e delegaçcão de privilégios em aplicações computacionais.

- Aplicações cliente-servidor com suporte aos protocolos SSL e TLS.
- Assinatura de documentos eletrônicos;

1.4.2 Aplicações proibidas para os certificados

O uso de certificados e chaves privadas emitidas pela AC UFSC sob esta DP/DPC está limitado às aplicações especificadas na Seção 1.4.1.

1.5 Dados para Contato

1.5.1 Entidade responsável por este documento

Esta política é administrada pela Universidade Federal de Santa Catarina (UFSC).

AC UFSC da ICPEDU
Núcleo de Processamento de Dados
Universidade Federal de Santa Catarina - UFSC
Bairro Trindade - Florianópolis
Santa Catarina - Brasil - CEP 88040-970
Fone: +55 (48) 3721-9000 - FAX: +55 (48) 3721-7766
E-mail:ac-ufsc@ac.ufsc.br

1.5.2 Ponto de contato

O ponto de contato para esta DPC e outros assuntos relacionados é

Nome:	Universidade Federal de Santa Catarina (UFSC) Núcleo de Processamento de Dados (NPD) Direção
Endereço:	Campus Universitário
Bairro:	Trindade
CEP:	88040 - 970
Telefone:	55 48 3721 7636
Página web:	http://ac.ufsc.br
E-mail:	ac-ufsc@ac.ufsc.br

1.5.3 Procedimentos de aprovação da PC

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

1.6 Definições e Acrônimos

AC	Autoridade Certificadora
AC Raiz	Autoridade Certificadora Raiz da ICPEDU
AC Correio	Autoridade Certificadora de Correio Eletrônico da ICPEDU
AC UFSC	Autoridade Certificadora da UFSC
AR	Autoridade de Registro
CG	Comitê Gestor da ICPEDU
DN	Distinguished Name
DPC	Declaração de Práticas de Certificação
FIPS	Federal Information Processing Standard
HSM	Hardware Secure Module
HLB	Hora Legal Brasileira
ICP	Infra-Estrutura de Chaves Públicas
ICPEDU	Infra-estrutura de Chaves Públicas para Pesquisa e Ensino
IDS	Intrusion Detection System
ISO	International Standards Organization (Organização Internacional de Padrões)
ITU	International Telecommunications Union
LabSEC	Laboratório de Segurança em Computação da UFSC
LCR	Lista de Certificados Revogados
NPD	Núcleo de Processamento de Dados
NTP	Network Time Protocol
OCSP	On-line Certificate Status Protocol
OID	Object Identifier
Parte confiante	Entidade que age confiando no teor e na validade de certificados de terceiros
PC	Política de Certificados
PCN	Plano de Continuidade de Negócio
PEM	Privacy-enhanced Electronic Mail
PIN	Personal Identification Number
Ponto de Atualizacão	É a data em que resta um período de validade exatamente igual ao período de validade dos certificados que esta AC emite.
PS	Política de Segurança
RFC	Request For Comments
RNP	Rede Nacional de Ensino e Pesquisa
RSA	Algoritmo RSA de chave pública
SGCI	Sistema Gerenciador de Certificados Digitais da ICPEDU
SSL	Secure Sockets Layer (Camada de Soquete Seguro)

Status do Certificado	Estado de validade do certificado, que pode vigente ou revogado
UFSC	Universidade Federal de Santa Catarina
URL	Uniform Resource Locator (Localizador de Recurso Uniforme)
UTC	Coordinated Universal Time

Capítulo 2

Responsabilidades referentes a publicações e repositórios

2.1 Repositório

O AC UFSC mantém o seu repositório na URL:

`http://ac.ufsc.br/repositorio`

2.2 Publicação de informações

O repositório contém as seguintes informações:

- Certificados emitidos pela AC UFSC, em formatos apropriados;
- Todos os certificados emitidos pela AC, ou informações sobre cada um deles;
- Versão atual e anteriores da lista de certificados revogados (LCR) da AC UFSC;
- Versão atual e anteriores das PCs e DPCs da AC UFSC.

2.3 Freqüência de publicação

O repositório é atualizado, sempre que houver mudança nas informações listadas na Seção 2.2.

2.4 Controles de acesso aos repositórios

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

Capítulo 3

Identificação e Autenticação

3.1 Estrutura de Nomes

3.1.1 Tipos de nomes

Os nomes usados no certificado devem seguir a padrão X.500 e ser apropriados para a aplicação na qual serão usados. A identificação dos titulares de certificados é feita pelos campos listados na Tabela A.1

Em casos nos quais é necessário emitir certificados com outro tipo de nome distinto (DN) será feita através de uma avaliação do gerente da AC UFSC.

3.1.2 Necessidade de que nomes sejam significativos

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. A AC-UFSC reserva-se ao direito de negar um nome de AC ou AR, caso não seja representativo e significativo do serviço que o mesmo irá prover. Não são admitidos caracteres especiais ou de acentuação nos campos do DN. Os valores para o nome distinto da AC UFSC podem ser encontrados na tabela A.1 definida na seção A.1 e 7.1.4.

3.1.3 Anonimato dos titulares de certificado

A AC UFSC não emitirá certificados com suporte ao anonimato.

3.1.4 Regras para interpretação dos diversos formatos de nomes

Os nomes são interpretados conforme estabelecido na tabela A.1 definida na seção A.1 e 7.1.4.

3.1.5 Unicidade dos nomes

O *Subject Name* de um certificado é único no conjunto de certificados válidos emitidos pela AC UFSC, como mostrado nas tabelas A.1 A.2

3.1.6 Reconhecimento, autenticação e papel de marcas registradas

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 da Identidade Inicial

3.2.1 Método para prova da posse de chave privada

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

3.2.2 Autenticação da identidade organizacional

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

3.2.3 Autenticação da identidade individual

O requerente deverá apresentar-se a autoridade de registro munido de sua identidade na UFSC que comprove seu vínculo com a Instituição e outro documento de identidade oficial com foto.

3.2.4 Dados dos titulares de certificados que não são verificados

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

3.2.5 Validação de autoridade

O documento do representante legal atribuindo ao requerente como representante legal da AC é suficiente para a validação da autoridade.

3.2.6 Critérios para interoperabilidade

Não estipulado.

3.3 Identificação e Autenticação para Requisição de Substituição de Chaves

3.3.1 Identificação e autenticação para troca de chaves de rotina

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

3.3.2 Identificação e autenticação para troca de chaves após revogação

A requisição recebida após uma revogação será tratada como uma nova requisição.

3.4 Identificação e Autenticação para Requisição de Revogação

A solicitação de revogação do certificado de uma AC deve ser feita pelo responsável ou representante legal da unidade organizacional a qual a AC está vinculada. Nos demais casos, os donos do certificado podem fazê-lo a AR ou diretamente a AC. O mesmo processo de autenticação adotado na solicitação 3.2.1 3.2.2 3.2.3 de um certificados deve ser adotado na sua revogação,

Capítulo 4

Requisitos Operacionais do Ciclo de Vida do Certificado

4.1 Procedimentos do requerente para solicitar o certificado

4.1.1 Quem pode submeter uma solicitação de certificado

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

4.1.2 Processo de solicitação e responsabilidades

O requerente deverá se dirigir pessoalmente às instalações da AC UFSC, munido do documento de identificação oficial com foto, comprovante de inscrição no SIAPE, o arquivo contendo a requisição de certificado e um endereço de e-mail válido.

4.2 Processamento da solicitação pela AR

4.2.1 Realização das funções de identificação e autenticação

A identificação e autenticação do requerente será realizada pessoalmente nas instalações da AC UFSC.

4.2.2 Aprovação ou rejeição das solicitações

Uma vez validado os documentos de identificação e do arquivo contendo a requisição do certificado de AC, a AC UFSC definirá uma data para a emissão do certificado. 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. Critérios adicionais como: a adequação da solicitação a PC/DPC também pode ser usada como critério para aprovar ou rejeitar uma requisição de certificado. Devem ser mantidos registros sobre todas as requisições aprovadas ou rejeitadas.

4.2.3 Tempo para processamento das solicitações

O tempo esperado para o processamento de uma requisição é de até 7 dias úteis.

4.3 Processamento da solicitação pela AC

4.3.1 Ações da AC durante a emissão de certificado

A AC UFSC verifica se a requisição está devidamente assinada com a chave privada da AC requerente. Em seguida, os operadores da AC UFSC autenticam-se no módulo de hardware seguro para liberar o uso da chave de assinatura da AC UFSC. Após isso, o administrador da AC UFSC, utilizando o sistema de gerenciamento de certificados digitais (SGCI) procede a emissão do certificado. O certificado é então exportado para uma mídia portátil.

4.3.2 Notificação do solicitante pela AC sobre a emissão de certificado

Assim que o certificado da AC é emitido, é enviado um e-mail para o requerente notificando-o que o certificado está disponível.

4.4 Aceitação do certificado pelo requerente

4.4.1 Conduta que constitui a aceitação de certificado

Não estipulado.

4.4.2 Publicação do certificado pela AC

Os certificados emitidos para as ACs são publicados imediatamente após a sua emissão.

4.4.3 Notificação da emissão de certificado pela AC para outras entidades

Nenhuma outra entidade é notificada após a emissão de um certificado.

4.5 Utilização de pares de chaves e de certificados

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

Os titulares dos certificados das ACs são responsáveis pela proteção da chave privada. Estas devem ser geradas e armazenadas em módulos de hardware seguros (HSM). O uso da chave privada deve respeitar todas as políticas impostas pela AC UFSC, seja indiretamente através da sua DPC, PS ou de extensões contendo políticas registradas em seu certificado, respeitando as

recomendações descritas na seção 1.4. A ocorrência de qualquer anormalidade ou suspeita de comprometimento da chave privada da AC, a AC UFSC deve ser imediatamente informada.

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

As entidades confiantes devem:

- estar cientes das informações presentes neste documento;
- verificar a LCR emitida pela AC UFSC antes de aceitar o certificado da AC como válido;
- verificar as políticas críticas inclusas no certificado da AC.

4.6 Reemissão de certificados por troca do prazo de validade

A AC UFSC não renova certificados. O titular de um certificado de AC pode solicitar um novo certificado de acordo com os procedimentos descritos na Seção 4.1.

4.6.1 Circunstância para renovação de certificados

Não se aplica.

4.6.2 Quem pode solicitar renovação

Não se aplica.

4.6.3 Processamento de solicitações de renovação

Não se aplica.

4.6.4 Notificação de nova emissão de certificado para o titular

Não se aplica.

4.6.5 Conduta que constitui aceitação de um certificado renovado

Não se aplica.

4.6.6 Publicação do certificado renovado pela AC

Não se aplica.

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

Não se aplica.

4.7 Reemissão de certificados por troca de chaves

A AC UFSC não re-emite um certificado de uma AC pela simples troca do par de chaves criptográficas. O titular da AC pode solicitar um novo certificado de acordo com os procedimentos descritos na Secão 4.1.

4.7.1 Circunstâncias para substituição das chaves criptográficas

Não se aplica.

4.7.2 Quem pode solicitar a certificação de uma nova chave pública

Não se aplica.

4.7.3 Processamento de solicitações de substituição de certificados

Não se aplica.

4.7.4 Notificação de nova emissão de certificado para o titular

Não se aplica.

4.7.5 Conduta para a aceitação de um novo certificado

Não se aplica.

4.7.6 Publicação do novo certificado

Não se aplica.

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

Não se aplica.

4.8 Reemissão de certificados por troca de dados

A AC UFSC não realiza a modificação de certificados. O titular da AC pode solicitar um novo certificado de acordo com os procedimentos descritos na Seção 4.1.

4.8.1 Circunstância para modificação de certificados

Não se aplica.

4.8.2 Quem pode solicitar a modificação de certificados

Não se aplica.

4.8.3 Processamento de solicitações de modificação de certificados

Não se aplica.

4.8.4 Notificação de nova emissão de certificado para o titular

Não se aplica.

4.8.5 Conduta que constitui aceitação de um certificado modificado

Não se aplica.

4.8.6 Publicação do certificado modificado pela AC

Não se aplica.

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

Não se aplica.

4.9 Revogação e Suspensão

4.9.1 Circunstâncias para revogação

Um certificado deve ser revogado obrigatóriamente quando:

- Em caso de comprometimento da chave pública da AC UFSC, todos os certificados emitidos por ela devem ser imediatamente revogados.
- For constatado o não cumprimento da PC/DPC;
- For constatada a emissão imprópria ou defeituosa;
- As informações que ele contém estão incorretas;
- O titular de certificado não deseja mais ser vinculado à AC UFSC;
- Houver dissolução da AC UFSC que emitiu o certificado; ou
- Houver comprometimento da chave privada ou da sua mídia armazenadora.

4.9.2 Quem pode solicitar revogação

Uma solicitação de revogação pode ser feita por:

- Por determinação do CG ICPEDU;
- Por determinação da AC que emitiu o certificado;
- Por solicitação do responsável pelo certificado (titulares em caso de certificados pessoais ou alguém que represente responsabilidade pela máquina ou serviço certificado); ou
- Por determinação judicial.

4.9.3 Procedimento para solicitação de revogação

O processo de revogação deve seguir as mesmas recomendações da Seção 3.4. E deve ser mantido um registro de todas as solicitações de revogações.

4.9.4 Prazo para a solicitação de revogação

A solicitação de revogação deve ser feita à AC UFSC no prazo máximo de 1 dia útil após a ocorrência de uma das circunstâncias apresentadas na Seção 4.9.1.

4.9.5 Prazo para a AC processar a solicitação de revogação

O tempo esperado para o processamento de uma solicitação é de 1 dia útil.

4.9.6 Requisitos para verificação de revogação por entidades confiantes

As entidades confiantes devem sempre utilizar a LCR da AC UFSC para verificar se o certificado da AC subsequente continua válido. Também deve ser confirmada a autenticidade da LCR, através da verificação da assinatura da AC e do período de validade.

4.9.7 Freqüência de emissão de LCRs

As LCRs são emitidas sempre que um conjunto de certificados é revogado e no máximo a cada 112 dias e publicadas imediatamente após a emissão.

4.9.8 Latência máxima para LCRs

As LCRs são publicadas no repositório da AC UFSC assim que forem emitidas.

`http://ac.ufsc.br/repositorio`

4.9.9 Mecanismos para verificação on-line do status de certificados

A AC UFSC não disponibiliza serviço on-line de revogação ou de verificação de estado de certificado.

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

Não se aplica.

4.9.11 Outras formas de comunicação de revogação

Não estipulada.

4.9.12 Procedimentos adicionais no caso de comprometimento da chave privada

Não estipulado.

4.9.13 Circunstâncias para suspensão

A AC UFSC não realiza a suspensão de certificados.

4.9.14 Quem pode solicitar a suspensão

Não se aplica.

4.9.15 Procedimento para solicitação de suspensão

Não se aplica.

4.9.16 Limites para o período de suspensão

Não se aplica.

4.10 Serviços de Status de Certificado

4.10.1 Características operacionais

A AC UFSC utiliza LCRs como único mecanismo de verificação do estado dos certificados emitidos,

4.10.2 Disponibilidade do serviço

As LCRs estarão disponíveis no repositório da AC UFSC conforme a Seção 2.1.

4.10.3 Características opcionais

Não estipulada.

4.11 Encerramento do vínculo com a AC

O representante legal da unidade organizacional deve informar a AC UFSC, através de e-mail assinado digitalmente ou por documento papel, que a AC deixará de operar. Ao receber esta informação, a AC UFSC procederá a revogação do certificado da AC. Outra situação na qual o vínculo é encerrado é quando o certificado é revogado ou expirado.

4.12 Custódia e recuperação de chaves

A AC UFSC não oferece os serviços de proteção e recuperação das chaves privadas das ACs subordinadas.

4.12.1 Políticas e práticas para custódia e recuperação de chaves

Não se aplica.

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

Não se aplica.

Capítulo 5

Controles operacionais, gerenciais e de instalações físicas

5.1 Controles de Segurança Física

5.1.1 Localização e construção das instalações físicas

A AC UFSC está no Ambiente Seguro (Sala Cofre) da UFSC.

5.1.2 Acesso físico

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.

O sistema de certificação da AC UFSC está situado em um ambiente seguro.

5.1.3 Energia e refrigeração

A AC UFSC, os repositórios e a AR estão localizados em ambiente seguro que, além de conectados à rede elétrica, dispõe dos seguintes recursos:

a) gerador principal;

b) gerador reserva;

c) sistema de no-breaks;

d) sistema de aterramento e proteção a descargas atmosféricas;

e) iluminação de emergência.

O sistema de ar condicionado é tolerante a falhas com controle de calor e umidade, independente do sistema de ar condicionado da construção onde está localizado.

Adicionalmente, as facilidades listadas seguem as especificações de disponibilidade definidas no documento de Políticas de Segurança.

5.1.4 Exposição a água

A Sala Cofre é completamente a prova d'água.

5.1.5 Prevenção e proteção contra incêndio

Dentro do ambiente da Sala Cofre existem sensores que detectam a menor presença de fumaça. Na ocorrência da mesma, alarmes são disparados. Adicionalmente, um gás especial é lançado para promover o encerramento do possível foco de incêndio. O núcleo da Sala Cofre é a prova de incêndio.

5.1.6 Armazenamento de mídia

A Sala Cofre possui cofres especiais para o armazenamento e proteção de mídias eletrônicas removíveis. Toda mídia sensível são armazenadas em local seguro e apropriado de acordo com as especificações do fabricante, acessível apenas ao pessoal autorizado. Sua entrada, saída e utilização deve ser registradas a fim de manter uma trilha de auditoria. Informação cujo tempo de armazenamento necessário é maior que a vida útil da mídia, devem ser armazenadas também em outros locais para evitar perda de informação proveniente da degradação da mídia.

5.1.7 Descarte de lixo

Toda mídia eletrônica, papel, memória e qualquer outro meio que possa conter informação considerada confidencial pela AC UFSC devem ser totalmente destruídos fisicamente antes do descarte.

5.1.8 Cópias de segurança em outras instalações

Serão utilizadas as instalações do Núcleo de Processamento de Dados da UFSC para o armazenamento de cópias de segurança das mídias ou arquivos da AC UFSC. Os mesmos requisitos de segurança de armazenamento de mídias como especificado na Política de Seguraça da AC UFSC devem ser atendidas.

5.2 Procedimentos de Controle

5.2.1 Papéis de confiança

A AC UFSC estabelece um mínimo de 4 (quatro) perfis distintos para sua operação, distinguindo as operações do dia-a-dia do sistema, o gerenciamento e auditoria destas operações, bem como o gerenciamento de mudanças substanciais no sistema. A divisão de responsabilidades entre os perfis é a seguinte:

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. 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 grupo 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.

5.2.2 Número de pessoas necessárias por tarefa

A AC UFSC implementa o controle multiusuário, por meio de segredo compartilhado, para a geração e a utilização da chave privada da AC UFSC, conforme o descrito no item 6.2.8. Todas as tarefas executadas no ambiente onde está localizado o equipamento de certificação da AC UFSC necessitam da presença de no mínimo duas (2) pessoas. As demais tarefas da AC UFSC podem ser executadas por um único funcionário. Todas as pessoas devem pertencer ao quadro funcional efetivo da UFSC.

5.2.3 Identificação e autenticação para cada papel

Todos os membros dos perfis estabelecidos na Seção 5.2.1 devem possuir um smartcard para se autenticar perante o módulo de segurança criptográfica (HSM). Quanto ao sistema de gerenciamento de certificados digitais (SGCI), os administrador e os operadores possuem uma senha secreta.

5.2.4 Papéis que requerem separação de responsabilidades

As pessoas que exercem papel de auditor não podem exercer os papéis de administrador e operador

5.3 Controle do Pessoal

Todos os funcionários da AC UFSC que executam tarefas operacionais, gerenciais e de auditoria têm registrado um termo de responsabilidade e sigilo.

5.3.1 Requisitos de qualificação, experiência e conformidade com obrigações governamentais

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 obrigações respeitando os regulamentos da UFSC.

5.3.2 Procedimentos de verificação de antecedentes

O pessoal envolvido na operacão da AC UFSC, deve pertencer ao quadro de funcionários da UFSC.

5.3.3 Requisitos de treinamento

Todo o pessoal envolvido na operação da AC UFSC são capacitados por cursos internos da UFSC para este fim.

5.3.4 Requisitos de freqüência de treinamento

Sempre que houver alterações em procedimentos ou quaisquer modificações na plataforma computacional, um novo treinamento será realizado.

5.3.5 Freqüência e seqüência para revezamento de trabalho

Não estipulado.

5.3.6 Sanções para ações não autorizadas

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

5.3.7 Requisitos para prestadores de serviço independentes

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, exigindo relatórios e registros das operações dos prestadores de serviço.

5.3.8 Documentação fornecida aos funcionários

A AC UFSC disponibiliza para todo o seu pessoal:

a) sua PC/DPC, PS;

b) documentação operacional relativa a suas atividades;

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

5.4 Sistemas de auditoria e procedimentos para registro de eventos

Tanto o sistema de gerenciamento de certificados digitais (SGCI) quanto o módulo de segurança criptográfica (HSM) registram automaticamente todos os eventos envolvidos na geração de certificados digitais e LCRs. Além disso, qualquer operação da AC UFSC está sujeita a aprovação e execução de uma cerimônia formal, com geração de um relatório detalhado de todas as ocorrências.

5.4.1 Tipo de eventos registrados

Os seguintes eventos são registrados: 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 todos 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.

5.4.2 Freqüência de análise dos registros de eventos

Os registros de eventos são analisados mensalmente.

5.4.3 Período de retenção para registros de eventos

Os registros de eventos são arquivados por no mínimo 5 anos.

5.4.4 Proteção de registros de eventos

Os registros de eventos são armazenados em discos nos servidores que hospedam o sistema de certificação digital e suas cópias de segurança arquivados em mídias armazenadas em cofres dentro da Sala Cofre e em um sistema backup no NPD da UFSC.

5.4.5 Procedimentos para cópias de segurança de registros de eventos

As cópias de segurança dos registros de eventos são armazenados de forma cifrada em mídia eletrônica removível. A periodicidade da cópia deve ser mensal. A integridade das cópias de segurança é verificada anualmente.

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

Todos os sistemas de eventos para auditoria utilizados pela AC UFSC em seus procedimentos operacionais são internos.

5.4.7 Notificação do sujeito causador do evento

Não estipulado.

5.4.8 Avaliação de vulnerabilidades

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 UFSC além da plataforma hospedeira do seu repositório. Também serão analisados os registros do ambiente seguro. Avaliações de vulnerabilidades devem ser feitas mensalmente (ou sempre que forem identificadas ou reportadas vulnerabilidades que afetem ou possam afetar os sistemas) e as medidas cabíveis para minimizar o risco relacionado a elas devem ser tomadas. O pessoal responsável pela segurança das operações da AC UFSC 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.

5.5 Arquivamento de Registros

5.5.1 Tipos de registros armazenados

Além dos registros de eventos para auditoria mencionados na Seção 5.4.1 também são arquivados:

- Registros de mudanças, programadas ou não, no software, hardware ou procedimentos de operação dos sistemas;
- Documentação de credenciamento das Autoridades Certificadoras;
- Documentação relacionada a solicitação de certificados;
- Listas de certificados revogados;
- Certificados emitidos.

5.5.2 Período de retenção dos registros

Os registros de são arquivados por no mínimo 5 anos, em mídias não volátil.

5.5.3 Proteção dos registros

Acesso ao arquivo é exclusivo dos administradores e auditores. Os arquivo são armazenado em mídia não volátil e em local seguro. As mídia são protegidas:

a) fatores ambientais, como: temperatura, umidade e magnetismo;

b) fatores temporais, devendo ser substituída:

   i) a cada 5 anos,

   ii) para atualização tecnológica,

c) quando se fizer necessário.

A proteção criptográfica das mídia é adotada quando a classificação da informação assim exigir. Todos os registros arquivados são classificados e armazenados com requisitos de segurança compatíveis com sua classificação, conforme a Política de Segurança da AC UFSC.

5.5.4 Procedimentos para cópias de segurança dos registros

A cópia de segurança do arquivo é armazenada assinada digitalmente pelo gerente em mídia não volátil, que deve ser trocada a cada 5 anos. As cópias de segurança do arquivo são feitas a cada 6 meses. E sua localização definida na Seção 5.1.8.

5.5.5 Requisitos para datação dos registros

Todos os registros devem conter informações de data e hora.

5.5.6 Sistema de recolhimento de registros (interno ou externo)

O sistema de coleta de informações para arquivamento é interno, feito pela própria AC UFSC.

5.5.7 Procedimentos para obtenção e verificação dos registros armazenados

Informações do arquivo só podem ser obtidas mediante aprovação do gerente da AC UFSC. O procedimento de verificação da integridade das informações extraídas é feita com auxílio de funções de resumo criptográfico do arquivo.

5.6 Nova Chave Pública para a AC

Um novo par de chaves para a AC UFSC deve ser gerado três meses antes do ponto de atualização de seu certificado.

5.7 Comprometimento e Recuperação de Desastre

A recuperação de desastre está definida no plano de segurança da Sala Cofre.

5.7.1 Procedimentos para tratamentos de desastres e comprometimentos

Conforme plano de segurança da Sala Cofre da UFSC.

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

Conforme plano de segurança da Sala Cofre da UFSC.

5.7.3 Procedimentos para comprometimento de chave privada de entidade

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

5.7.4 Capacidade para continuidade de negócios após desastre

Conforme plano de segurança da Sala Cofre da UFSC.

5.8 Finalização da AC ou AR

O representante legal da unidade organizacional da UFSC onde está vinculada a AC deve notificar a AC UFSC quanto a descontinuidade dos serviços de uma AC. Ao encerrar suas operações, a AC deverá:

- Notificar as ARs credenciadas;
- Notificar titulares de certificados e entidades confiantes;
- Notificar contatos de segurança relevantes;
- Revogar todos os certificados emitidos;
- Emitir e publicar LCRs;
- Destruir qualquer cópia das chaves privadas;
- Arquivar os registros de forma segura.
- Os registros devem ser mantidos pela entidade responsável para futuras revisões e auditorias, por um período de 5 (cinco) anos.

Capítulo 6

Controles Técnicos de Segurança

6.1 Geração e Instalação do Par de Chaves

6.1.1 Geração de pares de chaves

Os pares de chaves criptográficas da AC UFSC e de suas ACs subordinadas e ARs vinculadas são gerados em módulos de segurança criptográfica (HSM). O algoritmo a ser utilizado para as chaves criptográficas é o RSA..

6.1.2 Fornecimento de chave privada ao titular

Não se aplica, uma vez que as chaves criptográficas são geradas pelo próprio titular.

6.1.3 Entrega da chave pública à Autoridade Certificadora

As chaves públicas são encaminhadas para a AR UFSC através de arquivos de requisição de certificados no formato PKCS#10 [**?**].

6.1.4 Divulgação da chave pública da AC às partes confiantes

As chaves públicas da AC UFSC e das ACs subordinadas estão publicadas em seu repositório.
A divulgação do certificado da AC UFSC para seus usuários é realizada:

a) no repositório da AC UFSC;

b) no sítio da AC UFSC ou das ACs subordinadas;

6.1.5 Tamanhos de chaves

O tamanho das chaves criptográficas assimétricas da AC UFSC e das suas ACs subordinadas devem utilizar chaves com tamanho de 2048 bits RSA.

6.1.6 Geração dos parâmetros de chave pública e verificação de qualidade

As chaves são geradas de acordo com os padrões definidos no documento Padrões e Algoritmos Criptográficos da ICPEDU [**?**].

Os parâmetros de geração de chaves assimétricas da AC UFSC devem seguir as recomendações internacionais de qualidade de chaves assimétricas, tais como aqueles descritos pela FIPS 140-2[**?**].

6.1.7 Propósitos de uso de chaves

As chaves privadas das ACs imediatamente subordinadas pela AC UFSC podem ser utilizadas para qualquer finalidade aprovada em sua DPC. A chave privada da AC UFSC só pode ser utilizada para assinar os certificados das ACs e ARs subordinadas e LCRs. Os certificados das ARs só devem ser utilizados para atividades requeridas ás atividades de uma ARs.

6.2 Proteção de chaves privadas e controles tecnológicos de módulos criptográficos

A AC UFSC utiliza um hardware criptográfico para gerar e armazenar seu par de chaves, emitir seu certificado e os certificados das ACs de nível imediatamente subseqüente ao seu e assinar suas LCRs. O hardware criptográfico possui um mecanismo de proteção contra violações lógicas e físicas.

A chave privada é usada pelo operador de uma AC ou AR no SGCI após ser ativada pelo grupo de operadores do HSM. Ao término do uso, o operador do SGCI deve proceder a sua desativação. O Comitê Gestor da AC UFSC é responsável pela decisão de destruição da chave privada da AC UFSC.

6.2.1 Padrões e controles de módulos criptográficos

A AC UFSC utiliza um hardware criptográfico conforme estabelecido na Seção 6.2.11.

6.2.2 Número de operadores para o Controle da chave privada

A chave privada da AC UFSC é liberada para uso por um número mínimo de 2 operadores de no máximo 4.

6.2.3 Custódia de chaves privadas

A AC UFSC não realiza a custódia de chaves privadas.

6.2.4 Cópias de segurança de chaves privadas

A cópia da chave privada das ACs devem ser registradas e mantidas em um HSM de backup, guardado em um cofre seguro, e feita mediante autorização formal do gerente da AC e su-

pervisionada por participantes do grupo de administradores e auditores. Cópias de segurança para ARs e entidades finais deve ser considerada conforme a necessidade da instituição.

6.2.5 Arquivamento de chaves privadas

A chave privada da AC UFSC é arquivada internamente ao HSM e na forma de cópia de segurança, conforme descrito na seção 6.2.4.

6.2.6 Transferência de chaves privadas de/para módulos criptográficos

A única forma de exportação e importação da chave privada da AC UFSC é através de uma cópia de segurança sob a responsabilidade do grupo de administradores, conforme descrito na Seção 6.2.4. A chave privada é mantida cifrada quando fora do módulo criptográfico.

6.2.7 Armazenamento de chaves privadas em módulos criptográficos

A chave privada é armazenada na forma cifrada na memória permanente do módulo criptográfico.

6.2.8 Método para ativação de chaves privadas

A chave privada da AC UFSC é ativada pelo grupo de operadores do HSM, conforme a Seção 6.2.2. Cada membro do grupo possui um smartcard e respectivo PIN que são utilizados em conjunto para liberar o uso da chave privada. Sempre que for feita a ativação da chave para assinar certificados ou LCRs, o grupo de operadores do HSM da AC UFSC libera a chave para 100 usos. A chave privada é utilizada pelo operador da AC UFSC no SGCI para assinar LCRs e certificados digitais. Após o uso, a chave deve ser descarregada da memória. O número de vezes que a chave foi utilizada num procedimento deve ser explicado no relatório do cerimonial de execução do procedimento.

6.2.9 Método para desativação de chaves privadas

Para desativar a chave privada da AC UFSC, os operadores do SGCI devem executar o comando de descarregar a chave por meio do sistema de gerenciamento remoto do HSM (OpenHSMd Client). Além disso, a chave privada é automaticamente desativada quando o HSM é desligado ou o número de usos especificado na Seção 6.2.8 é alcançado.

6.2.10 Método para destruição de chaves privadas

A chave privada da AC UFSC é destruída pelo apagamento da memória onde está o arquivo contendo a chave privada, esta atividade deve ser registrada para posterior auditoria.

6.2.11 Avaliação requerida de módulos criptográficos

A AC UFSC utiliza hardware criptográfico construído de acordo com as recomendações do FIPS 140-2, nível 3[**?**] ou compatível.

6.3 Outros Aspectos do Gerenciamento das Chaves

6.3.1 Armazenamento de chaves públicas

Os certificados da AC UFSC e de todas as ACs subordinadas são armazenados durante toda a vida útil da AC.

As chaves públicas da AC UFSC e das ACs de nível imediatamente subseqüente ao seu são permanentemente armazenadas no formato PEM em mídia digital e impressas em papel.

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

A chave privada da AC UFSC é utilizada apenas durante o período de validade do certificado correspondente. A chave pública da AC UFSC deverá estar disponível por tempo indeterminado, para verificação de assinaturas geradas durante o período de validade do certificado correspondente. Para entidades finais vínculadas, o período de utilização do par de chaves deve ser o mesmo da validade do certificado.

6.4 Ativação dos Dados

Todos as informações e dispositivos de hardware tais como senhas, PINs de smartcards e smartcards são armazenados em um cofre da Sala Cofre para uso durante todo o tempo de vida da AC UFSC.

6.4.1 Geração e instalação de dados de ativação

Os PINs e senhas são definidos no documento de cerimônia de criação da chave privada da AC.

6.4.2 Proteção de dados de ativação

Os dados de ativação são protegidos contra cópia e perda indevidas. O acesso aos dados de ativação são feitos da mesma forma que os utilizados para acesso ao HSM. A AC UFSC 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.

6.4.3 Outros aspectos de dados de ativação

Não estipulado.

6.5 Controles de segurança computacional

Todos os sistemas computacionais da AC UFSC relacionados com gerenciamento do ciclo de vida dos certificados operam off-line e possuem clara separação das tarefas e atribuições de cada perfil como definido na Seção 5.2.1, usam criptografia para segurança da base de dados, geram e armazenam registros para auditoria e possuem mecanismos para cópias de segurança.

6.5.1 Requisitos técnicos específicos de segurança computacional

O computador que hospeda o sistema de gerenciamento de certificados digitais (SGCI) é de uso exclusivo da AC UFSC. Este computador não é conectado em rede e não é modificado durante a sua vida útil. A substituição do computador, por outro deve ser feita a partir de um cerimônia especialmente concebida para este fim.

6.5.2 Classificação de segurança computacional

O computador contendo a AC UFSC, antes de ser utilizado para gerar o certificado da AC, é verificado e corrigido quanto a todas as falhas conhecidas de segurança.

6.6 Controles técnicos de ciclo de vida

6.6.1 Controles de desenvolvimento de sistemas

A AC Raiz utiliza um sistema de gerenciamento de certificados digitais e um módulo criptográfico elaborados sob uma metodologia de desenvolvimento de sistemas baseada no CMMi nível 2[**?**]; fazendo uso de sistemas de controle de versões, notificação de erros e melhorias, definição de planos de requisitos, projeto, qualidade, configuração e testes.

6.6.2 Controles de gerenciamento de segurança

Os controles de segurança da Sala Cofre, onde está instalada a AC UFSC, serão renovados periodicamente de acordo com a política de segurança da Sala Cofre. O GOPAC será o responsável por verficar se os requisitos apresentados na Seção 6.5.1 são atendidos.

6.6.3 Controles de segurança de ciclo de vida

Não estipulado.

6.7 Controles para a Segurança da Rede de Comunicações

A rede de comunicação de dados interna da Sala Cofre é protegida por filtros de pacotes e possui sistemas de detecção de intrusões (IDS). Salienta-se que a AC UFSC estará em equipamento sem conexão a rede de comunicação de dados. O ambiente de rede que hospeda a AC UFSC é configurado com todas as características de segurança consideradas boas práticas pela ICPEDU e estabelecidas na política de segurança da AC UFSC.

6.8 Carimbo do Tempo

Os relógios internos de todos os subsistemas da Sala Cofre, incluindo os equipamentos da AC UFSC estarão sincronizados com o servidor NTP da RNP. Os equipamentos off-line serão atualizado manualmente, sempre que inicializados.

Capítulo 7

Perfis dos Certificados, LCR e OCSP

7.1 Perfil dos Certificados

Os certificados estão em conformidade com o padrão definido na RFC 3280 [**?**].

7.1.1 Versão

A AC UFSC emitirá certificados digitais X.509 versão 3.

7.1.2 Extensões

As extensões são definidas seção A.2.2

7.1.3 Identificadores de objeto dos algoritmos

Os OIDs dos algoritmos utilizados para definir certificados digitais são:

Tabela 7.1: OID dos algoritmos utilizados

Função	Nome	OID
Função hash	Id-sha1	1.3.14.3.2.26
Ciframento	rsaEncryption	1.2.840.113549.1.1.1
Assinatura	sha1WithRSAEncryption	1.2.840.113549.1.1.5

7.1.4 Formatos dos nomes

O formato dos nomes são definidas na Tabela A.1

7.1.5 Restrições para nomes

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) A.4.

7.1.6 Identificador de objeto da PC

Ver seção 1.2.

7.1.7 Uso da extensão Policy Constraints

Não estipulada.

7.1.8 Sintaxe e semântica dos qualificadores de política

Não estipulada.

7.1.9 Semântica de processamento para a extensão crítica Certificate Policies

Haverá três dados em *Certificate Policies*: um ponteiro URL para a versão eletrônica desta PC/DPC e um texto explicativo simplificado da aplicação dos certificados emitidos no âmbito da UFSC, como estabelecido Tabela A.3.

7.2 Perfil da LCR

O formato da LCR emitida pela AC UFSC está em conformidade com a RFC3280.

7.2.1 Versão

Número de versão: versão 2. De acordo com perfil definido pelo padrão X-509.

7.2.2 Extensões da LCR e de entradas da LCR

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. As extensões para a LCR da AC UFSC podem ser encontradas na tabela A.3 da seção A.3

7.3 Perfil do OCSP

A AC UFSC não oferece o serviço on-line de verificação de estado de certificado (OCSP).

7.3.1 Versão

Não se aplica.

7.3.2 Extensões do OCSP

Não se aplica.

Capítulo 8

Auditoria de conformidade e outras avaliações

As auditorias e avaliações realizadas no âmbito da AC UFSC têm por objetivo verificar se os processos, procedimentos e atividades das entidades integrantes da AC UFSC estão em conformidade com suas respectivas DPC, PC, PS e demais normas e procedimentos estabelecidos.

8.1 Freqüência ou circunstâncias das avaliações

A AC UFSC é auditada anualmente.

8.2 Identidade e qualificações do avaliador

As avaliações são realizadas pelo grupo de avaliadores, especialmente treinados para este fim. E indicados pelo comite Gestor da ICPEDU.

8.3 Relação entre o avaliador e a entidade avaliada

Os avaliadores formam uma equipe distinta dos grupos de administração e operação da AC UFSC.

8.4 Tópicos cobertos na avaliação

Verificação da conformidade da AC UFSC com esta DPC e com as políticas e regras estabelecidas no contexto da ICPEDU. Aspectos como gerência das chaves e gerência do ciclo de vida do certificado devem ser avaliados com especial cuidado.

8.5 Ações tomadas resultantes de deficiências

Na ocorrência de qualquer deficiência, notifica-se o responsável pela AC UFSC para tomar as ações cabíveis. O gerente da AC deverá estabelecer e manter um plano de ação para corrigir

qualquer não conformidade encontrada durante as avaliações encaminhar um relatório para o CG da ICPEDU descrevendo as medidas tomadas.

8.6 Comunicação dos resultados

Os resultados das auditorias serão encaminhados ao gerente da AC UFSC. E o gerente da AC deverá encaminhar os resultados de avaliações e um relatório com medidas tomadas para corrigir as não conformidades encontradas para o Comite Gestor da ICPEDU.

Capítulo 9

Aspectos Legais e Assuntos Gerais

A AC UFSC é um serviço interno da UFSC e não oferece qualquer garantia além das especificadas nesta DPC às ACs e ARs imediatamente subordinadas.

9.1 Taxas

9.1.1 Taxas de emissão e renovação de certificados

Não serão cobradas.

9.1.2 Taxas para acesso aos certificados

Não serão cobradas.

9.1.3 Taxas para revogação ou para informações de estado

Não serão cobradas.

9.1.4 Outras taxas

Não estipulada.

9.1.5 Política de reembolso

Não se aplica.

9.2 Responsabilidade Financeira

A AC UFSC não terá qualquer responsabilidade financeira, quanto ao mau uso de sua estrutura PKI.

9.2.1 Cobertura de Seguro

Não se aplica.

9.2.2 Outros ativos

Não se aplica.

9.2.3 Cobertura de seguro ou garantia para entidades finais

Não se aplica.

9.3 Informações Confidenciais

9.3.1 Escopo de informações confidenciais

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) Medidas de segurança relativas:

   (a) à operação de hardware e software da ICPEDU; e

   (b) aos serviços de certificação.

9.3.2 Informações fora do escopo de informações confidenciais

São consideradas informações não confidenciais:

- certificados das ACs UFSC e credenciadas;
- listas de certificados revogados;
- versões publicadas de PCs, DPCs e Política de Segurança (PS).

9.3.3 Responsabilidade de proteção de informações confidenciais

A AC UFSC se compromete a manter a confidencialidade das informações classificadas como confidenciais.

9.4 Privacidade das Informações Pessoais

9.4.1 Plano de privacidade

A AC UFSC não emite certificados para usuários finais e, portanto, não se aplicam considerações sobre a privacidade de informações pessoais. As ACs subordinadas que emitirem certificados seguirão a PS da AC UFSC.

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

Autorizações formais podem ser apresentadas de três formas:

a) por meio eletrônico, contendo assinatura válida garantida por certificado reconhecido pela ICPEDU;

b) por meio de pedido escrito com firma reconhecida;

c) através de formulário eletrônico seguro, desde que comprovada autenticidade do autorizador.

Nenhuma liberação de informação é permitida sem autorização formal. Quando necessário o armazenamento de informações pessoais do representante das ACs subordinadas. Será observado a legislação institucional ou local vigente, nos padrões atualmente disponíveis.

9.4.2 Informação tratada como privada

Toda informação é tratada como privada, com exceção da informação disponibilizada no certificado.

9.4.3 Informação não considerada privada

É toda aquela que seu titular de certificado ou representante legal liberar formalmente como descrito na seção 9.4.1.

9.4.4 Responsabilidade de proteção de informação considerada privada

A AC UFSC é responsável pela proteção de qualquer informação considerada privada.

9.4.5 Aviso e consentimento para uso de informação privada

As entidades envolvidas devem consentir formalmente, por escrito, a utilização e divulgação de qualquer informação considerada como privada.

9.4.6 Circunstâncias para revelação de informações confidenciais em processos judiciais e administrativos

Não estipulado.

9.4.7 Outras circunstâncias para revelação de informações

Não estipulado.

9.5 Direitos de Propriedade Intelectual

Será observado a legislação institucional ou local vigente atualmente disponível.

9.6 Representações e Garantias

9.6.1 Garantias de ACs

Não estipulada.

9.6.2 Garantias de ARs

Não estipulada.

9.6.3 Garantias de titulares

Não estipulada.

9.6.4 Garantias de entidades confiantes

Não estipulada.

9.6.5 Garantias de outros participantes

Não estipulada.

9.7 Renúncia das Garantias

Não se aplica.

9.8 Limitações das Responsabilidades

Não estipulada.

9.9 Indenização

Não estipulada.

9.10 Finalização

9.10.1 Prazo de Validade

Esta DPC entra em vigor no momento da sua publicação e é válida até que uma nova DPC seja publicada ou seja revogada por determinação explícita do responsável pela AC UFSC.

9.10.2 Finalização

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.

9.10.3 Efeitos do finalização e Provisões Remanecentes

Os certificados emitidos no período de validade de uma DPC permanecem sujeitos às suas determinações até o final do período de validade do certificado.

9.11 Notificações individuais e comunicações com participantes

As notificações serão feitas por e-mail.

9.12 Emendas

9.12.1 Procedimento para emendas

Compete à AC UFSC propor alterações à PC/DPC. A nova versão resultante das alterações deve ser encaminhada ao CG para aprovação. O nome do arquivo da nova versão da PC/DPC no repositório da AC UFSC deve seguir a convenção de nomenclatura definida no anexo **??**.

9.12.2 Período e mecanismo de notificação

O surgimento de novas versões da DPC será devidamente noticiado no repositório da AC UFSC. como descrito na Seção 2.1.

9.12.3 Circunstâncias nas quais o identificador de objeto deve ser modificado

Sempre que surgirem novas versões, o identificador de objeto será mudado.

9.13 Procedimentos para a Resolução de Disputas

Não estipulado.

9.14 Leis Governamentais

A AC UFSC respeita a Legislação vigente no país.

9.15 Conformidade com leis aplicáveis

Não estipulado.

9.16 Provisões Diversas

9.16.1 Concordância completa

Não estipulado.

9.16.2 Delegação de direitos e obrigações

Não estipulado.

9.16.3 Acordo entre as partes em caso de revogação de cláusula pela justiça

Não estipulado.

9.16.4 Responsabilidades relacionadas a encargos jurídicos

Não estipulado.

9.16.5 Força maior

Não estipulado.

9.17 Outras Provisões

Não estipulado.

9.18 Referências

[FIPS1402] National Institute of Standards and Technology, Security Requirements for Cryptographic Modules, FIPS 140-2, Março 2001.

[ICPEDU06] Comitê Técnico de Políticas daCriptográficos da ICPEDU, 2005. ICPEDU, Padrões e Algoritmos

[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.

[RFC3280] R. Housley, W. Polk, W. Ford, D. Solo, Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 3280, Abril 2002. http://www.ietf.org/rfc/rfc3280.txt

[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/rfc

[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 3647, Novembro 2003. http://www.ietf.org/rfc/rfc5280.txt

Apêndice A

Formatos de dados

A.1 Formato do Distinguished Name

A Tabela A.1 apresenta do nome distinto (DN) dos certificados emitidos pela AC UFSC. Para garantir a interoperabilidade dos certificados digitais com as mais diversas aplicações, fica proíbido o uso de caracteres de acentuação no *Distinguished Name* dos certificados.

	Usuário	**Serviço**	**Autoridade Certificadora**
C	BR	BR	BR
ST	SC	SC	SC
L	Florianopolis	Florianopolis	Florianopolis
O	UFSC	UFSC	UFSC
O	ICPEDU	ICPEDU	ICPEDU
OU	usuario	hostname	Autoridade Certificadora
CN	nome usuário	nome servidor (FDQN)	nome da AC

Tabela A.1: Distinguished Name

A.2 Formato do certificado

A.2.1 Atributos básicos

Os atributos básicos dos certificados estão descritos na Tabela A.2.

	nome atributo	**descrição atributo**	valor
conteúdo	`version`	versão do padrão X.509	v3
	`serialNumber`	número serial do certificado	diferente para cada cert
	`signature`	algoritmo de assinatura	Sha1WithRSAEncryption
	`issuer`	emissor, sempre uma AC	DN da AC.
	`validity`	intervalo de validade	validade em anos, conforme solicitação da AC.
	`subject`	titular do certificado	DN do titular.
	`subjectPublicKeyInfo`	chave pública	diferente para cada certificado.
	`issuerUniqueID`	não é usado	
	`subjectUniqueID`	não é usado	
	extensions	extensões, discutidos na Seção 7.1.2	
envelope	`signatureAlgorithm`	algoritmo de assinatura	Sha1WithRSAEncryption.
	`signatureValue`	valor da assinatura	diferente para cada certificado.

Tabela A.2: Atributos básicos dos certificados

A.2.2 Extensões

Para certificados de usuários e de serviços:

- Basic Contraints: crítica, CA:false.
- Subject Key Identifier: não-crítica, contém o resumo criptográfico da chave pública do próprio certificado.
- Key Usage: crítica, Digital Signature, Non-repudiation e Key Encipherment.
- Certificate Policies: não-crítica, especifica o identificador de objeto da PC/DPC da AC UFSC e o atributo id-qt-cps com a URL desta PC/DPC: http://ac.ufsc.br/repositorio/dpc-ac-ufsc.pdf
- CRL Distribution Points: não crítica, contém a URL da LCR da AC UFSC: http://ac.ufsc.br/repositorio/acufsc.crl
- Subject Key Identifier: não-crítica, contém o resumo criptográfico da chave pública do certificado.
- Authority Key Identifier: não-crítica, contém o resumo criptográfico da chave pública da AC UFSC.

- Nos certificados de usuários o campo Subject Alternative Name deve ter a entrada RFC822 Name contendo o e-mail do usuário.

Para certificados de autoridades certificadoras:

- Basic Contraints: crítica, CA:true.
- Subject Key Identifier: não-crítica, contém o resumo criptográfico da chave pública do próprio certificado.
- Key Usage: crítica, Certificate Signing e CRL Signing.
- Certificate Policies: não-crítica, especifica o identificador de objeto da PC/DPC da AC UFSC e o atributo id-qt-cps com a URL desta PC/DPC: http://ac.ufsc.br/repositorio/dpc-ac-ufsc.pdf.
- CRL Distribution Points: nãao crítica, contém a URL da LCR da AC UFSC: http://ac.ufsc.br/repositorio/acufsc.crl.
- Subject Key Identifier: não-crítica, contém o resumo criptográfico da chave pública do certificado.
- Authority Key Identifier: não-crítica, contém o resumo criptográfico da chave pública da AC UFSC.

O texto a ser colocado na extensão de políticas de certificado é o seguinte: Este certificado é para uso exclusivo dos usuários e aplicações internas da UFSC. Utilize certificados ICP-Brasil caso seja necessário assinar documentos eletrônicos com eficácia jurídica.

A.3 Formato da Lista de Certificados Revogados

A Tabela A.3 apresenta as extensões e respectivas entradas da LCRs emitidas.

Tabela A.3: Extensões da LCR.

Extensão	**Crítica**	**Conteúdo**
authorityKeyIdentifier	sim	hash da chave pública da AC UFSC
crlNumber	sim	contém um número seqüencial para cada LCR emitida

A.4 Restrições para nomes

Descrição Código NBR9611 (hexadecimal), outros símbolos permitidos.

Símbolo	Descrição	Código
	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