UNIVERSIDADE FEDERAL FLUMINENSE

DANIEL CORDEIRO MARQUES

DESENVOLVENDO POLÍTICAS E PRÁTICAS CONFIÁVEIS DE CERTIFICAÇÃO DIGITAL

NITERÓI

2010

UNIVERSIDADE FEDERAL FLUMINENSE

DANIEL CORDEIRO MARQUES

DESENVOLVENDO POLÍTICAS E PRÁTICAS CONFIÁVEIS DE CERTIFICAÇÃO DIGITAL

Trabalho submetido ao Curso de Bacharelado em Ciência da Computação da Universidade Federal Fluminense como requisito parcial para a obtenção do título de Bacharel em Ciência da Computação. Área de concentração: Segurança da Informação.

Orientador:
Prof. PhD. EUGENE FRANCIS VINOD REBELLO

NITERÓI

2010

Ficha Catalográfica elaborada pela Biblioteca da Escola de Engenharia e Instituto de Computação da UFF

M357 Marques, Daniel Cordeiro

Desenvolvendo políticas e práticas confiáveis de certificação digital / Daniel Cordeiro Marques. – Niterói, RJ : [s.n.], 2010.

227 f.

Trabalho (Conclusão de Curso) – Departamento de Computação, Universidade Federal Fluminense, 2010.

Orientador: Eugene Francis Vinod Rebello

1. Segurança da Informação. 2. Autoridade certificadora. 3. Certificação Digital. 4. Ciência da Computação. I. Título.

CDD 005.8

Desenvolvendo Políticas e Práticas Confiáveis de Certificação Digital

Daniel Cordeiro Marques

Trabalho submetido ao Curso de Bacharelado em Ciência da Computação da Universidade Federal Fluminense como requisito parcial para a obtenção do título de Bacharel em Ciência da Computação.

Aprovada por:

Prof. PhD. Eugene Francis Vinod Rebello / IC-UFF
(Presidente)

Profa. D.Sc. Aline de Paula Nascimento / IC-UFF

Prof. PhD. Célio Vinicius Neves de Albuquerque / IC-UFF

D.Sc. Jacques Alves da Silva / IC-UFF

Niterói, 09 de julho de 2010.

"Um campeão é aquele que se levanta,
mesmo quando ele não pode".
Jack Dempsey.

Agradecimentos

De todo o trabalho, essa provavelmente foi a parte mais difícil de escrever. Tantas pessoas me apoiaram e participaram ativa ou passivamente durante minha formação, que seria impossível citar cada um aqui. Peço que me desculpe, caso seu nome não esteja aqui. Meus mais sinceros agradecimentos:

Primeiramente a Deus, em todas as suas formas e nomes, e ao meu Padrinho, por todas as oportunidades de crescimento que surgem em minha vida.

Aos meus pais, Decio e Deise, por todo sacrifício que fizeram para que eu recebesse educação de qualidade inquestionável, possibilitando a minha formação pessoal e profissional. Sem eles e seu apoio incondicional em todos os momentos da minha vida, nada disso seria possível. Amo muito vocês.

A minha avó Licinia por todo apoio e carinho nas horas de dificuldade. Ao meu avô Djalma pelos valiosos conselhos e pela companhia inseparável nos jogos do nosso querido Fluminense (que com certeza colaboraram enormemente como válvula de escape para a correria do dia-a-dia). E é claro, minha avó Elza, por sempre ter uma palavra de otimismo nos momentos em que nada parecia dar certo.

A minha irmã Andrea por estar sempre presente, estimulando e nunca me deixando desistir. Aos meus sobrinhos Matheus e Lucas, por nunca me fazerem esquecer o lado divertido da vida. E é claro, ao meu cunhado Márcio pelos papos mais diversos na mesa do almoço.

Aos meus tios-avós Ronaldo e Talita, pelo carinho enorme e pelo suporte espiritual, sempre me oferecendo algo positivo.

A minha querida namorada Renata, pela paciência, carinho e compreensão excepcionais enquanto eu escrevia esse trabalho. Seu apoio foi determinante para que esse texto pudesse ser terminado.

Aos meus amados amigos Thiago Siqueira e Vanessa Maia, fiéis companheiros que me apoiaram nos momentos mais difíceis, me ajudando a superar os mais diversos desafios e obstáculos. Estejam certos da sua importância no meu crescimento pessoal.

A minha amiga Beatriz Motta, pela ajuda nos cálculos da vida e com o Latex, além dos ouvidos sempre disponíveis e conselhos mil.

A amiga Cristiane Vidal pelas conversas, apoio e risadas incontáveis.

A querida Agatha Hencsey, que acompanhou boa parte da luta em busca da graduação e que sempre apoiou e torceu pela realização dos meus sonhos e projetos pessoais.

A toda Turma 204.31, minha família durante toda a graduação. Jamais esquecerei vocês. Meu muito obrigado também à Karen Valente, Leonardo Quirino, Carol Cruz e Clayton Reis, que assumiram importante papel durante a minha formação na UFF.

Ao amigo Daniel Souza, eterno colaborador e parceiro de trabalhos.

A toda equipe do SGCLab, onde passei a maior parte da minha vida acadêmica, desenvolvendo esse e tantos outros projetos. Em especial, meu muito obrigado aos amigos Alexandre Sena e Aline Nascimento, pelos valiosos conselhos; Henrique Bueno, Carlos Henrique "Bill" Nicodemus, Eduardo "Satan" Ramos e Sean Crammond, grandes amigos e companheiros. E é claro, o grande Felipe "Xoxó" Ribeiro, pela enorme paciência ao me ajudar com Física XX. Agradeço também ao nosso querido Jacques Alves da Silva, sem o qual nenhum trabalho desenvolvido no laboratório da Pós-Graduação do IC/UFF seria minimamente possível.

Ao pessoal da Pós-Graduação em Computação do IC/UFF, em especial meus amigos Luciene Motta e Diego Brandão, apoio indispensável para que esse trabalho fosse finalizado.

Aos companheiros do GT-ICPEDU, em especial: André Marins, André Landim, Beatriz Zoss, Jonathan Kohler, Iara Machado, Marcelo Carlomagno e professor Ricardo Custódio. Por todo conhecimento adquirido durante a minha participação no GT.

Ao professor Marcos Machado, pelos ensinamentos e conversas, e a todos os companheiros da Equipe Boxe Thai - Athivação, cujo alto astral no treino me dá forças para continuar lutando no dia-a-dia.

Aos funcionários do IC/UFF, em especial: Carlinhos, Marister, Mateus, Thiago, Rafael e Carlos pela eterna boa vontade com todos os alunos que precisam de alguma ajuda.

Aos professores do IC/UFF, em especial: Anna Dolesji, Célio Albuquerque, Cristina Boeres e Simone Martins, pelo carinho, respeito e pelo exemplo a ser seguido na docência.

Por fim, mas não menos importante, agradeço ao meu orientador, o professor Vinod Rebello. Primeiramente, por ter acreditado em um aluno, na época de CR baixo, com

nada, além de vontade de aprender. Em segundo lugar, por ter sido muito mais que um orientador, mas um amigo e mentor dos mais pacientes. Jamais esquecerei todo apoio que me foi dado, principalmente nos momentos de maior dificuldade.

Muito obrigado. Espero um dia poder retribuir da mesma forma tudo o que vocês todos fizeram por mim.

Este trabalho é dedicado ao meu grande irmão Arthur, que infelizmente não pode compartilhar em vida esse momento comigo, e ao meu afilhado Arthurzinho, muito querido por todos nós.

Daniel.

Resumo

Certificados digitais estão se tornando uma popular solução de segurança para transações eletrônicas, especialmente com o crescimento do comércio eletrônico no mundo. Entretanto, a tecnologia por si só não é suficiente; é necessário estabelecer um conjunto de políticas e práticas confiáveis para suportar sua utilização. Um dos maiores desafios no gerenciamento de serviços de certificação digital é elaborar documentos de Política de Certificado (PC) e Declaração de Prática de Certificação (DPC). Fornecer aos usuários informações suficientes para decidir se devem ou não confiar em uma Autoridade Certificadora não é trivial: do lado da Autoridade Certificadora (AC), o que constitui uma política ou prática confiável? Do ponto de vista do usuário, que critérios o ajudam a estabelecer se as informações fornecidas por uma AC são ou não confiáveis? Este trabalho propõe um conjunto de critérios a ser utilizado tanto por autores de PCs e DPCs quanto por usuários fornecendo informações para elaboração e avaliação de políticas e práticas confiáveis, no contexto de uma Infraestrutura de Chaves Públicas Educacional de âmbito nacional.

Palavras-chave: Infraestrutura de Chaves Públicas, Segurança da Informação, Gerenciamento de Confiança, Políticas de Certificado

Abstract

Digital certificates are becoming a popular security solution for electronic transactions, especially with the growth of e-commerce around the world. However, technology in itself is not sufficient; it is necessary to establish a set of trustworthy policies and practices to support their use. One of the major challenges in managing digital certification services is to prepare Certificate Policies (CP) and Certification Practice Statements (CPS). Provide users with enough information to decide whether to trust a Certificate Authority is not trivial: for the Certification Authority (CA), what would constitute a reliable policy or practice? From the standpoint of the user, what criteria can help determine whether a information provided by a CA can be trusted or not? This work proposes a set of criteria to be used by both authors of CP/CPS documents and certificate users by providing information for design and evaluation of trustworthy policies and practices, in the context of a national educational public key infrastructure.

Keywords: Public key Infrastructure, Information Security, Trust Management, Certificate Policies

Palavras-chave

1. Infraestrutura de Chaves Públicas
2. Políticas de Certificado
3. Gerenciamento de Confiança
4. Segurança da Informação

Glossário

AC	:	Autoridade Certificadora;
AGP	:	Autoridade de Gerência de Políticas;
AES	:	Advanced Encryption Standard;
AR	:	Autoridade de Registro;
CG	:	Comitê Gestor;
CFM	:	Conselho Federal de Medicina;
DES	:	Data Encryption Standard;
DPC	:	Declaração de Prática de Certificação;
IC	:	Instituto de Computação;
ICP	:	Infraestrutura de Chaves Públicas;
ICP-Brasil	:	Infraestrutura de Chaves Públicas Brasileira;
ICPEDU	:	Infraestrutura de Chaves Públicas para Ensino e Pesquisa;
Ifes	:	Instituições Federais de Ensino;
LCR	:	Lista de Certificados Revogados;
MD5	:	Message-Digest algorithm 5;
NIST	:	National Institute of Standards and Technology;
PC	:	Política de Certificado;
PCI DSS	:	Payment Card Industry Data Security Standard;
PGP	:	Pretty Good Privacy;
PS	:	Política de Segurança;
RFC	:	Request for Comments;
RNP	:	Rede Nacional de Ensino e Pesquisa;
SHA	:	Secure Hash Algorithm;
SGSI	:	Sistema de Gerenciamento de Segurança da Informação;
SPKI	:	Simple Public Key Infraestructure;
SRF	:	Secretaria de Receita Federal;
UFF	:	Universidade Federal Fluminense;
UP	:	Unidade de Pesquisa;
VPN	:	Virtual Private Networks;

Conteúdo

Lista de Figuras

Lista de Tabelas

Capítulo 1

Introdução

É notável o rápido avanço nas tecnologias da informação e comunicação (TIC), permitindo a disponibilização de cada vez mais informações on-line. Entretanto, o valor estratégico de alguns desses dados não pode ser descartado; alguns são essenciais para o ganho de produtividade, redução de custos e ampliação do valor do produto. No meio acadêmico, os resultados das pesquisas precisam ser mantidos consistentes, enquanto devem estar disponíveis apenas para quem é autorizado a utilizá-los. Por outro lado, o usuário que fornece seus dados pessoais em um sistema Internet Banking, não deseja tê-los expostos em meios de comunicação abertos. Vê-se, portanto, uma enorme dependência da informação. Portanto, dada a importância desses dados no mundo moderno, garantir que estes serão mantidos em segurança é uma atividade crítica.

1.1 Princípios Básicos de Segurança da Informação

Sêmola (2003) define Segurança da Informação como "uma área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade". Ou seja: o objetivo principal é preservar três princípios básicos:

Disponibilidade: a informação deve estar disponível sempre que o usuário autorizado necessitar.

Confidencialidade: a informação deve estar disponível para acesso, criação e modificação apenas para o usuário autorizado.

Integridade: deve-se garantir que a informação é mantida nas mesmas condições disponibilizada pelo autor, mesmo que não estejam corretas.

Dessa forma, a Segurança da Informação deve permitir a minimização dos riscos que causem a quebra de um desses princípios. Além disso, deve ser mantidos certos controles sobre a informação, a fim de se assegurar alguns aspectos básicos associados aos princípios citados anteriormente:

Autorização: um usuário deve ser autorizado a acessar aquela informação, de acordo com o seu nível de privilégio, apenas após sua correta identificação e autenticação.

Auditoria: é preciso garantir que o uso da informação seja passível de análise, possibilitando descobrir quem a acessou e quando, por exemplo.

Autenticidade: deve ser possível garantir que os participantes de uma comunicação são realmente quem dizem ser.

Irretratabilidade (não-repúdio): deve ser possível identificar de forma única o autor da informação, que não poderá rejeitar a atividade sobre ela.

Para que seja possível manter os princípios básicos e seus aspectos associados, é preciso observar que não se trata apenas da tecnologia. Uma boa estratégia de Segurança da Informação considera pessoas, processos e fatores tecnológicos de forma global e equilibrada. Para tanto, é necessário estabelecer um conjunto de políticas e práticas que guiem as atividades envolvendo as informações, garantindo que sejam feitas de forma correta e segura.

1.2 Conformidade com padrões e requisitos legais

Há ainda a questão da conformidade com os padrões e requisitos legais. O PCI Security Standards Council[1] estabeleceu uma série de padrões para garantir a segurança de dados dos clientes de cartões de crédito, como o Data Security Standard. O PCI DSS compreende um conjunto de requisitos básicos que as operadoras de cartão de crédito devem seguir, para garantir a segurança dos seus dados. Entre eles, há a necessidade de

[1] O PCI Security Standards Council, fundado pela American Express, Discover Financial Services, JCB International, MasterCard Worldwide e Visa Inc., é responsável pelo desenvolvimento, gerenciamento, educação e conscientização sobre os Padrões de Segurança da indústria de pagamento utilizando cartões.

utilizar criptografia para transmissão de dados e um sistema de gestão de identidades e autenticação para os usuários dos sistemas financeiros. O não cumprimento desses requisitos acarreta em sanções que variam de multas ao descredenciamento do estabelecimento comercial.

No Brasil, o Conselho Federal de Medicina (CFM) determina, em sua Resolução nº. 1.821/2007(CFM, 2007), normas técnicas sobre a digitalização e uso de sistemas informatizados para guarda e manuseio de prontuários, onde exige a utilização de certificados e assinaturas digitais para este fim. Além disso, a Secretaria de Receita Federal (SRF) instituiu a Instrução Normativa nº. 695/06 (SRF, 2006), que impõe o uso de certificados digitais para a entrega de declaração de Pessoas Jurídicas.

Nesse contexto, Infraestruturas de Chaves Públicas (ICPs) têm-se tornado populares, por apresentarem uma solução de autenticação flexível, possibilitando a conformidade com os mais diversos padrões e regulamentações que exigem a utilização de sistemas com forte esquema de autenticação, e um melhor controle sobre as identidades dos usuários. ICPs fornecem mecanismos que permitem garantir a preservação dos princípios básicos de segurança. Através da criptografia, é possível proteger as informações contra acessos não autorizados; certificados digitais e assinaturas digitais, por exemplo, permitem a identificação de usuários e do emissor de uma mensagem. O assunto é abordado com mais clareza no capítulo 2.

1.3 Objetivos do trabalho

O componente principal de uma Infraestrutura de Chaves Públicas é a Autoridade Certificadora. Ela é responsável por emitir os certificados digitais usados para a identificação de usuários, recursos ou serviços. Sua função é agir como uma âncora de confiança, estabelecendo uma relação confiável entre duas entidades que, normalmente, não se conhecem previamente.

Do ponto de vista do usuário, entretanto, é preciso determinar em que Autoridade Certificadora (AC) confiar, e para quais aplicações, tanto para ter seu certificado emitido quanto para aceitar o de outro usuário. Do lado da AC, é necessário estabelecer políticas e práticas que forneçam um serviço de certificação digital de qualidade, e possibilitem aos usuários optar pelos seus certificados.

O objetivo desse trabalho é fornecer um conjunto de requisitos que permita às Autori-

dades Certificadoras estabelecerem políticas e práticas confiáveis, baseadas em padrões já consolidados de segurança da informação e certificação digital, e fornecer aos usuários de certificados digitais critérios para decidir se devem ou não confiar nos certificados emitidos por elas.

1.4 Organização do trabalho

Este trabalho está organizado da seguinte forma: o segundo capítulo apresenta os conceitos fundamentais de Infraestruturas de Chaves Públicas (ICP). São abordados temas como criptografia de chaves simétrica e assimétrica, assinaturas digitais, quem são os participantes de uma ICP e seu papel na infraestutura, modelos de confiança e possíveis aplicações. O terceiro capítulo apresenta trabalhos relacionados ao tema, servindo de base para este trabalho ou como uma possibilidade de aplicação. O quarto capítulo trata da definição de políticas e práticas, apresentando a metodologia utilizada para a definição de requisitos estabelecidos para apoiar a elaboração de documentos confiáveis, e mostra também um estudo de caso onde os requisitos desenvolvidos foram aplicados. O quinto e último capítulo conclui o trabalho, apresentando também uma breve sugestão de trabalhos futuros.

Três apêndices são fornecidos. No apêndice A, o relatório técnico *Mapeamento entre Padrões de Certificação Digital e Segurança da Informação e a RFC 3647* foi adicionado na íntegra, fornecendo o mapeamento completo entre os documentos utilizados como referência e a RFC 3647 (CHOKHANI et al., 2003). O apêndice B traz um template para apoiar a atividade de elaboração de documentos de PC/DPC, utilizados para fornecer aos usuários informações sobre as políticas e práticas adotadas pela AC para gerenciar o ciclo de vida dos certificados emitidos. O apêndice C apresenta os critérios fornecidos aos revisores de PC/DPC para avaliação desses documentos.

Capítulo 2

Infraestruturas de Chaves Públicas

Este capítulo trata os conceitos fundamentais sobre Infraestrutura de Chaves Públicas (ICPs), abordando temas como as motivações para sua existência, os elementos que a compõe e introduzindo a importância das políticas e práticas para estabelecimento da relação de confiança entre Autoridade Certificadora (AC) e usuários de certificado.

2.1 Noções gerais de criptografia

Desde os tempos antigos, o homem deseja manter suas informações a salvo de modificações ou consultas indesejadas. Dessa necessidade, surgiu a Criptografia, a ciência de escrever uma determinada mensagem (que nos tempos atuais não incluem apenas texto, mas imagens, sons e outros objetos digitais) de forma cifrada, tornando-o legível apenas para o destinatário capaz de decifrá-lo.

Conforme observado por Menezes, Oorschot e Vanstone (2001), o objetivo principal da Criptografia é tratar quatro características da Segurança da Informação vistas anteriormente: confidencialidade, integridade, autenticação e irretratabilidade (ou não-repúdio). As técnicas utilizadas para alcançar esse objetivo são explicadas nas seções que seguem sem, no entanto, se aprofundar no assunto. Caso seja desejável conhecer mais sobre o tópico, as leituras de (SCHNEIER, 1996) e (MENEZES; OORSCHOT; VANSTONE, 2001) são recomendadas.

Além da mensagem a ser cifrada, uma chave também é passada como parâmetro aos algoritmos criptográficos. A chave é o dado que especifica como a transformação de mensagem limpa para cifrada ocorrerá. Seu tamanho pode variar e, ao estabelecê-lo, o risco de exposição das informações protegidas deve ser considerado. De acordo com a utilização

dessas chaves, existem duas categorias de mecanismos para cifrar uma mensagem: criptografia de chave simétrica e de chave assimétrica (ou de chave pública). Combinada ao conceito de *hashing*, é possível garantir também a autenticidade das mensagem utilizando assinaturas digitais, conforme será visto mais adiante.

2.1.1 Criptografia de Chave Simétrica

A criptografia de chave simétrica é a forma clássica de troca de informações cifradas. Emissor e Receptor da mensagem utilizam uma mesma chave secreta para cifrá-la e decifrá-la.

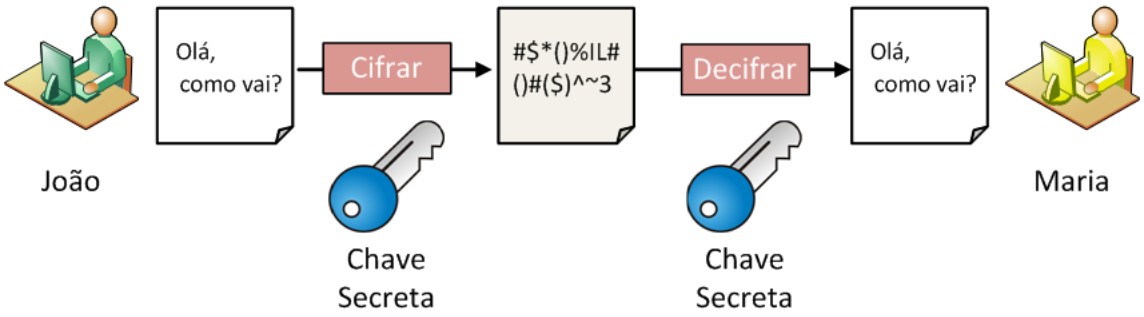

Figura 2.1: Criptografia de Chave Simétrica.

No exemplo acima, João deseja enviar uma mensagem secreta para Maria. Para isso, João cifra o conteúdo da mensagem utilizando uma chave, que compartilha com Maria, e a envia. Maria, então, utiliza essa mesma chave para decifrar a mensagem e ter acesso ao conteúdo.

Apesar de simples, esse tipo de abordagem apresenta alguns problemas fundamentais. Não é possível garantir se João foi realmente o emissor, pois a mesma chave é compartilhada pelos dois. Portanto, não é possível garantir a irretratabilidade (não-repúdio) na comunicação. Isso pode ser um contratempo, em um cenário onde dois usuários não se conhecem previamente (como um servidor web que envia uma mensagem ao usuário, mas o usuário não consegue se certificar de que aquele é realmente o servidor certo). Para que a irretratabilidade seja garantida, é preciso que cada grupo de usuários possua sua própria chave secreta, tornando a solução pouco escalável: supondo um grupo de aproximadamente 300 (trezentos) usuários, cada par de usuários que deseja estabelecer uma comunicação segura necessitará de uma chave secreta distinta das outras. No pior caso, em que um usuário deseja se comunicar com todos os outros, é necessário que este gerencie

300 chaves secretas (isto é, duzentas e noventa e nove chaves, além da sua).

Há também a necessidade de transmitir a chave secreta para o receptor (no exemplo anterior, Maria) sem expô-la a terceiros. Um indivíduo malicioso com intenção de alterar a mensagem pode fazê-lo, caso tenha acesso a chave, e reenviá-la para Maria, sem que essa perceba a modificação.

Alguns exemplos de algoritmos de chave simétrica são: *Data Encryption Standard* (DES) (NIST, 1999), seu sucessor o *Advanced Encryption Standard* (AES) (DAEMEN; RIJMEN, 2002) e o *Blowfish* (SCHNEIER, 1994).

2.1.2 Criptografia de Chave Assimétrica

Em 1976, W. Diffie e M. E. Hellman apresentaram um novo método para a troca de informações cifradas: a criptografia de chave assimétrica. O emissor agora possui um par de chaves relacionadas, porém distintas. Uma das chaves é usada para cifrar, enquanto a outra é utilizada para decifrar a mensagem.

O objetivo desta distinção entre as chaves é tornar inviável computacionalmente a obtenção de uma chave a partir de seu respectivo par. Essa propriedade permite a disponibilização de uma delas publicamente para os emissores (sendo chamada, portanto, de Chave Pública). A outra, que deve ser conhecida apenas pelo dono do par de chaves (receptor da mensagem), é chamada de Chave Privada.

A figura 2.2 exemplifica a comunicação utilizando a criptografia assimétrica. Maria envia sua chave pública (Pub) para João, que a utilizará para cifrar a mensagem. Maria, então, utiliza a chave privada (Priv) relacionada para decifrar a mensagem. Como a chave privada (Priv) é de posse exclusivamente de Maria, é possível garantir que apenas ela terá acesso ao conteúdo da mensagem.

Para garantir a autenticidade da mensagem, um processo semelhante pode ser seguido: João cifra a mensagem com sua chave privada e envia a Maria. De posse da chave pública de João, Maria pode decifrar a mensagem e se certificar de que está se comunicando com o João certo.

Entretanto, ainda existem problemas relacionados à distribuição segura das chaves. Um terceiro pode interceptar a chave pública de Maria, e enviar sua própria a João. Esse tipo de ataque, conhecido como *Man-in-the-middle*: João, então, passaria a enviar as mensagens cifradas para o terceiro, acreditando ser para Maria.

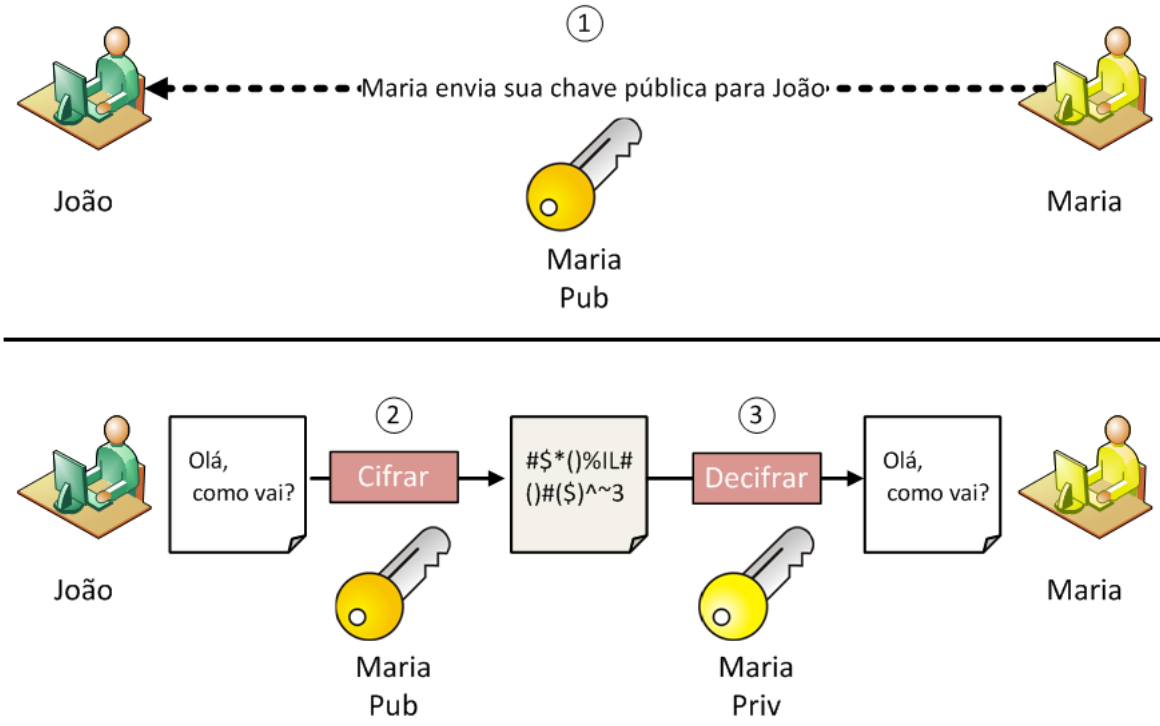

Figura 2.2: Criptografia de Chave Assimétrica.

Nota-se, então, que há a necessidade de um repositório seguro de chaves públicas. O invés de receber a chave pública do receptor, o emissor precisa apenas resgatá-la e seguir os procedimentos normais. Contudo, isso só é verdade se as partes envolvidas na comunicação confiarem no repositório. Além disso, como um usuário pode confiar que o outro é realmente quem diz ser? Em comunicações onde não há conhecimento prévio entre as partes, essa questão ainda não pode ser respondida com absoluta certeza. O gerenciamento dessa confiança é, todavia, complexo; e da necessidade de gerenciar essa relação de confiança, surgem as infraestruturas de chaves públicas, tratadas nesse capítulo.

O mais conhecido algoritmo de chave assimétrica (ou de chave pública) é o RSA, apresentado por Rivest, Shamir e Adleman em 1978, e usado em diversas aplicações de comercio eletrônico e transações bancárias.

2.1.3 Funções de Resumo (Hash)

(BINDER, 2004) define a aplicação de uma função resumo como “o método usado para obter uma "impressão digital"de uma dada mensagem, que pode ser usada para verificar sua integridade, mas não para reproduzi-la” (Figura 2.3). Isso é possível graças a duas propriedades das funções de resumo:

Uma dada entrada gera sempre a mesma saída: Uma mensagem dada como entrada de uma função resumo deve gerar o mesmo hash. Portanto, qualquer alteração na mensagem resultará em um hash diferente.

A função resumo deve funcionar em apenas uma direção: A partir de um hash, não deve ser possível obter a mensagem.

Figura 2.3: Geração de *hash* (BINDER, 2004).

Exemplos de algoritmos hash incluem o *Message-Digest algorithm 5* (MD5) - cuja possibilidade de utilizar colisões para obter a mensagem já foi comprovada em (WANG; YU, 2005) - desenvolvido por Ron Rivest; a família *Secure Hash Algorithm* (SHA), desenvolvida pela Agência de Segurança Nacional Norte-americana (*National Security Agency* - NSA) e o *Whirlpool*, desenvolvido por Vincent Rijmen e pelo brasileiro Paulo S. L. M. Barreto.

2.1.4 Assinaturas Digitais

Assinaturas digitais combinam criptografia de chave pública com funções de resumo, a fim de prover autenticação das mensagens. A figura apresenta o processo para assinar digitalmente uma mensagem.

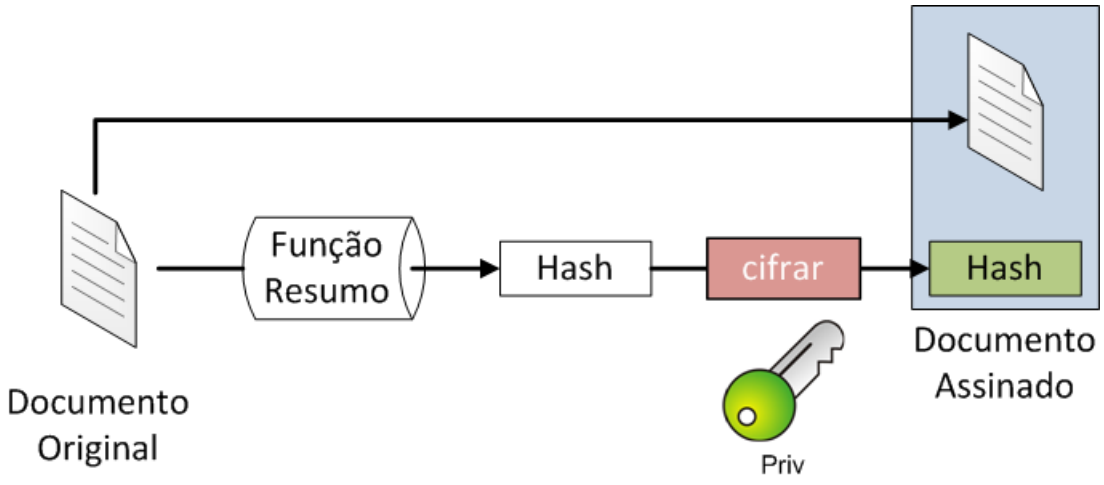

Figura 2.4: Assinando digitalmente um documento.

Um *hash* do documento é gerado por uma função resumo qualquer. Esse *hash* é então cifrado utilizando a chave privada de João, criando a assinatura digital. A assinatura é anexada à mensagem original, e enviada. Maria, então, separa a assinatura da mensagem pura e gera um *hash* da mesma. Ao decifrar a assinatura com a chave pública de João, Maria é capaz de comparar os *hashes* obtidos e verificar se são idênticos (figura 2.5). Em caso afirmativo, três propriedades podem ser verificadas:

- **Autenticidade:** Como o *hash* foi cifrado utilizando-se a chave privada de João, apenas sua chave pública relacionada é capaz de decifrá-la. Dessa forma, Maria sabe que foi realmente enviada por João.
- **Irretratabilidade:** Analogamente, apenas João poderia ter assinado a mensagem, pois só é possível para Maria verificar o *hash* usando a chave pública de João.
- **Integridade:** Como o *hash* gerado originalmente é idêntico ao obtido durante a verificação, sabe-se que a mensagem não foi alterada durante a transmissão.

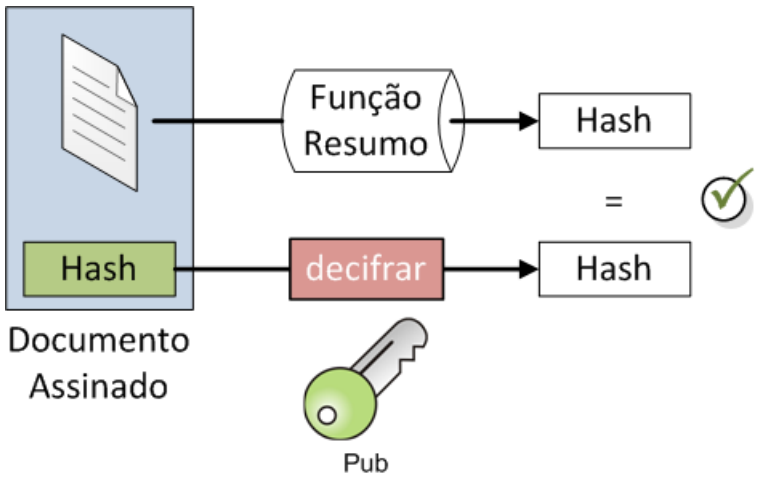

Figura 2.5: Verificando a assinatura do documento.

Portanto, nota-se que a idéia principal da assinatura digital é a mesma de uma assinatura de próprio punho.

2.2 Certificados Digitais

Certificados Digitais (tratados aqui apenas como "certificados"a partir de agora) são estruturas contendo informações do detentor de uma chave pública. Sua função é garantir que uma entidade é dono de um par de chaves, pois estabelece uma relação de um-para-um

entre o titular do certificado e a chave pública correspondente. Dessa forma, age como um documento digital, identificando pessoas, recursos ou serviços.

Existem diversos tipos diferentes de certificados (ADAMS; LLOYD, 2002) como, por exemplo:

Certificados X.509: Certificados que seguem o padrão ITU-T Recommendation X.509, onde uma chave pública é relacionada a um Distinguished Name (Nome Distinto, português) único, verificado por Autoridade Certificadora. Os certificados X.509 são compostos por campos como, por exemplo: versão do certificado, número serial do certificado, assinatura do certificado, nome do titular e emissor do certificado, entre outros.

Certificados PGP (*Pretty Good Privacy*): Certificados onde o portador é identificado por um nome escolhido pelo próprio. Essa relação é corroborada por outros usuários, que assinam o certificado, formando uma Teia de Confiança (*Web of Trust*).

Certificados SPKI (Simple Public Key Infrastructure): São certificados cujo foco maior é a autorização e não a identificação, portanto, mais simples. Identifica o portador de um certificado apenas pela chave pública. Listas de Controle de Acesso (*Access Control Lists - ACL*) podem ser usadas para garantir autorização de uma chave a um serviço e informações do portador são solicitadas apenas se necessário.

Certificados de atributo: Certificados assinados por uma Autoridade Certificadora de atributos, que liga informação do seu portador a um conjunto de atributos.

Este trabalho foca essencialmente na utilização de certificados X.509 versão 3 (figura 2.6), conforme previsto na RFC 3280 (CHOKHANI et al., 2003), por ser atualmente o tipo de certificado utilizado com mais frequência. Entretanto, os requisitos aqui propostos podem ser úteis também para os demais tipos de certificado.

É importante notar que os certificados possuem um ciclo de vida, que vai desde sua emissão até o fim de sua validade. Isso ocorre por vários motivos, como possibilidade de mudanças nas informações que ele representa e os rápidos avanços tecnológicos, que podem acarretar na exposição da chave pública. Identifica-se então, mais uma necessidade: o gerenciamento desses certificados. Além disso, ainda há a necessidade de confiar na veracidade das informações presentes no certificado.

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=BR, O=ICPEDU, O=UFF BrGrid CA, CN=UFF Brazilian Grid Certification Authority
        Validity
            Not Before: Jul 11 17:46:58 2006 GMT
            Not After : Jul 11 17:46:58 2016 GMT
        Subject: C=BR, O=ICPEDU, O=UFF BrGrid CA, CN=UFF Brazilian Grid Certification Authority
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:f1:30:69:53:89:b4:da:d3:85:84:bf:bc:b1:b6:
                    ca:7a:8a:1c:d3:60:46:9b:78:32:cb:43:87:ee:4e:
                    7a:9e:99:03:1a:47:74:df:98:8d:af:17:27:e4:d6:
                    8e:f4:c0:98:2b:cb:0d:4b:ce:43:59:af:93:d6:0f:
                    60:f0:fb:3a:07:c3:86:bb:68:bb:32:3b:30:71:9d:
                    a6:88:b9:2a:f4:a0:97:a7:2b:77:ff:50:0a:ac:af:
                    c0:32:d9:58:35:58:9c:b8:51:49:a3:cb:38:8a:93:
                    87:ef:04:f7:d7:08:1e:76:f9:d9:f8:9e:0c:6e:20:
                    0c:be:70:3f:9d:33:90:40:c9:a9:22:7d:70:85:08:
                    6f:66:25:f8:19:40:0b:b7:d5:13:aa:0e:79:58:b7:
                    98:12:69:44:79:82:54:f6:a3:4a:fa:ac:3a:c3:76:
                    7f:3b:7e:55:32:3b:27:b4:eb:ab:78:9c:bb:99:d1:
                    6d:97:f9:ae:3f:90:ec:4a:b6:e2:60:bb:0c:79:13:
                    8c:99:1d:5e:e4:7c:91:8c:8c:68:5a:47:27:93:91:
                    e9:49:99:19:6e:fc:5d:f5:ae:6e:59:0e:e2:c5:a6:
                    c8:a8:ab:3a:c6:4e:1c:e8:59:d3:c9:74:6a:dc:cc:
                    01:c3:a4:c9:2b:57:e8:cb:c2:9d:89:b7:9e:6c:34:
                    28:8b
                Exponent: 65537 (0x10001)
```

Figura 2.6: Trecho de um certificado X.509.

2.3 Infraestruturas de Chaves Públicas (ICPs)

De acordo com o *National Institute of Standards and Technology*[1], Infraestruturas de Chaves Públicas (ICPs) relacionam chaves públicas a entidades, possibilitando que outras entidades verifiquem esses relacionamentos, e provendo os serviços necessários para o gerenciamento progressivo das chaves em um ambiente distribuído. Ou, de forma simplificada, uma ICP é o conjunto de softwares, hardwares, processos e pessoas que suportam o gerenciamento do ciclo de vida dos certificados.

Uma ICP é composta por diversos compontes, entre eles:

- **Autoridades Certificadoras (ACs)**, responsáveis pelo gerenciamento do ciclo de vida dos certificados.
- **Autoridades de Registro (ARs)**, responsáveis pela coleta e verificação de informações dos titulares de certificado.

[1] O *National Institute of Standards and Technology*(NIST) é agência nacional de tecnologia do governo norte-americano. O NIST contribui com a indústria desenvolvendo e aplicando tecnologias, métricas e padrões.

- **Titular de Certificado**, detentor da chave pública certificada pela AC.
- **Entidade Confiante**, que recebe um certificado e decide por confiar nele ou não.
- **Repositório**, onde as ACs disponibilizam certificados e informações relevantes aos titulares e entidades cofniantes.

O papel desses componentes na ICP é descrito a seguir.

2.3.1 Autoridades Certificadoras (AC)

Como visto anteriormente, existe a necessidade de garantir a identidade de um usuário, não conhecido previamente, durante uma transação. Em um ambiente com muitos usuários, muitas vezes geograficamente dispersos, essa questão pode ser um desafio. Como solução, uma Terceira Parte Confiável (TCP) surge para garantir a confiança entre as duas partes, de forma transitiva (Figura 2.7). Ou seja: Se João confia na TCP, que garante a veracidade na identidade fornecida por Maria, ele pode confiar também em Maria.

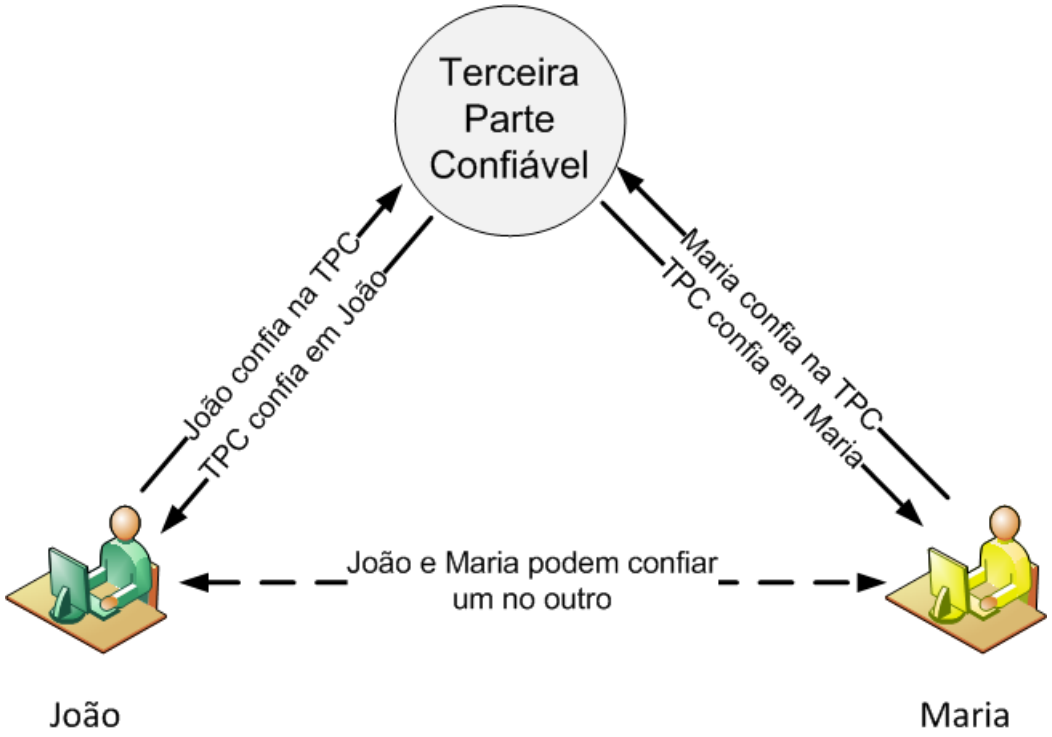

Figura 2.7: Relação de confiança estabelecida de forma transitiva.

Nesse sentido, o papel principal de uma Autoridade Certificadora (AC) é certificar que um determinado par de chaves é realmente relacionado a uma identidade. Na seção 2.2, essa relação pôde ser representada por uma estrutura: o certificado digital. O que

a AC faz, em termos gerais, é assinar essa relação (isto é, o certificado), assegurando a relação. Portanto, AC é responsável pela emissão (geração e assinatura) de certificados, manutenção do *status* de seus certificados, emissão de Listas de Certificados Revogados (LCRs) e manutenção de um arquivo de *status* dos certificados previamente emitidos.

Para facilitar a compreensão do papel de uma AC, pode-se fazer uma analogia relacionando AC e um cartório: Se uma pessoa deseja que seu documento (no caso da ICP, o certificado) seja amplamente aceito, ela solicita que um cartório o reconheça. Por ser de fé pública (ou seja, reconhecido por um grupo em geral), todos aqueles que confiam no cartório confiarão também no documento.

2.3.2 Autoridades de Registro (AR)

O NIST (2001) apresenta a Autoridade de Registro como uma entidade na qual a AC confia para registrar e autenticar os usuários para identificação na AC. Dessa forma, a responsabilidade da AR é reunir as informações fornecidas pelos usuários e analisá-las, a fim de garantir a sua validade. Com base nessa análise a AR deverá, então, decidir se deve ou não aceitar o credenciamento de um usuário. Em caso afirmativo, os dados coletados são encaminhados de forma segura à AC, para compor os campos do certificado. No caso de usuários finais, por exemplo, a AC pode solicitar um documento de identidade legalmente válido (passaporte, por exemplo) e uma forma de identificação funcional (como um crachá), para obter informações pessoais e de relacionamento com a unidade organizacional, respectivamente.

As atividades de identificação e autenticação dos usuários são as mais importantes no contexto de uma ICP. Portanto, a AR deve garantir que as informações fornecidas foram validadas corretamente e que o solicitante do certificado realmente possui a chave privada relacionada.

2.3.3 Repositórios

Os repositórios são diretórios usados pela AC para fornecer informações relevantes aos participantes da ICP. Nele estão disponíveis os certificados válidos, as Políticas de Certificado (PCs) e Declarações de Prática de Certificação (DPCs) da AC, as Listas de Certificados Revogados (LCRs), entre outros artefatos. Sua função principal é fornecer à AC uma forma de guardar, distribuir e gerenciar atualizações em certificados, além de

prover às entidades confiantes informações necessárias para verificar a validade de um certificado (MARQUES; REBELLO, 2008).

2.3.4 Titulares de Certificado

São aqueles cuja informação está contida no certificado, e detém a chave pública em questão. Titulares de Certificado não precisam ser apenas pessoas; podem também ser recursos (como um servidor), serviços (como um portal de comércio eletrônico) ou outras ACs.

2.3.5 Entidades Confiantes

As entidades confiantes são àquelas que recebem o certificado para uma aplicação, e verificam sua informação junto à AC. São, por exemplo, receptores de uma mensagem assinada digitalmente ou, ainda, o usuário de um servidor que aceita seu certificado para iniciar a comunicação.

Para decidir confiar em um determinado certificado, as entidades confiantes devem verificar alguns fatores:

Expiração do certificado: a entidade confiante deve verificar se o certificado recebido ainda está dentro do período de validade. Caso contrário, deve rejeitá-lo.

Lista de Certificados Revogados (LCR): a LCR é uma lista contendo os certificados revogados pela AC por motivos diversos. Entre eles, pode-se citar: comprometimento da chave privada do titular, inconsistência nas informações do certificado e não-cumprimento das políticas da AC.

Confiança na AC que emitiu o certificado: antes de aceitar um certificado, a entidade confiante deve verificar se confia na AC que o emitiu, e se foi realmente emitido por ela.

É importante notar que a AC confiável pode não ser diretamente relacionada ao certificado que se deseja verificar. A AC que o emitiu pode ser subordinada a AC confiável, ou distante desta por vários níveis. Nesse caso, é preciso obter diversos certificados até se chegar a AC confiável para, então, tomar a decisão de confiar no certificado ou não.

2.3.6 Caminhos de Certificação

Essa cadeia de certificados, iniciada com um certificado que pode ser validado por uma das âncoras de confiança[2] da entidade confiante, e terminada com o certificado a ser validado, é chamada de Caminho de Certificação (HOUSLEY et al., 2002), (COOPER et al., 2003).

Adams e Lloyd (2002) apresentam as duas principais fases para o processamento do caminho de certificação (ADAMS; LLOYD, 2002):

1. **Construção do caminho de certificação**, que envolve a aquisição de todos os certificados necessários para formar o caminho. A partir do certificado de quem se deseja verificar a validade, adquire-se os certificados de todas as ACs até a AC que atua como âncora de confiança (figura 2.8).
2. **Validação do caminho de certificação**, que envolve verificar as informações de cada certificado do caminho (validade, assinatura, etc.). Um algortimo para efetuar essa validação é proposto na RFC 3280 (HOUSLEY et al., 2002).

Um certificado só será aceito se as duas fases forem efetuadas com sucesso. É importante salientar que o caminho de certificação não deve crescer indiscriminadamente. Quanto maior a distância entre a âncora de confiança e o certificado sendo verificado, mais fraca será a relação de confiança entre eles. Isso acontece pois, a medida que se distancia da AC que serve de âncora de confiança, fica mais difícil garantir que os controles de gerenciamento do ciclo de vida dos certificados estão de acordo com as expectativas do usuário. Para evitar esse problema, a AC pode restringir o crescimento do caminho através de suas políticas ou, no caso de certificados X.509, através de uma de suas estensões. O tamanho recomendado é de, no máximo, três níveis.

Como observado por Linn (2000), os caminhos de certificação se estendem a partir das âncoras de confiança das entidades confiantes. Dessa forma, é necessário conhecer que modelo de confiança é seguido na ICP para compreender o relacionamento entre as ACs.

2.3.7 Modelos de Confiança

Os modelos de confiança determinam como as ACs se relacionam, possibilitando o

[2] Âncora de confiança é a Autoridade Certificadora na qual a Entidade Confiante confia diretamente, em meio a conjunto de outras ACs.

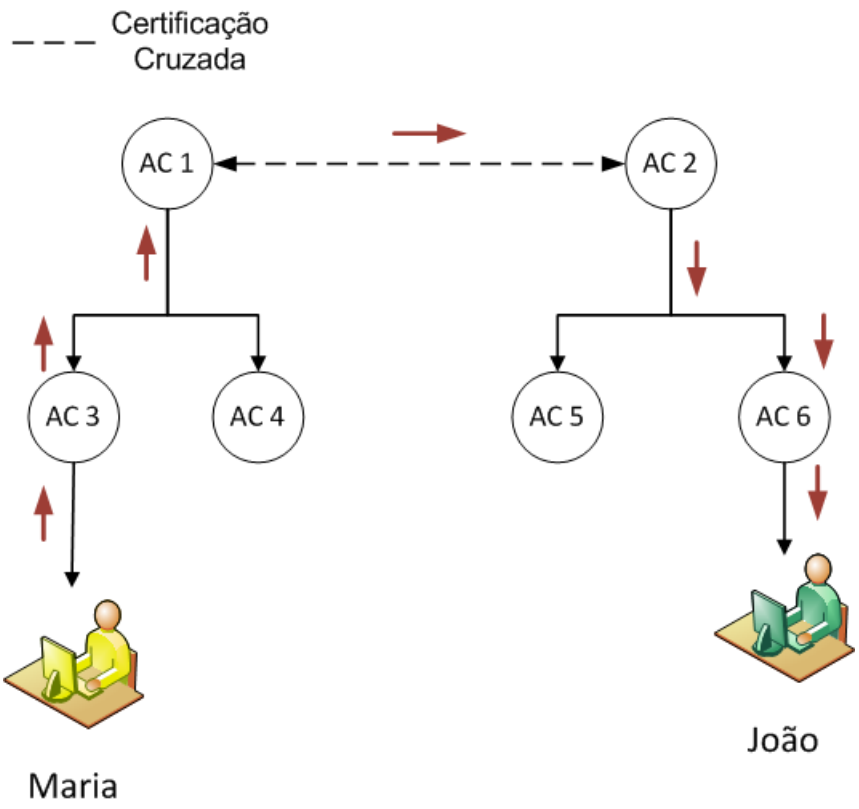

Figura 2.8: Caminho de Certificação de Maria até João.

estabelecimento da confiança entre as entidades que fazem parte da ICP. Adams e Lloyd (2002) e Binder (2004) salientam a importância da escolha do modelo de confiança: sua escolha é determinante na confiança depositada na ICP e na complexidade do processamento do caminho de certificação. Lekkas (2003) acrescenta que sua escolha deve considerar também a compatibilidade de políticas entre as ACs. Alguns dos modelos de confiança são apresentados a seguir.

2.3.7.1 Modelos Hierárquico

No modelo hierárquico, uma AC Raiz emite certificados para suas n ACs subordinadas. A AC Raiz, então, age como âncora de confiança para toda a infraestrutura abaixo dela. Comumente, ACs participantes de uma mesma hierarquia são regidas por um mesmo conjunto de políticas básicas.

Adams e Lloyd (2002) apresentam como a hierarquia é formada (ADAMS; LLOYD, 2002):

1. Uma AC Raiz é definida, e um certificado auto-assinado[3] é estabelecido como a base da confiança de todas as entidades que pertencem à hierarquia.
2. A AC Raiz assina certificados para as ACs imediatamente abaixo dela.
3. Cada uma dessas ACs podem emitir certificados para outras ACs subordinadas a ela, em um terceiro nível.
4. As ACs deste terceiro nível emitem certificados para os titulares de certificado.

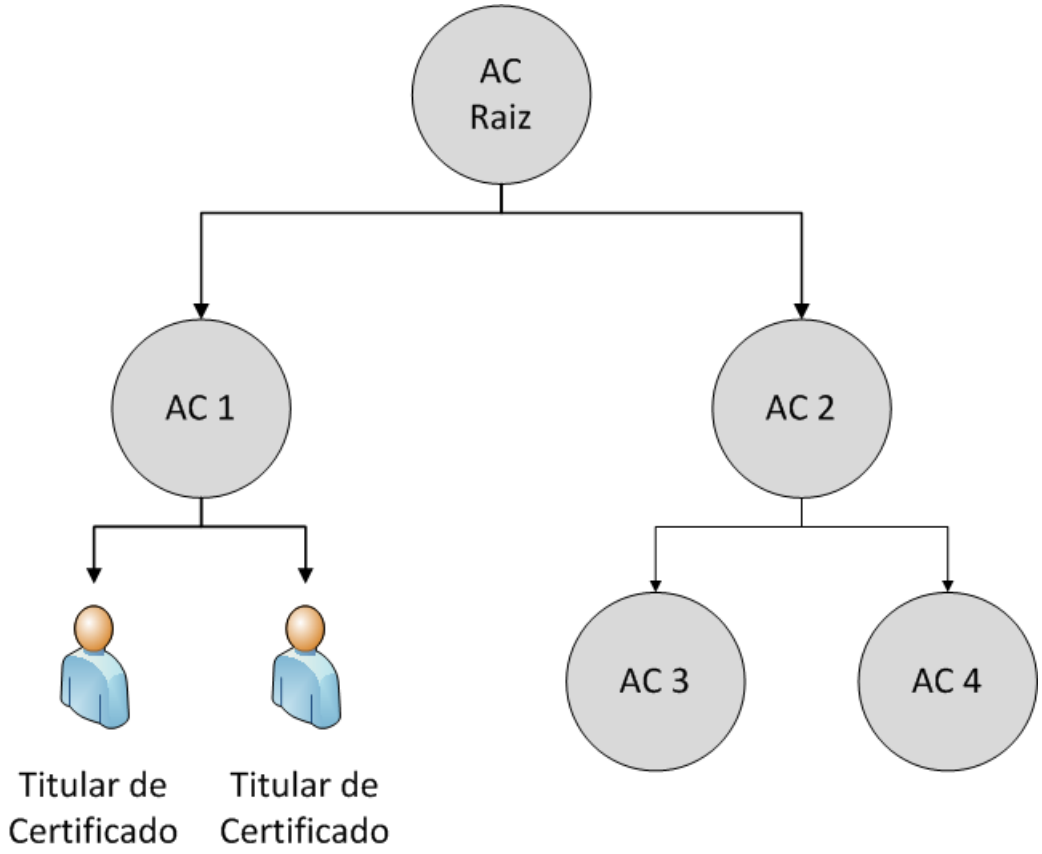

Figura 2.9: Modelo Hierárquico.

As ACs subordinadas não precisam assinar os certificados da AC superior. A construção do caminho de confiança é simples, por fornecer uma única cadeia válida do titular de certificado até a AC Raiz. É importante notar que o comprometimento do par de chaves da AC Raiz impacta em toda a infraestrututra.

2.3.7.2 Certificação Cruzada

Nesse modelo, ACs certificam outras ACs mutuamente, exceto quando certas restri-

[3] Um certificado auto-assinado é um certificado digital assinado pelo próprio titular do certificado.

ções de nome são aplicáveis (LINN, 2000). A construção do caminho de certificação é complexa, pois é possível que uma AC faça certificação cruzada com várias outras ACs. Portanto, é necessário decidir qual a cadeia correta a ser verificada.

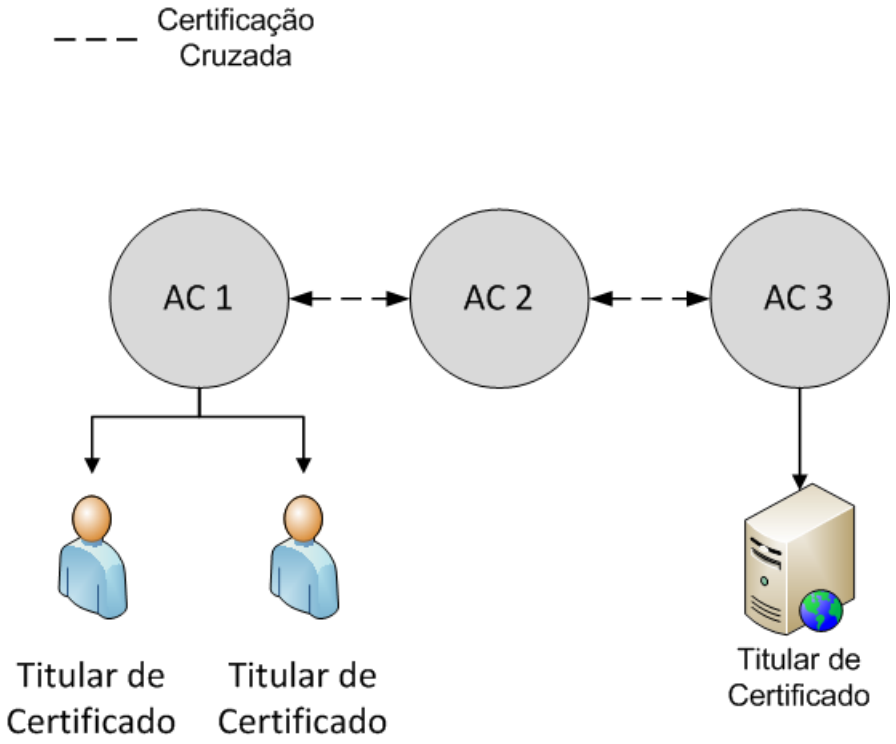

Figura 2.10: Certificação Cruzada.

Certificação cruzada pode ser utilizada para permitir interoperabilidade entre ACs de domínios diferentes (e consequentemente com requisitos diferentes), sem a necessidade de fornecer a chave pública da outra AC para todos os participantes da ICP. É possível usar um modelo híbrido, utilizando certificação cruzada e o modelo hierárquico, semelhante ao apresentado na figura 2.10. Nesse caso, a complexidade é reduzida, pois aproveita-se a vantagem da existência de um único caminho até uma determinada AC e diminui-se o número de certificações cruzadas. Entretanto, existe a possibilidade de perder o controle sobre os certificados emitidos pela outra AC. Dessa forma, há a necessidade de determinar restrições quanto aos nomes, políticas e tamanho do caminho de certificação a partir da AC certificada.

2.3.7.3 Autoridade Certificadora Ponte

Nesse modelo, uma AC de certificação cruzada centralizadora é utilizada. Apesar disso, essa AC não é raiz de uma hierarquia; sua função é apenas possibilitar a interconexão entre dois domínios, pois efetua certificação cruzada com ambos.

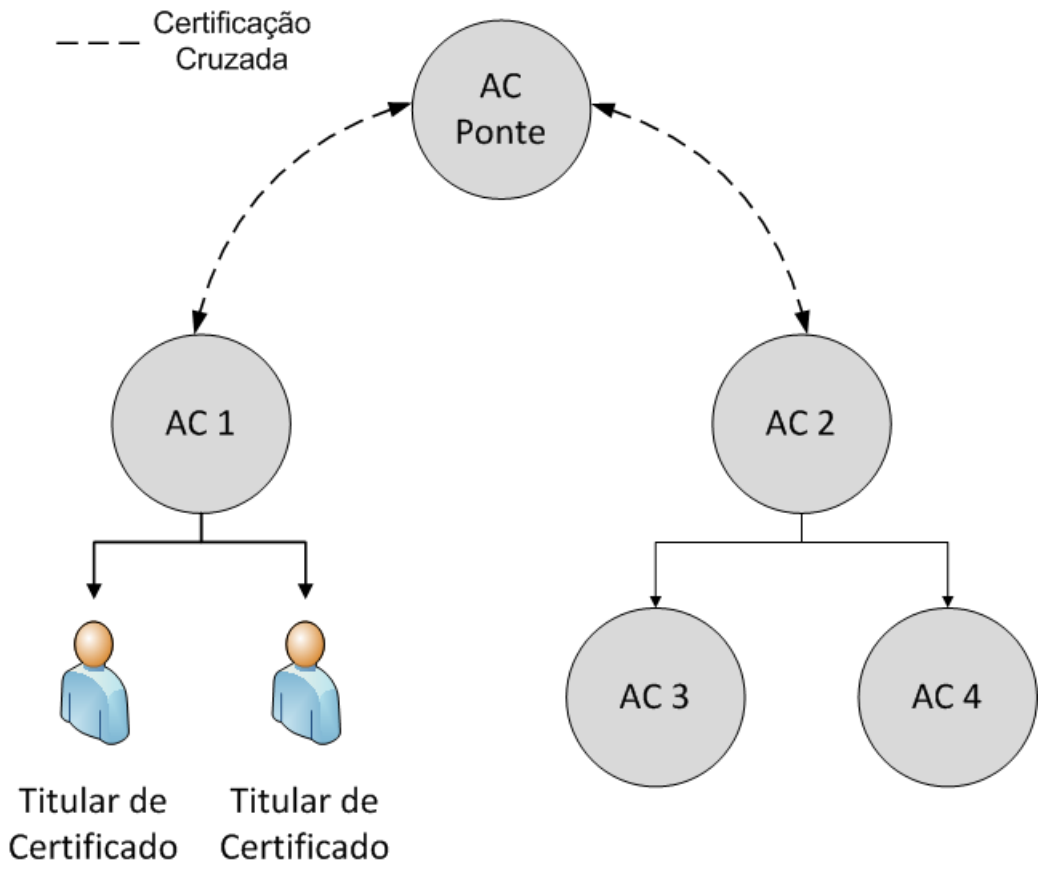

Figura 2.11: Autoridade Certificadora Ponte.

A diferença principal entre a utilização de uma AC Ponte e o modelo hierárquico está nas chaves que precisam ser armazenadas pelas entidades confiantes: no modelo hierárquico, é necessário armazenar todas as chaves públicas, até a AC Raiz; ao utilizar uma AC de ponte, apenas a chave pública da AC que emitiu o certificado do titular é guardada, e as demais são obtidas durante a formação do caminho de certificação (ADAMS; LLOYD, 2002).

2.3.7.4 Listas de Confiança

São listas com as chaves públicas das ACs consideradas confiáveis e, para que o certificado seja considerado válido, o caminho de certificação deve passar por uma delas. São comumente usadas em navegadores de Internet. De forma controlada, as federações funcionam como Listas de Confiança: um provedor de Identidade ou de Serviços, por exemplo, é considerado confiável ao cumprir um conjuno de políticas.

2.4 Aplicações para ICPs

Uma importante característica das ICPs é permitir a implantação de aplicações seguras. Basicamente, três serviços são oferecidos pelos certificados digitais e pares de chaves: assinaturas digitais, autenticação e criptografia.

2.4.1 Autenticação

É possível utilizar certificados digitais para identificar usuários e recursos antes de seu acesso ao sistema. Em portais *web*, por exemplo, o certificado pode substituir o par nome do usuário e senha para autenticação.

Outra funcionalidade é a possibilidade de prover autenticação única (*single sign-on*): um único certificado pode ser utilizado para autenticação em diversos sistemas. Um aluno da universidade pode, por exemplo, ter seu certificado emitido no momento da inscrição. A partir daí, este é utilizado para acessar o sistema de inscrição em disciplinas, a biblioteca e o servidor de correio eletrônico.

2.4.2 Assinaturas digitais

As assinaturas digitais oferecem uma forma de garantir a autenticidade das mensagens e a irretratabilidade. Essas propriedades permitem que o fluxo de documentos seja digitalizado: é possível, por exemplo, que o trâmite de processos em uma instituição utilize assinaturas digitais para substituir as assinaturas de próprio punho. Também pode-se verificar se uma mensagem eletrônica é realmente originada de um remetente através da verificação de sua assinatura digital.

2.4.3 Criptografia

As mensagens de correio eletrônico podem transitar de forma mais segura através da cifragem de seu conteúdo utilizando a chave pública dos destinatários. As Redes Privadas Virtuais (*Virtual Private Networks* - VPN) utilizam protocolos criptográficos que permitem o tráfego seguro de dados.

Mais informações sobre aplicações que podem se beneficiar do uso de certificados digitais podem ser encontradas em (ADAMS; LLOYD, 2002)

2.5 Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil)

O Presidente da República Fernando Henrique Cardoso instituiu, através da medida provisória 2.200-2 de 24 de agosto de 2001, "a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, para garantir a autenticidade, a integridade e a validade jurídica de documentos em forma eletrônica, das aplicações de suporte e das aplicações habilitadas que utilizem certificados digitais, bem como a realização de transações eletrônicas seguras" (BRASIL, 2001). Dessa forma, apenas certificados digitais emitidos por Autoridades Certificadoras credenciadas pela AC Raiz da ICP-Brasil possuem validade legal (salvo em comum acordo entre as partes).

Para fazer parte da ICP-Brasil, uma AC deve passar por um rígido conjunto de avaliações e seguir as disposições determinadas pelo Comitê Gestor da ICP-Brasil. Mais informações podem ser encontradas em (Comitê Gestor da ICP-BRASIL, 2008). Entretanto, os requisitos apresentados pela ICP-Brasil necessitam de um elevano investimento em infraestrutura e segurança, fator limitante para instituições de ensino e pesquisa com recursos financeiros escassos.

Capítulo 3

Trabalhos Relacionados

Em (LEKKAS, 2003), o autor analisa o conceito de confiança em Infraestruturas de Chaves Públicas, identificando como é estabelecida, gerenciada e suas diversas propriedades. São apresentados dois grandes problemas nas implementações modernas de ICPs: A capacidade mínima de interoperabilidade e interação entre elas, tanto em nível de políticas quanto funcionalidade; e a identificação clara do motivo pelo qual alguém deve confiar em uma AC. Ambos acarretam em limitações na usabilidade dos serviços de certificação oferecidos, especialmente por usuários certificados por diferentes ACs e desenvolvendo aplicações em diferentes contextos. O artigo propõe um banco de dados, chamado de Lista de Entidades Confiáveis (*Trusted Entities List - TEL*), que permite as entidades confiantes gerenciar suas relações de confiança. Para figurar nesta lista, as entidades devem estar em conformidade com um conjunto de políticas padrão. Os requisitos mínimos propostos nesse trabalho oferecem um conjunto de critérios que permite aos usuários classificar as entidades como confiáveis, possibilitando a definição do banco de dados proposto. As questões de interoperabilidade também podem ser minimizadas, dado que os requisitos propostos são baseados em referências técnicas de grande aceitação.

Lekkas discute também dois fatores de confiança das Autoridades Certificadoras: a qualidade dos serviços oferecidos (isto é, o quanto uma AC consegue atender as necessidades dos usuários certificados), que incluem requisitos qualitativos, quantitativos, de segurança e de conformidade com padrões e legislação vigente; e as regras e procedimentos contidos nas Políticas de Certificado e na Declaração de Práticas de Certificação, e evidências de conformidade com eles. Nesse sentido, este trabalho colabora ao fornecer insumos para a definição de provisões baseadas em padrões internacionais de segurança da informação e certificação digital, garantindo políticas com um nível elevado de qualidade. Avaliações podem ser feitas baseadas nesses documentos e no formulário de conformidade

no anexo.

Chadwick e Basden (2001) propõem a criação de um sistema especialista[1], capaz de calcular uma representação numérica da confiança em uma AC. O cálculo desse quociente é feito através da análise de uma base de conhecimento, estruturada de acordo com o arcabouço para PCs e DPCs. Pesos são definidos para cada componente que a compõe, a fim de representar sua relevância no valor final da confiança.

O artigo discute a estratégia aplicada para coletar as informações necessárias para compor a base de conhecimento, apresentando três abordagens - utilização de padrões como referência, captura de experiências de profissionais do tema e busca pelos princípios do domínio de conhecimento - demonstrando como podem ser refinadas e trabalhar harmonicamente. Por fim, uma tabela contendo o fator de confiança e a importância relativa associada é fornecida. Este trabalho utiliza as técnicas de coleta de informações discutidas pelos autores para estabelecer os requisitos propostos. O resultado deste esforço pode ser empregado na geração de uma base de conhecimento, a ser utilizada por um sistema especialista equivalente ao do artigo.

Schmeh faz diversas críticas ao principal arcabouço para elaboração de Políticas de Certficado (PCs) e Declarações de Práticas de Certificação (DPCs), a RFC 3647. O artigo lista os diversos problemas que um autor de PCs e DPCs enfrenta ao escrevê-los, dentre os quais a ausência de critérios para definição das provisões e a ausência de traduções formais e reconhecidas (tanto das seções, quanto de suas respectivas descrições) para outros idiomas além do inglês, mostram-se as mais graves. Nota-se o autor ressaltar que o desafio na elaboração de PCs e DPCs, nesse último caso, é provocado pela necessidade de considerar as aplicações locais. Algumas soluções para contornar os problemas são sugeridas no texto de (SCHMEH, 2007).

Nesse sentido, este trabalho colabora ao sugerir traduções para português do Brasil dos títulos e descrições das seções, além de oferecer critérios para elaboração das provisões que consideram o contexto local, isto é, as necessidades do ambiente de ensino e pesquisa. Isso quer dizer que foram levados em conta a Heterogeneidade dos ambientes e o custo de implantação dos requisitos porpostos, por exemplo.

[1] Aplicações de Inteligência Artificial que utilizam conhecimento baseado na experiência de especialistas humanos para fornecer a solução de um problema.

Capítulo 4

Definindo Políticas e Práticas Confiáveis

Para que um titular de certificado ou entidade confiante possa estabelecer uma relação de confiança com a AC, é necessário que eles conheçam e compreendam como são executadas as tarefas de gerenciamento do ciclo de vida de seus certificados. Este capítulo aborda como é possível oferecer essas informações e como definir políticas e práticas para o gerenciamento confiável do serviço de certificação digital.

4.1 Confiando em Autoridades Certificadoras

Toda a funcionalidade da ICP está baseada na confiança depositada pelos usuários na AC. Contudo, dada a subjetividade do termo *confiança*, o estabelecimento dessa relação não é trivial. Lekkas (2003), no entanto, apresenta algumas características interessantes desse conceito, do ponto de vista de uma ICP. Duas delas são pertinentes no contexto deste trabalho:

Crença do usuário nas operações da AC: titulares de certificado precisam acreditar que os sistemas que suportam as operações da AC são exatamente o que dizem, operacional e tecnologicamente.

Risco aceitável: titulares de certificado e entidades confiantes precisam acreditar que riscos envolvidos na operação foram reduzidos para um nível aceitável.

É possível notar, portanto, que perder a confiança em uma AC é fácil: basta que AC não corresponda as expectativas das entidades confiantes em minimar os riscos no gerenciamento de chaves e no oferecimento de seus serviços de certificação digital.

Além disso, Hunt salienta que a "criptografia de chaves públicas por si só não é suficiente" (HUNT, 2001). E lista três requisitos que também devem estar presentes nas operações de uma AC:

- Políticas de segurança sob as quais os sistemas deverão operar;
- Produtos para gerenciar o ciclo de vida dos certificados;
- Procedimentos para geração e distribuição de certificados e chaves.

Dessa forma, conforme observado por Marques e Rebello, "a AC deve, portanto, oferecer informações suficientes para apoiar a parte confiante e o titular do certificado (isto é, a entidade identificada pelo certificado e relacionada a um par de chaves) na decisão de utilizar ou não um certificado em uma determinada aplicação".

Atualmente, essas informações são fornecidas aos interessados através de um conjunto de documentos que descrevem as políticas e práticas da AC, no que diz respeito ao gerenciamento do ciclo de vida dos certificados. Os mais comuns são:

Política de Segurança (PS), que define as regras que regem a utilização das informações e equipamentos da AC.

Política de Certificados (PC), que define como os certificados devem ser emitidos e usados.

Declaração de Práticas de Certificação (DPC), que apresenta os procedimentos da AC para gerenciar o ciclo de vida dos certificados.

Plano de Continuidade de Negócios (PCN), que contém informações sobre como a AC continuará oferecendo o serviço de certificação após um desastre ou evento que cause danos às suas operações.

Acordos com usuários, que são estabelecidos entre titulares de certificado, entidades confiantes e a AC, para garantir que os certificados serão usados de forma aceitável e que questões de privacidade serão tratadas pelos participantes da ICP.

Outros documentos, dentro desse contexto, que podem apoiar o gerenciamento do serviço de certificação digital são os manuais de operação da AC e da AR e materiais de treinamento. Para mais exemplos e informações sobre esses documentos, é recomendada

a leitura de (CHOKHANI et al., 2003), (FRASER, 1997), (BOWEN; HASH; WILSON, 2006) e (SWANSON et al., 2010).

O escopo deste trabalho está limitado às Políticas de Certificado (PC) e Declarações de Práticas de Certificação (DPC). Contudo, a importância dos demais não deve ser descartada; as informações contidas neles podem servir de insumo para PC e DPC, ao mesmo tempo em que estas podem referenciar os primeiros. Lekkas (2003) faz especial menção à relevância do PCN no estabelecimento da confiança, pois os usuários dos certificados (titulares e entidades confiantes) precisam saber como proceder em caso de interrupção dos serviços da AC.

4.2 Políticas de Certificado (PC) e Declarações de Práticas de Certificação (DPC)

Chokani et. al (2003) definem uma Política de Certificados (PC) como "um conjunto de diretivas que define a aplicabilidade de um certificado a um dado domínio como, por exemplo, uma comunidade em particular ou classe de aplicações". Dessa forma, a PC é a responsável por fornecer ao usuário do certificado informações a respeito das regras de gerenciamento e uso dos certificados. Portanto, é comum uma AC publicar mais de uma PC (ou políticas em um mesmo documento de PC), a fim de abordar diferentes aplicações.

Uma Declaração de Prática de Certificação (DPC) é um relato das atividades (práticas) exercidas por uma AC 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 (CHOKHANI et al., 2003). Ou seja, é através da DPC que a AC apresenta que ações são tomadas para que seus sistemas sejam utilizados e gerenciados de forma segura e confiável, de acordo com a PC.

4.2.1 Relação entre PC e DPC

PC e DPC são documentos complementares. Enquanto a PC determina as regras que guiarão o serviço de certificação digital ("o que" deve ser feito), a DPC descreve os procedimentos executados para que essas regras sejam cumpridas (isto é, "como" são executadas as atividades necessárias) (MARQUES; REBELLO, 2009). É comum encontrá-los compondo um único documento (chamando aqui de PC/DPC). Dessa forma, as informações de ambas são concentradas, facilitando a consulta. Como dito anteriormente, esses

documentos devem ser tornados públicos. Entretanto, uma AC pode optar por divulgar apenas parte dele (por questões de segurança ou organização interna).

É preciso atentar para o fato que, "conforme o serviço oferecido pela AC evolui, a prática pode mostrar a necessidade de alteração das políticas estabelecidas. Isso significa que as estipulações tanto de uma PC quanto de uma DPC são dinâmicas, e frequentemente renovadas para se adequar a novas demandas das partes confiantes, tecnologias, requisitos legais ou identificados pelo grupo de usuários" (MARQUES; REBELLO, 2010).

Ainda que sua importância seja grande para o estabelecimento em uma AC, a elaboração desses documentos ainda é uma atividade complexa. Além disso, de posse da PC e da DPC, titulares de certificado e entidades confiantes não possuem critérios para definir se uma AC é ou não confiável através de sua análise. Essas questões serão analizadas mais adiante. O objetivo deste trabalho é definir um conjunto de requisitos mínimos que permita aos usuários avaliar a confiança nas PCs e DPCs e ofereça critérios confiáveis para guiar os autores desses documentos no processo de elaboração.

4.3 Desafios na elaboração e avaliação de PCs e DPCs

Os autores do documento de PC e DPC contam com um arcabouço para a elaboração de PCs e DPCs. A RFC 3647 (CHOKHANI et al., 2003) provê uma lista de tópicos considerados relevantes para esses documentos, de acordo com a aplicação a qual os certificados emitidos são destinados. Os tópicos são tratados através de um conjunto de provisões, agrupadas em componentes (representada em nove capítulos dos documentos). São eles:

1. **Introdução:** identifica e introduz as entidades envolvidas, o escopo da atuação da Autoridade Certificadora, e aplicabilidade dos certificados emitidos no âmbito da ICP.

2. **Responsabilidades Referentes a Publicações e Repositórios:** aborda a responsabilidade da Autoridade Certificadora no que diz respeito à divulgação de informações, necessárias para que uma entidade possa confiar nos certificados emitidos (como as PCs e DPCs e os próprios certificados, por exemplo) e gerência dos repositórios onde ficam disponíveis.

3. **Identificação e Autenticação:** aborda o formato dos nomes presentes no certificado, além dos métodos para validar a identidade de uma entidade antes da emissão do certificado.

4. **Requisitos Operacionais do Ciclo de Vida do Certificado:** estabelece os procedimentos adotados pela AC para gerenciar o ciclo de vida dos certificados, de sua solicitação até expiração ou revogação.

5. **Controles Operacionais, Gerenciais e de Instalações Físicas:** estabelece os controles operacionais, de segurança de pessoal e de segurança física do ambiente operacional da AC, usados com o objetivo de prover confiabilidade nas operações da ICP para seus participantes.

6. **Controles Técnicos de Segurança:** trata dos controles utilizados pela ICP no que tange a criação do par de chaves, algoritmos criptográficos, tamanho e proteção das chaves, por exemplo.

7. **Perfis dos Certificados, LCR e OCSP** define o conteúdo e formato de certificados e Listas de Certificados Revogados (LCRs), tratando de que campos estão presentes, como devem ser preenchidos e interpretados.

8. **Auditoria de Conformidade:** considerações envolvendo auditoria e outras avaliações periódicas dos participantes da ICP, em particular da AC, a fim de determinar se as entidades estão em conformidade com os controles impostos pela PC/DPC, PS e demais critérios. Inclui os tópicos cobertos, periodicidade e metodologia utilizada para a avaliação.

9. **Assuntos Legais e Assuntos Gerais:** aborda assuntos diversos relacionados a provisões legais, taxas a serem cobradas pelos serviços oferecidos, entre outros. O foco está nos aspectos legais e do negócio, portanto menos técnico que as demais seções.

A RFC 3647 mostra, também, sugestões sobre como o conteúdo das seções deve ser abordado. O arcabouço não determina qualquer provisão, possibilitando sua aplicação em qualquer ICP.

Atualmente, a RFC 3647 é o padrão *de facto* para elaboração dos documentos de PC e DPC. Entretanto, Schmeh apresenta em (SCHMEH, 2007) diversas deficiências existentes no arcabouço, dentre as quais é importante citar:

A RFC 3647 não é oficialmente um padrão. Por possuir caráter informacional, autores de PC e DPC optam por seguir o modelo proposto. Dessa forma, é comum que a estrutura proposta não seja seguida à risca. Ocasionalmente, documentos de PC/DPC não apresentam seções potencialmente úteis aos usuários.

O conjunto de provisões não é intuitivo. Os títulos de seções e respectivas descrições propostas podem ocasionar interpretações imprecisas. Também não fica claro em que seções devem ficar certas provisões, o que muitas vezes faz com que fiquem distribuídas pelo texto, dificultando a leitura.

Não existem traduções oficiais da RFC 3647. O que dificulta ainda mais a elaboração de documentos em outras línguas que não o inglês, decorrente das diversas possibilidades de traduções para os títulos das seções.

Os iniciantes na elaboração desses documentos encontram nesses problemas o primeiro desafio para a criação de PCs e DPCs. A falta de uma descrição mais clara e exemplificada dos documentos torna a atividade mais complexa. Não fornecer nenhuma provisão ao autor, apesar de benéfico para adaptação em diferentes ambientes, também faz com que os autores não possuam uma base do que é confiável a princípio para, a partir daí, definir suas próprias provisões.

Além disso, havendo a necessidade de viabilizar a interoperabilidade entre ACs com diferentes políticas, a falta de padronização das seções e provisões pode dificultar a análise dos documentos. Do ponto de vista dos titulares de certificado e entidades confiantes, não existem critérios claros para que uma avaliação objetiva da confiança possa ser feita. Dessa forma, surge a necessidade de estabelecer uma forma de garantir que os serviços oferecidos pela Autoridade Certificadora são confiáveis e prover uma maneira de viabilizar a decisão de confiar em uma AC. Este trabalho visa oferecer um conjunto de referências para compor esses espaços, possibilitando a definição de um modelo confiável para elaboração de documentos de PC/DPC.

4.4 Definição de Requisitos para PCs e DPCs

A definição dos requisitos a serem utilizados para a elaboração de PCs e DPCs confiáveis pode ser dividido em três fases:

1. Coleta e análise de referências para compor os requisitos
2. Mapeamento das referências no formato da RFC 3647
3. Estabelecimento dos requisitos para PCs e DPCs

As fases são explicadas a seguir.

4.4.1 Coleta e análise de referências

A primeira fase consistiu na seleção, coleta e análise de informações que pudessem servir de base para a definição dos requisitos propostos. Para essa atividade, Chadwick e Basden (2001) apresentam três alternativas para obtê-las:

Utilização de referências reconhecidas como padrões. Que apresenta a vantagem de ser reconhecida como confiável por uma comunidade mas que, por outro lado, pode conter informação desatualizada.

Captura da experiência e visão de especialistas e profissionais da área. Cuja vantagem está na visão mais prática e atual das informações podendo, entretanto, haver discordância entre os profissionais entrevistados.

Busca pelos princípios do domínio de conhecimento. Que os autores definem como ser a respostas para as perguntas "Por quê?" e "Por que não?", com a idéia principal de compreender as variações em diferentes ambientes e representá-las.

De acordo com Lekkas (2003), a confiança está baseada na percepção de validade e precisão de quem avalia os serviços oferecidos pela AC. O autor também evidencia que o senso de segurança do cliente é determinado, praticamente, pela confiança que ele deposita na eficiência dos mecanismos de tratamento dos riscos que uma AC supostamente possui. Portanto, para compor os requisitos utilizados, optou-se pela utilização de padrões cuja confiança pré-estabelecida pela comunidade de segurança da informação é notória (figura 4.1). Ou seja, as referências utilizadas são reconhecidos e consolidadas como padrões, permitindo que confiança depositadas neles por esta comunidade seja entendida para os documentos de PC e DPC. As seguintes referências foram determinadas relevantes no contexto desse trabalho (MARQUES; REBELLO, 2010):

- ISO/IEC 27001:2005 - *Information technology - Security techniques - Information security management systems - Requirements*: A International Organization for Standardization (ISO) é uma organização não-governamental reconhecida mundialmente, sendo a maior desenvolvedora e editora de padrões nos mais diversos setores. A ISO/IEC 27001 é um padrão para Sistemas de Gerenciamento de Segurança de Informações (SGSIs), cujo objetivo principal é prover um modelo para estabelecer, implementar, operar, monitorar, revisar e manter um SGSI, a partir de uma abordagem baseada em processos.

- ISO/IEC 27002:2005 - *Information technology - Security techniques - Code of practice for information security management*: É um padrão para ser usado associado à ISO/IEC 27001, que define boas práticas para estabelecer, implementar, operar, monitorar, revisar e manter um SGSI. Também procura oferecer um guia para "desenvolvimento de padrões organizacionais de segurança e práticas efetivas de gerenciamento de segurança e para ajudar a estabelecer confiança em relações inter-organizacionais".

- NIST SP 800-53 Rev. 2 - *Recommended Security Controls for Federal Information Systems*: É uma publicação do National Institute of Standards and Technology NIST - agência federal não-regulatória da câmara de comércio norte-americana - que serve como guia para estabelecer e escolher controles de segurança para sistemas de informação, e atualmente é usado como critério para auditoria dos sistemas de informação das unidades federais do governo norte-americano. É baseado em diversos outros documentos do NIST relacionados à Segurança de Informações e define níveis quantitativos de segurança de acordo com os controles apresentados, agrupados em famílias. Essa organização foi seguida durante este trabalho, a fim de manter a relação proposta por seus autores.

- ETSI TS 102 042 - *Policy Requirements for Certification Authorities Issuing Public Key Certificates*: O European Telecommunications Standards Institute (ETSI) produz padrões para Tecnologias da Informação e Comunicação (TIC) aplicáveis globalmente. A especificação técnica TS 102 042 é baseada na mesma abordagem da TS 101 456, que provê um conjunto de requisitos para operação e gerenciamento de autoridades certificadoras emitindo certificados digitais qualificados de acordo com a diretiva 1999/93/EC do Parlamento Europeu e do Council on a Community framework for electronic signatures. A TS 102 042, entretanto, é aplicável a requisitos gerais de serviços de certificação digital.

- ANSI/X9 X9.79-1:2001 - *Financial Services Public Key Infrastructure (PKI) Policy and Practices Framework*: O American National Standards Institute (ANSI) supervisiona a criação, divulgação e utilização de milhares de normas e orientações que, impactam diretamente em diversas empresas dos mais diferentes setores. Define os componentes de uma ICP e um arcabouço para requisitos de políticas e práticas.

A RFC 3647, fornece a estrutura dos documentos, facilitando a comparação entre diferentes PCs e DPCs. Dessa forma, os padrões são utilizados para compor as provisões

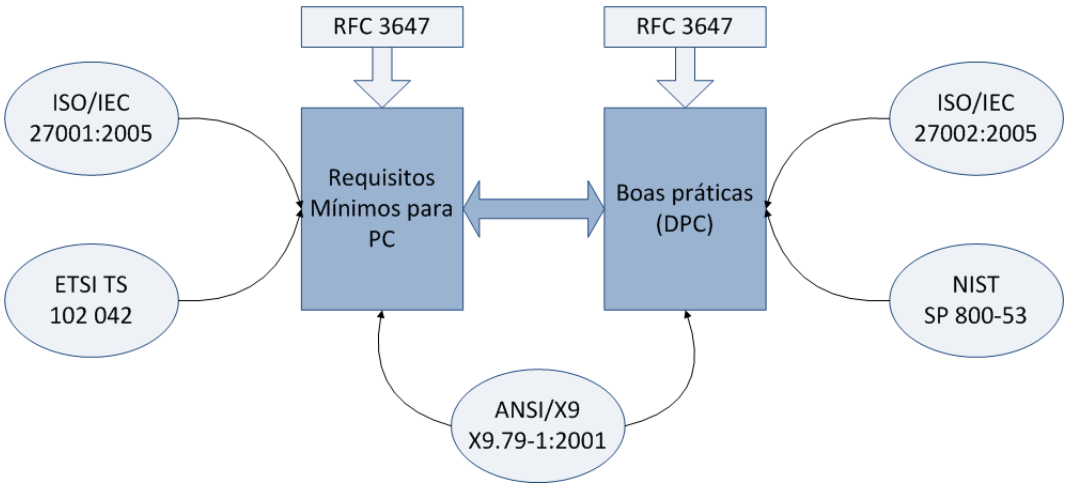

Figura 4.1: Representação gráfica do mapeamento.

e preencher as lacunas do arcabouço. O problema da desatualização da informação é contornado através do estabelecimento de um processo de revisão dos requisitos gerados, permitindo que estejam em conformidade com as versões mais atuais. A segunda estratégia de coleta de conhecimento também foi utilizada, a fim de garantir a adequabilidade dos requisitos a realidade atual do gerenciamento de um serviço de certificação digital.

4.4.2 Mapeamento de referências na RFC 3647

A tarefa seguinte consistiu no mapeamento dessas referências no formato da RFC 3647. Deve-se notar que este trabalho considera a utilização de um documento único, que representa PC e DPC (chamado aqui de PC/DPC) simultaneamente.

Dada a necessidade de tornar o trabalho aplicável no contexto das ICPs brasileiras, as seções previstas pelo arcabouço foram traduzidas para Português do Brasil. Para isso, conforme sugerido por Schmeh (2007) e a fim de manter o alinhamento com a legislação vigente, a DPC da AC Raiz da ICP Brasil (Comitê Gestor da ICP-BRASIL, 2008) foi analisada. Entretanto, até o momento, a própria ainda não foi adaptada para a RFC 3547; suas provisões ainda seguem o formato da RFC 2527 (CHOKHANI; FORD, 1999), que foi substituída pelo arcabouço mais atual. Dessa forma, o apêndice A de (MARQUES; REBELLO, 2010) apresenta uma sugestão de tradução para os capítulos e seções de documentos de PC/DPC.

O esforço de mapeamento resultou em uma tabela com os componentes da RFC 3647 e suas respectivas descrições, seguidas de colunas para cada referência utilizada. As linhas então foram preenchidas com os itens a serem consultados pelo autor de documentos de

PC/DPC ao estabelecer suas provisões.

Tabela 4.1: Excerto do mapeamento entre a seção 5 da RFC 3647 e as referências selecionadas

Componentes da RFC 3647	**Descrição do componente**	**ANSI X9.79:2001**	**NIST SP 800-53**
5.3.2 Background check procedures	Descreve os procedimentos seguidos para verificar os antecedentes antes da contratação de um funcionário que ocupará papéis de confiança ou outras funções importantes.	A.5.3 Personnel Security Controls B.1.2 Security Management B.1.4 Personnel Security	Família Personnel Security
5.3.3 Training requirements	Estabelece o processo de treinamento pelo qual o pessoal deverá passar.	A.5.3 Personnel Security Controls B.1.2 Security Management B.1.4 Personnel Security	Família Awareness and Training
5.3.4 Retraining frequency and requirements	Estabelece a freqüência na qual deve haver um novo treinamento para o pessoal da AC.	A.5.3 Personnel Security Controls B.1.2 Security Management B.1.4 Personnel Security	Família Awareness and Training

A tabela 4.1 apresenta exemplos do mapeamento efetuado. O mapeamento completo pode ser encontrado no apêndice B de (MARQUES; REBELLO, 2010).

4.4.3 Estabelecimento dos Requisitos

A partir do mapeamento apresentado na subseção 4.4.2, foi possível definir um conjunto de requisitos, baseados no conteúdo dos padrões citados. Contudo, objetivando oferecer provisões que pudessem ser aplicadas em ICPs reais, mais uma das alternativas apresentadas por Chadwick e Basden (2001) foi utilizada: os requisitos propostos foram encaminhados para revisão de especialistas e profissionais da área de certificação digital. Participaram desse grupo pesquisadores da Universidade Federal de Santa Catarina (UFSC), da Universidade Federal de Minas Gerais (UFMG), da Universidade Federal Fluminense (UFF), do Laboratório Nacional de Computação Científica (LNCC), além de representantes do Centro de Atendimento a Incidentes de Segurança (CAIS) da RNP e de uma empresa privada especializada em módulos criptográficos. Uma nova versão foi gerada, comportando agora os dados provenientes da análise feita por esse grupo.

O resultado são políticas e práticas associadas, que oferecem um nível mínimo de

segurança e qualidade as operações do serviço de certificação digital. A partir daí, o autor de PC/DPC pode adaptá-las de acordo com seu próprio ambiente e requisitos da comunidade que irá atender. Exemplos dessas provisões são encontrados a seguir:

Exemplo 1 (Seção 5.3.2 da RFC 3647):

> **5.3.2 Procedimentos de verificação de antecedentes**
> 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. 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;
> d) Antecedentes criminais do candidato.

Exemplo 2: (Seção 5.3.3 da RFC 3647)

> **5.3.3 Requisitos de treinamento**
> 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.

Exemplo 3 (Seção 5.3.4 da RFC 3647):

> **5.3.4 Requisitos de frequência de treinamento**
> O pessoal de operação da AC e AR deve ser treinado nos procedimentos descritos na PC/DPC com frequência de um ano, ou sempre que surgirem alterações significativas.

Para os usuários (entidades confiantes e titulares de certificado) agora é possível determinar a compatibilidade das políticas e práticas com o suas necessidades, além de possuir uma garantia mínima de qualidade em um serviço cujos padrões de operação ele confia.

Todavia, esses produtos devem ser mutáveis: com o passar dos anos, surgem novas técnicas de segurança e certificação digital; os requisitos devem, portanto, sofrer alterações para que um nível mínimo de confiança seja mantido.

4.5 Processo de elaboração de Políticas e Práticas Confiáveis

A partir dos requisitos propostos, então, é possível estabelecer políticas e práticas confiáveis seguindo o roteiro, ilustrado pelo diagrama de atividades da figura 4.2:

1. Criação de um *template* estruturado no formato proposto pela RFC 3647
2. Identificar requisitos legais, organizacionais e de aplicação;
3. Preenchimento do *template* de acordo aos requisitos organizacionais, identificados através do passo anterior, e requisitos da aplicação;
4. Revisão das estipulações definidas a partir dos requisitos propostos de acordo com os padrões de segurança e certificação;
5. Revisão geral do texto para garantir a consistência das provisões;
6. Implementar as políticas determinadas, verificando se são viáveis e fazendo modificações necessárias;
7. Avaliar conformidade entre práticas e políticas, efetuando qualquer modificação que seja necessária para garanti-la;
8. Publicação.

Um *template* baseado nas traduções propostas em (MARQUES; REBELLO, 2010) pode ser encontrado no anexo B e utilizado pelos autores de PCs/DPCs para preenchê-los com suas próprias provisões. Os passos dois e três são necessários pois, como posto por Schmeh (2007), é necessário levar em conta requisitos legais obrigatórios. Outros critérios que devem ser considerados são os requisitos organizacionais e de aplicação, para que o serviço de certificação digital seja oferecido de acordo com as necessidades das partes envolvidas. Esses passos não devem ser negligenciados, dada a importância na minimização dos riscos envolvidos no gerenciamento da AC.

No passo quatro, as provisões devem ser revisadas utilizando os requisitos obtidos através dos padrões de segurança e certificação. A PC/DPC deve fazer referência a esses padrões no texto, informando ao usuário a preocupação da AC em oferecer um serviço de certificação digital de qualidade, alinhado com medidas reconhecidamente seguras. Esse passo não deve ser negligenciado, dada sua importância no estabelecimento da confiança.

A política então deve ser implementada através das práticas. Durante os passos seis e sete, é possível que uma regra definida não seja viável na realidade atual da Autoridade Certificadora. Portanto, será necessário efetuar mudanças nas políticas para adequá-las ao escopo do serviço oferecido.

Finalmente, no passo oito, o documento deve ser tornado público. O objetivo é fornecer aos usuários dos certificados (titulares de certificado e entidades confiantes), ou outro grupo que deseje avaliar as políticas e práticas da AC, as informações necessárias para decidir se devem ou não aceitar os certificados emitidos pela AC.

4.6 Estudo de Caso: a ICPEDU

A Infraestrutura de Chaves Públicas para Ensino e Pesquisa (ICPEDU) é uma iniciativa da Rede Nacional de Ensino e Pesquisa (RNP) que consiste na criação de uma ICP dentro do ambiente Instituições Federais de Ensino Superior (Ifes) e Unidades de pesquisa (UPs).

Os certificados digitais emitidos pelas ACs da ICPEDU são utilizados apenas em aplicações acadêmicas e de pesquisa; portanto, não possuem validade legal e não substitui certificados emitidos pela InfraEstrutura de Chaves Públicas Brasileiras (ICP-Brasil), a ICP oficial do Brasil.

4.6.1 Modelo de confiança e governança na ICPEDU

A ICPEDU optou por utilizar o modelo de confiança hierárquico: uma AC Raiz é responsável por emitir certificados digitais para outras Autoridades Certificadoras, gerenciadas pelas Ifes e UPs. Essas ACs são, então, responsáveis pela emissão de certificados dentro do seu próprio domínio.

Durante a fase piloto, a ICPEDU foi gerenciada por dois grupos:

o Comitê Gestor (CG) é composto por representantes dos grupos que operam a AC

Raiz, da Autoridade de Gerência de Políticas e do meio acadêmico. Sua função é administrativa, como representar a ICPEDU e decidir pela entrada ou exclusão de uma instituição na infraestrutura.

a Autoridade de Gerência de Políticas (AGP) é composta por representantes técnicos das instituições participantes e por especialistas em segurança da informação e certificação digital. Sua função é técnica, como a avaliação das ACs candidatas a fazer parte da infraestrutura e o estabelecimento de políticas que permitam estabelecer confiança na ICPEDU.

Além do CG e da AGP, dois outros grupos atuam nas atividades operacionais da AC Raiz: o Grupo de Operações da AC Raiz (GOPAC), cujas funções envolvem o gerenciamento do ciclo de vida dos certificados emitidos pela mesma, e o Grupo de Operações da AR Raiz (GOPAR), encarregado da identificação e autenticação das instituições e seus responsáveis.

4.6.2 Utilização dos requisitos mínimos na ICPEDU

Dadas as possíveis limitações de recursos financeiros de instituições de ensino e pesquisa que desejassem inserir suas ACs na infraestrutura, em diversos casos impossibilitando a utilização de certificados ICP-Brasil, estabeleceu-se um conjunto de critérios para atender à ICPEDU . A fim de adequar os requisitos ao ambiente proposto pela ICPEDU, suas provisões foram revisadas para considerar as particularidades da infraestrutura. Portanto, a Política de Segurança (PS) da ICPEDU e os padrões de algoritmos criptográficos, por exemplo, passaram a ser considerados. Gerou-se, a partir daí, um documento intitulado "*Requisitos Mínimos para Políticas de Certificado e Melhores Práticas de Certificação da ICPEDU*" (AGP-ICPEDU, 2008b), que compreende também um conjunto de boas práticas de certificação digital associadas, dentro do contexto da ICPEDU. Sua organização se dá da seguinte forma:

- Uma **Descrição** que apresenta a proposta da seção de forma geral.
- **Requisitos Mínimos** que compreendem as exigências nas políticas de certificado das Autoridades Certificadoras para participar na ICPEDU.
- **Melhores Práticas** que sugerem, no âmbito da ICPEDU, as melhores técnicas para execução das atividades de gerenciamento do ciclo de vida dos certificados.

- **Exemplos** de textos oferecidos como uma guia para que os autores de PC/DPC.

Os resultados do esforço deste trabalho são utilizados como requisitos de observância obrigatória na elaboração dos documentos de PC/DPC da ICPEDU.

O produto é fornecido às ACs candidatas a fazer parte da infraestrutura, que devem escrever documentos de PC/DPC e submetê-los a AGP para avaliação. O gerente da AGP então aloca revisores, que analisam o documento de PC/DPC da instituição. Contudo, como apontado por Lekkas (2003), o processo de avaliação de confiança não é trivial. Para facilitar a tarefa, um conjunto de critérios baseados nos requisitos estabelecidos são disponibilizados aos revisores, que examinam os documentos face esses parâmetros.

Os revisores interagem com os autores da PC/DPC até que os critérios sejam cumpridos, emitindo um parecer sobre a análise.

Exemplos de provisões retiradas de PCs/DPCs já aprovadas são apresentadas a seguir:

Exemplo 4 (AGP-ICPEDU, 2008a):

> **5.3.2 Procedimentos de verificação de antecedentes**
> Todo funcionário da AC Raiz em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados deve:
> a) ser submetido aos mesmos critérios utilizados para contratação de funcionários da organização responsável pela AC Raiz;
> b) apresentar duas cartas de recomendação de pressionais da área de segurança;
> Alem dos critérios descidos acima, o responsável pela AC Raiz deverá ter seu nome submetido a aprovação do comitê gestor da ICPEDU.

Exemplo 5 (Unicamp, 2008):

> **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 Unicamp além da plataforma hospedeira do seu repositório. Também serão analisados os registros do ambiente seguro.

Em uma fase posterior, as ACs são auditadas por um grupo competente, a fim de garantir que as estipulações do documento de PC/DPC estão sendo cumpridas.

Deve-se notar que os requisitos evoluem com o passar do tempo. Sempre que houver necessidade de alterações (caso ocorram mudanças nos documentos utilizados como referência, por exemplo), o processo é repetido. Essas mudanças devem ser controladas e acompanhar também a evolução da própria ICP. A manutenção desse ciclo é importante para que a confiança na ICP seja garantida.

Dessa forma, os requisitos assumem o papel de fatores básicos de confiança na ICPEDU. Uma entidade confiante que recebe um certificado emitido por uma AC da infraestrutura pode decidir aceitá-lo ou não, estando ciente da conformidade desta AC com os critérios estabelecidos.

4.6.3 Benefícios obtidos através da utilização dos requisitos

Para os autores de documentos de PC/DPC da ICPEDU, os requisitos atuam oferecendo um nível mínimo de confiança a ser atingindo. Associados às boas práticas apresentadas, apóiam a equipe da AC no estabelecimento de um serviço de certificação digital de qualidade. Isso motivou a solicitação de adesão de outras instituições a infraestrutura, incluindo agências do governo como, por exemplo, o Conselho Nacional de Desenvolvimento Científico e Tecnológico (CNPq).

Durante a interação com os representantes das instituições participantes, estes informaram que a melhora na captação de recursos financeiros pelo departamento de Tecnologia da Informação, com o objetivo de atender aos requisitos e melhorar a segurança como um todo.

Do ponto de vista dos titulares de certificado e entidades confiantes, a AC é minimamente confiável, uma vez que a autoridade certificadora que emitiu o certificado foi credenciada para a ICPEDU - garantindo, por tanto, a conformidade com os requisitos.

Os padrões nos quais os requisitos estabelecidos são definidos também servem como critério para determinar se uma Autoridade Certificadora pode ou não fazer parte das listas de confiança dos principais navegadores disponíveis do mercado. A conformidade com esses requisitos permite, então, a solicitação de inclusão do certificado da AC na distribuição de navegadores como o Mozilla Firefox e o Microsoft Internet Explorer. Para que seja possível integrar a lista de confiança do Mozilla Firefox, por exemplo, é necessária

uma análise do documento de PC/DPC, buscando por evidências de conformidade com alguns dos padrões utilizados nesse trabalho.

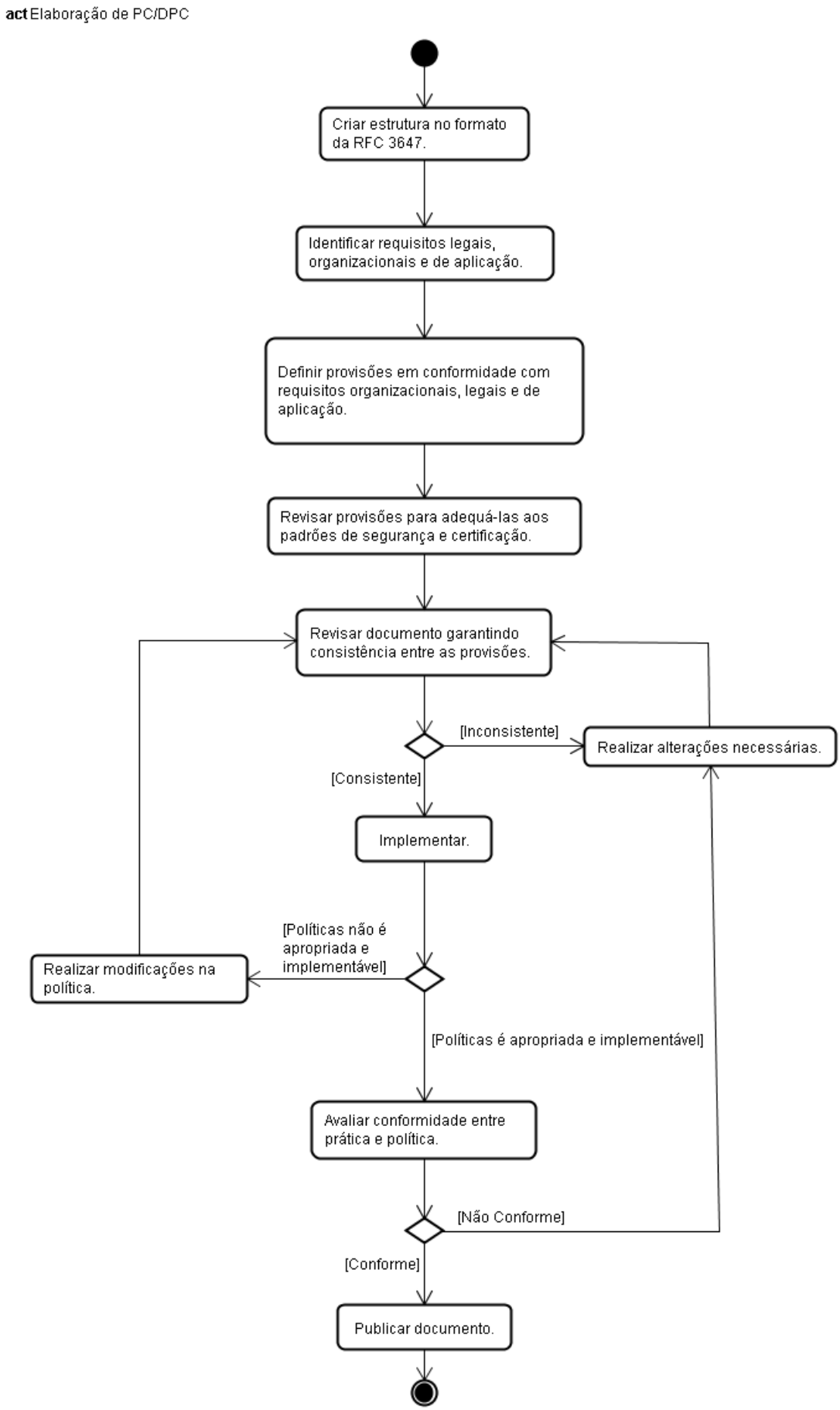

Figura 4.2: Processo de ealaboração de PC/DC.

Capítulo 5

Conclusão

Os avanços das Tecnologias da Informação e Comunicação (TIC) facilitam a divulgação de informações, e o oferecimento de serviços aos usuários. Na mesma proporção, cresce a disponibilização de dados sensíveis em meios de comunicação abertos. Surge então a preocupação em manter esses dados a salvo de ameaças, que possam afetar sua integridade, disponibilidade e confiabilidade. Há ainda o desejo de garantir alguns aspectos associados, como determinar se um usuário está ou não autorizado a acessar a informação, se ela é autêntica e possibilitar a auditoria nas ações efetuadas sobre ela.

Diffie e Hellman apresentam, nos anos 70, uma forma de atender a essas necessidades: a criptografia de chaves públicas. Utilizando um par de chaves diferentes, porém relacionadas, é possível transmitir informações de forma segura, garantindo que serão acessíveis apenas pelo destinatário. Utilizando esse conceito, as assinaturas digitais permitem também verificar se o emissor é realmente quem diz ser e, graças à utilização de *hashes*, possibilita conferir se o conteúdo da mensagem foi alterado. O gerenciamento dessas chaves, contudo, é problemático: como distribuí-las de forma segura? Como garantir a veracidade da identidade dos usuários?

Nesse contexto, surgem as Infraestruturas de Chaves Públicas (ICPs). De forma simplificada, ICPs são o conjunto de softwares, hardwares, processos e pessoas que suportam o gerenciamento do ciclo de vida dos certificados digitais, estruturas que relacionam entidades as suas chaves públicas. Por funcionar como uma identidade digital deve-se prover mecanismos que possibilitem a outras entidades verificar a validade desse relacionamento. Isso é possível através da inserção de uma terceira parte: a Autoridade Certificadora (AC). A AC age como âncora de confiança, permitindo o estabelecimento de uma relação de confiança entre duas entidades de forma transitiva. Entretanto, para que isso seja verdade, as entidades envolvidas em uma transição devem confiar na AC. Portanto, esta deve

prover aos usuários informações suficientes para que possam decidir se devem ou não confiar nos certificados emitidos por ela. Isso é feito através de documentos publicados pela AC, conhecidos como a Política de Certificados (PC) e a Declaração de Práticas de Certificação (DPC). PC e DPC podem também ser apresentados como um único documento, conhecido como PC/DPC.

Utilizando as técnicas de coleta de informação apresentadas por Chadwick e Basden (2001), este trabalho estabeleceu um conjunto de requisitos baseados nos principais padrões de segurança da informação e certificação digital. Ao segui-los, o autor de documentos de PC/DPC é capaz de definir políticas e práticas que possibilitem o oferecimento de um serviço de certificação digital de qualidade, característica identificada por Lekkas (2003) como essencial para o estabelecimento da confiança na AC. Um mapeamento completo entre os padrões e o principal arcabouço para elaboração de PCs e DPCs pode ser encontrado no anexo (Anexo do relatório técnico). O trabalho também se apresenta como uma solução aos problemas descritos por Schmeh (2007), ao sugerir uma tradução para português do Brasil das seções de um documento de PC/DPC, e apresentando um modelo para elaboração de documentos de PC/DPC.

O resultado deste esforço está sendo utilizado como um conjunto de requisitos mínimos de observância obrigatória na Infraestrutura de Chaves Públicas para Ensino e Pesquisa (ICPEDU), uma iniciativa da Rede Nacional de Ensino e Pesquisa (RNP). Um estudo de caso abordando sua aplicação nesse contexto é mostrado no capítulo 2.

Por fim, este trabalho contribui ao fornecer um conjunto de critérios aos usuários de certificados digitais e aos autores de documentos de PC/DPC para determinar que provisões sejam consideradas confiáveis nesses documentos, ao fornecer traduções para as seções propostas pela RFC 3647, ao apresentar um modelo de mapeamento entre as seções da RFC 3647 e as normas e padrões de segurança e certificação digital (figura 4.1), que pode ser utilizado em qualquer ICP dentro e fora do Brasil.

5.1 Trabalhos Futuros

Do ponto de vista do usuário (ou ainda, de uma Autoridade Certificadora buscando operar em conjunto com outra), a análise da confiança em uma AC pode ser simplificada através da automatização desse processo. O desenvolvimento de um software que efetue a comparação de um documento de PC/DPC com os requisitos propostos, é interessante para agilizar a avaliação desses documentos e pode utilizar os requisitos propostos como

critério para determinação de um índice de confiança.

A definição de uma métrica, baseada no resultado desse trabalho é importante para a definição de diferentes perfis. Estabelecer vários níveis de confiança (*Levels of Assurance - LoA*) permite ao usuário determinar o quanto uma AC é confiável para determinada aplicação, e decidir melhor se deve ou não aceitar um certificado. No contexto das federações, é possível estabelecer que conjunto de requisitos são aplicáveis de acordo com o serviço que será provido pela entidade federada.

Finalmente, outros documentos (como o Plano de Continuidade de Negócios - PCN) que não são abordados neste trabalho, também são importantes para garantir um serviço de certificação digital de qualidade. Futuramente, devem ser estabelecidos critérios para a elaboração desses documentos.

Referências

ADAMS, C.; LLOYD, S. *Understanding PKI: Concepts, Standards, and Deployment Considerations*. 2. ed. [S.l.]: Addison-Wesley Professional, 2002. ISBN 0672323915.

Autoridade de Gerência de Políticas da ICPEDU. *Declaração de Práticas de Certificação da Autoridade Certificadora Raiz da ICPEDU*. Brasil: Grupo de Operações da Autoridade Certificadora Raiz (GOPAR), 2008.

Autoridade de Gerência de Políticas da ICPEDU. *Requisitos Mínimos para Políticas de Certificado e Melhores Práticas de Certificação da ICPEDU*. Brasil: Rede Nacional de Ensio e Pesquisa (RNP), 2008.

BINDER, J. C. Public key infrastructure ("PKIs"): What are they? In: VACCA, J. R. *Public Key Infrastructure: Building Trusted Applications and Web Services*. 1. ed. [S.l.]: Auerbach Publications, 2004. p. 7–32.

BOWEN, P.; HASH, J.; WILSON, M. *Information Security Handbook: A Guide for Managers. NIST Special Publication 800-100*. Estados Unidos da América: National Institute of Standards and Technology, 2006.

BRASIL. *Medida Provisória nº 2.200-2 - Institui a Infra-Estrutura de Chaves Públicas Brasileira - ICP-Brasil, e dá outras providências.* Brasil: Diário Oficial, Agosto 2001.

CHADWICK, D. W.; BASDEN, A. Evaluating trust in a public key certification authority. *Computers & Security*, v. 20, n. 7, p. 592–611, 2001.

CHOKHANI, S.; FORD, W. *Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework. RFC 2527*. Estados Unidos da América: RFC Editor, 1999.

CHOKHANI, S.; FORD, W.; SABETT, R.; MERRILL, C.; WU, S. *Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework. RFC 3647*. Estados Unidos da América: RFC Editor, 2003.

Comitê Gestor da ICP-BRASIL. *Declaração de Práticas de Certificação da Autoridade Certificadora Raiz da ICP-BRASIL*. Brasil: Instituto Nacional de Tecnologia da Informação - ITI, 2008.

Conselho Federal de Medicina. *Resolução CFM nº 1.821 - Aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, e dá outras providências.* Brasil: Diário Oficial, Julho 2007.

COOPER, M.; DZAMBASOW, Y.; HESSE, P.; JOSEPH, S.; NICHOLAS, R. *Internet X.509 Public Key Infrastructure: Certification Path Building. RFC 4158*. Estados Unidos da América: RFC Editor, 2003.

DAEMEN, J.; RIJMEN, V. *The Design of Rijndael: AES - The Advanced Encryption Standard*. Berlin, Heidelberg, New York: Springer Verlag, 2002. ISBN 3-540-42580-2.

FRASER, B. *Site Security Handbook. RFC RFC2196*. United States: RFC Editor, 1997.

HOUSLEY, R.; POLK, W.; FORD, W.; SOLO, D. *Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile. RFC 3280*. Estados Unidos da América: RFC Editor, 2002.

HUNT, R. Pki and digital certification infrastructure. In: *ICON '01: Proceedings of the 9th IEEE International Conference on Networks*. Washington, DC, USA: IEEE Computer Society, 2001. p. 234. ISBN 0-7695-1186-4.

LEKKAS, D. Establishing and managing trust within the public key infrastructure. *Computer Communications*, v. 26, n. 16, p. 1815–1825, 2003.

LINN, J. *Trust Models and Management in Public-Key Infrastructures*. [S.l.]: RSA Laboratories, 2000.

MARQUES, D. C.; REBELLO, V. E. F. Certificação digital: Políticas de certificado e segurança para infra-estruturas de chaves públicas. *XVIII Seminário de Iniciação Científica e Prêmio Vasconcelos Torres*, 2008.

MARQUES, D. C.; REBELLO, V. E. F. Um conjunto de requisitos para políticas de certificado e declarações de práticas de certificação (resumo estendido). In: *Anais do IX Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais*. Campinas, SP, Brasil: Sociedade Brasileira de Computação, 2009. p. 249–250.

MARQUES, D. C.; REBELLO, V. E. F. *Mapeamento entre padrões de certificação digital e Segurança da Informação e a RFC 3647. Relatório Técnico*. Niterói, RJ, Brasil, 2010.

MENEZES, A.; OORSCHOT, P. van; VANSTONE, S. *Handbook of Applied Cryptography*. 5. ed. [S.l.]: CRC Press, 2001. ISBN 0849385237.

National Institute of Standards and Technology. *Data Encryption Standard (DES). Federal Information Processing Standards Publication 46-3*. Estados Unidos da América: National Institute of Standards and Technology, 1999.

SCHMEH, K. A critical view on rfc 3647. In: LOPEZ, J.; SAMARATI, P.; FERRER, J. L. (Ed.). *EuroPKI*. [S.l.]: Springer, 2007. (Lecture Notes in Computer Science, v. 4582), p. 369–374. ISBN 978-3-540-73407-9.

SCHNEIER, B. Description of a new variable-length key, 64-bit block cipher (blowfish. In: *In Fast Software Encryption, Cambridge Security Workshop Proceedings*. [S.l.]: Springer-Verlag, 1994. p. 191–204.

SCHNEIER, B. *Applied Cryptography: Protocols, Algorithms, and Source Code in C, Second Edition*. 2nd. ed. [S.l.]: Wiley, 1996. ISBN 0471117099.

Secretaria de Receita Federal. *Instrução Normativa SRF nº 625 - Dispõe sobre a Declaração de Débitos e Créditos Tributários Federais (DCTF).* Brasil: Diário Oficial, Dezembro 2006.

SÊMOLA, M. *Gestão da Segurança da Informação: Uma visão executiva.* 14. ed. [S.l.]: Elsevier, 2003. ISBN 8535211918.

SWANSON, M.; BOWEN, P.; WOHL, A. P.; GALLUP, D.; LYNES, D. *Contingency Planning Guide for Federal Information Systems. NIST Special Publication SP 800-34 Rev. 1.* Estados Unidos da América: National Institute of Standards and Technology, 2010.

Universidade Estadual de Campinas. *Declaração de Práticas de Certificação da Autoridade Certificadora da Unicamp.* Brasil: Universidade Estadual de Campinas, 2008.

WANG, X.; YU, H. How to break md5 and other hash functions. In: CRAMER, R. (Ed.). *EUROCRYPT.* [S.l.]: Springer, 2005. (Lecture Notes in Computer Science, v. 3494), p. 19–35. ISBN 3-540-25910-4.

APÊNDICE A – Mapeamento entre Padrões de Certificação Digital e Segurança da Informação e a RFC 3647

Este apêndice apresenta na íntegra o relatório técnico Mapeamento entre Padrões de Certificação Digital e Segurança da Informação e a RFC 3647, referenciado em diversas partes do texto. No relatório, o Anexo A apresenta as sugestões de tradução das seções da RFC 3647 para Português do Brasil, enquanto o Anexo B traz o mapeamento completo entre os padrões de Certificação Digital e de Segurança da Informação e a RFC 3647.

Mapeamento entre Padrões de Certificação Digital e Segurança da Informação e a RFC 3647

Daniel C. Marques, Vinod E. F. Rebello

Instituto de Computação
Universidade Federal Fluminense (UFF) – Niterói, RJ – Brasil
{dmarques, vinod}@ic.uff.br

Abstract. *One of the major challenges of managing a digital certification service is the development of Certificate Policies and Certification Practices Statements (CP/CPS) that provide relying parties with sufficient information to allow them to decide whether or not to trust a particular Certification Authority. This work proposes a mapping between information security and digital certification standards and the most important framework used to develop these CP/CPS documents, the RFC 3647, to facilitate the establishment of a trust relationship between the elements of a Public Key Infrastructure in a transitive manner.*

Resumo. *Um dos maiores desafios no gerenciamento de serviços de certificação digital é elaborar documentos de Política de Certificado e Declaração de Prática de Certificação (PC/DPC) que forneçam aos usuários informações suficientes para decidir se devem ou não confiar em uma Autoridade Certificadora. Este trabalho propõe um mapeamento entre padrões de segurança da informação e certificação digital e o principal arcabouço para elaboração desses documentos de PC/DPC, a RFC 3647, possibilitando o estabelecimento de uma relação de confiança entre os elementos de uma Infraestrutura de Chaves Públicas de forma transitiva.*

1. Introdução

A possibilidade de disponibilizar cada vez mais informações on-line e do crescimento da utilização de serviços como *Internet Banking*, ocasiona o aumento no volume de dados sensíveis disponíveis em meios de comunicação abertos. Consequentemente, a preocupação com sua integridade e autenticidade torna-se relevante, dada a demanda por mecanismos que controlem e registrem acessos e mudanças a estes dados. É o caso das bases de dados científicas: os resultados das pesquisas precisam ser mantidos consistentes, enquanto devem estar disponíveis apenas para quem é autorizado a utilizá-los. Surgem, também, padrões e regulamentações que exigem a utilização de sistemas com forte esquema de autenticação, e que permitam melhor controle sobre as identidades dos usuários.

Infraestruturas de Chaves Públicas (ICPs) tem-se tornado populares, por apresentarem uma solução de autenticação flexível, possibilitando a conformidade com os mais diversos requisitos técnicos e legais. O Conselho Federal de Medicina (CFM) determina, em sua Resolução [CFM 1821/2007], normas técnicas sobre a digitalização e

uso de sistemas informatizados para guarda e manuseio de prontuários, onde exige a utilização de certificados e assinaturas digitais para este fim.

Nesse contexto, uma Autoridade Certificadora (AC) age como âncora de confiança, estabelecendo uma relação confiável entre as entidades envolvidas em uma transação eletrônica. Contudo, seu gerenciamento apresenta um desafio: dada a subjetividade do conceito de confiança, essa relação transitiva só é possível se houver alguma forma de conhecer a AC o suficiente, para que uma opinião seja formada a seu respeito [Lekkas, 2003].

Atualmente, uma AC fornece aos seus usuários um conjunto de documentos com informações sobre suas políticas e procedimentos de gerenciamento dos serviços oferecidos por ela. Desses, a Política de Certificado (PC) e a Declaração de Prática de Certificação (DPC), são comumente divulgados. Ainda assim, a dificuldade em determinar se um certificado deve ou não ser aceito pela entidade confiante, sem prévio conhecimento da organização que administra a AC persiste, pois o padrão *de facto* utilizado atualmente para a elaboração desses documentos - a RFC 3647 [Chokani *et al*., 2003] do Internet Engineering Task Force - apresenta um arcabouço genérico para apoiar a elaboração desses documentos. Por esse motivo, não oferece critérios a serem considerados pelas entidades confiantes, restando ainda alguma complexidade no trabalho de elaboração de PCs e DPCs e deixando dúvidas sobre o que uma entidade confiante deve exigir de uma AC considerada confiável.

O objetivo deste trabalho é estabelecer um conjunto de requisitos que permita o preenchimento das lacunas deixadas pela RFC 3647 através de normas técnicas e padrões reconhecidos e consolidados de segurança e de certificação digital, definindo um conjunto de critérios a serem considerados por autores de PCs e DPCs e entidades confiantes. Este trabalho contribui ao determinar uma forma de preencher as lacunas deixadas pelo principal arcabouço para definição de políticas e procedimentos de certificação digital, ao estabelecer um modelo para elaboração de PCs e DPCs e fornecendo um template em português do Brasil para esses documentos.

Os requisitos resultantes deste esforço estão atualmente em vigor, servindo como critério parcial de observância obrigatória pelas ACs que desejam fazer parte da Infraestrutura de Ensino e Pesquisa (ICPEDU).

O restante do relatório está organizado da seguinte maneira. A seção 2 lista os trabalhos relacionados. A seção 3 apresenta o conceito de Política de Certificado (PC) e Declaração de Práticas de Certificação (DPC), sua relação e papel na confiança da ICP. A seção 4 aborda o principal arcabouço para a elaboração de PC e DPC, e discute alguns dos problemas existentes no documento. A seção 5 estabelece um modelo de mapeamento das principais normas técnicas e padrões de segurança da informação e certificação digital para suprir as lacunas deixadas pelo arcabouço citado na seção 3, enquanto a seção 6 conclui o trabalho.

2. Trabalhos Relacionados

[Lekkas, 2003] apresenta a noção de confiança e suas propriedades (como transitividade e seletividade), aborda também o problema do estabelecimento de confiança entre duas entidades através da utilização de uma terceira parte confiável (TPC) por ambas.

Discute fatores que refletem no nível de confiança das entidades na TPC são analisados e discutidos.

Em [Chadwick e Basden 2001], os autores apresentam um sistema especialista para cálculo de um quociente de confiança. Discutem a estratégia análise de conhecimento utilizada para coleta de informações, que servem de entrada para uma base de conhecimento dos fatores que afetam o valor final desse quociente.

[Schmeh, 2007] faz uma análise das principais deficiências da RFC 3647 e discute soluções para contorná-las e minimizar a dificuldade na elaboração de documentos de PC e DPC.

[Casola *et al*., 2007] apresenta maneiras de automatizar o processo de avaliação do nível de segurança de uma Autoridade Certificadora, comparando suas políticas a um *template* pré-determinado.

3. Política de Certificado e Declaração de Práticas de Certificação

Serviços de certificação digital são baseados em uma relação de confiança estabelecida entre a Autoridade Certificadora (AC) que emite os certificados digitais e as entidades envolvidas em uma transação eletrônica. Entretanto, devido à subjetividade do termo "confiança", o processo para estabelecimento dessa relação não é simples.

A AC deve, portanto, oferecer informações suficientes para apoiar a parte confiante e o titular do certificado (isto é, a entidade identificada pelo certificado e relacionada a um par de chaves) na decisão de utilizar ou não um certificado em uma determinada aplicação. A solução largamente adotada é a elaboração de documentos que descrevem as políticas e procedimentos adotados pela AC no gerenciamento do ciclo de vida de seus certificados, como a Política de Segurança (PS), o Plano de Continuidade de Negócios (PCN), a Política de Uso Aceitável (PUA), a Política de Certificados (PC) e a Declaração de Práticas de Certificação (DPC). Os dois últimos serão descritos com mais detalhes ao longo da seção, estando a elaboração dos demais - bem como de outros documentos que suportam as operações de uma AC - fora do escopo deste trabalho. Entretanto, sua relevância nas operações da AC não pode ser descartada. No contexto de uma ICP, a PS definirá os regras e mecanismos de relacionados à segurança das informações sob os quais as operações da AC serão efetuadas. No PCN, a AC deve divulgar o plano para recuperação das atividades de gerenciamento do ciclo de vida do certificado em caso de desastres. Na PUA, o foco está no uso permitido e proibido dos certificados, por parte de seus titulares, e dos equipamentos da AC por parte da equipe de operação. Portanto, PS, PCN, PUA e demais procedimentos internos (de recursos humanos, requisitos de treinamento, entre outros) devem ser considerados no momento da elaboração dos documentos, e referenciados quando apropriado.

A RFC 3647 [Chokani *et al*., 2003] define que uma Política de Certificados (PC) é um conjunto de diretivas que define a aplicabilidade de um certificado a um dado domínio como, por exemplo, uma comunidade em particular ou classe de aplicações. A PC é o canal que provê informações que permitam ao usuário do certificado identificar se este é apropriado para um uso em particular. Consequentemente uma AC pode publicar mais de uma PC (ou diferentes políticas em um único documento de PC), dependendo da aplicação ou tipo de certificado.

Conforme definido pelo mesmo documento, uma Declaração de Práticas de Certificação (DPC) é um relato das atividades (práticas) exercidas por uma AC 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.

A PC e a DPC podem ser publicados como um único documento – referido neste trabalho como PC/DPC –, e apenas trechos específicos do texto podem ser publicados, de acordo com a necessidade da ICP.

3.1. Relação entre PC e DPC

A PC e a DPC estão fortemente relacionadas. Em termos gerais, enquanto a PC define as regras de operação da uma AC (isto é, "o que" deve ser feito), a DPC descreve a implementação das regras definidas pela PC (ou seja, "como" são executadas as atividades necessárias para cumprir os requisitos estipulados).

É importante notar que, conforme o serviço oferecido pela AC evolui, a prática pode mostrar a necessidade na alteração das políticas estabelecidas. Isso significa que as estipulações tanto de uma PC quanto de uma DPC são dinâmicas, e frequentemente renovadas para se adequar a demandas novas das partes confiantes, requisitos legais ou identificados pelo grupo de usuários.

4. Um arcabouço para elaboração de PC/DPC: a RFC 3647

A RFC 3647 [Chokani *et al.*, 2003], que substitui a RFC 2527 [Chokani e Ford, 1999], apresenta um arcabouço para elaboração de PC e DPC, provendo aos autores uma lista de tópicos considerados potencialmente relevantes para esses documentos. Os tópicos são abordados em um conjunto de provisões agrupadas em nove capítulos (ou componentes), onde algumas podem não ser relevantes de acordo com a aplicação. Os componentes são apresentados a seguir em português:

1. **Introdução:** identifica e introduz as entidades envolvidas, o escopo da atuação da Autoridade Certificadora, e aplicabilidade dos certificados emitidos no âmbito da ICP.
2. **Responsabilidades Referentes a Publicações e Repositórios:** 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.
3. **Identificação e Autenticação:** aborda os nomes presentes no certificado, além dos métodos para validar a identidade de uma entidade antes da emissão do certificado.
4. **Requisitos Operacionais do Ciclo de Vida do Certificado:** estabelece os procedimentos adotados pela AC para gerenciar o ciclo de vida dos certificados, de sua solicitação até expiração ou revogação.
5. **Controles Operacionais, Gerenciais e de Instalações Físicas:** estabelece os controles operacionais, de segurança de pessoal e de segurança física usados para prover confiabilidade nas operações da ICP para seus participantes.

6. **Controles Técnicos de Segurança:** 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.
7. **Perfis dos Certificados, LCR e OCSP:** define o conteúdo e formato de certificados e Listas de Certificados Revogados (LCRs), tratando de que campos estão presentes, como devem ser preenchidos e interpretados.
8. **Auditoria de Conformidade:** 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. Inclui os tópicos cobertos, periodicidade e metodologia utilizada para a avaliação.
9. **Assuntos Legais e Assuntos Gerais:** aborda assuntos diversos relacionados a provisões legais, taxas a serem cobradas pelos serviços oferecidos, entre outros. O foco está nos aspectos legais e do negócio, portanto menos técnico que as demais seções.

A RFC 3647 mostra, também, sugestões sobre como o conteúdo das seções deve ser abordado.

Apesar de ser atualmente a base utilizada em vários documentos de PC/DPC pelo mundo, a RFC 3647 apresenta diversos problemas, conforme apontado em [Schmeh, 2007]. Primeiramente, dado seu caráter informacional, o arcabouço não pode se considerado oficialmente como um padrão. Isso leva a utilização dos mais diversos formatos para o desenvolvimento de documentos de PC/DPC. Sua organização não é intuitiva, e alguns títulos de seções provisões e suas respectivas descrições podem ocasionar interpretações imprecisas.

O arcabouço não determina qualquer provisão, possibilitando sua aplicação em qualquer ICP. Dessa forma, surge a necessidade de um conjunto de provisões que permita preencher as lacunas deixadas. Esse trabalho visa oferecer um conjunto de referências para compor esses espaços, possibilitando a definição de um modelo confiável para elaboração de documentos de PC/DPC.

5. Estabelecendo requisitos para Políticas de Certificado

A RFC 3647 definirá o formato no qual os documentos de PC/DPC serão elaborados. A partir dele, é possível extrair a organização das seções e provisões. Estas serão que serão preenchidas com o resultado da análise das referências, descritas mais adiante.

A experiência na elaboração de documentos de PC/DPC e da discussão com gerentes de AC mostrou que a primeira dificuldade encontrada é o estabelecimento de requisitos que atendam uma determinada comunidade. As políticas e procedimentos que guiam as operações de gerenciamento do ciclo de vida de certificado variam de acordo com o ambiente e aplicações nos quais seu par de chaves será utilizado.Dessa forma, o passo seguinte à construção da estrutura baseada na RFC 3647 é a análise da política de segurança e demais documentos operacionais e regimento interno da organização que irá gerenciar a AC.

5.1. Análise de referências e estabelecimento de requisitos

Em [Chadwick e Basden 2001], os autores apresentam alternativas para aquisição do conhecimento necessário para uma avaliação de confiança. Dentre as apresentadas, este trabalho utiliza padrões já reconhecidos relacionados à segurança da informação e certificação digital para definir o conjunto de referências que servirão de complemento à estrutura da RFC 3647. Essa abordagem permite o estabelecimento da relação de confiança entre AC e usuário de certificado de forma transitiva, pois, por conter conhecimento já consolidado e amplamente considerado como confiável, a AC que segue os padrões citados consegue garantir que os serviços de certificação oferecidos são gerenciados e operados de forma confiável.

Foi feita uma pesquisa para levantar os principais padrões e guias que pudessem suportar os processos de operação e gerenciamento de um serviço de certificação digital. Como base para seleção dos documentos, foi considerada a confiança pré-estabelecida pela comunidade de segurança da informação (isto é, documentos reconhecidos e consolidados como padrões). As seguintes referências foram determinadas relevantes no contexto desse trabalho:

- ISO/IEC 27001:2005 – *Information technology - Security techniques - Information security management systems – Requirements*: A International Organization for Standardization (ISO) é uma organização não-governamental reconhecida mundialmente, sendo a maior desenvolvedora e editora de padrões nos mais diversos setores. A ISO/IEC 27001 é um padrão para Sistemas de Gerenciamento de Segurança de Informações (SGSIs), cujo objetivo principal é prover um modelo para estabelecer, implementar, operar, monitorar, revisar e manter um SGSI, a partir de uma abordagem baseada em processos.
- ISO/IEC 27002:2005 - *Information technology - Security techniques - Code of practice for information security management*: É um padrão para ser usado associado à ISO/IEC 27001, que define boas práticas para estabelecer, implementar, operar, monitorar, revisar e manter um SGSI. Também procura oferecer um guia para "desenvolvimento de padrões organizacionais de segurança e práticas efetivas de gerenciamento de segurança e para ajudar a estabelecer confiança em relações inter-organizacionais".
- NIST SP 800-53 Rev. 2 - *Recommended Security Controls for Federal Information Systems*: É uma publicação do National Institute of Standards and Technology NIST - agência federal não-regulatória da câmara de comércio norte-americana - que serve como guia para estabelecer e escolher controles de segurança para sistemas de informação. É baseado em diversos outros documentos do NIST relacionados à Segurança de Informações e define níveis quantitativos de segurança de acordo com os controles apresentados, agrupados em famílias. Essa organização foi seguida durante este trabalho, a fim de manter a relação proposta por seus autores.
- ETSI TS 102 042 – *Policy Requirements for Certification Authorities Issuing Public Key Certificates*: O European Telecommunications Standards Institute (ETSI) produz padrões para Tecnologias da Informação e

Comunicação (TIC) aplicáveis globalmente. A especificação técnica TS 102 042 é baseada na mesma abordagem da TS 101 456, que provê um conjunto de requisitos para operação e gerenciamento de autoridades certificadoras emitindo certificados digitais qualificados de acordo com a diretiva 1999/93/EC do Parlamento Europeu e do *Council on a Community framework for electronic signatures*. A TS 102 042, entretanto, é aplicável a requisitos gerais de serviços de certificação digital.

- ANSI/X9 X9.79-1:2001 – *Financial Services Public Key Infrastructure (PKI) Policy and Practices Framework:* O American National Standards Institute (ANSI) supervisiona a criação, divulgação e utilização de milhares de normas e orientações que, impactam diretamente em diversas empresas dos mais diferentes setores. Define os componentes de uma ICP e um arcabouço para requisitos de políticas e práticas. Autoridades Certificadoras que implementam o padrão suportam múltiplas políticas que incorporam o uso de assinaturas digitais.

5.2. Mapeamento de referências na estrutura da RFC 3647

Passada a fase de levantamento e análise individual das referências, foi possível estabelecer uma relação entre os PC, DPC e os documentos pesquisados (Figura 1).

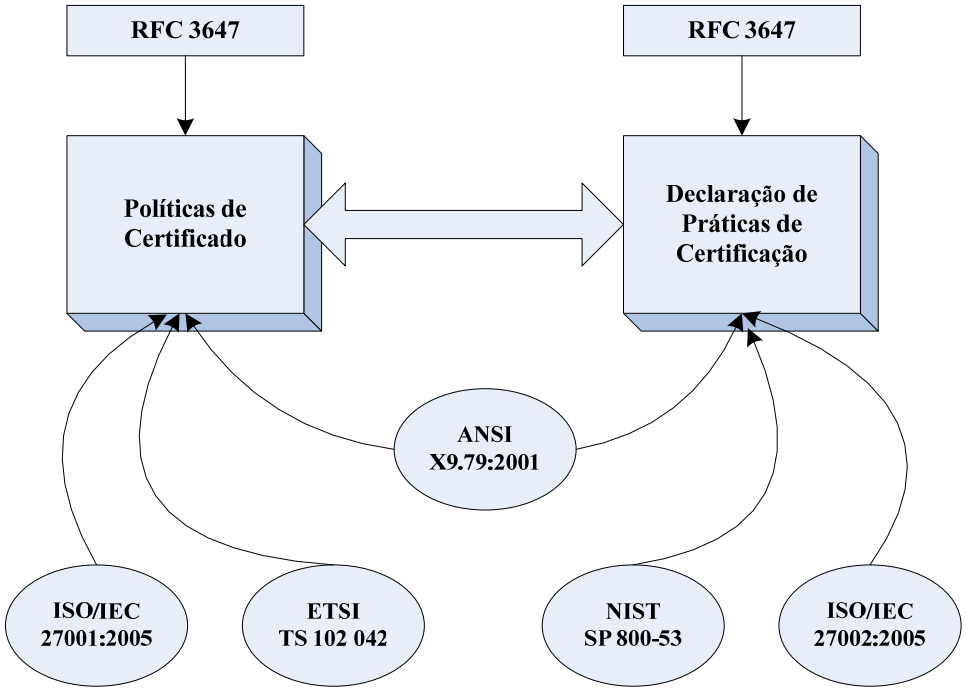

Figura 1. Relacionamento entre as referências e os documentos de PC e DPC

Para executar a tarefa do mapeamento, uma tabela contendo os componentes da RFC 3647 e suas respectivas definições foi criada. Entretanto, conforme comentado na seção anterior, a RFC 3647 nem sempre apresenta uma descrição formal do componente, sendo marcada na tabela como “Não Aplicável”. Para cada referência,

uma coluna foi estabelecida, contendo os itens relacionados ao componente presente na linha. A relação entre estes foi determinada a partir de três critérios:

- Relevância no contexto apresentado pelo componente;
- Análise do conteúdo da seção da referência;
- A experiência pessoal dos autores com o gerenciamento de segurança da informação e serviços de certificação digital;

É importante notar que existe certa correlação entre alguns dos padrões sugeridos, a exemplo de [ISO 27001] e [ISO 27002]. Nesse caso, as referências são usadas de forma complementar: a primeira apóia a definição de requisitos para políticas, enquanto a segunda fornece conteúdo relevante para uma boa implementação.

Tabela 1. Excerto do mapeamento seção 5 da RFC 3647 e as referências selecionadas

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	NIST SP 800-53
5.3.2 Background check procedures*	Descreve os procedimentos seguidos para verificar os antecedentes antes da contratação de um funcionário que ocupará papéis de confiança ou outras funções importantes.	A.5.3 Personnel Security Controls B.1.2 Security Management B.1.4 Personnel Security	Família Personnel Security
5.3.3 Training requirements*	Estabelece o processo de treinamento pelo qual o pessoal deverá passar.	A.5.3 Personnel Security Controls B.1.2 Security Management B.1.4 Personnel Security	Família Awareness and Training
5.3.4 Retraining frequency and requirements*	Estabelece a freqüência na qual deve haver um novo treinamento para o pessoal da AC.	A.5.3 Personnel Security Controls B.1.2 Security Management B.1.4 Personnel Security	Família Awareness and Training

Tabela 2. Excerto do mapeamento entre a seção 8 da RFC 3647 e as referências selecionadas

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	NIST SP 800-53
8.1 Frequency or circumstances of assessment*	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.	A.2.5 Compliance Audit B.1.10 Monitoring and Compliance	Famílias Certification, Accreditation, and Security Assessments e Audit and Accountability
8.2 Identity/qualifications of assessor*	Estabelece quem pode conduzir as avaliações, isto é, sua identidade e qualificações.	A.2.5 Compliance Audit B.1.10 Monitoring and Compliance	Famílias Certification, Accreditation, and Security Assessments e Audit and Accountability
8.3 Assessor's relationship to assessed entity*	Estabelece a relação do avaliador com a entidade avaliada, e sua autonomia.	A.2.5 Compliance Audit B.1.10 Monitoring and Compliance	Famílias Certification, Accreditation, and Security Assessments e Audit and Accountability

As Tabelas 1 e 2 apresentam excertos do mapeamento da Seção 5 - Controles Operacionais, Gerenciais e de Instalações Físicas, que pode ser encontrado na íntegra no Anexo A. Aqui, apenas o mapeamento para ANSI X9.79:2001 e o NIST SP 800-53 foi mantido, por limitações de espaço.

5.3. Elaborando um documento de PC/DPC utilizando o mapeamento proposto

É possível estabelecer o seguinte conjunto de atividades para a elaboração de uma PC/DPC:

1. Criação de um *template* estruturado no formato proposto pela RFC 3647;
2. Identificar requisitos legais, organizacionais e de aplicação;
3. Preenchimento do *template* de acordo aos requisitos organizacionais, identificados através do passo anterior, e requisitos da aplicação;
4. Revisão das estipulações definidas a partir dos requisitos de acordo com as normas e padrões de segurança e certificação;
5. Revisão geral do texto para garantir a consistência das provisões;
6. Implementar as políticas determinadas, verificando se são viáveis e fazendo modificações necessárias;
7. Avaliar conformidade entre política e prática, efetuando qualquer modificação que seja necessária para garanti-la;

8.Publicação

Como as referências usadas no mapeamento são, em sua maioria, genéricas (isto é, determinam linhas gerais que devem ser adaptadas para uma situação específica), os passos 2 e 3 são necessários para se compreender o contexto no qual o serviço de certificação digital está inserido. O passo 4 é extremamente importante para garantir as operações da AC estejam de acordo com padrões reconhecidos de segurança. Aqui, pode surgir a necessidade de uma análise mais cuidadosa, ocasionada por uma divergência entre as referências e as políticas e procedimentos identificados no passo 2. O resultado dessa análise poderá motivar mudanças políticas e procedimentos da organização, além do âmbito da ICP. O passo 5 é necessário dado a ambiguidade na RFC 3647 discutida anteriormente, reduzindo a possibilidade de inconsistências entre provisões. A tabela permite, então, que o autor das políticas e procedimentos da AC tenha acesso às referências de forma indexada, facilitando o processo de revisão.

Feito isso, as políticas devem ser aplicadas. Durante esse processo, é possível que a equipe da AC perceba que elas não sejam implementáveis (por restrições de tempo ou orçamento, por exemplo). Nesse caso, as provisões precisam ser revisadas, a fim de adequá-las a realidade da AC. A seguir, a conformidade entre a política e a prática deve ser verificada, a fim de alinhas as operações da AC ao estipulado nos documentos de PC e DPC.

Por fim, o documento precisa ser publicado. A AC deve disponibilizar, em um repositório de acesso público, toda a PC e DPC ou partes que considere relevantes. Dessa forma, usuários que desejem ter seus certificados emitidos pela AC, podem conhecer melhor como esta gerencia o ciclo de vida de seus certificados.

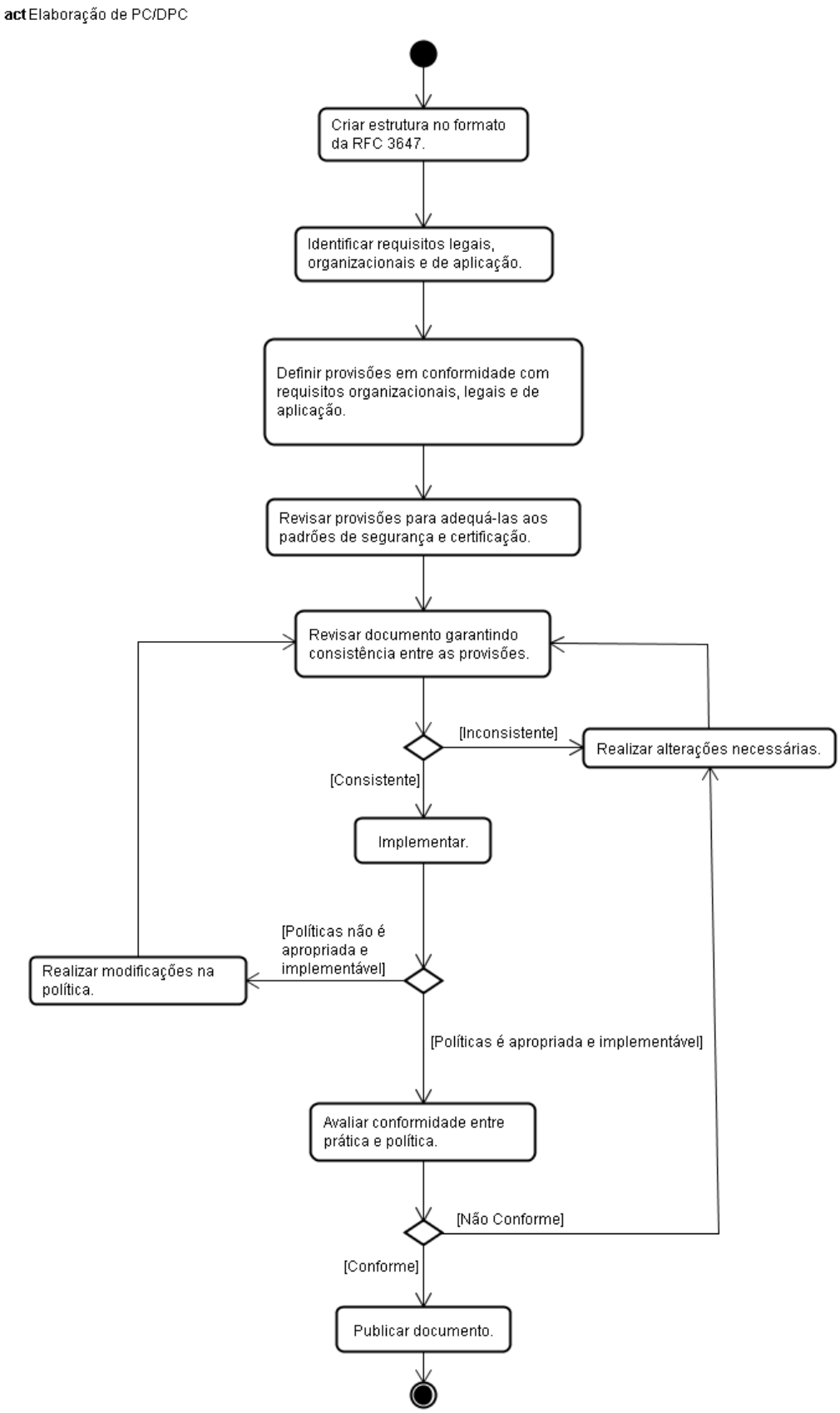

Figura 2. Passos para a elaboração de documentos de PC/DPC

6. Resultados

O mapeamento aqui proposto foi utilizado para a definição de um conjunto de requisitos mínimos para Políticas de Certificado. A partir deles, boas práticas associadas foram estabelecidas, compondo um documento intitulado "Requisitos Mínimos para Políticas de Certificado e Boas Práticas de Certificação da ICPEDU" [Autoridade de Gerência de Políticas da ICPEDU, 2009], fornecido aos Gerentes das ACs candidatas a fazer parte da ICP. Suas PCs e DPCs devem seguir as estipulações desse documento, que são de observância obrigatória para a adesão à ICPEDU. A Infraestrutura de Chaves Públicas para Ensino e Pesquisa (ICPEDU) é uma iniciativa da Rede Nacional de Ensino e Pesquisa (RNP). Sua proposta consiste na implantação de uma infraestrutura nacional de criação de certificados digitais, dentro do ambiente das Instituições Federais de Ensino Superior (Ifes) e Unidades de pesquisa (UPs). A seguir, um trecho do documento exemplifica os requisitos estabelecidos:

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.*

Durante o processo de adesão das instituições, suas PCs e DPCs são revisadas com o objetivo de verificar sua conformidade com os requisitos mínimos. Estes requisitos colaboram como uma solução para os problemas na utilização da RFC 3647 apresentados por [Schmeh, 2007]. Fornecer critérios para os usuários decidirem se devem ou não confiar em uma AC da ICPEDU, sem que leiam todas as PCs e DPCs da infraestrutura.

Esses requisitos também podem ser utilizados como entrada para a base de conhecimento necessária ao sistema especialista proposto por [Chadwick e Basden 2001] para avaliar a confiança a partir de PCs e DPCs, bem como referência para a comparação automática proposta em [Casola *et al*., 2007].

7. Conclusão

Ao passo que as Infraestruturas de Chave Pública se popularizam, novos desafios surgem para estabelecer a confiança entre titulares de certificado, entidades confiantes e Autoridades Certificadoras. Nesse contexto, as Políticas de Certificado e Declarações de Prática de Certificação assumem um papel crucial por fornecer informações suficientes para tal, permitindo a uma entidade escolher se deve ou não confiar em quem os emitiu. Entretanto, a experiência mostra que complexidade na elaboração de documentos

confiáveis é grande dada as lacunas existentes no arcabouço frequentemente utilizado para a atividade.

Algumas das referências utilizadas no trabalho (como as normas ISO 27001 e ISO 27002, por exemplo) são, em essência, genéricas. Isso significa que o autor que utilize a abordagem, deve conhecer o contexto no qual as provisões feitas nos documentos serão inseridas. Por isso, é recomendado que sejam consideradas políticas e procedimentos da organização que proverá o serviço de certificação e requisitos da aplicação na qual os certificados emitidos serão utilizados.

O mapeamento aqui proposto resolve parcialmente o problema oferecendo um ponto de partida aos autores de PC e DPC, de forma a suportar o processo de escrita e revisão desses documentos. Além disso, uma relação de confiança é estabelecida de forma transitiva, pois, a AC assume seguir determinações reconhecidas como confiáveis. O mapeamento completo pode ser encontrado no anexo A. O conjunto de passos determinado no item 5.3 deste relatório pode ser utilizado como guia, principalmente por aqueles que não possuem experiência na elaboração dos documentos.

Este trabalho foi utilizado como base para o desenvolvimento de um conjunto de requisitos para Autoridades Certificadoras participantes da ICPEDU. No futuro, será estendido para um guia de elaboração de Políticas de Certificado e Declarações de Prática de Certificação - no formato da RFC 3647 - com objetivo de facilitar a escrita, resolver os problemas de duplicidade e inconsistência e possibilitar a comparação automática entre documentos de PC/DPC, permitido o estabelecimento matemático de níveis de confiança.

Referências

American National Standards Institute/X9 (2005), ANSI/X9 X9.79-1: Financial Services Public Key Infrastructure (PKI) Policy and Practices Framework

Autoridade de Gerência de Políticas da ICPEDU (2009), Requisitos Mínimos para Políticas de Certificado e Boas Práticas de Certificação da ICPEDU, Disponível em: http://www.icp.edu.br/wiki/documentos

Canadian Institute of Chartered Accountants (2008), WEBTRUST For Certification Authorities – Extended Validation Audit Criteria, Disponível em: http:// http://www.webtrust.org/index.cfm/ci_id/43988/la_id/1.htm

Casola, V., Luna, J., Manso, O., Mazzoca, N., Medina, M., Rak, M. (2007), Static evaluation of Certificate Policies for GRID PKIs interoperability, Proceedings of the First International Conference on Availability, Reliability and Security (ARES'07).

Chadwick, D. W., e Basden, A. (2001), Evaluating Trust in a Public Key Certification Authority, Computers & Security, 20(7), 592-611, doi:10.1016/S0167-4048(01)00710-6.

Chokhani , S., e Ford, W. (1999), RFC 2527: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Disponível em: http://www.ietf.org/rfc/rfc2527.txt

Chokhani , S., Ford, W., Sabett, R., Merrill, C. e Wu, S. (2003), RFC 3647: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Disponível em: http://www.ietf.org/rfc/rfc3647.txt

Conselho Regional de Medicina (CRM) (2007), Resolução CFM Nº. 1.821: Aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde, Disponível em: http://www.sbis.org.br/site/site.dll/noticia?pagina=1&item=51

Cooper , D., Santesson, S., Farrel, S., Boeyen, S., Housley, R. Polk e W. (2008), RFC 5280: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Disponível em: http://www.ietf.org/rfc/rfc5280.txt

European Telecommunications Standards Institute/Technical Committee Electronic Signatures and Infrastructures (2002), ETSI TS 101 456: Policy requirements for certification authorities issuing qualified certificates

European Telecommunications Standards Institute/Technical Committee Electronic Signatures and Infrastructures (2005), ETSI TS 102 042: Policy requirements for certification authorities issuing public key certificates

International Organization for Standardization/International Electrotechnical Commission (2005), ISO/IEC 27001: Information technology - Security techniques - Information security management systems – Requirements

International Organization for Standardization/International Electrotechnical Commission (2005), ISO/IEC 27002: Information technology - Security techniques - Code of Practice for Information Security Management

Lekkas, D. (2003), Establishing and managing trust within the public key infrastructure, Computer Communications, 26(16), 1815-1825.

National Institute of Standards and Technology (2007), Special Publication, NIST SP 800-53: Recommended Security Controls for Federal Information Systems

Schmeh, K. (2007), A Critical View on RFC 3647, in Public Key Infrastructure, pp. 369-374, EuroPKI 2007.

Anexo A – Sugestões de tradução dos componentes da RFC 3647 para português do Brasil

Conforme identificado por [Schmeh, 2007], não existem traduções oficiais dos componentes da RFC 3647. Essa questão pode dificultar a padronização dos documentos de PC e DPC em português do Brasil. Uma sugestão de tradução é apresentada a seguir, a fim de minimizar o problema.

Procurou-se apresentar nomes que representassem facilmente o objetivo das seções em português do Brasil, ainda que mantendo o sentido original do títulos.

Componentes da RFC 3647	Descrição do componente	Tradução para português do Brasil
1. Introduction	-	**1. Introdução**
1.1 Overview	Provê uma introdução geral ao documento, podendo ser usado para prover uma apresentação da ICP na qual a PC/DPC se aplica.	**1.1 Visão geral**
1.2 Document name and Identification	Provê quaisquer nomes ou outros identificadores aplicáveis, como identificadores de objetos ASN.1, para o documento.	**1.2 Nome do document e identificação**
1.3 PKI Participants	Apresenta a identidade ou tipos de entidades que assumem os papéis da ICP.	**1.3 Participantes da ICP**
1.3.1 Certification authorities*	Apresenta as ACs responsáveis pela emissão dos certificados na ICP.	1.3.1 Autoridades Certificadoras
1.3.2 Registration authorities*	Apresenta os responsáveis pelas funções de identificação e registro na ICP.	1.3.2 Autoridades de Registro
1.3.3 Subscribers*	Apresenta potenciais titulares de certificados.	1.3.3 Titulares dos Certificados
1.3.4 Relying parties*	Apresenta potenciais entidades que confiam nos certificados, recebendo e-mails assinados, por exemplo.	1.3.4 Entidades Confiantes
1.3.5 Other participants*	Apresenta outras entidades que ofereçam serviços relacionados a certificação digital para a ICP.	1.3.5 Outros Participantes
1.4 Certificate Usage	Contém usos reconhecidos como apropriados ou proibidos para os certificados da ICP, podendo considerar níveis de confiança previamente estabelecidos para determinadas aplicações.	**1.4 Uso do Certificado**

Componentes da RFC 3647	Descrição do componente	Tradução para português do Brasil
1.4.1 Appropriate certificate uses*	Lista os tipos de aplicações para as quais o uso do certificado é apropriado.	1.4.1 Aplicações apropriadas para os certificados
1.4.2 Prohibited certificate uses*	Lista os tipos de aplicações para as quais o uso do certificado é proibido.	1.4.2 Aplicações proibidas para os certificados
1.5 Policy Administration	Apresenta informações de contato para questões relacionadas ao documento de PC/DPC.	**1.5 Dados para contato**
1.5.1 Organization administering the document*	Apresenta informações sobre a organização que administra o documento.	1.5.1 Entidade responsável por este documento
1.5.2 Contact person*	Apresenta informações para contato da pessoa responsável pelo documento, podendo ser um papel na operação da AC.	1.5.2 Ponto de Contato
1.5.3 Person determining CPS suitability for the policy*	Apresenta a pessoa (ou papel) responsável por garantir a adequação da DPC à política de uma determinada ICP, caso haja uma Autoridade de Gerência de Política responsável.	1.5.3 Responsável por determinar adequabilidade da DPC à política
1.5.4 CPS approval procedures*	Apresenta os procedimentos para a aprovação da DPC, no caso anterior.	1.5.4 Procedimentos de aprovação da PC
1.6 Definitions and Acronyms	Lista definições e acrônimos usados no documento.	**1.6 Definições e Acrônimos**
1.6.1 Definitions*	Apresenta definições dos termos usados na PC/DPC.	1.6.1 Definições*
1.6.2 Acronyms*	Apresenta acrônimos e seus significados usados na PC/DPC	1.6.2 Acrônimos*
2. Publication and Repository Responsabilities	-	2. Responsabilidades referentes a publicações e repositórios
2.1 Repositories*	Identifica os repositórios onde as informações da AC estarão disponíveis.	2.1 Repositórios
2.2 Publication of certification information*	Apresenta as informações da AC que serão publicadas e os mecanismos usados para fazê-lo.	2.2 Publicação de informações
2.3 Time or frequency of publication*	Informa quando e com que freqüência as informações apresentadas anteriormente são publicadas.	2.3 Frequência de publicação

Componentes da RFC 3647	Descrição do componente	Tradução para português do Brasil
2.4 Access controls on repositories*	Apresenta os controles impostos nos objetos repositórios para garantir a integridade da informação apresentada.	2.4 Controles de acesso aos repositórios
3. Identification and Authentication	-	**3. Identificação e Autenticação**
3.1 Naming	Apresenta provisões a respeito dos nomes utilizados nos certificados emitidos pela AC.	**3.1 Estrutura de Nomes**
3.1.1 Types of names*	Apresenta o formato dos nomes designados aos titulares dos certificados, como X.500, RFC 822 e X.400.	3.1.1 Tipos de nomes
3.2.2 Need for names to be meaningful*	Informa se os nomes nos certificados emitidos devem ou não ser significativos.	3.1.2 Necessidade de que nomes sejam significativos
3.3.3 Anonymity or pseudonymity of subscribers*	Informa se um titular de certificado pode ou não ser anônimo ou usar pseudônimos, e quais pseudônimos serão designados a eles.	3.1.3 Anonimato dos titulares de certificado
3.1.4 Rules for interpreting various name forms*	Apresenta as regras para interpretação dos nomes, como X.500 e RFC 822.	3.1.4 Regras para interpretação dos diversos formatos de nomes
3.1.5 Uniqueness of names*	Determina se os nomes devem ou não ser únicos no universo da ICP.	3.1.5 Unicidade dos nomes
3.1.6 Recognition, authentication, and role of trademarks*	Apresenta os procedimentos para reconhecimento, autenticação de marcas registradas e o seu papel na nomeação dos titulares.	3.1.6 Reconhecimento, autenticação e papel de marcas registradas
3.2 Initial Identity Validation	Aborda os procedimentos de identificação e autenticação para o registro inicial de cada tipo de titular de certificado (AC, AR, entre outros).	**3.2 Validação Inicial da Identidade**
3.2.1 Method to prove possession of private key*	Estabelece os métodos que deverão ser usados pela AC para comprovar que o solicitante possui a chave privada que faz par a chave pública que está sendo registrada.	3.2.1 Método para prova de posse da chave privada

Componentes da RFC 3647	Descrição do componente	Tradução para português do Brasil
3.2.2 Authentication of organization identity*	Apresenta os requisitos para identificação e autenticação da identidade organizacional do titular do certificado ou participante da ICP. Pode ser uma consulta aos registros da organização, por exemplo.	3.2.2 Autenticação da identidade organizacional
3.2.3 Authentication of individual identity*	Apresenta os requisitos para identificação e autenticação da identidade do titular do certificado ou de um indivíduo atuando em nome de uma organização.	3.2.3 Autenticação da identidade individual
3.2.4 Non-verified subscriber information*	Lista as informações do titular de certificado que não são verificadas inicialmente.	3.2.4 Dados dos titulares de certificado que não são verificados
3.2.5 Validation of authority*	Apresenta os procedimentos para verificar se um indivíduo tem direito ou permissão para agir em nome de uma organização.	3.2.5 Validação de autoridade
3.2.6 Criteria for interoperation*	Apresenta os critérios utilizados para que uma AC que deseje fazer parte da ICP possa fazê-lo.	3.2.6 Critérios para interoperabilidade
3.3 Identification and Authentication for Re-key Requests	Aborda os procedimentos de identificação e autenticação para solicitações de troca de par de chaves (isto é, um novo certificado é emitido com um novo par de chaves, mas mantendo os atributos anteriores).	**3.3 Identificação e Autenticação para Requisição de Substituição de Chaves**
3.3.1 Identification and authentication for routine re-key*	Apresenta os requisitos para identificação e autenticação para requisições de troca de par de chaves de rotina, quando ainda há uma chave privada válida.	3.3.1 Identificação e autenticação para troca de chaves de rotina
3.3.2 Identification and authentication for re-key after revocation*	Apresenta os requisitos para identificação e autenticação para requisições de troca de par de chaves após a revogação do certificado.	3.3.2 Identificação e autenticação para troca de chaves após revogação
3.4 Identification and Authentication for Revocation Requests	Aborda os procedimentos de identificação e autenticação para solicitações de revogação de certificados (pedidos assinados pela chave privada correspondente, verificação pessoal da AR, por exemplo).	3.4 Identificação e Autenticação para Requisição de Revogação

Componentes da RFC 3647	Descrição do componente	Tradução para português do Brasil
4 Certificate Life-Cycle Operational Requirements	-	**4 Requisitos Operacionais do Ciclo de Vida do Certificado**
4.1 Certificate Application	Trata dos requisitos relacionados à solicitação de um certificado.	4.1 Procedimentos do requerente para solicitar o certificado
4.1.1 Who can submit a certificate application*	Apresenta quem pode solicitar um certificado a AC.	4.1.1 Quem pode submeter uma solicitação de certificado
4.1.2 Enrollment process and responsibilities*	Apresenta o procedimento para solicitação do certificado e as responsabilidades do solicitante associadas a esse processo.	4.1.2 Processo de solicitação e responsabilidades
4.2 Certificate Application Processing	Descreve o conjunto de passos que serão seguidos para processamento das solicitações, causado a aceitação ou rejeição destas, de acordo com um o critério estabelecido.	**4.2 Processamento da solicitação pela AR**
4.2.1 Performing identification and authentication functions*	Descreve os procedimentos para identificação e autenticação para validar a solicitação.	4.2.1 Realização das funções de identificação e autenticação
4.2.2 Approval or rejection of certificate applications*	Estabelece o critério que determinará a aceitação ou rejeição de um pedido de certificado.	4.2.2 Aprovação ou rejeição das solicitações
4.2.3 Time to process certificate applications*	Estabelece um limite de tempo para o processamento das solicitações por parte da AC e/ou AR.	4.2.3 Tempo para processamento das solicitações
4.3 Certificate Issuance	Descreve os elementos relacionados a assinatura (emissão) do certificado solicitado.	**4.3 Processamento da solicitação pela AC**
4.3.1 CA actions during certificate issuance*	Descreve as ações da AC durante a emissão do certificado.	4.3.1 Ações da AC durante a emissão de certificado
4.3.2 Notification to subscriber by the CA of issuance of certificate*	Descreve os meios pelos quais o solicitante será informado da emissão do certificado.	4.3.2 Notificação da emissão do certificado pela AC para o solicitante
4.4 Certificate Acceptance	Apresenta o procedimento para solicitação do certificado e as resposabilidades do solicitante associadas a esse processo.	4.4 Aceitação do certificado pelo solicitante
4.4.1 Conduct constituting certificate acceptance*	Descreve os requisitos e procedimentos operacionais referentes à aceitação do certificado emitido.	4.4.1 Conduta que constitui a aceitação do certificado

Componentes da RFC 3647	Descrição do componente	Tradução para português do Brasil
4.4.2 Publication of the certificate by the CA*	Descreve os requisitos e procedimentos operacionais referentes à publicação do certificado emitido.	4.4.2 Publicação do certificado pela AC
4.4.3 Notification of certificate issuance by the CA to other entities*	Estabelece se haverá notificação de outras entidades sobre a emissão do certificado, seus requisitos e procedimentos.	4.4.3 Notificação da emissão do certificado pela AC para outras entidades
4.5 Key Pair and Certificate Usage	Apresenta as responsabilidades na utilização do par de chaves e respectivo certificado.	**4.5 Utilização de pares de chaves e de certificados**
4.5.1 Subscriber private key and certificate usage*	Estabelece as responsabilidades do titular do certificado pela utilização das chaves privadas e dos certificados.	4.5.1 Responsabilidade pela utilização das chaves privadas e dos certificados por parte dos titulares
4.5.2 Relying party public key and certificate usage*	Estabelece as responsabilidades da entidade confiante pela utilização das chaves públicas e dos certificados.	4.5.2 Responsabilidade pela utilização das chaves públicas e dos certificados por parte das entidades confiantes
4.6 Certificate Renewal	Apresenta os procedimentos, responsabilidades e circunstâncias para renovação do certificado, isto é, emissão de um novo certificado em substituição ao antigo com os mesmos atributos do certificado e par de chaves do titular.	**4.6 Reemissão de certificados por troca do prazo de validade**
4.6.1 Circumstance for certificate renewal*	Estabelece as circunstâncias sob as quais uma renovação deve ser solicitada, quando aplicável.	4.6.1 Circunstância para renovação de certificados
4.6.2 Who may request renewal*	Estabelece quem está autorizado a solicitar a renovação de um certificado, se aplicável.	4.6.2 Quem pode solicitar renovação
4.6.3 Processing certificate renewal requests*	Estabelece as medidas que AC e AR devem tomar para validar e responder pedidos de renovação, quando aplicável.	4.6.3 Processamento de solicitações de renovação
4.6.4 Notification of new certificate issuance to subscriber*	Estabelece se a AC comunicará o titular do certificado sobre a renovação, e os procedimentos e requisitos para fazê-lo.	4.6.4 Notificação de nova emissão de certificado para o titular
4.6.5 Conduct constituting acceptance of a renewal certificate*	Estabelece a conduta de um titular de certificado que caracterize a aceitação de um certificado renovado.	4.6.5 Conduta que constitui aceitação de um certificado renovado
4.6.6 Publication of the renewal certificate by the CA*	Especifica os locais de publicação dos certificados renovados.	4.6.6 Publicação do certificado renovado pela AC

Componentes da RFC 3647	Descrição do componente	Tradução para português do Brasil
4.6.7 Notification of certificate issuance by the CA to other entities*	Estabelece se a AC comunicará outras entidades (AR e partes confiantes, por exemplo) sobre a renovação.	4.6.7 Notificação pela AC da emissão de um certificado para outras entidades
4.7 Certificate Re-key	Apresenta os procedimentos, responsabilidades e circunstâncias para renovação do certificado, isto é, emissão de um novo certificado em substituição ao antigo com os mesmos atributos do certificado e um novo par de chaves do titular.	**4.7 Reemissão de certificados por troca de chaves**
4.7.1 Circumstance for certificate re-key*	Estabelece as circunstâncias sob as quais as chaves criptográficas devem ser trocadas, quando aplicável.	4.7.1 Circunstâncias para substituição das chaves criptográficas
4.7.2 Who may request certification of a new public key*	Estabelece, quando aplicável, quem está autorizado a solicitar a troca de chaves de um certificado.	4.7.2 Quem pode solicitar a certificação de uma nova chave pública
4.7.3 Processing certificate re-keying requests*	Estabelece as medidas tomadas por AC ou AR para processar solicitações de substituição de par de chaves de certificados.	4.7.3 Processamento de solicitações de substituição de certificados
4.7.4 Notification of new certificate issuance to subscriber*	Estabelece se a AC comunicará o titular do certificado sobre a emissão do novo certificado, e os procedimentos e requisitos para fazê-lo.	4.7.4 Notificação de nova emissão de certificado para o titular
4.7.5 Conduct constituting acceptance of a re-keyed certificate*	Estabelece a conduta de um titular de certificado que caracterize a aceitação do novo certificado.	4.7.5 Conduta para a aceitação de um novo certificado
4.7.6 Publication of the re-keyed certificate by the CA*	Especifica os locais e procedimentos de publicação dos novos certificados.	4.7.6 Publicação do novo certificado
4.7.7 Notification of certificate issuance by the CA to other entities*	Estabelece se a AC comunicará outras entidades (AR e partes confiantes, por exemplo) sobre a emissão do novo certificado.	4.7.7 Notificação pela AC da emissão de um certificado para outras entidades
4.8 Certificate Modification	Apresenta os procedimentos, responsabilidades e circunstâncias para modificação do certificado, isto é, emissão de um novo certificado em substituição ao antigo com modificações nos atributos do certificado e mantendo par de chaves do titular.	**4.8 Reemissão de certificados por troca de dados**

Componentes da RFC 3647	Descrição do componente	Tradução para português do Brasil
4.8.1 Circumstance for certificate modification*	Estabelece as circunstâncias sob um certificado pode ser modificado.	4.8.1 Circunstâncias para modificação de certificados
4.8.2 Who may request certificate modification*	Estabelece, quando aplicável, quem está autorizado a solicitar a modificação de um certificado.	4.8.2 Quem pode solicitar a modificação de um certificado
4.8.3 Processing certificate modification requests*	Estabelece as medidas tomadas por AC ou AR para processar solicitações de modificação de certificados.	4.8.3 Processamento de solicitações de modificação de certificados
4.8.4 Notification of new certificate issuance to subscriber*	Estabelece se a AC irá comunicar o titular sobre a emissão do novo certificado.	4.8.4 Notificação de nova emissão de certificado para o titular
4.8.5 Conduct constituting acceptance of modified certificate*	Estabelece a conduta de um titular de certificado que caracterize a aceitação de um novo certificado modificado.	4.8.5 Conduta para a aceitação de um novo certificado modificado
4.8.6 Publication of the modified certificate by the CA*	Especifica os locais e procedimentos de publicação do certificado modificado.	4.8.6 Publicação do certificado pela AC
4.8.7 Notification of certificate issuance by the CA to other entities*	Estabelece se a AC comunicará outras entidades (AR e partes confiantes, por exemplo) sobre a modificação no certificado.	4.8.7 Notificação pela AC da emissão de um certificado para outras entidades
4.9 Certificate Revocation and Suspension	Apresenta os procedimentos, responsabilidades e circunstâncias para revogação e suspensão de certificados.	**4.9 Revogação e Suspensão**
4.9.1 Circumstances for revocation*	Estabelece as circunstâncias sob as quais um certificado deve ser revogado.	4.9.1 Circunstâncias para revogação de certificados
4.9.2 Who can request revocation*	Estabelece quem está autorizado a solicitar a revogação de um certificado.	4.9.2 Quem pode solicitar revogação
4.9.3 Procedure for revocation request*	Estabelece as medidas tomadas por AC ou AR para processar solicitações de revogação de certificados.	4.9.3 Processamento de solicitações de revogação
4.9.4 Revocation request grace period*	Estabelece um prazo para solicitação de revogação caso ocorra qualquer circunstância definida no item 4.9.1.	4.9.4 Prazo para solicitação de revogação

Componentes da RFC 3647	Descrição do componente	Tradução para português do Brasil
4.9.5 Time within which CA must process the revocation request*	Estabelece um prazo para AC processar uma solicitação de revogação.	4.9.5 Prazo para a AC processar a solicitação de revogação
4.9.6 Revocation checking requirement for relying parties*	Estabelece mecanismos que devem ser usados pelas entidades confiantes a fim de verificar o status de certificados e determinar se são confiáveis.	4.9.6 Requisitos para verificação de revogação por entidades confiantes
4.9.7 CRL issuance frequency (if applicable)*	Estabelece a freqüência na qual uma nova Lista de Certificados Revogados (LCR) deve ser emitida, se aplicável.	4.9.7 Freqüência de emissão de LCRs
4.9.8 Maximum latency for CRLs (if applicable)*	Estabelece o tempo máximo entre a geração de uma LCR e sua publicação no repositório da AC, se aplicável.	4.9.8 Latência máxima para LCRs
4.9.9 On-line revocation/status checking availability*	Estabelece, se aplicável, um mecanismo on-line que permita a verificação do status do certificado.	4.9.9 Mecanismos para verificação on-line do status de certificados
4.9.10 On-line revocation checking requirements*	Define as obrigações das entidades confiantes quanto à verificação on-line do status de certificados	4.9.10 Obrigações da entidade confiante de verificar on-line o status de certificados
4.9.11 Other forms of revocation advertisements available*	Estabelece formas alternativas de comunicação de revogação.	4.9.11 Outras formas de comunicação de revogação
4.9.12 Special requirements for key compromise*	Estabelece procedimentos específicos para revogações em caso de comprometimento de chave privada.	4.9.12 Procedimentos adicionais no caso de comprometimento da chave privada
4.9.13 Circumstances for suspension*	Estabelece as circunstâncias sob um certificado pode ser suspenso.	4.9.13 Circunstâncias para suspensão de certificados
4.9.14 Who can request suspension*	Estabelece quem está autorizado a solicitar a suspensão de um certificado.	4.9.14 Quem pode solicitar suspensão
4.9.15 Procedure for suspension request*	Estabelece as medidas tomadas por AC ou AR para processar solicitações de suspensão de certificados.	4.9.15 Processamento de solicitações de suspensão
4.9.16 Limits on suspension period*	Define um período máximo de suspensão de certificados.	4.9.16 Limites para o período de suspensão

Componentes da RFC 3647	Descrição do componente	Tradução para português do Brasil
4.10 Certificate Status Services	Apresenta as características e requisitos do serviço de verificação de status de certificados providos pela AC para as entidades confiantes.	**4.10 Serviços de status de certificado**
4.10.1 Operational characteristics*	Estabelece as características do serviço de verificação do status de certificados.	4.10.1 Características operacionais
4.10.2 Service availability*	Define a disponibilidade do serviço e sob que circunstâncias ele pode se tornar indisponível.	4.10.2 Disponibilidade do serviço
4.10.3 Optional features*	Define quaisquer características opcionais dos serviços de verificação de status de certificado.	4.10.3 Características operacionais
4.11 End of Subscription	Estabelece os procedimentos que caracterizam o encerramento do vínculo do titular com a AC.	**4.11 Encerramento do vínculo com a AC**
4.12 Key Escrow and Recovery	Apresenta as características e requisitos para custódia e recuperação de chaves privadas, quando o serviço é oferecido pela AC ou uma terceira parte confiável.	**4.12 Custódia e recuperação de chaves**
4.12.1 Key escrow and recovery policy and practices*	Define um documento ou estabelece práticas e políticas para custódia e recuperação de chaves.	4.12.1 Políticas e práticas para custódia e recuperação de chaves
4.12.2 Session key encapsulation and recovery policy and practices*	Define um documento ou Estabelece práticas e políticas para custódia e recuperação de chaves de sessão.	4.12.2 Políticas e práticas para custódia e recuperação de chaves de sessão
5. Facility, Management, and Operational Controls	-	**5. Controles operacionais, gerenciais e de instalações físicas**
5.1 Physical Security Controls	Apresenta os controles de segurança física nas instalações que abrigam os sistemas da AC.	**5.1 Controles de Segurança Física**
5.1.1 Site location and construction*	Define a localização do ambiente que abriga os sistemas da AC, bem como os requisitos de segurança da construção.	5.1.1 Localização e construção das instalações físicas
5.1.2 Physical Access*	Define os mecanismos de controle de acesso físico ao ambiente que abriga a AC.	5.1.2 Acesso físico

Componentes da RFC 3647	Descrição do componente	Tradução para português do Brasil
5.1.3 Power and air conditioning*	Estabelece as medidas tomadas para manutenção da energia e da temperatura ideal no local de operação da AC.	5.1.3 Energia e refrigeração
5.1.4 Water exposures*	Define as medidas tomadas para evitar a exposição dos sistemas a enchentes e alagamentos.	5.1.4 Exposição à água
5.1.5 Fire prevention and protection*	Define as medidas tomadas para evitar a exposição dos sistemas incêndios.	5.1.5 Prevenção e proteção contra incêndio
5.1.6 Media storage*	Define os requisitos para prevenção contra acesso, modificação, remoção e destruição não autorizada à mídia armazenada.	5.1.6 Armazenamento de mídia
5.1.7 Waste disposal*	Define os requisitos para descarte de informações sensíveis e dispositivos eletrônicos que são não mais necessários.	5.1.7 Descarte de lixo
5.1.8 Off-site backup*	Define os requisitos para cópias de segurança em outras instalações, como sua freqüência e considerações de segurança por não estar presente no ambiente principal.	5.1.8 Cópias de segurança em outras instalações
5.2 Procedural Controls	Apresenta os controles de segurança física nas instalações que abrigam os sistemas da AC.	**5.2 Procedimentos de Controle**
5.2.1 Trusted roles*	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.	5.2.1 Papéis de Confiança
5.2.2 Number of persons required per task*	Especificar o número de pessoas necessárias para executar as tarefas listadas, caso sejam necessários controles de multiusuário.	5.2.2 Número de pessoas necessárias por tarefa
5.2.3 Identification and authentication for each role *	Especificar os controles necessários para identificar e autenticar os indivíduos na atuação de seus papéis.	5.2.3 Identificação e autenticação para cada papel
5.2.4 Roles requiring separation of duties*	Especifica papéis que não podem ser exercidos simultaneamente pelo mesmo indivíduo.	5.2.4 Papéis que requerem separação de responsabilidade

Componentes da RFC 3647	Descrição do componente	Tradução para português do Brasil
5.3 Personnel Controls	Apresenta os controles de segurança dos recursos humanos envolvidos na operação dos sistemas da AC.	**5.3 Controle de Pessoal**
5.3.1 Qualifications, experience, and clearance requirements*	Especifica os requisitos para contratação de pessoal que atuará em papéis de confiança.	5.3.1 Requisitos de qualificação, experiência e conformidade com obrigações governamentais
5.3.2 Background check procedures*	Descreve os procedimentos seguidos para verificar os antecedentes antes da contratação de um funcionário que ocupará papéis de confiança ou outras funções importantes.	5.3.2 Procedimentos de verificação de antecedentes
5.3.3 Training requirements*	Estabelece o processo de treinamento pelo qual o pessoal deverá passar.	5.3.3 Requisitos de treinamento
5.3.4 Retraining frequency and requirements*	Estabelece a freqüência na qual deve haver um novo treinamento para o pessoal da AC.	5.3.4 Requisitos de freqüência de treinamento
5.3.5 Job rotation frequency and sequence*	Estabelece a freqüência de revezamento no exercício de papéis.	5.3.5 Freqüência e seqüência para revezamento de trabalho
5.3.6 Sanctions for unauthorized actions*	Estabelece as medidas tomadas caso haja alguma ação não autorizada.	5.3.6 Sanções para ações não autorizadas
5.3.7 Independent contractor requirements*	Estabelece os controles sobre pessoal externo ao quadro de empregados da instituição na prestação de serviço para a mesma.	5.3.7 Requisitos para prestadores de serviços independentes
5.3.8 Documentation supplied to personnel*	Estabelece que documentos serão fornecidos ao pessoal responsável pela operação da AC ou AR.	5.3.8 Documentação fornecida aos funcionários
5.4 Audit Logging Procedures	Apresenta os sistemas de registro de eventos e auditoria implementados com o propósito de manter um ambiente seguro.	**5.4 Sistemas de auditoria e procedimentos para registro de eventos**
5.4.1 Types of events recorded*	Especifica que eventos serão registrados para compor a trilha de auditoria.	5.4.1 Tipos de eventos registrados
5.4.2 Frequency of processing log*	Especifica a freqüência na qual os registros de auditoria são analisados em busca de um evento suspeito e então arquivados.	5.4.2 Freqüência de análise dos registros de auditoria

Componentes da RFC 3647	Descrição do componente	Tradução para português do Brasil
5.4.3 Retention period for audit log*	Especifica o período de arquivamento dos registros de auditoria, isto é, por quanto tempo serão armazenados.	5.4.3 Período de arquivamento de registros de auditoria
5.4.4 Protection of audit log*	Especifica os controles impostos às atividades relacionadas à administração dos registros de auditoria, como acesso e modificação, por exemplo.	5.4.4 Proteção de registros de eventos
5.4.5 Audit log backup procedures*	Especifica os procedimentos para cópias de segurança de registros de eventos.	5.4.5 Procedimentos para cópias de segurança de registros de eventos
5.4.6 Audit collection system (internal vs external)*	Especifica se o sistema de recolhimento de registros de eventos é interno (ou seja, pertence à organização) ou externo (está fora das dependências da organização).	5.4.6 Sistema de recolhimento de registros de eventos (interno ou externo)
5.4.7 Notification to event-causing subject*	Especifica se o causador de um evento será ou não notificado sobre a auditoria.	5.4.7 Notificação do sujeito causador do evento
5.4.8 Vulnerability assessments*	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.	5.4.8 Avaliação de vulnerabilidades
5.5 Records Archival	Apresenta as políticas para arquivamento ou retenção dos registros.	**5.5 Arquivamento de Registros**
5.5.1 Types of records archived*	Especifica que registros serão arquivados, isto é, retidos em local separado para posterior auditoria, se necessário.	5.5.1 Tipos de registros armazenados
5.5.2 Retention period for archive*	Especifica por quanto tempo os registros arquivados serão retidos.	5.5.2 Período de retenção dos registros arquivados
5.5.3 Protection of archive*	Especifica os controles impostos a acessos, modificações, exclusões, entre outros, aos registros arquivados.	5.5.3 Proteção dos registros armazenados
5.5.4 Archive backup procedures*	Especifica os procedimentos para cópias de segurança dos registros arquivados.	5.5.4 Procedimentos para cópias dos registros armazenados

Componentes da RFC 3647	Descrição do componente	Tradução para português do Brasil
5.5.5 Requirements for time-stamping of records*	Especifica os requisitos para manter uma linha do tempo a partir da data e hora dos registros armazenados.	5.5.5 Requisitos para datação dos registros armazenados
5.5.6 Archive collection system (internal or external)*	Especifica se o sistema de recolhimento de registros arquivados é interno (ou seja, pertence à organização) ou externo (está fora das dependências da organização).	5.5.6 Sistema de recolhimento de registros arquivados (interno ou externo)
5.5.7 Procedures to obtain and verify archive information*	Especifica os procedimentos para obter e verificar os registros arquivados.	5.5.7 Procedimentos para obtenção e verificação dos registros armazenados
5.6 Key Changeover	Especifica os procedimentos para divulgação da chave pública da AC para as entidades confiantes após o processo de troca de chaves da AC.	**5.6 Nova Chave Pública para a AC**
5.7 Compromise and Disaster Recovery	Apresenta os requisitos relacionados aos procedimentos de recuperação das atividades da AC e notificação em caso de comprometimento ou desastre.	**5.7 Comprometimento e Recuperação de Desastre**
5.7.1 Incident and compromise handling procedures	Especifica os procedimentos para relatar e tratar incidentes e comprometimentos, incluindo da chave privada da AC.	5.7.1 Procedimentos para tratamento de incidentes e comprometimentos
5.7.2 Computing resources, software, and/or data are corrupted	Especifica os procedimentos para o caso de comprometimento de recursos que suportam a operação da AC ou ARs.	5.7.2 Procedimentos para o caso de comprometimento de recursos computacionais, software e/ou dados
5.7.3 Entity private key compromise procedures	Descreve os procedimentos de recuperação a serem tomados no caso do comprometimento da chave privada da entidade.	5.7.3 Procedimentos para o comprometimento de chave privada de entidade
5.7.4 Business continuity capabilities after a disaster	Especifica resumidamente os procedimentos definidos no plano de continuidade de negócios aplicáveis.	5.7.4 Procedimentos para continuidade de negócio após desastre
5.8 CA or RA Termination	Descreve as providências tomadas quando houver finalização desta AC.	**5.8 Finalização da AC ou AR**
6 Technical Security Controls		**6. Controles Técnicos de Segurança**

Componentes da RFC 3647	Descrição do componente	Tradução para português do Brasil
6.1 Key Pair Generation and Installation *	Apresenta os requisitos para geração e instalação do par de chaves da AC, AR, etc.	**6.1 Geração e Instalação do Par de Chaves**
6.1.1 Key pair generation*	Estabelece quem será responsável pela geração do par de chaves da entidade que solicita um certificado e como a atividade é realizada.	6.1.1 Geração do par de chaves
6.1.2 Private key delivery to subscriber*	Estabelece os métodos utilizados para que a chave privada seja entregue de forma segura ao titular do certificado.	6.1.2 Fornecimento de chave privada ao titular
6.1.3 Public key delivery to certificate issuer*	Estabelece os métodos utilizados para que a chave pública de um certificado seja entregue de forma segura à Autoridade Certificadora.	6.1.3 Entrega da chave pública à Autoridade Certificadora
6.1.4 CA public key delivery to relying parties*	Estabelece os métodos utilizados para que a chave pública da AC seja disponibilizada de forma segura para as entidades confiantes.	6.1.4 Divulgação da chave pública da AC às partes confiantes
6.1.5 Key sizes*	Estabelece o tamanho mínimo das chaves geradas.	6.1.5 Tamanho das chaves
6.1.6 Public key parameters generation and quality checking*	Estabelece quem é responsável pela geração dos parâmetros da chave pública e os procedimentos de verificação de sua qualidade durante este processo.	6.1.6 Geração dos parâmetros de chave pública e verificação de qualidade
6.1.7 Key usage purposes (as per X509 v3 key usage field)*	Estabelece para que propósitos as chaves podem ser usadas ou são restritos.	6.1.7 Propósito de uso de chaves
6.2 Private Key Protection and Cryptographic Module Engineering Controls	Apresenta os requisitos para proteção da chave privada do titular e utilização de módulos criptográficos.	**6.2 Proteção de Chaves Privadas e Controles Tecnológicos de módulos Criptográficos**
6.2.1 Cryptographic module standards and controls*	Estabelece os padrões e controles requeridos para os módulos criptográficos.	6.2.1 Padrões e controles de módulos criptográficos

Componentes da RFC 3647	Descrição do componente	Tradução para português do Brasil
6.2.2 Private key (n out of m) multi-person control*	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.	6.2.2 Número de operadores para o Controle da Chave Privada
6.2.3 Private key escrow*	Estabelece quem é responsável pela custódia das chaves privadas como é feita e os controles de segurança envolvidos, se aplicável.	6.2.3 Custódia de chaves privadas
6.2.4 Private key backup*	Estabelece como é feita a cópia de segurança da chave privada da AC, AR e entidades finais, se aplicável.	6.2.4 Cópias de segurança de chaves privadas
6.2.5 Private key archival*	Estabelece como é feito o arquivamento da cópia da chave privada, isto é, seu armazenamento por um período de tempo longo, se aplicável.	6.2.5 Arquivamento de chaves privadas
6.2.6 Private key transfer into or from a cryptographic module*	Estabelece as circunstâncias nas quais a chave privada pode ser transferida de ou para um módulo criptográfico, e os procedimentos envolvidos na tarefa.	6.2.6 Transferência de chaves privadas de/para módulos criptográficos
6.2.7 Private key storage on cryptographic module*	Estabelece como as chaves privadas devem estar armazenadas nos módulos criptográficos.	6.2.7 Armazenamento de chaves privadas em módulos criptográficos
6.2.8 Method of activating private key*	Estabelece quem pode usar as chaves privadas, que ações devem ser tomadas para a ativação e o período em que a chave pode ficar ativa.	6.2.8 Método para ativação de chaves privadas
6.2.9 Method of deactivating private key*	Estabelece quem pode desativar as chaves privadas e que ações devem ser tomadas para a desativação.	6.2.9 Método para desativação de chaves privadas
6.2.10 Method of destroying private key*	Estabelece quem pode destruir as chaves privadas, que ações devem ser tomadas para efetuar a tarefa.	6.2.10 Método para destruição de chaves privadas
6.2.11 Cryptographic Module Rating*	Provê características sobre módulos criptográficos a serem utilizados.	6.2.11 Avaliação requerida de módulos criptográficos

Componentes da RFC 3647	Descrição do componente	Tradução para português do Brasil
6.3 Other Aspects of Key Pair Management	Apresenta outros aspectos do gerenciamento do par de chaves, como arquivamento da chave pública.	**6.3 Outros Aspectos do Gerenciamento de Chaves**
6.3.1 Public key archival*	Estabelece se as chaves públicas dos participantes da ICP devem ou não ser arquivadas e que controles são utilizados para mantê-las seguras.	6.3.1 Armazenamento de chaves públicas
6.3.2 Certificate operational periods and key pair usage periods*	Estabelece o período operacional do certificado e o tempo de vida do par de chaves.	6.3.2 Períodos operacionais de certificados e períodos de utilização de pares de chaves
6.4 Activation Data	Apresenta os requisitos para proteção dos dados de ativação, isto é, dados que são necessários para utilizar chaves privadas e módulos criptográficos, além dos próprios. É importante que considerem todo o ciclo de vida dos dados de ativação.	**6.4 Dados de Ativação**
6.4.1 Activation data generation and installation*	Estabelece os dados de ativação usados para ativar as chaves privadas, bem como seus métodos de geração e instalação.	6.4.1 Geração e instalação dos dados de ativação
6.4.2 Activation data protection*	Estabelece os procedimentos para proteção dos dados de ativação das chaves privadas.	6.4.2 Proteção dos dados de ativação
6.4.3 Other aspects of activation data*	Estabelece outros aspectos sobre os dados de ativação.	6.4.3 Outros aspectos de dados de ativação
6.5 Computer Security Controls	Apresenta os requisitos de segurança computacional que são utilizados para manter o ambiente seguro, além de requisitos para avaliação e certificação de produtos relacionados ao gerenciamento do ciclo de vida dos certificados. Uma métrica pode ser necessária para apoiar a avaliação da eficácia desses controles.	6.5 Controles de Segurança computacional
6.5.1 Specific computer security technical requirements*	Descreve controles técnicos de segurança computacional estabelecidos para garantir uma operação segura da AC.	6.5.1 Requisitos técnicos específicos de segurança computacional
6.5.2 Computer security rating*	Estabelece índices de segurança independentes para avaliação de sistemas relacionados às operações da AC.	6.5.2 Classificação de segurança computacional

Componentes da RFC 3647	Descrição do componente	Tradução para português do Brasil
6.6 Life Cycle Security Controls	Apresenta os controles aplicados no desenvolvimento dos sistemas (como boas práticas de engenharia de software e segurança no desenvolvimento) e gerenciamento de segurança (como procedimentos e ferramentas que garantam a integridade dos sistemas).	**6.6 Controles técnicos de ciclo de vida**
6.6.1 System development controls*	Estabelece controles sobre o desenvolvimento dos sistemas utilizados para o gerenciamento do ciclo de vida dos certificados.	6.6.1 Controles de desenvolvimento de sistemas
6.6.2 Security management controls*	Estabelece controles usados para garantir que os sistemas estão operando corretamente e de forma consistente com a configuração desejada.	6.6.2 Controles do gerenciamento de segurança
6.6.3 Life cycle security controls*	Estabelece controles segurança no ciclo de vida do software.	6.6.3 Controles de segurança de ciclo de vida
6.7 Network Security Controls	Estabelece controles sobre a rede de comunicações, especialmente sobre aquelas usadas pela AC e AR.	**6.7 Controles para a Segurança da Rede de Comunicações**
6.8 Timestamping	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.	
7 Certificate, CRL, and OCSP Profiles		**7. Perfis dos Certificados, LCR e OCSP**
7.1 Certificate Profile	Especifica o formato dos certificados emitidos, incluindo informações sobre versão, extensões, etc. Mais informações sobre esses perfis podem ser encontradas em [Cooper et al., 2008].	**7.1 Perfil dos Certificados**
7.1.1 Version number(s)*	Define a versão dos certificados emitidos pela AC.	7.1.1 Versão
7.1.2 Certificate extensions*	Define as extensões utilizadas nos certificados emitidos pela AC.	7.1.2 Extensões
7.1.3 Algorithm object identifiers*	Define os OIDs dos algortimos criptográficos.	7.1.3 Identificadores de objeto dos algoritmos

Componentes da RFC 3647	Descrição do componente	Tradução para português do Brasil
7.1.4 Name forms*	Define formato do Distinguished Name (DN) dos certificados emitidos pela AC.	7.1.4 Formato dos nomes
7.1.5 Name constraints*	Define as restrições aplicáveis para nomes de titulares de certificados.	7.1.4 Restrições para nomes
7.1.6 Certificate policy object identifier*	Apresenta o OID da PC, que constará no certificado emitido..	7.1.6 Identificador de objeto da PC
7.1.7 Usage of Policy Constraints extension*	Define o uso da extensão Policy Constraints pela AC, e as limitações impostas por ela.	7.1.7 Uso da extensão Policy Constraints
7.1.8 Policy qualifiers syntax and semantics*	Define se a AC utiliza os qualificadores de política com a extensão certificate policies para transportar informações e define que informações são transportadas	7.1.8 Sintaxe e semântica dos qualificadores de política
7.1.9 Processing semantics for the critical Certificate Policies extension*	Define se a AC marca como crítica a extensão *certificate policies* ou requer que uma AC subordinada o faça.	7.1.9 Semântica de processamento para a extensão Certificate Policies marcada como crítica
7.2 CRL Profile	Especifica o formato das Listas de Certificados Revogados (LCRs) emitidas, incluindo informações sobre versão, extensões, etc. Mais informações sobre esses perfis podem ser encontradas em [Cooper et al., 2008].	**7.2 Perfil da LCR**
7.2.1 Version number(s)*	Define a versão das LCRs emitidas pela AC.	7.2.1 Versão
7.2.2 CRL and CRL entry extensions*	Descreve as extensões de LCR utilizadas e sua criticidade.	7.2.2 Extensões da LCR e de entradas da LCR
7.3 OCSP Profile	Apresenta considerações sobre a implementação do Online Certificate Status Profile (OCSP) emitidas, incluindo informações sobre versão, extensões, etc. Mais informações sobre esses perfis podem ser encontradas em [Cooper et al., 2008].	**7.3 Perfil da OCSP**
7.3.1 Version number(s)	Define a versão da OCSP disponível para verificar o status dos certificados.	7.3.1 Versão
7.3.2 OCSP extensions	Define as extensões usadas pela OCSP.	7.3.2 Extensões OCSP

Componentes da RFC 3647	Descrição do componente	Tradução para português do Brasil
8. Compliance Audit and Other Assessment		8. Auditoria de conformidade e outras avaliações
8.1 Frequency or circumstances of assessment*	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.	**8.1 Freqüência ou circunstâncias das avaliações**
8.2 Identity/qualifications of assessor*	Estabelece quem pode conduzir as avaliações, isto é, sua identidade e qualificações.	**8.2 Identidade e qualificações do avaliador**
8.3 Assessor's relationship to assessed entity*	Estabelece a relação do avaliador com a entidade avaliada, e sua autonomia.	**8.3 Relação entre o avaliador e a entidade avaliada**
8.4 Topics covered by assessment*	Estabelece os requisitos que serão avaliados.	**8.4 Tópicos cobertos na avaliação**
8.5 Actions taken as a result of deficiency*	Estabelece as ações tomadas quando alguma não-conformidade é encontrada após uma avaliação.	**8.5 Ações tomadas resultantes de deficiências**
8.6 Communication of results*	Estabelece quem terá acesso aos resultados das avaliações, e como serão divulgados.	**8.6 Comunicação dos resultados**
9. Other Business and Legal Matters		**9. Aspectos Legais e Assuntos Gerais**
9.1 Fees	Apresenta considerações sobre taxas cobradas pela AC, AR ou repositórios.	**9.1 Taxas**
9.1.1 Certificate issuance or renewal fees*	Estabelece uma taxa pela prestação dos serviços de emissão e renovação de certificados.	9.1.1 Taxas de emissão e renovação de certificados
9.1.2 Certificate access fees*	Estabelece uma taxa para utilização dos certificados pelas entidades confiantes.	9.1.2 Taxas para acesso aos certificados
9.1.3 Revocation or status information access fees*	Estabelece uma taxa pela prestação dos serviços de revogação ou informação de estados dos certificados.	9.1.3 Taxas revogação ou informações de estado
9.1.4 Fees for other services*	Estabelece uma taxa pela prestação de serviços não definidos anteriormente.	9.1.4 Outras taxas
9.1.5 Refund policy*	Estabelece uma política de reembolso das taxas pagas pela prestação de serviços.	9.1.5 Política de reembolso

Componentes da RFC 3647	Descrição do componente	Tradução para português do Brasil
9.2 Financial Responsibility	Apresenta considerações sobre recursos disponibilizados para ACs, ARs e outros participantes que estejam provendo serviços que suportem suas responsabilidades operacionais, como o pagamento em caso de danos e ações indevidas.	**9.2 Responsabilidade Financeira**
9.2.1 Insurance coverage*	Estabelece a cobertura de seguro de um participante sobre os riscos de suas responsabilidades.	9.2.1 Cobertura de Seguro
9.2.2 Other assets*	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.	9.2.2 Outros ativos
9.2.3 Insurance or warranty coverage for end-entities*	Estabelece a cobertura de seguro de terceiros envolvidos na participação de uma entidade na ICP.	9.2.3 Cobertura de Seguro ou garantia para entidades finais
9.3 Confidentiality of Business Information	Apresenta considerações sobre o tratamento de informações consideradas confidenciais.	**9.3 Informações confidenciais**
9.3.1 Scope of confidential information*	Define que informações são consideradas confidenciais.	9.3.1 Escopo de informações confidenciais
9.3.2 Information not within the scope of confidential information*	Define que informações não são consideradas confidenciais.	9.3.2 Informações fora do escopo de informações confidenciais
9.3.3 Responsibility to protect confidential information*	Define responsáveis pela guarda e proteção de informações consideradas confidenciais.	9.3.3 Responsabilidade de proteção de informações confidenciais
9.4 Privacy of Personal Information	Apresenta as medidas que devem ser tomadas pela AC para proteger informações de identificação pessoal de solicitantes, titulares de certificado ou outros participantes da ICP, devendo considerar a legislação aplicável.	**9.4 Privacidade de Informações Pessoais**
9.4.1 Privacy plan*	Define o plano de privacidade aplicável às atividades dos participantes.	9.4.1 Plano de Privacidade
9.4.2 Information treated as private*	Define que informações são tratadas como privadas.	9.4.2 Informação tratada como privada
9.4.3 Information not deemed private*	Define que informações não são tratadas como privadas.	9.4.3 Informação não considerada privada

Componentes da RFC 3647	Descrição do componente	Tradução para português do Brasil
9.4.4 Responsibility to protect private information*	Estabelece a responsabilidade pela proteção de informações que são tratadas como privadas.	9.4.4 Responsabilidade de proteção de informação privada
9.4.5 Notice and consent to use private information*	Estabelece os requisitos para determinar o consentimento do uso de uma informação privada por parte do dono.	9.4.5 Aviso e consentimento para o uso de informação privada
9.4.6 Disclosure pursuant to judicial or administrative process*	Define as circunstâncias nas quais é requerida ao participante a divulgação de informações consideradas privadas para atender processos administrativos.	9.4.6 Circunstâncias para revelação de informações confidenciais em processos judiciais e administrativos
9.4.7 Other information disclosure circumstances*	Define outras circunstâncias nas quais é requerida ao participante a divulgação de informações consideradas privadas.	9.4.7 Outras Circunstâncias para revelação de informações
9.5 Intellectual Property Rights	Estabelece os direitos de propriedade intelectual sobre vários aspectos, como certificados, PCs, DPCs, nomes, bancos de dados, entre outros.	**9.5 Direitos de Propriedade Intelectual**
9.6 Representations and Warranties	Apresenta informações sobre garantias e representações para as entidades participantes da ICP.	**9.6 Representações e Garantias**
9.6.1 CA representations and warranties*	Estabelece as garantias oferecidas pela AC na prestação do serviço de certificação.	9.6.1 Garantias de AC
9.6.2 RA representations and warranties*	Estabelece as garantias oferecidas pela AR na prestação do serviço de autenticação.	9.6.2 Garantias de AR
9.6.3 Subscriber representations and warranties*	Estabelece as garantias oferecidas pelos titulares na utilização de certificados.	9.6.3 Garantias de titulares de certificado
9.6.4 Relying party representations and warranties*	Estabelece as garantias oferecidas pelas entidades confiantes na utilização de certificados.	9.6.4 Garantias de entidades confiantes
9.6.5 Representations and warranties of other participants*	Estabelece as garantias oferecidas por outros participantes da ICP.	9.6.5 Garantias de outros participantes
9.7 Disclaimers of Warranties	O conteúdo é composto por renúncias de garantias que possam existir no documento ou impostas pela lei aplicável, por exemplo.	**9.7 Renúncia das Garantias**

Componentes da RFC 3647	Descrição do componente	Tradução para português do Brasil
9.8 Limitations of Liability	Descreve limitações de responsabilidades atreladas aos acordos de aceitação por parte dos usuários e entidades confiantes, por exemplo.	**9.8 Limitações das Responsabilidades**
9.9 Indemnities	Estabelece indenizações decorrentes de conduta de uma entidade que cause dano à outra.	**9.9 Indenização**
9.10 Term and Termination	Apresenta o período na qual as provisões da PC/DPC se mantêm válidas, e as circunstâncias nas quais o documento, parte dele ou sua aplicação sobre um determinado participantes deixa de ter validade.	**9.10 Finalização**
9.10.1 Term*	Estabelece o período de validade das provisões do documento.	9.10.1 Prazo de validade
9.10.12 Termination	Estabelece o prazo em que o documento ou parte dele deixa de ter efeito.	9.10.2 Finalização
9.10.13 Effect of termination and survival*	Descreve as conseqüências da terminação de validade do documento.	9.10.3 Efeitos de finalização e provisões remanescentes
9.11 Individual notices and communications with participants	Estabelece a forma de comunicação entre os participantes para que seja legalmente efetiva.	**9.11 Notificações Individuais e Comunicações com Participantes**
9.12 Amendments	Apresenta os procedimentos para efetuar emendas no documento de PC/DPC.	**9.12 Emendas**
9.12.1 Procedure for amendment*	Estabelece os procedimentos tomados quando necessárias emendas nos documentos.	9.12.1 Procedimento para emendas
9.12.2 Notification mechanism and period*	Estabelece os mecanismos utilizados para notificar os interessados, caso haja emendas no documento.	9.12.2 Período e mecanismo de notificação
9.12.3 Circumstances under which OID must be changed*	Circunstâncias nas quais as emendas acarretam na mudança do identificador de objeto do documento.	9.12.3 Circunstâncias nas quais o identificador de objeto deve ser modificado
9.13 Dispute Resolution Procedures	Determina os procedimentos utilizados para resolver disputas envolvendo as provisões dos documentos da ICP.	**9.13 Procedimentos para Resolução de Disputas**

Componentes da RFC 3647	Descrição do componente	Tradução para português do Brasil
9.14 Governing Law	Estabelece que as atividades da AC devem estar conformes com a legislação vigente no país.	**9.14 Leis Governamentais**
9.15 Compliance with Applicable Law	Estabelece provisões para garantir a conformidade das atividades da AC com a legislação vigente no país.	**9.15 Conformidade com as leis aplicáveis**
9.16 Miscellaneous Provisions	Apresenta provisões diversas, que não se encaixam em seções anteriores.	**9.16 Provisões Diversas**
9.16.1 Entire agreement*	Estabelece a concordância completa entre as partes cobertas no documento.	9.16.1 Concordância completa
9.16.2 Assignment*	Estabelece os limites de delegação de direitos e obrigações das entidades participantes.	9.16.2 Delegação de direitos e obrigações
9.16.3 Severability*	Estabelece um acordo entre as partes definindo que a revogação de uma cláusula não afete a validade de todo documento.	9.16.3 Acordo entre as partes em caso de revogação de cláusula pela justiça
9.16.4 Enforcement (attorneys' fees and waiver of rights)*	Estabelece quem será responsável por arcar com as despesas relacionadas aos encargos jurídicos.	9.16.4 Responsabilidades relacionadas a encargos jurídicos
9.16.5 Force Majeure*	Estabelece como serão tratados eventos fora do controle da AC.	9.16.5 Força maior
9.17 Other Provisions	Estabelece termos e responsabilidades gerais que não se enquadrem em nenhuma das seções anteriores.	9.15 Outras Provisões

Anexo B – Mapeamento entre as seções da RFC 3647 e as normas técnicas e padrões utilizados

Os títulos das seções foram mantidos em inglês para facilitar a consulta ao documento original. O conjunto de provisões é descrito na seção "4. *Contents of a Set of Provisions*" da RFC 3647 [Chokani et al., 2003].

Uma sugestão de tradução das seções para português do Brasil pode ser encontrada no Anexo B.

Legenda:

N/A – Não Aplicável

* - Não previsto explicitamente na RFC 3647

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
1. Introduction						
1.1 Overview	Provê uma introdução geral ao documento, podendo ser usado para prover uma apresentação da ICP na qual a PC/DPC se aplica.	A.1.1 Overview	N/A	N/A	N/A	N/A
1.2 Document name and Identification	Provê quaisquer nomes ou outros identificadores aplicáveis, como identificadores de objetos ASN.1, para o documento.	A.1.2 Identification	N/A	N/A	8.1 Certificate policy management Item (i)	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
1.3 PKI Participants	Apresenta a identidade ou tipos de entidades que assumem os papéis da ICP.					
1.3.1 Certification authorities*	Apresenta as ACs responsáveis pela emissão dos certificados na ICP.	A.1.3 Community and Applicability	N/A	N/A	N/A	N/A
1.3.2 Registration authorities*	Apresenta os responsáveis pelas funções de identificação e registro na ICP.	A.1.3 Community and Applicability	N/A	N/A	N/A	N/A
1.3.3 Subscribers*	Apresenta potenciais titulares de certificados.	A.1.3 Community and Applicability	N/A	N/A	N/A	N/A
1.3.4 Relying parties*	Apresenta potenciais entidades que confiam nos certificados, recebendo e-mails assinados, por exemplo.	A.1.3 Community and Applicability	N/A	N/A	N/A	N/A
1.3.5 Other participants*	Apresenta outras entidades que ofereçam serviços relacionados a certificação digital para a ICP.	A.1.3 Community and Applicability	N/A	N/A	7.1 Certification practice statement Item (b) 7.4.1 Security Management Item (b)	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
1.4 Certificate Usage	Contém usos reconhecidos como apropriados ou proibidos para os certificados da ICP, podendo considerar níveis de confiança previamente estabelecidos para determinadas aplicações.					
1.4.1 Appropriate certificate uses*	Lista os tipos de aplicações para as quais o uso do certificado é apropriado.	A.1.3 Community and Applicability	N/A	N/A	8.1 Certificate policy management Item (a)	N/A
1.4.2 Prohibited certificate uses*	Lista os tipos de aplicações para as quais o uso do certificado é proibido.	A.1.3 Community and Applicability	N/A	N/A	8.1 Certificate policy management Item (a)	N/A
1.5 Policy Administration	Apresenta informações de contato para questões relacionadas ao documento de PC/DPC.					
1.5.1 Organization administering the document*	Apresenta informações sobre a organização que administra o documento.	A.1.4 Contact Details B.1.1 Certification Practice Statement and Certificate Policy Management	A.6.1 Internal organization	6.1 Internal organization	8.1 Certificate policy management Item (b)	N/A
1.5.2 Contact person*	Apresenta informações para contato da pessoa responsável pelo documento, podendo ser um papel na operação da AC.	A.1.4 Contact Details	A.6.1 Internal organization	6.1 Internal organization	N/A	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
1.5.3 Person determining CPS suitability for the policy*	Apresenta a pessoa (ou papel) responsável por garantir a adequação da DPC à política de uma determinada ICP, caso haja uma Autoridade de Gerência de Política responsável.	A.1.4 Contact Details B.1.1 Certification Practice Statement and Certificate Policy Management	A.6.1 Internal organization	6.1 Internal organization	7.1 Certification practice statement Itens (e), (f) e (g) 8.1 Certificate policy management Item (b)	N/A
1.5.4 CPS approval procedures*	Apresenta os procedimentos para a aprovação da DPC, no caso anterior.	B.1.1 Certification Practice Statement and Certificate Policy Management	N/A	N/A	7.1 Certification practice statement Itens (g) e (h) 8.1 Certificate policy management Item (b), (d), (e)	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
1.6 Definitions and Acronyms	Lista definições e acrônimos usados no documento.					
1.6.1 Definitions*	Apresenta definições dos termos usados na PC/DPC.	N/A	N/A	N/A	N/A	N/A
1.6.2 Acronyms*	Apresenta acrônimos e seus significados usados na PC/DPC	N/A	N/A	N/A	N/A	N/A
2. Publication and Repository Responsabilities						
2.1 Repositories*	Identifica os repositórios onde as informações da AC estarão disponíveis.	A.2.4 Publication and Repositories	N/A	N/A	N/A	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
2.2 Publication of certification information*	Apresenta as informações da AC que serão publicadas e os mecanismos usados para fazê-lo.	A.2.4 Publication and Repositories B.1.1 Certification Practice Statement and Certificate Policy Management B.3.5 Certificate Distribution B.3.8 Certificate Status Information Processing	N/A	N/A	7.1 Certification practice statement Item (c) 7.3.4 Dissemination of terms and conditions 7.3.5 Certificate dissemination 8.1 Certificate policy management Item (f) e (g)	N/A
2.3 Time or frequency of publication*	Informa quando e com que freqüência as informações apresentadas anteriormente são publicadas.	A.2.4 Publication and Repositories	N/A	N/A	N/A	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
2.4 Access controls on repositories*	Apresenta os controles impostos nos objetos repositórios para garantir a integridade da informação apresentada.	A.2.4 Publication and Repositories	A.6.2 External parties A.11.1 Business requirement for access control A.11.2 User access management	6.2 External parties 11.1 Business requirement for access control 11.2 User access management	7.4.6 System access management Item (j)	Famílias Access Control e Identification and Authentication
3. Identification and Authentication						
3.1 Naming	Apresenta provisões a respeito dos nomes utilizados nos certificados emitidos pela AC.					
3.1.1 Types of names*	Apresenta o formato dos nomes designados aos titulares dos certificados, como X.500, RFC 822 e X.400.	A.3.1 Initial Registration B.3.1 Subscriber Registration	N/A	N/A	N/A	N/A
3.2.2 Need for names to be meaningful*	Informa se os nomes nos certificados emitidos devem ou não ser significativos.	A.3.1 Initial Registration B.3.1 Subscriber Registration	N/A	N/A	N/A	N/A
3.3.3 Anonymity or pseudonymity of subscribers*	Informa se um titular de certificado pode ou não ser anônimo ou usar pseudônimos, e quais pseudônimos serão designados a eles.	N/A	N/A	N/A	N/A	Família Identification and Authentication

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
3.1.4 Rules for interpreting various name forms*	Apresenta as regras para interpretação dos nomes, como X.500 e RFC 822.	A.3.1 Initial Registration B.3.1 Subscriber Registration	N/A	N/A	N/A	N/A
3.1.5 Uniqueness of names*	Determina se os nomes devem ou não ser únicos no universo da ICP.	A.3.1 Initial Registration B.3.1 Subscriber Registration	N/A	N/A	7.3.3 Certificate generation Item (e)	Família Identification and Authentication
3.1.6 Recognition, authentication, and role of trademarks*	Apresenta os procedimentos para reconhecimento, autenticação de marcas registradas e o seu papel na nomeação dos titulares.	A.3.1 Initial Registration B.3.1 Subscriber Registration	N/A	N/A	N/A	N/A
3.2 Initial Identity Validation	Aborda os procedimentos de identificação e autenticação para o registro inicial de cada tipo de titular de certificado (AC, AR, entre outros).					
3.2.1 Method to prove possession of private key*	Estabelece os métodos que deverão ser usados pela AC para comprovar que o solicitante possui a chave privada que faz par a chave pública que está sendo registrada.	A.3.1 Initial Registration B.3.1 Subscriber Registration	N/A	N/A	7.3.1 Subject registration Item (o)	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
3.2.2 Authentication of organization identity*	Apresenta os requisitos para identificação e autenticação da identidade organizacional do titular do certificado ou participante da ICP. Pode ser uma consulta aos registros da organização, por exemplo.	A.3.1 Initial Registration B.3.1 Subscriber Registration	N/A	N/A	7.3.1 Subject registration Itens (d), (g), (h) e (n)	N/A
3.2.3 Authentication of individual identity*	Apresenta os requisitos para identificação e autenticação da identidade do titular do certificado ou de um indivíduo atuando em nome de uma organização.	A.3.1 Initial Registration B.3.1 Subscriber Registration	N/A	N/A	7.3.1 Subject registration Itens (d), (e), (f), (g), (l), (m) e (n)	Família Identification and Authentication
3.2.4 Non-verified subscriber information*	Lista as informações do titular de certificado que não são verificadas inicialmente.	N/A	N/A	N/A	N/A	N/A
3.2.5 Validation of authority*	Apresenta os procedimentos para verificar se um indivíduo tem direito ou permissão para agir em nome de uma organização.	A.3.1 Initial Registration B.3.1 Subscriber Registration	N/A	N/A	7.3.1 Subject registration Itens (k) e (n)	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
3.2.6 Criteria for interoperation*	Apresenta os critérios utilizados para que uma AC que deseje fazer parte da ICP possa fazê-lo.	N/A	N/A	N/A	N/A	N/A
3.3 Identification and Authentication for Re-key Requests	Aborda os procedimentos de identificação e autenticação para solicitações de troca de par de chaves (isto é, um novo certificado é emitido com um novo par de chaves, mas mantendo os atributos anteriores).					
3.3.1 Identification and authentication for routine re-key*	Apresenta os requisitos para identificação e autenticação para requisições de troca de par de chaves de rotina, quando ainda há uma chave privada válida.	A.3.2 Routine Re-key	N/A	N/A	7.3.2 Certificate renewal, rekey and update	Família Identification and Authentication
3.3.2 Identification and authentication for re-key after revocation*	Apresenta os requisitos para identificação e autenticação para requisições de troca de par de chaves após a revogação do certificado.	A.3.3 Re-key after Revocation – No Key Compromise	N/A	N/A	7.3.2 Certificate renewal, rekey and update	Família Identification and Authentication
3.4 Identification and Authentication for Revocation Requests	Aborda os procedimentos de identificação e autenticação para solicitações de revogação de certificados (pedidos assinados pela chave privada correspondente, verificação pessoal da AR, por exemplo).	A.3.4 Revocation Request	N/A	N/A	7.3.6 Certificate revocation and suspension Item (c)	Família Identification and Authentication

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
4 Certificate Life-Cycle Operational Requirements						
4.1 Certificate Application	Trata dos requisitos relacionados à solicitação de um certificado.					
4.1.1 Who can submit a certificate application*	Apresenta quem pode solicitar um certificado a AC.	N/A	N/A	N/A	N/A	N/A
4.1.2 Enrollment process and responsibilities*	Apresenta o procedimento para solicitação do certificado e as responsabilidades do solicitante associadas a esse processo.	A.2.2 Obligations A.4.1 Certificate Application	N/A	N/A	N/A	N/A
4.2 Certificate Application Processing	Descreve o conjunto de passos que serão seguidos para processamento das solicitações, causado a aceitação ou rejeição destas, de acordo com um o critério estabelecido.					
4.2.1 Performing identification and authentication functions*	Descreve os procedimentos para identificação e autenticação para validar a solicitação.	A.4.1 Certificate Application	N/A	N/A	7.3.1 Subject registration Item (q) 7.3.3 Certificate generation Itens (f) e (g)	N/A
4.2.2 Approval or rejection of certificate applications*	Estabelece o critério que determinará a aceitação ou rejeição de um pedido de certificado.	A.4.1 Certificate Application	N/A	N/A	N/A	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
4.2.3 Time to process certificate applications*	Estabelece um limite de tempo para o processamento das solicitações por parte da AC e/ou AR.	A.4.1 Certificate Application	N/A	N/A	N/A	N/A
4.3 Certificate Issuance	Descreve os elementos relacionados a assinatura (emissão) do certificado solicitado.					
4.3.1 CA actions during certificate issuance*	Descreve as ações da AC durante a emissão do certificado.	A.4.2 Certificate Issuance B.3.4 Certificate Issuance	N/A	N/A	7.3.3 Certificate generation Itens (b), (c)	N/A
4.3.2 Notification to subscriber by the CA of issuance of certificate*	Descreve os meios pelos quais o solicitante será informado da emissão do certificado.	A.2.2 Obligations A.4.2 Certificate Issuance B.3.4 Certificate Issuance	N/A	N/A	7.3.5 Certificate dissemination	N/A
4.4 Certificate Acceptance	Apresenta o procedimento para solicitação do certificado e as resposabilidades do solicitante associadas a esse processo.					
4.4.1 Conduct constituting certificate acceptance*	Descreve os requisitos e procedimentos operacionais referentes à aceitação do certificado emitido.	A.4.3 Certificate Acceptance	N/A	N/A	N/A	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
4.4.2 Publication of the certificate by the CA*	Descreve os requisitos e procedimentos operacionais referentes à publicação do certificado emitido.	A.2.2 Obligations A.4.3 Certificate Acceptance B.3.5 Certificate Distribution	N/A	N/A	N/A	N/A
4.4.3 Notification of certificate issuance by the CA to other entities*	Estabelece se haverá notificação de outras entidades sobre a emissão do certificado, seus requisitos e procedimentos.	A.2.2 Obligations	N/A	N/A	7.3.5 Certificate dissemination	N/A
4.5 Key Pair and Certificate Usage	Apresenta as responsabilidades na utilização do par de chaves e respectivo certificado.					
4.5.1 Subscriber private key and certificate usage*	Estabelece as responsabilidades do titular do certificado pela utilização das chaves privadas e dos certificados.	A.2.2 Obligations B.2.5 CA Key Usage	N/A	N/A	7.2.5 Certification Authority key Usage	N/A
4.5.2 Relying party public key and certificate usage*	Estabelece as responsabilidades da entidade confiante pela utilização das chaves públicas e dos certificados.	A.2.2 Obligations	N/A	N/A	N/A	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
4.6 Certificate Renewal	Apresenta os procedimentos, responsabilidades e circunstâncias para renovação do certificado, isto é, emissão de um novo certificado em substituição ao antigo com os mesmos atributos do certificado e par de chaves do titular.					
4.6.1 Circumstance for certificate renewal*	Estabelece as circunstâncias sob as quais uma renovação deve ser solicitada, quando aplicável.	N/A	N/A	N/A	N/A	N/A
4.6.2 Who may request renewal*	Estabelece quem está autorizado a solicitar a renovação de um certificado, se aplicável.	B.3.2 Certificate Renewal (if supported)	N/A	N/A	N/A	N/A
4.6.3 Processing certificate renewal requests*	Estabelece as medidas que AC e AR devem tomar para validar e responder pedidos de renovação, quando aplicável.	B.3.2 Certificate Renewal (if supported)	N/A	N/A	7.3.2 Certificate renewal, rekey and update	N/A
4.6.4 Notification of new certificate issuance to subscriber*	Estabelece se a AC comunicará o titular do certificado sobre a renovação, e os procedimentos e requisitos para fazê-lo.	A.2.2 Obligations B.3.2 Certificate Renewal (if supported)	N/A	N/A	N/A	N/A
4.6.5 Conduct constituting acceptance of a renewal certificate*	Estabelece a conduta de um titular de certificado que caracterize o aceite do certificado renovado.	N/A	N/A	N/A	N/A	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
4.6.6 Publication of the renewal certificate by the CA*	Especifica os locais de publicação dos certificados renovados.	A.2.2 Obligations B.3.2 Certificate Renewal (if supported) B.3.5 Certificate Distribution	N/A	N/A	N/A	N/A
4.6.7 Notification of certificate issuance by the CA to other entities*	Estabelece se a AC comunicará outras entidades (AR e partes confiantes, por exemplo) sobre a renovação.	A.2.2 Obligations B.3.2 Certificate Renewal (if supported)	N/A	N/A	N/A	N/A
4.7 Certificate Re-key	Apresenta os procedimentos, responsabilidades e circunstâncias para renovação do certificado, isto é, emissão de um novo certificado em substituição ao antigo com os mesmos atributos do certificado e um novo par de chaves do titular.					
4.7.1 Circumstance for certificate re-key*	Estabelece as circunstâncias sob as quais as chaves criptográficas devem ser trocadas, quando aplicável.	B.2.3 CA Public Key Distribution	N/A	N/A	N/A	N/A
4.7.2 Who may request certification of a new public key*	Estabelece, quando aplicável, quem está autorizado a solicitar a troca de chaves de um certificado.	N/A	N/A	N/A	N/A	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
4.7.3 Processing certificate re-keying requests*	Estabelece as medidas tomadas por AC ou AR para processar solicitações de substituição de par de chaves de certificados.	B.3.3 Certificate Rekey B.3.4 Certificate Issuance	N/A	N/A	7.3.2 Certificate renewal, rekey and update	N/A
4.7.4 Notification of new certificate issuance to subscriber*	Estabelece se a AC comunicará o titular do certificado sobre a emissão do novo certificado, e os procedimentos e requisitos para fazê-lo.	A.2.2 Obligations B.3.3 Certificate Rekey B.3.4 Certificate Issuance	N/A	N/A	N/A	N/A
4.7.5 Conduct constituting acceptance of a re-keyed certificate*	Estabelece a conduta de um titular de certificado que caracterize a aceitação do novo certificado.	N/A	N/A	N/A	N/A	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
4.7.6 Publication of the re-keyed certificate by the CA*	Especifica os locais e procedimentos de publicação dos novos certificados.	A.2.2 Obligations B.2.3 CA Public Key Distribution B.3.3 Certificate Rekey B.3.4 Certificate Issuance B.3.5 Certificate Distribution	N/A	N/A	7.3.2 Certificate renewal, rekey and update	N/A
4.7.7 Notification of certificate issuance by the CA to other entities*	Estabelece se a AC comunicará outras entidades (AR e partes confiantes, por exemplo) sobre a emissão do novo certificado.	A.2.2 Obligations B.3.3 Certificate Rekey	N/A	N/A	N/A	N/A
4.8 Certificate Modification	Apresenta os procedimentos, responsabilidades e circunstâncias para modificação do certificado, isto é, emissão de um novo certificado em substituição ao antigo com modificações nos atributos do certificado e mantendo par de chaves do titular.					
4.8.1 Circumstance for certificate modification*	Estabelece as circunstâncias sob um certificado pode ser modificado.	N/A	N/A	N/A	N/A	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
4.8.2 Who may request certificate modification*	Estabelece, quando aplicável, quem está autorizado a solicitar a modificação de um certificado.	N/A	N/A	N/A	N/A	N/A
4.8.3 Processing certificate modification requests*	Estabelece as medidas tomadas por AC ou AR para processar solicitações de modificação de certificados.	A.2.2 Obligations	N/A	N/A	7.3.2 Certificate renewal, rekey and update	N/A
4.8.4 Notification of new certificate issuance to subscriber*	Estabelece se a AC irá comunicar o titular sobre a emissão do novo certificado.	A.2.2 Obligations B.3.4 Certificate Issuance	N/A	N/A	N/A	N/A
4.8.5 Conduct constituting acceptance of modified certificate*	Estabelece a conduta de um titular de certificado que caracterize a aceitação de um novo certificado modificado.	N/A	N/A	N/A	N/A	N/A
4.8.6 Publication of the modified certificate by the CA*	Especifica os locais e procedimentos de publicação do certificado modificado.	A.2.2 Obligations B.3.5 Certificate Distribution	N/A	N/A	7.3.2 Certificate renewal, rekey and update	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
4.8.7 Notification of certificate issuance by the CA to other entities*	Estabelece se a AC comunicará outras entidades (AR e partes confiantes, por exemplo) sobre a modificação no certificado.	A.2.2 Obligations	N/A	N/A	N/A	N/A
4.9 Certificate Revocation and Suspension	Apresenta os procedimentos, responsabilidades e circunstâncias para revogação e suspensão de certificados.					
4.9.1 Circumstances for revocation*	Estabelece as circunstâncias sob as quais um certificado deve ser revogado.	A.4.4 Certificate Suspension and Revocation B.3.6 Certificate Revocation	N/A	N/A	7.3.6 Certificate revocation and suspension Item (a)	N/A
4.9.2 Who can request revocation*	Estabelece quem está autorizado a solicitar a revogação de um certificado.	A.4.4 Certificate Suspension and Revocation B.3.6 Certificate Revocation	N/A	N/A	7.3.6 Certificate revocation and suspension Item (a)	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
4.9.3 Procedure for revocation request*	Estabelece as medidas tomadas por AC ou AR para processar solicitações de revogação de certificados.	A.4.4 Certificate Suspension and Revocation B.3.6 Certificate Revocation	N/A	N/A	7.3.6 Certificate revocation and suspension Itens (a), (b), (c), (d), (e) e (h)	N/A
4.9.4 Revocation request grace period*	Estabelece um prazo para solicitação de revogação caso ocorra qualquer circunstância definida no item 4.9.1.	A.4.4 Certificate Suspension and Revocation	N/A	N/A	N/A	N/A
4.9.5 Time within which CA must process the revocation request*	Estabelece um prazo para AC processar uma solicitação de revogação.	A.4.4 Certificate Suspension and Revocation	N/A	N/A	7.3.6 Certificate revocation and suspension Item (a)	N/A
4.9.6 Revocation checking requirement for relying parties*	Estabelece mecanismos que devem ser usados pelas entidades confiantes a fim de verificar o status de certificados e determinar se são confiáveis.	A.2.2 Obligations A.4.4 Certificate Suspension and Revocation B.3.6 Certificate Revocation	N/A	N/A	N/A	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
4.9.7 CRL issuance frequency (if applicable)*	Estabelece a freqüência na qual uma nova Lista de Certificados Revogados (LCR) deve ser emitida, se aplicável.	A.4.4 Certificate Suspension and Revocation B.3.8 Certificate Status Information Processing	N/A	N/A	7.3.6 Certificate revocation and suspension Item (g)	N/A
4.9.8 Maximum latency for CRLs (if applicable)*	Estabelece o tempo máximo entre a geração de uma LCR e sua publicação no repositório da AC, se aplicável.	A.4.4 Certificate Suspension and Revocation	N/A	N/A	N/A	N/A
4.9.9 On-line revocation/status checking availability*	Estabelece, se aplicável, um mecanismo on-line que permita a verificação do status do certificado.	A.2.2 Obligations A.4.4 Certificate Suspension and Revocation	N/A	N/A	7.3.6 Certificate revocation and suspension Itens (i), (j), (k) e (l) 7.4.6 System access management Itens (k) e (l)	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
4.9.10 On-line revocation checking requirements*	Define as obrigações das entidades confiantes quanto à verificação on-line do status de certificados	A.2.2 Obligations A.4.4 Certificate Suspension and Revocation B.3.6 Certificate Revocation	N/A	N/A	N/A	N/A
4.9.11 Other forms of revocation advertisements available*	Estabelece formas alternativas de comunicação de revogação.	A.2.2 Obligations A.4.4 Certificate Suspension and Revocation B.3.6 Certificate Revocation	N/A	N/A	N/A	N/A
4.9.12 Special requirements for key compromise*	Estabelece procedimentos específicos para revogações em caso de comprometimento de chave privada.	A.4.4 Certificate Suspension and Revocation	N/A	N/A	N/A	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
4.9.13 Circumstances for suspension*	Estabelece as circunstâncias sob um certificado pode ser suspenso.	A.4.4 Certificate Suspension and Revocation B.3.7 Certificate Suspension (if supported)	N/A	N/A	7.3.6 Certificate revocation and suspension Item (a)	N/A
4.9.14 Who can request suspension*	Estabelece quem está autorizado a solicitar a suspensão de um certificado.	A.4.4 Certificate Suspension and Revocation B.3.7 Certificate Suspension (if supported)	N/A	N/A	7.3.6 Certificate revocation and suspension Item (a)	N/A
4.9.15 Procedure for suspension request*	Estabelece as medidas tomadas por AC ou AR para processar solicitações de suspensão de certificados.	A.4.4 Certificate Suspension and Revocation B.3.7 Certificate Suspension (if supported)	N/A	N/A	7.3.6 Certificate revocation and suspension Itens (a), (b), (c), (d), (e) e (h)	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
4.9.16 Limits on suspension period*	Define um período máximo de suspensão de certificados.	A.4.4 Certificate Suspension and Revocation B.3.7 Certificate Suspension (if supported)	N/A	N/A	N/A	N/A
4.10 Certificate Status Services	Apresenta as características e requisitos do serviço de verificação de status de certificados providos pela AC para as entidades confiantes.					
4.10.1 Operational characteristics*	Estabelece as características do serviço de verificação do status de certificados.	B.3.8 Certificate Status Information Processing	A.11.1 Business requirement for access control A.11.2 User access management	11.1 Business requirement for access control 11.2 User access management	7.4.6 System access management Item (j), (k) e (l)	Famílias Access Control, Maintenance, System and Communications Protection e System and Information Integrity
4.10.2 Service availability*	Define a disponibilidade do serviço e sob que circunstâncias ele pode se tornar indisponível.	N/A	N/A	N/A	N/A	Família Maintenance
4.10.3 Optional features*	Define quaisquer características opcionais dos serviços de verificação de status de certificado.	N/A	N/A	N/A	N/A	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
4.11 End of Subscription	Estabelece os procedimentos que caracterizam o encerramento do vínculo do titular com a AC.	N/A	N/A	N/A	N/A	N/A
4.12 Key Escrow and Recovery	Apresenta as características e requisitos para custódia e recuperação de chaves privadas, quando o serviço é oferecido pela AC ou uma terceira parte confiável.					
4.12.1 Key escrow and recovery policy and practices*	Define um documento ou estabelece práticas e políticas para custódia e recuperação de chaves.	B.2.4 CA Key Escrow (if supported)	N/A	N/A	7.2.4 Key escrow	N/A
4.12.2 Session key encapsulation and recovery policy and practices*	Define um documento ou Estabelece práticas e políticas para custódia e recuperação de chaves de sessão.	B.2.4 CA Key Escrow (if supported)	N/A	N/A	7.2.4 Key escrow	N/A
5. Facility, Management, and Operational Controls						
5.1 Physical Security Controls	Apresenta os controles de segurança física nas instalações que abrigam os sistemas da AC.					
5.1.1 Site location and construction*	Define a localização do ambiente que abriga os sistemas da AC, bem como os requisitos de segurança da construção.	A.5.1 Physical Security Controls B.1.2 Security Management B.1.5 Physical and Environmental Security	A.9.1 Secure áreas	9.1 Secure areas	7.4.4 Physical and environmental security Itens (f) e (g)	Família Physical and Environmental Protection

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
5.1.2 Physical Access*	Define os mecanismos de controle de acesso físico ao ambiente que abriga a AC.	A.5.1 Physical Security Controls B.1.2 Security Management B.1.5 Physical and Environmental Security	A.9.1 Secure áreas A.11.1 Business requirement for access control A.11.2 User access management	.9.1 Secure áreas 11.1 Business requirement for access control 11.2 User access management	7.4.4 Physical and environmental security Itens (a), (c), (d), (e), (f) e (h)	Família Accesss Control e Família Physical and Environmental Protection
5.1.3 Power and air conditioning*	Estabelece as medidas tomadas para manutenção da energia e da temperatura ideal no local de operação da AC.	A.5.1 Physical Security Controls B.1.2 Security Management B.1.5 Physical and Environmental Security	A.9.1 Secure areas A.9.2 Equipment security	9.1 Secure areas 9.2 Equipment security	7.4.4 Physical and environmental security Itens (b) e (g)	Família Physical and Environmental Protection
5.1.4 Water exposures*	Define as medidas tomadas para evitar a exposição dos sistemas a enchentes e alagamentos.	A.5.1 Physical Security Controls B.1.2 Security Management B.1.5 Physical and Environmental Security	A.9.1 Secure areas A.9.2 Equipment security	9.1 Secure areas 9.2 Equipment security	7.4.4 Physical and environmental security Itens (b) e (g)	Família Physical and Environmental Protection

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
5.1.5 Fire prevention and protection*	Define as medidas tomadas para evitar a exposição dos sistemas incêndios.	A.5.1 Physical Security Controls B.1.2 Security Management B.1.5 Physical and Environmental Security	A.9.1 Secure areas A.9.2 Equipment security	A.9.1 Secure areas A.9.2 Equipment security	7.4.4 Physical and environmental security Itens (b) e (g)	Família Physical and Environmental Protection
5.1.6 Media storage*	Define os requisitos para prevenção contra acesso, modificação, remoção e destruição não autorizada à mídia armazenada.	A.5.1 Physical Security Controls B.1.2 Security Management B.1.5 Physical and Environmental Security B.1.6 Operations Management	A.9.2 Equipment security A.10.7 Media handling	9.2 Equipment security 10.7 Media handling	7.2.7 Life cycle management of cryptographic hardware used to sign certificates Item (b) 7.4.4 Physical and environmental security Item (h) 7.4.5 Operations management Item (c), (d), (e) e (f)	Famílias Media Protection e Physical and Environmental Protection

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
5.1.7 Waste disposal*	Define os requisitos para descarte de informações sensíveis e dispositivos eletrônicos que são não mais necessários.	A.5.1 Physical Security Controls B.1.2 Security Management B.1.5 Physical and Environmental Security B.1.6 Operations Management B.2.6 CA Key Destruction	9.2 Equipment security 10.7 Media handling	9.2 Equipment security 10.7 Media handling	7.2.7 Life cycle management of cryptographic hardware used to sign certificates Item (e) 7.4.6 System access management Item (g)	Família Media Protection
5.1.8 Off-site backup*	Define os requisitos para cópias de segurança em outras instalações, como sua freqüência e considerações de segurança por não estar presente no ambiente principal.	A.5.1 Physical Security Controls B.1.2 Security Management	A.10.5 Back-up	10.5 Back-up	7.2.7 Life cycle management of cryptographic hardware used to sign certificates Item (b)	Família Physical and Environmental Protection

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
5.2 Procedural Controls	Apresenta os controles de segurança física nas instalações que abrigam os sistemas da AC.					
5.2.1 Trusted roles*	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.	A.5.2 Procedural Controls B.1.2 Security Management	A.6.1 Internal organization	6.1 Internal organization	7.4.3 Personnel security Itens (c) e (h)	Família Access Control
5.2.2 Number of persons required per task*	Especificar o número de pessoas necessárias para executar as tarefas listadas, caso sejam necessários controles de multiusuário.	A.5.2 Procedural Controls B.1.2 Security Management B.1.7 System Access Management	A.11.1 Business requirement for access control	11.1 Business requirement for access control	7.2.7 Life cycle management of cryptographic hardware used to sign certificates Item (c)	N/A
5.2.3 Identification and authentication for each role *	Especificar os controles necessários para identificar e autenticar os indivíduos na atuação de seus papéis.	A.5.2 Procedural Controls B.1.2 Security Management B.1.7 System Access Management	A.6.1 Internal organization A.11.2 User access management	6.1 Internal organization 11.2 User access management	7.4.6 System access management Itens (c), (d), (e) e (f)	Família Access Control

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
5.2.4 Roles requiring separation of duties*	Especifica papéis que não podem ser exercidos simultaneamente pelo mesmo indivíduo.	A.5.2 Procedural Controls B.1.2 Security Management B.1.6 Operations Management B.1.7 System Access Management	A.10.1 Operational procedures and responsibilities A.11.1 Business requirement for access control	10.1 Operational procedures and responsibilities 11.1 Business requirement for access control	7.4.3 Personnel security Item (d)	Família Access Control
5.3 Personnel Controls	Apresenta os controles de segurança dos recursos humanos envolvidos na operação dos sistemas da AC.					
5.3.1 Qualifications, experience, and clearance requirements*	Especifica os requisitos para contratação de pessoal que atuará em papéis de confiança.	A.5.3 Personnel Security Controls B.1.2 Security Management B.1.4 Personnel Security	A.8.1 Prior to employment	8.1 Prior to employment	7.4.3 Personnel security Itens (a), (f), (g), (i)	Família Personnel Security

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
5.3.2 Background check procedures*	Descreve os procedimentos seguidos para verificar os antecedentes antes da contratação de um funcionário que ocupará papéis de confiança ou outras funções importantes.	A.5.3 Personnel Security Controls B.1.2 Security Management B.1.4 Personnel Security	A.8.1 Prior to employment	8.1 Prior to employment	7.4.3 Personnel security Item (g), (j)	Família Personnel Security
5.3.3 Training requirements*	Estabelece o processo de treinamento pelo qual o pessoal deverá passar.	A.5.3 Personnel Security Controls B.1.2 Security Management B.1.4 Personnel Security	A.8.2 During employment	8.2 During employment	7.4.3 Personnel security Item (f)	Família Awareness and Training
5.3.4 Retraining frequency and requirements*	Estabelece a freqüência na qual deve haver um novo treinamento para o pessoal da AC.	A.5.3 Personnel Security Controls B.1.2 Security Management B.1.4 Personnel Security	A.8.2 During employment	8.2 During employment	N/A	Família Awareness and Training

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
5.3.5 Job rotation frequency and sequence*	Estabelece a freqüência de revezamento no exercício de papéis.	A.5.3 Personnel Security Controls	N/A	8.2 During employment	N/A	N/A
5.3.6 Sanctions for unauthorized actions*	Estabelece as medidas tomadas caso haja alguma ação não autorizada.	A.5.3 Personnel Security Controls B.1.2 Security Management	A.8.2 During employment	8.2 During employment	7.4.3 Personnel security Item (b)	Família Personnel Security
5.3.7 Independent contractor requirements*	Estabelece os controles sobre pessoal externo ao quadro de empregados da instituição na prestação de serviço para a mesma.	A.5.3 Personnel Security Controls B.1.2 Security Management B.1.4 Personnel Security	A.6.2 External parties A.10.2 Third party service delivery management	6.2 External parties 10.2 Third party service delivery management	7.1 Certification practice statement Item (b) 7.4.1 Security Management Itens (b) e (g) 7.5 Organizational Itens (g)	Família Access Control e Personnel Security
5.3.8 Documentation supplied to personnel*	Estabelece que documentos serão fornecidos ao pessoal responsável pela operação da AC ou AR.	A.5.3 Personnel Security Controls B.1.2 Security Management	A.5.1 Information security policy A.10.1 Operational procedures and responsibilities	5.1 Information security policy 10.1 Operational procedures and responsibilities	N/A	Família Personnel Security

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
5.4 Audit Logging Procedures	Apresenta os sistemas de registro de eventos e auditoria implementados com o propósito de manter um ambiente seguro.					
5.4.1 Types of events recorded*	Especifica que eventos serão registrados para compor a trilha de auditoria.	A.4.5 Security Audit Procedures B.1.2 Security Management B.1.11 Event Journaling	A.10.10 Monitoring	10.10 Monitoring	7.4.5 Operations management Item (i)	Família Access Control Família Audit and Accountability
5.4.2 Frequency of processing log*	Especifica a freqüência na qual os registros de auditoria são analisados em busca de um evento suspeito e então arquivados.	A.4.5 Security Audit Procedures B.1.2 Security Management B.1.11 Event Journaling	A.6.1 Internal organization A.10.10 Monitoring	6.1 Internal organization 10.10 Monitoring	7.4.5 Operations management Item (j)	Família Audit and Accountability
5.4.3 Retention period for audit log*	Especifica o período de arquivamento dos registros de auditoria, isto é, por quanto tempo serão armazenados.	A.4.5 Security Audit Procedures B.1.2 Security Management B.1.11 Event Journaling	A.10.10 Monitoring	10.10 Monitoring	N/A	Família Audit and Accountability

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
5.4.4 Protection of audit log*	Especifica os controles impostos às atividades relacionadas à administração dos registros de auditoria, como acesso e modificação, por exemplo.	A.4.5 Security Audit Procedures B.1.2 Security Management B.1.11 Event Journaling	A.10.10 Monitoring	10.10 Monitoring	7.4.6 System access management Itens (c), (d), (e) e (f)	Família Audit and Accountability
5.4.5 Audit log backup procedures*	Especifica os procedimentos para cópias de segurança de registros de eventos.	A.4.5 Security Audit Procedures B.1.2 Security Management B.1.11 Event Journaling	A.10.5 Back-up A.10.10 Monitoring	10.5 Back-up 10.10 Monitoring	N/A	Família Audit and Accountability
5.4.6 Audit collection system (internal vs external)*	Especifica se o sistema de recolhimento de registros de eventos é interno (ou seja, pertence à organização) ou externo (está fora das dependências da organização).	A.4.5 Security Audit Procedures B.1.2 Security Management B.1.11 Event Journaling	N/A	N/A	N/A	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
5.4.7 Notification to event-causing subject*	Especifica se o causador de um evento será ou não notificado sobre a auditoria.	A.4.5 Security Audit Procedures B.1.2 Security Management B.1.11 Event Journaling	N/A	N/A	N/A	Família Access Control
5.4.8 Vulnerability assessments*	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.	A.4.5 Security Audit Procedures B.1.2 Security Management B.1.11 Event Journaling	A.12.6 Technical Vulnerability Management	12.6 Technical Vulnerability Management	N/A	Família Risk Assessment
5.5 Records Archival	Apresenta as políticas para arquivamento ou retenção dos registros.					
5.5.1 Types of records archived*	Especifica que registros serão arquivados, isto é, retidos em local separado para posterior auditoria, se necessário.	A.4.6 Records Archival B.1.11 Event Journaling	A.10.10 Monitoring	10.10 Monitoring	7.4.11 Recording of information concerning certificates Itens (d), (g), (h), (i), (j), (k), (l), (m), (n) e (o)	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
5.5.2 Retention period for archive*	Especifica por quanto tempo os registros arquivados serão retidos.	A.4.6 Records Archival B.1.11 Event Journaling	A.10.10 Monitoring	10.10 Monitoring	7.4.11 Recording of information concerning certificates Itens (e)	N/A
5.5.3 Protection of archive*	Especifica os controles impostos a acessos, modificações, exclusões, entre outros, aos registros arquivados.	A.4.6 Records Archival B.1.11 Event Journaling	A.10.10 Monitoring	10.10 Monitoring	7.4.6 System access management Itens (c), (d), (e) e (f) 7.4.11 Recording of information concerning certificates Itens (a), (b), (c), (e) e (f)	N/A
5.5.4 Archive backup procedures*	Especifica os procedimentos para cópias de segurança dos registros arquivados.	A.4.6 Records Archival B.1.11 Event Journaling	A.10.5 Back-up A.10.10 Monitoring	10.5 Back-up 10.10 Monitoring	N/A	N/A
5.5.5 Requirements for time-stamping of records*	Especifica os requisitos para manter uma linha do tempo a partir da data e hora dos registros armazenados.	A.4.6 Records Archival B.1.11 Event Journaling	A.10.10 Monitoring	10.10 Monitoring	7.4.11 Recording of information concerning certificates Item (d)	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
5.5.6 Archive collection system (internal or external)*	Especifica se o sistema de recolhimento de registros arquivados é interno (ou seja, pertence à organização) ou externo (está fora das dependências da organização).	A.4.6 Records Archival B.1.11 Event Journaling	N/A	N/A	N/A	N/A
5.5.7 Procedures to obtain and verify archive information*	Especifica os procedimentos para obter e verificar os registros arquivados.	A.4.6 Records Archival B.1.11 Event Journaling	N/A	N/A	7.4.11 Recording of information concerning certificates Item (c)	N/A
5.6 Key Changeover	Especifica os procedimentos para divulgação da chave pública da AC para as entidades confiantes após o processo de troca de chaves da AC.	A.4.7 Key Changeover	N/A	N/A	7.2.1 Certification authority key generation Itens (e)	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
5.7 Compromise and Disaster Recovery	Apresenta os requisitos relacionados aos procedimentos de recuperação das atividades da AC e notificação em caso de comprometimento ou desastre.					
5.7.1 Incident and compromise handling procedures	Especifica os procedimentos para relatar e tratar incidentes e comprometimentos, incluindo da chave privada da AC.	B.1.6 Operations Management B.1.9 Business Continuity Management	A.13.1 Reporting information security events and weaknesses A.13.2 Management of information security incidents and improvements	13.1 Reporting information security events and weaknesses 13.2 Management of information security incidents and improvements	7.4.5 Operations management Itens (b) e (h) 7.4.8 Business continuity management and incident handling	Famílias Contingency Planning e Incident Response
5.7.2 Computing resources, software, and/or data are corrupted	Especifica os procedimentos para o caso de comprometimento de recursos que suportam a operação da AC ou ARs.	B.1.6 Operations Management B.1.9 Business Continuity Management	N/A	N/A	7.4.5 Operations management Item (b)	Família Contingency Planning

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
5.7.3 Entity private key compromise procedures	Descreve os procedimentos de recuperação a serem tomados no caso do comprometimento da chave privada da entidade.	A.2.2 Obligations B.1.6 Operations Management B.1.9 Business Continuity Management	A.13.1 Reporting information security events and weaknesses A.13.2 Management of information security incidents and improvements	13.1 Reporting information security events and weaknesses 13.2 Management of information security incidents and improvements	N/A	Famílias Contingency Planning e Incident Response
5.7.4 Business continuity capabilities after a disaster	Especifica resumidamente os procedimentos definidos no plano de continuidade de negócios aplicáveis.	B.1.6 Operations Management B.1.9 Business Continuity Management	A.14.1 Information security aspects of business continuity management	14.1 Information security aspects of business continuity management	7.4.8 Business continuity management and incident handling	Famílias Contingency Planning e Incident Response
5.8 CA or RA Termination	Descreve as providências tomadas quando houver finalização desta AC.	A.4.9 CA Termination B.1.9 Business Continuity Management	N/A	N/A	7.4.9 CA ternination	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
6 Technical Security Controls						
6.1 Key Pair Generation and Installation *	Apresenta os requisitos para geração e instalação do par de chaves da AC, AR, etc.					
6.1.1 Key pair generation*	Estabelece quem será responsável pela geração do par de chaves da entidade que solicita um certificado e como a atividade é realizada.	A.6.1 Key Pair Generation and Installation B.2.1 CA Key Generation B.2.9 CA-Provided Subscriber Key Management Services (if supported)	N/A	N/A	7.2.1 Certification authority key generation 7.2.8 CA provided subject key management services Itens (a) e (b) 7.3.3 Certificate generation Itens (b) 7.4.4 Physical and environmental security Itens (d)	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
6.1.2 Private key delivery to subscriber*	Estabelece os métodos utilizados para que a chave privada seja entregue de forma segura ao titular do certificado.	A.6.1 Key Pair Generation and Installation B.2.9 CA-Provided Subscriber Key Management Services (if supported)	N/A	N/A	7.2.8 CA provided subject key management services Itens (c), (d) e (e)	N/A
6.1.3 Public key delivery to certificate issuer*	Estabelece os métodos utilizados para que a chave pública de um certificado seja entregue de forma segura à Autoridade Certificadora.	A.6.1 Key Pair Generation and Installation	N/A	N/A	N/A	N/A
6.1.4 CA public key delivery to relying parties*	Estabelece os métodos utilizados para que a chave pública da AC seja disponibilizada de forma segura para as entidades confiantes.	A.6.1 Key Pair Generation and Installation B.2.3 CA Public Key Distribution	N/A	N/A	7.2.3 Certification authority public key distribution	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
6.1.5 Key sizes*	Estabelece o tamanho mínimo das chaves geradas.	A.6.1 Key Pair Generation and Installation B.2.1 CA Key Generation	N/A	N/A	7.2.1 Certification authority key generation Item (d)	N/A
6.1.6 Public key parameters generation and quality checking*	Estabelece quem é responsável pela geração dos parâmetros da chave pública e os procedimentos de verificação de sua qualidade durante este processo.	A.6.1 Key Pair Generation and Installation	N/A	N/A	N/A	N/A
6.1.7 Key usage purposes (as per X509 v3 key usage field)*	Estabelece para que propósitos as chaves podem ser usadas ou são restritos.	A.6.1 Key Pair Generation and Installation B.2.5 CA Key Usage	N/A	N/A	7.2.5 Certification authority key usage	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
6.2 Private Key Protection and Cryptographic Module Engineering Controls	Apresenta os requisitos para proteção da chave privada do titular e utilização de módulos criptográficos.					
6.2.1 Cryptographic module standards and controls*	Estabelece os padrões e controles requeridos para os módulos criptográficos.	A.6.2 Private Key Protection A.6.8 Cryptographic Module Engineering Controls B.2.2 CA Key Storage, Backup and Recovery B.2.8 CA Cryptographic Hardware Life Cycle Management	A.12.3 Cryptographic controls A.15.1 Compliance with legal requirements A.15.2 Compliance with security policies and standards, and technical compliance	12.3 Cryptographic controls 15.1 Compliance with legal requirements 15.2 Compliance with security policies and standards, and technical compliance	7.2.1 Certification authority key generation Itens (b) e (c) 7.2.7 Life cycle management of cryptographic hardware used to sign certificates	Famílias Access Control e Identification and Authentication

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
6.2.2 Private key (n out of m) multi-person control*	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.	A.6.2 Private Key Protection A.6.8 Cryptographic Module Engineering Controls B.1.7 System Access Management B.2.2 CA Key Storage, Backup and Recovery	A.12.3 Cryptographic controls	12.3 Cryptographic controls	7.2.1 Certification authority key generation Itens (a) 7.2.7 Life cycle management of cryptographic hardware used to sign certificates Item (c)	N/A
6.2.3 Private key escrow*	Estabelece quem é responsável pela custódia das chaves privadas como é feita e os controles de segurança envolvidos, se aplicável.	A.6.2 Private Key Protection B.2.9 CA-Provided Subscriber Key Management Services (if supported)	A.12.3 Cryptographic controls	12.3 Cryptographic controls	7.2.4 Key escrow	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
6.2.4 Private key backup*	Estabelece como é feita a cópia de segurança da chave privada da AC, AR e entidades finais, se aplicável.	A.6.2 Private Key Protection B.2.2 CA Key Storage, Backup and Recovery B.2.9 CA-Provided Subscriber Key Management Services (if supported)	A.10.5 Back-up A.12.3 Cryptographic controls	10.5 Back-up 12.3 Cryptographic controls	7.2.2 Certification authority key storage, backup and recovery Itens (c) e (d)	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
6.2.5 Private key archival*	Estabelece como é feito o arquivamento da cópia da chave privada, isto é, seu armazenamento por um período de tempo longo, se aplicável.	A.6.2 Private Key Protection B.2.2 CA Key Storage, Backup and Recovery B.2.7 CA Key Archival B.2.8 CA Cryptographic Hardware Life Cycle Management B.2.9 CA-Provided Subscriber Key Management Services	A.12.3 Cryptographic controls	12.3 Cryptographic controls	7.2.2 Certification authority key storage, backup and recovery Item (b)	N/A
6.2.6 Private key transfer into or from a cryptographic module*	Estabelece as circunstâncias nas quais a chave privada pode ser transferida de ou para um módulo criptográfico, e os procedimentos envolvidos na tarefa.	A.6.2 Private Key Protection B.2.2 CA Key Storage, Backup and Recovery B.2.8 CA Cryptographic Hardware Life	A.12.3 Cryptographic controls	12.3 Cryptographic controls	7.2.2 Certification authority key storage, backup and recovery Item (b)	N/A

		Cycle Management				
Componentes da RFC 3647	**Descrição do componente**	**ANSI X9.79:2001**	**ISO/IEC 27001:2005**	**ISO/IEC 27002:2005**	**ETSI TS 102 042**	**NIST SP 800-53**
6.2.7 Private key storage on cryptographic module*	Estabelece como as chaves privadas devem estar armazenadas nos módulos criptográficos.	A.6.2 Private Key Protection A.6.8 Cryptographic Module Engineering Controls B.2.2 CA Key Storage, Backup and Recovery B.2.8 CA Cryptographic Hardware Life Cycle Management	A.12.3 Cryptographic controls	12.3 Cryptographic controls	7.2.2 Certification authority key storage, backup and recovery Itens (a) e (e)	N/A
6.2.8 Method of activating private key*	Estabelece quem pode usar as chaves privadas, que ações devem ser tomadas para a ativação e o período em que a chave pode ficar ativa.	A.6.2 Private Key Protection A.6.8 Cryptographic Module Engineering Controls B.2.8 CA Cryptographic Hardware Life Cycle Management	A.12.3 Cryptographic controls	12.3 Cryptographic controls	N/A	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
6.2.9 Method of deactivating private key*	Estabelece quem pode desativar as chaves privadas e que ações devem ser tomadas para a desativação.	A.6.2 Private Key Protection A.6.8 Cryptographic Module Engineering Controls B.2.8 CA Cryptographic Hardware Life Cycle Management	A.12.3 Cryptographic controls	12.3 Cryptographic controls	N/A	N/A
6.2.10 Method of destroying private key*	Estabelece quem pode destruir as chaves privadas, que ações devem ser tomadas para efetuar a tarefa.	A.6.2 Private Key Protection A.6.8 Cryptographic Module Engineering Controls B.2.6 CA Key Destruction B.2.8 CA Cryptographic Hardware Life Cycle Management	A.12.3 Cryptographic controls	12.3 Cryptographic controls	7.2.6 End of CA key lifecycle	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
6.2.11 Cryptographic Module Rating*	Provê características sobre módulos criptográficos a serem utilizados.	A.6.2 Private Key Protection A.6.8 Cryptographic Module Engineering Controls B.2.8 CA Cryptographic Hardware Life Cycle Management	A.12.3 Cryptographic controls	12.3 Cryptographic controls	N/A	N/A
6.3 Other Aspects of Key Pair Management	Apresenta outros aspectos do gerenciamento do par de chaves, como arquivamento da chave pública.					
6.3.1 Public key archival*	Estabelece se as chaves públicas dos participantes da ICP devem ou não ser arquivadas e que controles são utilizados para mantê-las seguras.	A.6.3 Other Aspects of Key Pair Management	A.12.3 Cryptographic controls	12.3 Cryptographic controls	N/A	N/A
6.3.2 Certificate operational periods and key pair usage periods*	Estabelece o período operacional do certificado e o tempo de vida do par de chaves.	A.6.3 Other Aspects of Key Pair Management	A.12.3 Cryptographic controls	12.3 Cryptographic controls	N/A	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
6.4 Activation Data	Apresenta os requisitos para proteção dos dados de ativação, isto é, dados que são necessários para utilizar chaves privadas e módulos criptográficos, além dos próprios. É importante que considerem todo o ciclo de vida dos dados de ativação.					
6.4.1 Activation data generation and installation*	Estabelece os dados de ativação usados para ativar as chaves privadas, bem como seus métodos de geração e instalação.	A.6.4 Activation Data	N/A	N/A	N/A	N/A
6.4.2 Activation data protection*	Estabelece os procedimentos para proteção dos dados de ativação das chaves privadas.	A.6.4 Activation Data	N/A	N/A	N/A	N/A
6.4.3 Other aspects of activation data*	Estabelece outros aspectos sobre os dados de ativação.	A.6.4 Activation Data	N/A	N/A	N/A	N/A
6.5 Computer Security Controls	Apresenta os requisitos de segurança computacional que são utilizados para manter o ambiente seguro, além de requisitos para avaliação e certificação de produtos relacionados ao gerenciamento do ciclo de vida dos certificados. Uma métrica pode ser necessária para apoiar a avaliação da eficácia desses controles.					

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
6.5.1 Specific computer security technical requirements*	Descreve controles técnicos de segurança computacional estabelecidos para garantir uma operação segura da AC.	A.6.5 Computer Security Controls B.1.2 Security Management	A.5.1 Information security policy A.10.1 Operational procedures and responsibilities A.10.3 System planning and acceptance A.10.4 Protection against malicious and mobile code A.11.2 User access management A.11.4 Network access control A.11.5 Operating system access control A.11.6 Application and information access control	5.1 Information security policy 10.1 Operational procedures and responsibilities 10.3 System planning and acceptance 10.4 Protection against malicious and mobile code 11.2 User access management 11.4 Network access control 11.5 Operating system access control 11.6 Application and information access control	7.4.5 Operations management Item (a) 7.4.6 System access management Item (a) 8.1 Certificate policy management Item (c)	Famílias Access Control, Identification and Authentication, System and Communications Protection e System and Information Integrity

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
6.5.2 Computer security rating*	Estabelece índices de segurança independentes para avaliação de sistemas relacionados às operações da AC.	A.6.5 Computer Security Controls B.1.2 Security Management	N/A	N/A	N/A	N/A
6.6 Life Cycle Security Controls	Apresenta os controles aplicados no desenvolvimento dos sistemas (como boas práticas de engenharia de software e segurança no desenvolvimento) e gerenciamento de segurança (como procedimentos e ferramentas que garantam a integridade dos sistemas).					
6.6.1 System development controls*	Estabelece controles sobre o desenvolvimento dos sistemas utilizados para o gerenciamento do ciclo de vida dos certificados.	A.6.6 Life Cycle Security Controls B.1.2 Security Management B.1.8 Systems Development and Maintenance	A.10.1 Operational procedures and responsibilities A.10.3 System planning and acceptance A.12.1 Security requirements of information systems A.12.2 Correct processing in applications A.12.5 Security in development and support processes	10.1 Operational procedures and responsibilities 10.3 System planning and acceptance 12.1 Security requirements of information systems 12.2 Correct processing in applications 12.5 Security in development and support processes	7.4.7 Trustworthy sstems deployment and maintenance	Famílias Access Control, Configuration Management, Identification and Authentication, Família System and Services Acquisition e System and Information Integrity

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
6.6.2 Security management controls*	Estabelece controles usados para garantir que os sistemas estão operando corretamente e de forma consistente com a configuração desejada.	A.6.6 Life Cycle Security Controls B.1.2 Security Management B.1.3 Asset Classification and Management B.1.6 Operations Management B.1.7 System Access Management B.1.8 Systems Development and Maintenance	A.5.1 Information security policy A.7.1 Responsibility for assets A.10.1 Operational procedures and responsibilities A.10.4 Protection against malicious and mobile code A.11.1 Business requirement for access control A.11.2 User Access management A.11.3 User responsibilities A.11.6 Application and information access control A.12.4 Security of system files	5.1 Information security policy 7.1 Responsibility for assets 10.1 Operational procedures and responsibilities 10.4 Protection against malicious and mobile code 11.1 Business requirement for access control 11.2 User access management 11.3 User responsibilities 11.6 Application and information access control 12.4 Security of system files	7.4.1 Security Management 7.4.5 Operations management Item (k) 7.4.6 System access management Itens (h), (i) e (k)	Famílias Access Control, Configuration Management, Planning, System and Communications Protection e System and Information Integrity

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
6.6.3 Life cycle security controls*	Estabelece controles segurança no ciclo de vida do software.	A.6.6 Life Cycle Security Controls B.1.2 Security Management B.1.3 Asset Classification and Management B.1.6 Operations Management B.1.7 System Access Management B.1.8 Systems Development and Maintenance	A.5.1 Information security policy A.7.1 Responsibility for assets A.10.1 Operational procedures and responsibilities A.10.3 System planning and acceptance A.11.6 Application and information access control A.12.1 Security requirements of information systems A.12.4 Security of system files	5.1 Information security policy 7.1 Responsibility for assets 10.1 Operational procedures and responsibilities 10.3 System planning and acceptance 11.6 Application and information access control 12.1 Security requirements of information systems 12.4 Security of system files	7.4.2 Asset classification and management 7.4.5 Operations management Item (g) 7.4.7 Trustworthy sstems deployment and maintenance Item (b)	Famílias Configuration Management, Maintenance, Planning e System and Services Acquisition

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
6.7 Network Security Controls	Estabelece controles sobre a rede de comunicações, especialmente sobre aquelas usadas pela AC e AR.	A.6.7 Network Security Controls B.1.2 Security Management B.1.7 System Access Management	A.5.1 Information security policy A.7.1 Responsibility for assets A.9.2 Equipment security A.10.6 Network security management A.11.4 Network access control	5.1 Information security policy 7.1 Responsibility for assets 9.2 Equipment security 10.6 Network security management 11.4 Network access control	7.4.6 System access management Itens (a), (b), (h) e (i)	Famílias Access Control e System and Communications Protection
6.8 Timestamping	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.	N/A	A.10.10 Monitoring	10.10 Monitoring	N/A	Família Audit and Accountability

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
7 Certificate, CRL, and OCSP Profiles						
7.1 Certificate Profile	Especifica o formato dos certificados emitidos, incluindo informações sobre versão, extensões, etc. Mais informações sobre esses perfis podem ser encontradas em [Cooper et al., 2008].					
7.1.1 Version number(s)*	Define a versão dos certificados emitidos pela AC.	A.7.1 Certificate Profile	N/A	N/A	7.1 Certification practice statement Item (i)	N/A
7.1.2 Certificate extensions*	Define as extensões utilizadas nos certificados emitidos pela AC.	A.7.1 Certificate Profile	N/A	N/A	7.1 Certification practice statement Item (i)	N/A
7.1.3 Algorithm object identifiers*	Define os OIDs dos algortimos criptográficos.	A.7.1 Certificate Profile	N/A	N/A	7.1 Certification practice statement Item (i)	N/A
7.1.4 Name forms*	Define formato do Distinguished Name (DN) dos certificados emitidos pela AC.	A.7.1 Certificate Profile	N/A	N/A	7.1 Certification practice statement Item (i)	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
7.1.5 Name constraints*	Define as restrições aplicáveis para nomes de titulares de certificados.	A.7.1 Certificate Profile	N/A	N/A	7.1 Certification practice statement Item (i)	N/A
7.1.6 Certificate policy object identifier*	Apresenta o OID da PC, que constará no certificado emitido..	A.7.1 Certificate Profile	N/A	N/A	7.1 Certification practice statement Item (i)	N/A
7.1.7 Usage of Policy Constraints extension*	Define o uso da extensão Policy Constraints pela AC, e as limitações impostas por ela.	A.7.1 Certificate Profile	N/A	N/A	7.1 Certification practice statement Item (i)	N/A
7.1.8 Policy qualifiers syntax and semantics*	Define se a AC utiliza os qualificadores de política com a extensão certificate policies para transportar informações e define que informações são transportadas	A.7.1 Certificate Profile	N/A	N/A	7.1 Certification practice statement Item (i)	N/A
7.1.9 Processing semantics for the critical Certificate Policies extension*	Define se a AC marca como crítica a extensão *certificate policies* ou requer que uma AC subordinada o faça.	A.7.1 Certificate Profile	N/A	N/A	7.1 Certification practice statement Item (i)	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
7.2 CRL Profile	Especifica o formato das Listas de Certificados Revogados (LCRs) emitidas, incluindo informações sobre versão, extensões, etc. Mais informações sobre esses perfis podem ser encontradas em [Cooper et al., 2008].					
7.2.1 Version number(s)*	Define a versão das LCRs emitidas pela AC.	A.7.2 CRL Profile	N/A	N/A	7.1 Certification practice statement Item (i)	N/A
7.2.2 CRL and CRL entry extensions*	Descreve as extensões de LCR utilizadas e sua criticidade.	A.7.2 CRL Profile	N/A	N/A	7.1 Certification practice statement Item (i)	N/A
7.3 OCSP Profile	Apresenta considerações sobre a implementação do Online Certificate Status Profile (OCSP) emitidas, incluindo informações sobre versão, extensões, etc. Mais informações sobre esses perfis podem ser encontradas em [Cooper et al., 2008].					
7.3.1 Version number(s)	Define a versão da OCSP disponível para verificar o status dos certificados.	A.7.2 OCSP Profile	N/A	N/A	7.1 Certification practice statement Item (i)	N/A
7.3.2 OCSP extensions	Define as extensões usadas pela OCSP.	A.7.2 OCSP Profile	N/A	N/A	7.1 Certification practice statement Item (i)	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
8. Compliance Audit and Other Assessment						
8.1 Frequency or circumstances of assessment*	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.	A.2.5 Compliance Audit B.1.10 Monitoring and Compliance	A.6.1 Internal organization A.15.2 Compliance with security policies and standards, and technical compliance	6.1 Internal organization 15.2 Compliance with security policies and standards, and technical compliance	8.3 Conformance Item (d)	Famílias Certification, Accreditation, and Security Assessments e Audit and Accountability
8.2 Identity/qualifications of assessor*	Estabelece quem pode conduzir as avaliações, isto é, sua identidade e qualificações.	A.2.5 Compliance Audit B.1.10 Monitoring and Compliance	A.6.1 Internal organization	6.1 Internal organization	N/A	Famílias Certification, Accreditation, and Security Assessments e Audit and Accountability
8.3 Assessor's relationship to assessed entity*	Estabelece a relação do avaliador com a entidade avaliada, e sua autonomia.	A.2.5 Compliance Audit B.1.10 Monitoring and Compliance	A.6.1 Internal organization	6.1 Internal organization	8.3 Conformance Item (a)	Famílias Certification, Accreditation, and Security Assessments e Audit and Accountability

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
8.4 Topics covered by assessment*	Estabelece os requisitos que serão avaliados.	A.2.5 Compliance Audit B.1.10 Monitoring and Compliance	A.15.2 Compliance with security policies and standards, and technical compliance A.15.3 Information systems audit considerations	15.2 Compliance with security policies and standards, and technical compliance 15.3 Information systems audit considerations	8.3 Conformance Itens (e), (f), (g), (h), (i)	Famílias Certification, Accreditation, and Security Assessments e Audit and Accountability
8.5 Actions taken as a result of deficiency*	Estabelece as ações tomadas quando alguma não-conformidade é encontrada após uma avaliação.	A.2.5 Compliance Audit B.1.10 Monitoring and Compliance	N/A	N/A	8.3 Conformance Item (c)	Famílias Certification, Accreditation, and Security Assessments e Audit and Accountability
8.6 Communication of results*	Estabelece quem terá acesso aos resultados das avaliações, e como serão divulgados.	A.2.5 Compliance Audit B.1.10 Monitoring and Compliance	N/A	N/A	8.3 Conformance Itens (a), (b)	Famílias Certification, Accreditation, and Security Assessments e Audit and Accountability

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
9. Other Business and Legal Matters						
9.1 Fees	Apresenta considerações sobre taxas cobradas pela AC, AR ou repositórios.					
9.1.1 Certificate issuance or renewal fees*	Estabelece uma taxa pela prestação dos serviços de emissão e renovação de certificados.	N/A	N/A	N/A	N/A	N/A
9.1.2 Certificate access fees*	Estabelece uma taxa para utilização dos certificados pelas entidades confiantes.	N/A	N/A	N/A	N/A	N/A
9.1.3 Revocation or status information access fees*	Estabelece uma taxa pela prestação dos serviços de revogação ou informação de estados dos certificados.	N/A	N/A	N/A	N/A	N/A
9.1.4 Fees for other services*	Estabelece uma taxa pela prestação de serviços não definidos anteriormente.	N/A	N/A	N/A	N/A	N/A
9.1.5 Refund policy*	Estabelece uma política de reembolso das taxas pagas pela prestação de serviços.	N/A	N/A	N/A	N/A	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
9.2 Financial Responsibility	Apresenta considerações sobre recursos disponibilizados para ACs, ARs e outros participantes que estejam provendo serviços que suportem suas responsabilidades operacionais, como o pagamento em caso de danos e ações indevidas.					
9.2.1 Insurance coverage*	Estabelece a cobertura de seguro de um participante sobre os riscos de suas responsabilidades.	N/A	N/A	N/A	N/A	N/A
9.2.2 Other assets*	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.	N/A	N/A	N/A	N/A	N/A
9.2.3 Insurance or warranty coverage for end-entities*	Estabelece a cobertura de seguro de terceiros envolvidos na participação de uma entidade na ICP.	N/A	N/A	N/A	N/A	N/A
9.3 Confidentiality of Business Information	Apresenta considerações sobre o tratamento de informações consideradas confidenciais.					
9.3.1 Scope of confidential information*	Define que informações são consideradas confidenciais.	A.2.6 Confidenciality Policy	A.6.1 Internal organization	6.1 Internal organization	N/A	Família Access Control
9.3.2 Information not within the scope of confidential information*	Define que informações não são consideradas confidenciais.	A.2.6 Confidenciality Policy	A.6.1 Internal organization	6.1 Internal organization	N/A	Família Access Control

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
9.3.3 Responsibility to protect confidential information*	Define responsáveis pela guarda e proteção de informações consideradas confidenciais.	A.2.6 Confidenciality Policy A.10.7 Media handling	A.6.1 Internal organization	6.1 Internal organization	N/A	Famílias Access Control e Media Protection
9.4 Privacy of Personal Information	Apresenta as medidas que devem ser tomadas pela AC para proteger informações de identificação pessoal de solicitantes, titulares de certificado ou outros participantes da ICP, devendo considerar a legislação aplicável.					
9.4.1 Privacy plan*	Define o plano de privacidade aplicável às atividades dos participantes.	B.1.3 Asset Classification and Management	A.7.2 Information classification	7.2 Information classification	N/A	Família Access Control
9.4.2 Information treated as private*	Define que informações são tratadas como privadas.	B.1.3 Asset Classification and Management	A.7.2 Information classification	7.2 Information classification	N/A	N/A
9.4.3 Information not deemed private*	Define que informações não são tratadas como privadas.	N/A	A.7.2 Information classification	7.2 Information classification	N/A	N/A
9.4.4 Responsibility to protect private information*	Estabelece a responsabilidade pela proteção de informações que são tratadas como privadas.	N/A	A.7.2 Information classification A.10.7 Media handling	7.2 Information classification 10.7 Media handling	7.3.1 Subject registration Item (p)	Família Media Protection
9.4.5 Notice and consent to use private information*	Estabelece os requisitos para determinar o consentimento do uso de uma informação privada por parte do dono.	N/A	A.7.2 Information classification	7.2 Information classification	N/A	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
9.4.6 Disclosure pursuant to judicial or administrative process*	Define as circunstâncias nas quais é requerida ao participante a divulgação de informações consideradas privadas para atender processos administrativos.	N/A	A.7.2 Information classification	7.2 Information classification	7.4.11 Recording of information concerning certificates Item (c)	N/A
9.4.7 Other information disclosure circumstances*	Define outras circunstâncias nas quais é requerida ao participante a divulgação de informações consideradas privadas.	N/A	A.7.2 Information classification	7.2 Information classification	N/A	N/A
9.5 Intellectual Property Rights	Estabelece os direitos de propriedade intelectual sobre vários aspectos, como certificados, PCs, DPCs, nomes, bancos de dados, entre outros.	N/A	A.15.1 Compliance with legal requirements	15.1 Compliance with legal requirements	N/A	N/A
9.6 Representations and Warranties	Apresenta informações sobre garantias e representações para as entidades participantes da ICP.					
9.6.1 CA representations and warranties*	Estabelece as garantias oferecidas pela AC na prestação do serviço de certificação.	A.2.1 Liability	N/A	N/A	7.3.1 Subject registration 7.5 Organizational Item (e), (h) e (i)	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
9.6.2 RA representations and warranties*	Estabelece as garantias oferecidas pela AR na prestação do serviço de autenticação.	A.2.1 Liability	N/A	N/A	N/A	N/A
9.6.3 Subscriber representations and warranties*	Estabelece as garantias oferecidas pelos titulares na utilização de certificados.	A.2.1 Liability	A.6.2 External parties	6.2 External parties	N/A	N/A
9.6.4 Relying party representations and warranties*	Estabelece as garantias oferecidas pelas entidades confiantes na utilização de certificados.	A.2.1 Liability	A.6.2 External parties	6.2 External parties	N/A	N/A
9.6.5 Representations and warranties of other participants*	Estabelece as garantias oferecidas por outros participantes da ICP.	A.2.1 Liability	A.6.2 External parties	6.2 External parties	7.5 Organizational Item (g)	N/A
9.7 Disclaimers of Warranties	O conteúdo é composto por renúncias de garantias que possam existir no documento ou impostar pela lei aplicável, por exemplo.	A.2.1 Liability	N/A	N/A	N/A	N/A
9.8 Limitations of Liability	Descreve limitações de responsabilidades atreladas aos acordos de aceitação por parte dos usuários e entidades confiantes, por exemplo.	A.2.1 Liability	N/A	N/A	7.5 Organizational Item (d)	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
9.9 Indemnities	Estabelece indenizações decorrentes de conduta de uma entidade que cause dano à outra.	A.2.1 Liability	N/A	N/A	N/A	N/A
9.10 Term and Termination	Apresenta o período na qual as provisões da PC/DPC se mantêm válidas, e as circunstâncias nas quais o documento, parte dele ou sua aplicação sobre um determinado participantes deixa de ter validade.					
9.10.1 Term*	Estabelece o período de validade das provisões do documento.	N/A	N/A	N/A	N/A	N/A
9.10.12 Termination	Estabelece o prazo em que o documento ou parte dele deixa de ter efeito.	N/A	N/A	N/A	N/A	N/A
9.10.13 Effect of termination and survival*	Descreve as conseqüências da terminação de validade do documento.	N/A	N/A	N/A	N/A	N/A
9.11 Individual notices and communications with participants	Estabelece a forma de comunicação entre os participantes para que seja legalmente efetiva.	N/A	N/A	N/A	N/A	N/A
9.12 Amendments	Apresenta os procedimentos para efetuar emendas no documento de PC/DPC.					
9.12.1 Procedure for amendment*	Estabelece os procedimentos tomados quando necessárias emendas nos documentos.	A.8.1 Change Procedures A.8.3 Approval Procedures	N/A	N/A	N/A	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
9.12.2 Notification mechanism and period*	Estabelece os mecanismos utilizados para notificar os interessados, caso haja emendas no documento.	A.8.2 Publication and Notification Procedures	N/A	N/A	7.1 Certification practice statement Item (h) 8.2 Additional requirements	N/A
9.12.3 Circumstances under which OID must be changed*	Circunstâncias nas quais as emendas acarretam na mudança do identificador de objeto do documento.	A.8.1 Change Procedures	N/A	N/A	N/A	N/A
9.13 Dispute Resolution Procedures	Determina os procedimentos utilizados para resolver disputas envolvendo as provisões dos documentos da ICP.	A.2.3 Interpretation and Enforcement	N/A	N/A	7.5 Organizational Item (f)	N/A
9.14 Governing Law	Estabelece que as atividades da AC devem estar conformes com a legislação vigente no país.	A.2.3 Interpretation and Enforcement	N/A	N/A	7.4.10 Compliance with legal requirements 7.5 Organizational Item (c)	N/A
9.15 Compliance with Applicable Law	Estabelece provisões para garantir a conformidade das atividades da AC com a legislação vigente.	B.1.10 Monitoring and Compliance	A.15.1 Compliance with legal requirements	15.1 Compliance with legal requirements	7.4.10 Compliance with legal requirements	N/A

Componentes da RFC 3647	Descrição do componente	ANSI X9.79:2001	ISO/IEC 27001:2005	ISO/IEC 27002:2005	ETSI TS 102 042	NIST SP 800-53
9.16 Miscellaneous Provisions	Apresenta provisões diversas, que não se encaixam em seções anteriores.					
9.16.1 Entire agreement*	Estabelece a concordância completa entre as partes cobertas no documento.	N/A	N/A	N/A	N/A	N/A
9.16.2 Assignment*	Estabelece os limites de delegação de direitos e obrigações das entidades participantes.	N/A	N/A	N/A	N/A	N/A
9.16.3 Severability*	Estabelece um acordo entre as partes definindo que a revogação de uma cláusula não afete a validade de todo documento.	A.2.3 Interpretation and Enforcement	N/A	N/A	N/A	N/A
9.16.4 Enforcement (attorneys' fees and waiver of rights)*	Estabelece quem será responsável por arcar com as despesas relacionadas aos encargos jurídicos.	N/A	N/A	N/A	N/A	N/A
9.16.5 Force Majeure*	Estabelece como serão tratados eventos fora do controle da AC.	N/A	N/A	N/A	N/A	N/A
9.17 Other Provisions	Estabelece termos e responsabilidades gerais que não se enquadrem em nenhuma das seções anteriores.	N/A	N/A	N/A	7.5 Organizational Item (a) e (b)	N/A

APÊNDICE B – *Template* para PC/DPC em Português do Brasil

Este apêndice apresenta um *template* para elaboração de documentos de PC/DPC em português do Brasil. O espaço para as provisões é mantido em branco, para ser preenchido pelo autor de PC/DPC.

Política de Certificado e Declaração de Práticas de Certificação
[Nome da AC]

Versão [Versão do documento] – [Data da versão]

Sumário

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.

1.1 Visão Geral

[Insira o texto aqui]

1.2 Nome do Documento e Identificação

Titulo: Política de Certificação e Declaração de Práticas de Certificação da [Insira aqui o nome da sua Autoridade Certificadora]
Versão: [Insira aqui a versão do documento].
Data: [Insira aqui a data de criação do documento]
Aprovação: Este documento foi aprovado em [Insira aqui a data de aprovação do documento]
ANSI.1 OID: [Insira aqui o OID do documento]

1.3 Participantes da ICP

1.3.1 Autoridades Certificadoras

[Insira aqui o texto que identifica a AC]

1.3.2 Autoridades de Registro

[Insira aqui o texto que identifica as ARs relacionadas à AC]

1.3.3 Titulares dos Certificados

[Insira aqui o texto que caracteriza os titulares de certificado]

1.3.4 Entidades Confiantes

[Insira aqui o texto que identifica as entidades confiantes]

1.3.5 Outros Participantes

[Insira aqui o texto que caracteriza outros participantes da ICP]

1.4 Uso do Certificado

1.4.1 Aplicações apropriadas para os certificados

[Insira aqui o texto que relaciona os usos permitidos para os certificados emitidos]

1.4.2 Aplicações proibidas para os certificados

[Insira aqui o texto que relaciona os usos proibidos para os certificados emitidos]

1.5 Dados para Contato

1.5.1 Entidade responsável por este documento

[Insira aqui dados que identifiquem a entidade responsável pela elaboração e manutenção do documento]

O endereço postal para contato da [Insira aqui o nome da AC] é:

[Insira aqui o nome da AC],
[Insira o endereço postal completo da AC]

E-mail: [Insira o email de contato da AC aqui]
Website: [Insira aqui a url do website]

1.5.2 Ponto de Contato

A pessoa de contato para questões relacionadas a este documento é [Insira o nome do responsável aqui] e seus dados para contato são:

[Insira aqui o nome da AC],
[Insira o endereço postal completo do responsável]
Telefone: [Insira o telefone para contato aqui]

1.5.3 Procedimentos de aprovação da PC

[Insira o texto aqui]

1.6 Definições e Acrônimos

[Insira o texto aqui]

2. Responsabilidades referentes a publicações e repositórios

2.1 Repositórios

[Insira o texto aqui]

2.2 Publicação de informações

[Insira o texto aqui]

2.3 Freqüência de publicação

[Insira o texto aqui]

2.4 Controles de acesso aos repositórios

[Insira o texto aqui]

3. Identificação e Autenticação

3.1 Estrutura de Nomes

3.1.1 Tipos de nomes

[Insira o texto aqui]

3.1.2 Necessidade de que nomes sejam significativos

[Insira o texto aqui]

3.1.3 Anonimato dos titulares de certificado

[Insira o texto aqui]

3.1.4 Regras para interpretação dos diversos formatos de nomes

[Insira o texto aqui]

3.1.5 Unicidade dos nomes

[Insira o texto aqui]

3.1.6 Reconhecimento, autenticação e papel de marcas registradas

[Insira o texto aqui]

3.2 Validação da Identidade Inicial

3.2.1 Método para prova de posse da chave privada

[Insira o texto aqui]

3.2.2 Autenticação da identidade organizacional

[Insira o texto aqui]

3.2.3 Autenticação da identidade individual

[Insira o texto aqui]

3.2.4 Dados dos titulares de certificado que não são verificados

[Insira o texto aqui]

3.2.5 Validação de autoridade

[Insira o texto aqui]

3.2.6 Critérios para interoperabilidade

[Insira o texto aqui]

3.3 Identificação e Autenticação para Requisição de Substituição de Chaves

3.3.1 Identificação e autenticação para troca de chaves de rotina

[Insira o texto aqui]

3.3.2 Identificação e autenticação para troca de chaves após revogação

[Insira o texto aqui]

3.4 Identificação e Autenticação para Requisição de Revogação

[Insira o texto aqui]

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

[Insira o texto aqui]

4.1.2 Processo de solicitação e responsabilidades

[Insira o texto aqui]

4.2 Processamento da solicitação pela AR

4.2.1 Realização das funções de identificação e autenticação

[Insira o texto aqui]

4.2.2 Aprovação ou rejeição das solicitações

[Insira o texto aqui]

4.2.3 Tempo para processamento das solicitações

[Insira o texto aqui]

4.3 Processamento da solicitação pela AC

4.3.1 Ações da AC durante a emissão de certificado

[Insira o texto aqui]

4.3.2 Notificação da emissão do certificado pela AC para o solicitante

[Insira o texto aqui]

4.4 Aceitação do certificado

4.4.1 Conduta que constitui a aceitação do certificado

[Insira o texto aqui]

4.4.2 Publicação do certificado pela AC

[Insira o texto aqui]

4.4.3 Notificação da emissão do certificado pela AC para outras entidades

[Insira o texto aqui]

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

[Insira o texto aqui]

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

[Insira o texto aqui]

4.6 Reemissão de certificados por troca do prazo de validade

4.6.1 Circunstância para renovação de certificados

[Insira o texto aqui]

4.6.2 Quem pode solicitar renovação

[Insira o texto aqui]

4.6.3 Processamento de solicitações de renovação

[Insira o texto aqui]

4.6.4 Notificação de nova emissão de certificado para o titular

[Insira o texto aqui]

4.6.5 Conduta que constitui aceitação de um certificado renovado

[Insira o texto aqui]

4.6.6 Publicação do certificado renovado pela AC

[Insira o texto aqui]

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

[Insira o texto aqui]

4.7 Reemissão de certificados por troca de chaves

4.7.1 Circunstâncias para substituição das chaves criptográficas

[Insira o texto aqui]

4.7.2 Quem pode solicitar a certificação de uma nova chave pública

[Insira o texto aqui]

4.7.3 Processamento de solicitações de substituição de certificados

[Insira o texto aqui]

4.7.4 Notificação de nova emissão de certificado para o titular

[Insira o texto aqui]

4.7.5 Conduta para a aceitação de um novo certificado

[Insira o texto aqui]

4.7.6 Publicação do novo certificado

[Insira o texto aqui]

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

[Insira o texto aqui]

4.8 Reemissão de certificados por troca de dados

4.8.1 Circunstâncias para modificação de certificados

[Insira o texto aqui]

4.8.2 Quem pode solicitar a modificação de um certificado

[Insira o texto aqui]

4.8.3 Processamento de solicitações de modificação de certificados

[Insira o texto aqui]

4.8.4 Notificação de nova emissão de certificado para o titular

[Insira o texto aqui]

4.8.5 Conduta para a aceitação de um novo certificado modificado

[Insira o texto aqui]

4.8.6 Publicação do certificado pela AC

[Insira o texto aqui]

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

[Insira o texto aqui]

4.9 Revogação e Suspensão

4.9.1 Circunstâncias para revogação de certificados

[Insira o texto aqui]

4.9.2 Quem pode solicitar revogação

[Insira o texto aqui]

4.9.3 Processamento de solicitações de revogação

[Insira o texto aqui]

4.9.4 Prazo para solicitação de revogação

[Insira o texto aqui]

4.9.5 Prazo para a AC processar a solicitação de revogação

[Insira o texto aqui]

4.9.6 Requisitos para verificação de revogação por entidades confiantes

[Insira o texto aqui]

4.9.7 Freqüência de emissão de LCRs

[Insira o texto aqui]

4.9.8 Latência máxima para LCRs

[Insira o texto aqui]

4.9.9 Mecanismos para verificação on-line do status de certificados

[Insira o texto aqui]

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

[Insira o texto aqui]

4.9.11 Outras formas de comunicação de revogação

[Insira o texto aqui]

4.9.12 Procedimentos adicionais no caso de comprometimento da chave privada

[Insira o texto aqui]

4.9.13 Circunstâncias para suspensão de certificados

[Insira o texto aqui]

4.9.14 Quem pode solicitar suspensão

[Insira o texto aqui]

4.9.15 Processamento de solicitações de suspensão

[Insira o texto aqui]

4.9.16 Limites para o período de suspensão

[Insira o texto aqui]

4.10 Serviços de status de certificado

4.10.1 Características operacionais

[Insira o texto aqui]

4.10.2 Disponibilidade do serviço

[Insira o texto aqui]

4.10.3 Características operacionais

[Insira o texto aqui]

4.11 Encerramento do vínculo com a AC

[Insira o texto aqui]

4.12 Custódia e recuperação de chaves

4.12.1 Políticas e práticas para custódia e recuperação de chaves

[Insira o texto aqui]

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

[Insira o texto aqui]

5. Controles operacionais, gerenciais e de instalações físicas

5.1 Controles de Segurança Física

5.1.1 Localização e construção das instalações físicas

[Insira o texto aqui]

5.1.2 Acesso físico

[Insira o texto aqui]

5.1.3 Energia e refrigeração

[Insira o texto aqui]

5.1.4 Exposição à água

[Insira o texto aqui]

5.1.5 Prevenção e proteção contra incêndio

[Insira o texto aqui]

5.1.6 Armazenamento de mídia

[Insira o texto aqui]

5.1.7 Descarte de lixo

[Insira o texto aqui]

5.1.8 Cópias de segurança em outras instalações

[Insira o texto aqui]

5.2 Procedimentos de Controle

5.2.1 Papéis de Confiança

[Insira o texto aqui]

5.2.2 Número de pessoas necessárias por tarefa

[Insira o texto aqui]

5.2.3 Identificação e autenticação para cada papel

[Insira o texto aqui]

5.2.4 Papéis que requerem separação de responsabilidade

[Insira o texto aqui]

5.3 Controle de Pessoal

5.3.1 Requisitos de qualificação, experiência e conformidade com obrigações governamentais

[Insira o texto aqui]

5.3.2 Procedimentos de verificação de antecedentes

[Insira o texto aqui]

5.3.3 Requisitos de treinamento

[Insira o texto aqui]

5.3.4 Requisitos de freqüência de treinamento

[Insira o texto aqui]

5.3.5 Freqüência e seqüência para revezamento de trabalho

[Insira o texto aqui]

5.3.6 Sanções para ações não autorizadas

[Insira o texto aqui]

5.3.7 Requisitos para prestadores de serviços independentes

[Insira o texto aqui]

5.3.8 Documentação fornecida aos funcionários

[Insira o texto aqui]

5.4 Sistemas de auditoria e procedimentos para registro de eventos

5.4.1 Tipos de eventos registrados

[Insira o texto aqui]

5.4.2 Freqüência de análise dos registros de auditoria

[Insira o texto aqui]

5.4.3 Período de arquivamento de registros de auditoria

[Insira o texto aqui]

5.4.4 Proteção de registros de eventos

[Insira o texto aqui]

5.4.5 Procedimentos para cópias de segurança de registros de eventos

[Insira o texto aqui]

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

[Insira o texto aqui]

5.4.7 Notificação do sujeito causador do evento

[Insira o texto aqui]

5.4.8 Avaliação de vulnerabilidades

[Insira o texto aqui]

5.5 Arquivamento de Registros

5.5.1 Tipos de registros armazenados

[Insira o texto aqui]

5.5.2 Período de retenção dos registros arquivados

[Insira o texto aqui]

5.5.3 Proteção dos registros armazenados

[Insira o texto aqui]

5.5.4 Procedimentos para cópias dos registros armazenados

[Insira o texto aqui]

5.5.5 Requisitos para datação dos registros armazenados

[Insira o texto aqui]

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

[Insira o texto aqui]

5.5.7 Procedimentos para obtenção e verificação dos registros armazenados

[Insira o texto aqui]

5.6 Nova Chave Pública para a AC

[Insira o texto aqui]

5.7 Comprometimento e Recuperação de Desastre

5.7.1 Procedimentos para tratamento de incidentes e comprometimentos

[Insira o texto aqui]

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

[Insira o texto aqui]

5.7.3 Procedimentos para o comprometimento de chave privada de entidade

[Insira o texto aqui]

5.7.4 Procedimentos para continuidade de negócio após desastre

[Insira o texto aqui]

5.8 Finalização da AC ou AR

[Insira o texto aqui]

6. Controles Técnicos de Segurança

6.1 Geração e Instalação do Par de Chaves

6.1.1 Geração do par de chaves

[Insira o texto aqui]

6.1.2 Fornecimento de chave privada ao titular

[Insira o texto aqui]

6.1.3 Entrega da chave pública à Autoridade Certificadora

[Insira o texto aqui]

6.1.4 Divulgação da chave pública da AC às partes confiantes

[Insira o texto aqui]

6.1.5 Tamanho das chaves

[Insira o texto aqui]

6.1.6 Geração dos parâmetros de chave pública e verificação de qualidade

[Insira o texto aqui]

6.1.7 Propósito de uso de chaves

[Insira o texto aqui]

6.2 Proteção de Chaves Privadas e Controles Tecnológicos de módulos Criptográficos

6.2.1 Padrões e controles de módulos criptográficos

[Insira o texto aqui]

6.2.2 Número de operadores para o Controle da Chave Privada

[Insira o texto aqui]

6.2.3 Custódia de chaves privadas

[Insira o texto aqui]

6.2.4 Cópias de segurança de chaves privadas

[Insira o texto aqui]

6.2.5 Arquivamento de chaves privadas

[Insira o texto aqui]

6.2.6 Transferência de chaves privadas de/para módulos criptográficos

[Insira o texto aqui]

6.2.7 Armazenamento de chaves privadas em módulos criptográficos

[Insira o texto aqui]

6.2.8 Método para ativação de chaves privadas

[Insira o texto aqui]

6.2.9 Método para desativação de chaves privadas

[Insira o texto aqui]

6.2.10 Método para destruição de chaves privadas

[Insira o texto aqui]

6.2.11 Avaliação requerida de módulos criptográficos

[Insira o texto aqui]

6.3 Outros Aspectos do Gerenciamento de Chaves

6.3.1 Armazenamento de chaves públicas

[Insira o texto aqui]

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

[Insira o texto aqui]

6.4 Dados de Ativação

6.4.1 Geração e instalação dos dados de ativação

[Insira o texto aqui]

6.4.2 Proteção dos dados de ativação

[Insira o texto aqui]

6.4.3 Outros aspectos de dados de ativação

[Insira o texto aqui]

6.5 Controles de Segurança computacional

6.5.1 Requisitos técnicos específicos de segurança computacional

[Insira o texto aqui]

6.5.2 Classificação de segurança computacional

[Insira o texto aqui]

6.6 Controles técnicos de ciclo de vida

6.6.1 Controles de desenvolvimento de sistemas

[Insira o texto aqui]

6.6.2 Controles do gerenciamento de segurança

[Insira o texto aqui]

6.6.3 Controles de segurança de ciclo de vida

[Insira o texto aqui]

6.7 Controles para a Segurança da Rede de Comunicações

[Insira o texto aqui]

6.8 Carimbo do Tempo

[Insira o texto aqui]

7. Perfis dos Certificados, LCR e OCSP

7.1 Perfil dos Certificados

7.1.1 Versão

[Insira o texto aqui]

7.1.2 Extensões

[Insira o texto aqui]

7.1.3 Identificadores de objeto dos algoritmos

[Insira o texto aqui]

7.1.4 Formato dos nomes

[Insira o texto aqui]

7.1.5 Restrições para nomes

[Insira o texto aqui]

7.1.6 Identificador de objeto da PC

[Insira o texto aqui]

7.1.7 Uso da extensão *Policy Constraints*

[Insira o texto aqui]

7.1.8 Sintaxe e semântica dos qualificadores de política

[Insira o texto aqui]

7.1.9 Semântica de Processamento para a extensão crítica Certificate Policies

[Insira o texto aqui]

7.2 Perfil da LCR

[Insira o texto aqui]

7.2.1 Versão

[Insira o texto aqui]

7.2.2 Extensões da LCR e de entradas da LCR

[Insira o texto aqui]

7.3 Perfil da OCSP

7.3.1 Versão

[Insira o texto aqui]

7.3.2 Extensões OCSP

[Insira o texto aqui]

8. Auditoria de conformidade e outras avaliações

8.1 Freqüência ou circunstâncias das avaliações

[Insira o texto aqui]

8.2 Identidade e qualificações do avaliador

[Insira o texto aqui]

8.3 Relação entre o avaliador e a entidade avaliada

[Insira o texto aqui]

8.4 Tópicos cobertos na avaliação

[Insira o texto aqui]

8.5 Ações tomadas resultantes de deficiências

[Insira o texto aqui]

8.6 Comunicação dos resultados

[Insira o texto aqui]

.

9. Aspectos Legais e Assuntos Gerais

9.1 Taxas

9.1.1 Taxas de emissão e renovação de certificados

[Insira o texto aqui]

9.1.2 Taxas para acesso aos certificados

[Insira o texto aqui]

9.1.3 Taxas revogação ou informações de estado

[Insira o texto aqui]

9.1.4 Outras taxas

[Insira o texto aqui]

9.1.5 Política de reembolso

[Insira o texto aqui]

9.2 Responsabilidade Financeira

[Insira o texto aqui]

9.2.1 Cobertura de Seguro

[Insira o texto aqui]

9.2.2 Outros ativos

[Insira o texto aqui]

9.2.3 Cobertura de Seguro ou garantia para entidades finais

[Insira o texto aqui]

9.3 Informações confidenciais

9.3.1 Escopo de informações confidenciais

[Insira o texto aqui]

9.3.2 Informações fora do escopo de informações confidenciais

[Insira o texto aqui]

9.3.3 Responsabilidade de proteção de informações confidenciais

[Insira o texto aqui]

9.4 Privacidade das Informações Pessoais

9.4.1 Plano de Privacidade

[Insira o texto aqui]

9.4.2 Informação tratada como privada

[Insira o texto aqui]

9.4.3 Informação não considerada privada

[Insira o texto aqui]

9.4.4 Responsabilidade de proteção de informação privada

[Insira o texto aqui]

9.4.5 Aviso e consentimento para o uso de informação privada

[Insira o texto aqui]

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

[Insira o texto aqui]

9.4.7 Outras Circunstâncias para revelação de informações

[Insira o texto aqui]

9.5 Direitos de Propriedade Intelectual

[Insira o texto aqui]

9.6 Representações e Garantias

9.6.1 Garantias de AC

[Insira o texto aqui]

9.6.2 Garantias de AR

[Insira o texto aqui]

9.6.3 Garantias de titulares de certificado

[Insira o texto aqui]

9.6.4 Garantias de entidades confiantes

[Insira o texto aqui]

9.6.5 Garantias de outros participantes

[Insira o texto aqui]

9.7 Renúncia das Garantias

[Insira o texto aqui]

9.8 Limitações das Responsabilidades

[Insira o texto aqui]

9.9 Indenização

[Insira o texto aqui]

9.10 Finalização

9.10.1 Prazo de validade

[Insira o texto aqui]

9.10.2 Finalização

[Insira o texto aqui]

9.10.3 Efeitos de finalização e provisões remanescentes

[Insira o texto aqui]

9.11 Notificações Individuais e Comunicações com Participantes

[Insira o texto aqui]

9.12 Emendas

9.12.1 Procedimento para emendas

[Insira o texto aqui]

9.12.2 Período e mecanismo de notificação

[Insira o texto aqui]

9.12.3 Circunstâncias nas quais o identificador de objeto deve ser modificado

[Insira o texto aqui]

9.13 Procedimentos para Resolução de Disputas

[Insira o texto aqui]

9.14 Leis Governamentais

[Insira o texto aqui]

9.15 Conformidade com as leis aplicáveis

[Insira o texto aqui]

9.16 Provisões Diversas

9.16.1 Concordância completa

[Insira o texto aqui]

9.16.2 Delegação de direitos e obrigações

[Insira o texto aqui]

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

[Insira o texto aqui]

9.16.4 Responsabilidades relacionadas a encargos jurídicos

[Insira o texto aqui]

9.16.5 Força maior

[Insira o texto aqui]

9.15 Outras Provisões

[Insira o texto aqui]

10. Controle de Mudanças

Seção	**Mudança**	**Autor**	**Data**
[Insira a seção alterada aqui]	[Insira a mudança aqui]	[Autor]	01/01/01
[Insira a seção alterada aqui]	[Insira a mudança aqui]	[Autor]	01/01/01
[Insira a seção alterada aqui]	[Insira a mudança aqui]	[Autor]	01/01/01

APÊNDICE C – Critérios para Avaliação de PC/DPC

Este apêndice apresenta os critérios fornecidos aos revisores da Autoridade de Gerência de Políticas (AGP), da Infraestrutura de Chaves Públicas para Ensino e Pesquisa (ICPEDU). As perguntas formuladas possibilitam a avaliação de PC/DPC das Autoridades Certificadoras (AC) candidatas à fazer parte da ICP.

Seção	Critérios de Avaliação
1. Introdução	
1.1 Visão Geral	• O texto menciona a ICPEDU? • O texto menciona a conformidade com os requisitos mínimos e a RFC 3647? • O texto menciona brevemente a finalidade dos certificados e para quem se destinam?
1.2 Nome do Documento de Identificação	• O título define objetivamente o documento a que se refere? • O texto apresenta a versão atual do documento? • O documento possui um OID? Ele está correto?
1.3 Participantes da ICP	
1.3.1 Autoridades Certificadoras	• Quem é a AC? • Existem ACs subordinadas a esta AC? Quem são elas?
1.3.2 Autoridades de Registro	• A AC não assume papel de AR? • Uma AR principal é indicada?
1.3.3 Titulares de Certificados	• É possível reconhecer a quem os certificados se destinam?
1.3.4 Entidades Confiantes	• É possível reconhecer quem pode confiar nos certificados?
1.3.5 Outros Participantes	N/A
1.4 Uso do Certificado	
1.4.1 Aplicações apropriadas para os certificados	• O documento apresenta as restrições estipuladas pelos requisitos mínimos? • Qual o uso permitido dos certificados de entidade final?
1.4.2 Aplicações Proibidas para os certificados	• É possível reconhecer os para que atividades o uso dos certificados não é permitido?
1.5 Dados de Contato	
1.5.1 Entidade responsável pelo documento	• A entidade é identificada claramente? • Os dados para contato estão disponíveis?

Seção	Critérios de Avaliação
1.5.2 Ponto de Contato	• O PoC é identificado claramente? • Os dados para contato estão disponíveis?
1.5.3 Procedimentos de Aprovação da PC	• O texto requerido está presente? • Outros procedimentos de aprovação estão claramente identificados?
1.6 Definições e Acrônimos	N/A
2. Responsabilidades Referentes à Publicação de Repositórios	
2.1 Repositórios	• A AC disponibiliza um repositório público?
2.2 Publicação de Informações	• A AC disponibiliza seu certificado no repositório público? • A AC disponibiliza todos os certificados emitidos no repositório público? • A AC disponibiliza sua LCR no repositório público? • A AC disponibiliza todas as versões das PCs e DPCs aprovadas?
2.3 Freqüência de publicação	• O repositório é atualizado sempre que houver modificações nas informações citadas anteriormente?
2.4 Controles de acesso aos repositórios	N/A
3. Identificação e Autenticação	
3.1 Estrutura de Nomes	
3.1.1 Tipos de nomes	• O DN apresenta formato apropriado?
3.1.2 Necessidade de que nomes sejam significativos	• Os campos especificados expressam uma associação razoável com o nome real ou organização do titular do certificado? • Caracteres especiais são proibidos no DN?
3.1.3 Anonimato dos titulares de Certificado	• O anonimato de titular de certificado não é permitido?
3.1.4 Regras para interpretação dos diversos formatos de nomes	• É possível identificar a parte fixa e a parte variável do DN dos certificados emitidos?
3.1.5 Unicidade dos nomes	• A PC/DPC determina que o nome nos certificados seja único?

Seção	Critérios de Avaliação
3.1.6 Reconhecimento, autenticação e papel de marcas registradas	N/A
3.2 Validação da Identidade Inicial	
3.2.1 Método para a prova de posse da chave privada	• A AC descreve o método utilizado para comprovar a posse da chave privada claramente?
3.2.2 Autenticação da identidade organizacional	• O método utilizado pela AC é suficiente para identificar o solicitante como um membro da instituição?
3.2.3 Autenticação da identidade individual	• O documento solicitado possui validade legal? • O documento solicitado possui foto? • A AC registra os documentos encaminhados?
3.2.4 Dados dos Titulares de certificado que não são verificados	• Os dados que não são verificados são críticos para a utilização dos certificados ou para identificar o solicitante?
3.2.5 Validação de Autoridade	• O método apresentado para garantir que o solicitante possa agir em nome de outros, ou da AC, é válido?
3.2.6 Critérios para interoperabilidade	N/A
3.3 Identificação e Autenticação para Requisição de Substituição de Chaves	
3.3.1 Identificação e Autenticação para troca de chaves de rotina	• A AC utiliza um método de identificação que permita validar corretamente a identidade do solicitante?
3.3.2 Identificação e Autenticação para troca de chaves de rotina	• A AC exige os mesmos métodos de identificação e autenticação de solicitação de um novo certificado?
3.4 Identificação e Autenticação para requisição de revogação	• O responsável pela solicitação de revogação possui autoridade para fazê-lo? • A AC registra corretamente essa atividade?

Seção	Critérios de Avaliação
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	• O texto identifica quem pode solicitar os certificados? • Há restrições impostas? Elas estão claramente dispostas? • O texto identifica quem é responsável por autorizar as solicitações
4.1.2 Processo de solicitação e Responsabilidades	• É possível identificar claramente o processo de solicitação? • É possível identificar quem é responsável por receber a solicitação?
4.2 Processamento da solicitação pela AR	
4.2.1 Realização das funções de identificação e autenticação	• É possível identificar claramente que procedimentos são utilizados?
Seção	Critérios de Avaliação
4.2.2 Aprovação ou rejeição das solicitações	• A AC registra a aprovação e rejeição dos pedidos? • Os procedimentos para aprovação e rejeição de solicitações estão descritos?
4.2.3 Tempo para processamento das solicitações	N/A
4.3 Processamento da solicitação pela AC	
4.3.1 Ações da AC durante a solicitação	• A AC processa apenas pedidos aprovados pela AR?
4.3.2 Notificação da emissão do certificado pela AC para o solicitante	N/A
4.4 Aceitação do certificado	
4.4.1 Conduta que constitui a aceitação do certificado	N/A
4.4.2 Publicação do Certificado pela AC	• A AC publica os certificados logo que emitidos?
4.4.3 Notificação da emissão do certificado pela AC para outras entidades	N/A

Seção	Critérios de Avaliação
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	• A AC define como sendo do usuário a responsabilidade pela manutenção da chave privada e dos certificados? • A AC veta o uso de seu certificado senão para aquele exposto na PC/DPC?
4.5.2 Responsabilidade pela utilização das chaves privadas e dos certificados por parte das entidades confiantes	• É possível identificar claramente as responsabilidades da entidade confiante? Elas seguem os requisitos mínimos?
Seção	Critérios de Avaliação
4.6 Reeminssão de certificados por troca do prazo de validade	
4.6.1 Circunstância para renovação de certificados	• A AC permite renovação de certificados? • As renovações respeitam as restrições dos requisitos mínimos? • Um limite de renovações para o mesmo par de chaves é estabelecido? • As renovações de certificados expirados são proibidas?
4.6.2 Quem pode solicitar renovação	• Só é permitida a renovação pelo responsável pelo certificado?
4.6.3 Processamento de solicitações de renovação	N/A
4.6.4 Notificação de nova emissão de certificado para o titular	N/A
4.6.5 Conduta que constitui aceitação de um certificado renovado	N/A
4.6.6 Publicação do certificado renovado pela AC	N/A
4.6.7 Notificação pela AC da emissão de um certificado para outras entidades	N/A
4.7 Reeminssão de certificados por troca de chaves	
4.7.1 Circunstâncias para substituição das chaves criptográficas	• A substituição de chaves de certificados expirados é proibida?

Seção	Critérios de Avaliação
4.7.2 Quem pode solicitar a certificação de uma nova chave pública	• Só é permitida a certificação de uma chave pública pelo responsável pelo certificado?
4.7.3 Processamento de solicitações de substituição de certificados	N/A
4.7.4 Notificação de nova emissão de certificado para o titular	N/A
4.7.5 Conduta para a aceitação de um novo certificado	N/A
4.7.6 Publicação do novo certificado	• A AC publica os certificados renovados no repositório?
4.7.7 Notificação pela AC da emissão de um certificado para outras entidades	N/A
4.8 Reeminssão de certificados por troca de dados	
Não é permitida a modificação de dados dos certificados. Qualquer estipulação diferente é considerada uma não conformidade.	
4.9 Revogação e Suspensão	
4.9.1 Circunstâncias para revogação de certificados	• A PC/DPC determinar que os certificados devem ser revogados na ocorrência dos eventos listados?
4.9.2 Quem pode solicitar revogação	• A PC/DPC determinar que uma revogação pode ser solicitada pelas entidades listadas?
4.9.3 Processamento de solicitações de revogação	• Como a AC ou AR identifica o responsável pela solicitação? • Que ações são tomadas a seguir?
4.9.4 Prazo para solicitação de revogação	N/A
4.9.5 Prazo para a AC processar a solicitação de revogação	• A AC processa as revogações dentro do prazo definido?
4.9.6 Requisitos para verificação de revogação por entidades confiantes	• A LCR é utilizada para verificar se um certificado é válido?
4.9.7 Freqüência de emissão de LCRs	• Qual a freqüência de emissão da LCR?
4.9.8 Latência máxima para LCRs	• Qual o intervalo de tempo entre a emissão e publicação da LCR?
4.9.9 Mecanismos para verificação on-line do status de certificados	N/A

Seção	Critérios de Avaliação
4.9.10 Obrigações da entidade confiante de verificar on-line o status de certificados	N/A
4.9.11 Outras formas de comunicação de revogação	N/A
4.9.12 Procedimentos adicionais no caso de comprometimento da chave privada	N/A
4.9.13 Circunstâncias para suspensão de certificados	• A AC suspende certificados?
4.9.14 Quem pode solicitar suspensão	N/A
4.9.15 Processamento de solicitações de suspensão	N/A
4.9.16 Limites para o período de suspensão	N/A
4.10 Serviços de status de certificado	
4.10.1 Características operacionais	N/A
4.10.2 Disponibilidade do serviço	N/A
4.10.3 Características operacionais	N/A
4.11 Encerramento do vínculo com a AC	• Quando e como o vínculo do titular com a AC é encerrado?
4.12 Custódia e recuperação de chaves	
4.12.1 Políticas e práticas para custódia e recuperação de chaves	N/A
4.12.2 Políticas e práticas para custódia e recuperação de chaves de sessão	N/A
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 declara estar em um ambiente controlado, conforme as especificações dos requisitos?
5.1.2 Acesso físico	• O acesso físico ao ambiente de operação da AC é controlado?
5.1.3 Energia e refrigeração	• O ambiente possui recursos que o mantenham nas condições de operação estipuladas?
5.1.4 Exposição à água	• O ambiente possui recursos que o mantenham nas condições de operação estipuladas?
5.1.5 Prevenção e proteção contra incêndio	• O ambiente possui recursos que o mantenham nas condições de operação estipuladas?
5.1.6 Armazenamento de mídia	• O local de armazenamento das mídias sensíveis atende aos requisitos?

Seção	Critérios de Avaliação
5.1.7 Descarte de lixo	• Mídia contendo informação sensível é destruída de forma apropriada antes de ser descartada?
5.1.8 Cópias de segurança em outras instalações	• Há um local externo para armazenamento das cópias de segurança? • O local possui os controles de segurança apropriados?
5.2 Procedimentos de Controle	
5.2.1 Papéis de Confiança	• O pessoal envolvido nas operações da AC é funcionário da instituição? • As atribuições estão claramente documentadas para cada papel?
5.2.2 Número de pessoas necessárias por tarefa	N/A
5.2.3 Identificação e autenticação para cada papel	• O pessoal envolvido nas operações da AC é identificado de forma única? • Os smartcards são utilizados?
5.2.4 Papéis que requerem separação de responsabilidade	• Operadores e Administradores não exercem papel de auditor?
5.3 Procedimentos de Controle	
5.3.1 Requisitos de qualificação, experiência e conformidade com obrigações governamentais	• O pessoal da AC é composto apenas por pessoal pertencente ao quadro de funcionários da instituição?
5.3.2 Procedimentos de verificação de antecedentes	• O pessoal da AC é composto apenas por pessoal pertencente ao quadro de funcionários da instituição?
5.3.3 Requisitos de treinamento	• Há uma política de treinamento? • O treinamento empregado está de acordo com as necessidades da ICP?
5.3.4 Requisitos de freqüência de treinamento	• A freqüência de treinamento atende aos requisitos apresentados?
5.3.5 Freqüência e seqüência para revezamento de trabalho	N/A

Seção	Critérios de Avaliação
5.3.6 Sanções para ações não autorizadas	• A PC/DPC prevê algum tipo de sanção para ações não autorizadas? • A legislação vigente e o regimento interno da instituição são considerados?
5.3.7 Requisitos para prestadores de serviços independentes	• A PC/DPC prevê a assinatura de um termo de responsabilidade por parte dos prestadores de serviço? • A PC/DPC prevê alguma cláusula contratual que obrigue o contratado a seguir a PS e PC/DPC?
5.3.8 Documentação fornecida aos funcionários	• Que documentos são fornecidos aos funcionários?
5.4 Sistemas de auditoria e procedimentos para registro de eventos	
5.4.1 Tipos de eventos registrados	• Os eventos listados nos requisitos mínimos são registrados?
5.4.2 Freqüência de análise dos registros de auditoria	N/A
5.4.3 Período de arquivamento de registros de auditoria	• Por quanto tempo os registros de auditoria são guardados?
5.4.4 Proteção de registros de eventos	• Os registros são mantidos em local seguro? • São aplicados controles de segurança para evitar o acesso não autorizado?
5.4.5 Procedimentos para cópias de segurança de registros de eventos	• Como as cópias de segurança são feitas? • Existem mecanismos para verificar sua integridade?
5.4.6 Sistema de recolhimento de registros de eventos (interno ou externo)	N/A
5.4.7 Notificação do sujeito causador do evento	N/A
5.4.8 Avaliação de vulnerabilidades	• Os registros de eventos são analisados com a freqüência recomendada? • Que medidas são tomadas para reportar e minimizar o risco associado aos problemas encontrados?

Seção	Critérios de Avaliação
5.5 Arquivamento de Registros	
5.5.1 Tipos de registros armazenados	• Os registros de eventos recolhidos são arquivados? • Que outros eventos são arquivados?
5.5.2 Período de retenção dos registros arquivados	• Por quanto tempo os registros são arquivados?
5.5.3 Proteção dos registros armazenados	• Os registros armazenados são acessíveis apenas aos auditores e administradores? • É armazenado em mídia não volátil? • Que tipos de controles são empregados para evitar mudanças não autorizadas?
5.5.4 Procedimentos para cópias dos registros armazenados	• Como as cópias de segurança são feitas? • Existem mecanismos para verificar sua integridade?
5.5.5 Requisitos para datação dos registros armazenados	• A datação dos registros é garantida? • Existem mecanismos formais para garantir a integridade da data e hora dos registros armazenados?
5.5.6 Sistema de recolhimento de registros arquivados (interno ou externo)	N/A
5.5.7 Procedimentos para obtenção e verificação dos registros armazenados	N/A
5.6 Nova Chave Pública para a AC	• Um novo par de chaves é gerado no prazo estipulado?
5.7 Comprometimento e Recuperação de Desastre	
5.7.1 Procedimentos para tratamento de incidentes e comprometimentos	• Existe uma política formal de resposta e tratamento de incidentes de segurança? • Esta política está devidamente documentada? • O CAIS é notificado?
5.7.2 Procedimentos para o caso de comprometimento de recursos computacionais, software e/ou dados	N/A
5.7.3 Procedimentos para o comprometimento de chave privada de entidade	N/A
5.7.4 Procedimentos para continuidade de negócio após desastre	• A AC possui um Plano de Continuidade de Negócio?

Seção	Critérios de Avaliação
5.8 Finalização da AC ou AR	• A AC notifica os participantes listados nos requisitos mínimos?
6. Controles Técnicos de Segurança	
6.1 Geração e instalação do par de chaves	
6.1.1 Geração do par de chaves	• O procedimento para geração do par de chaves está descrito? • Um HSM aprovado foi utilizado?
6.1.2 Fornecimento de chave privada ao titular	N/A
6.1.3 Entrega da chave pública à Autoridade Certificadora	• Que processo é utilizado para entrega da chave pública? • Ela é entregue pelo representada legal?
6.1.4 Divulgação da chave pública da AC às partes confiantes	• O certificado da AC é disponibilizado nos locais indicados?
6.1.5 Tamanho das chaves	• O tamanho da chave está de acordo com o estipulado no documento em questão?
6.1.6 Geração dos parâmetros de chave pública e verificação de qualidade	• As chaves são geradas de acordo com os Padrões e Algoritmos Criptográficos da ICPEDU?
6.1.7 Propósito de uso de chaves	• As chaves são utilizadas apenas para as atividades relacionadas?
6.2 Proteção de chaves privadas e controles tecnológicos de módulos criptográficos	
6.2.1 Padrões e controles de módulos criptográficos	• Um HSM aprovado pela ICPEDU é utilizado?
6.2.2 Número de operadores para o Controle da Chave Privada	• O número mínimo e máximo de operadores é descrito?
6.2.3 Custódia de chaves privadas	• A custódia da chave privada é vetada?
6.2.4 Cópias de segurança de chaves privadas	• É feita alguma cópia de segurança da chave privada? • Quem é responsável pela cópia e recuperação? • Onde a cópia é armazenada?
6.2.5 Arquivamento de chaves privadas	• Como são mantidas as cópias de segurança? • Existe algum controle de acesso associado?
6.2.6 Transferência de chaves privadas de/para módulos criptográficos	• Como é feita a transferência chave privada? • Quem é responsável pela ação? • Ela permanece cifrada?

Seção	Critérios de Avaliação
6.2.7 Armazenamento de chaves privadas em módulos criptográficos	• De que forma a chave privada é armazenada?
6.2.8 Método para ativação de chaves privadas	• É possível identificar que ações são tomadas para ativação da chave privada? • Quem é responsável pela ativação da chave privada? • Por quanto tempo a chave fica ativa?
6.2.9 Método para desativação de chaves privadas	• É possível identificar que ações são tomadas para desativar a chave privada? • Quem é responsável por desativar a chave privada?
6.2.10 Método para destruição de chaves privadas	• Que métodos são utilizados para destruir a chave privada? • Quem é responsável por destruir a chave privada?
6.2.11 Avaliação requerida de módulos criptográficos	• Um HSM aprovado pela ICPEDU é utilizado?
6.3 Outros aspectos do gerenciamento de chaves	
6.3.1 Armazenamento de chaves públicas	• Como a chave pública da AC está armazenada?
6.3.2 Períodos operacionais de certificados e períodos de utilização de pares de chaves	• Qual o período útil do certificado? • Por quanto tempo o par de chaves pode der utilizado?
6.4 Dados de Ativação	
6.4.1 Geração e instalação dos dados de ativação	• Como são gerados os dados de ativação?
6.4.2 Proteção dos dados de ativação	• Como os dados de ativação são verificados e onde são armazenados?
6.4.3 Outros aspectos de dados de ativação	N/A
6.5 Controles de segurança computacional	
6.5.1 Requisitos técnicos específicos de segurança computacional	• A AC apresenta controles de segurança de acordo com a PS da ICPEDU?
6.5.2 Classificação de segurança computacional	N/A
6.6 Controles técnicos de ciclo de vida	
6.6.1 Controles de desenvolvimento de sistemas	• O software utilizado pela AC possui controles apropriados para garantir atualizações de segurança em tempo razoável?

Seção	Critérios de Avaliação
6.6.2 Controles do gerenciamento de segurança	• A AC utiliza algum processo de gerenciamento de segurança? • Este processo engloba as determinações da PS da ICPEDU?
6.6.3 Controles de segurança de ciclo de vida	N/A
6.7 Controles para a Segurança da Rede de Comunicações	• A rede do ambiente que hospeda a AC é controlada? • A rede está em conformidade com a PS da ICPEDU? • A rede segue alguma metodologia específica para seu gerenciamento?
6.8 Carimbo do Tempo	• Os equipamentos online utilizam um servidor NTP confiável? • Os equipamentos offline são ajustados a cada inicialização?
7. Perfis de Certificados, LCR e OCSP	
7.1 Perfis dos Certificados	
7.1.1 Versão	• A AC emitirá certificados X.509 v. 3? • Os certificados estão de acordo com o perfil estabelecido na RFC 3280?
7.1.2 Extensões	• O certificado da AC segue as especificações dos requisitos mínimos? • Os valores dos definidos em cada campo estão corretos?
7.1.3 Identificadores de objeto dos algoritmos	• É possível localizar os OIDs dos algoritmos criptográficos?
7.1.4 Formato dos nomes	• Os formatos de nome seguem as definições dos requisitos mínimos?
7.1.5 Restrições para nomes	• As restrições de nomes são seguidas?
7.1.6 Identificador de objeto da PC	• O OID apresentado é válido?
7.1.7 Uso da extensão *Policy Constraints*	N/A
7.1.8 Sintaxe e semântica dos qualificadores de política	N/A
7.1.9 Semântica de Processamento para a extensão crítica *Certificate Policies*	N/A

Seção	Critérios de Avaliação
7.2 Perfil da LCR	
7.2.1 Versão	• As LCRs emitidas são versão 2?
7.2.2 Extensões da LCR e de entradas da LCR	• A extensão *authorityKeyIdentifier* está definida com o hash da chave pública da AC? • A extensão *cRLNumber* está definida com um número seqüencial para cada LCR emitida?
7.3 Perfil da OSCP	
7.3.1 Versão	N/A
7.3.2 Extensões OCSP	N/A
8. Auditoria de Conformidade e Outras Avaliações	
8.1 Freqüência ou circunstâncias das avaliações	• A AC é avaliada pelo menos anualmente?
8.2 Identidade e qualificações do avaliador	• Quem é autorizado para fazer as avaliações da AC? • Que tipo de qualificação é exigida?
8.3 Relação entre o avaliador e a entidade avaliada	• Os avaliadores não fazem parte do grupo que administra ou opera a AC?
8.4 Tópicos cobertos na avaliação	• Os controles envolvendo o gerenciamento do ciclo de vida dos certificados são avaliados? • A conformidade com a PS, Requisitos Mínimos e com a DPC da AC Raiz é avaliado?
8.5 Ações tomadas resultantes de deficiências	• As avaliações são formalmente comunicadas ao gerente da AC? • Um plano de ação é desenvolvido para sanar as deficiências?
8.6 Comunicação dos resultados	• As deficiências são comunicadas ao CG junto com as medidas tomadas?
Seção	Critérios de Avaliação
9. Aspectos legais e Assuntos Gerais	
9.1 Taxas	
Nenhum critério é adotado nesta seção, pois não há estipulações.	
9.2 Responsabilidade Financeira	
9.2.1 Cobertura de Seguro	N/A
9.2.2 Outros ativos	N/A
9.2.3 Cobertura de Seguro ou garantia para entidades finais	N/A

Seção	Critérios de Avaliação
9.3 Informações Confidenciais	
9.3.1 Escopo de informações confidenciais	• As informações listadas são consideradas confidenciais?
9.3.2 Informações fora do escopo de informações confidenciais	• As informações listadas são públicas?
9.3.3 Responsabilidade de proteção de informações confidenciais	• As informações consideradas não confidenciais são protegidas contra acesso não autorizado?
9.4 Privacidade das Informações Pessoais	
9.4.1 Plano de Privacidade	N/A
9.4.2 Informação tratada como privada	• As informações de identificação do titular são tratadas como privadas?
9.4.3 Informação não considerada privada	• As informações que identificam o titular são tratadas como privadas?
9.4.4 Responsabilidade de proteção de informação privada	• AC se responsabiliza pelas informações consideradas privadas?
9.4.5 Aviso e consentimento para o uso de informação privada	• A AC prevê a utilização de um termo de divulgação de informação considerada privada?
9.4.6 Circunstâncias para revelação de informações confidenciais em processos judiciais e administrativos	N/A
9.4.7 Outras Circunstâncias para revelação de informações	N/A
9.5 Direitos de Propriedade Intelectual	N/A
9.6 Representações e Garantias	
Nenhum critério é adotado nesta seção, pois não há estipulações.	
9.7 Renúncia das Garantias	N/A
9.8 Limitações das Responsabilidades	N/A
9.9 Indenização	N/A
9.10 Finalização	
9.10.1 Prazo de validade	• O prazo da PC/DPC está estipulado corretamente?
9.10.2 Finalização	• Que motivos determinam o fim da aplicabilidade das provisões?
9.10.3 Efeitos de finalização e provisões remanescentes	N/A
9.11 Notificações Individuais e Comunicações com Participantes	N/A

Seção	Critérios de Avaliação
9.12 Informações Confidenciais	
9.12.1 Procedimento para emendas	• Emendas na PC e na DPC são encaminhadas para aprovação do CG?
9.12.2 Período e mecanismo de notificação	• As PCs e DPCs são publicadas no repositório da AC assim que aprovadas?
9.12.3 Circunstâncias nas quais o identificador de objeto deve ser modificado	• Um novo OID é dado a cada nova versão do documento?
9.13 Procedimentos para Resolução de Disputas	N/A
9.14 Leis Governamentais	• A AC se compromete a seguir a legislação vigente no país?
9.15 Conformidade com as leis aplicáveis	N/A
9.16 Provisões Diversas	
Nenhum critério é adotado nesta seção, pois não há estipulações.	
9.17 Outras Provisões	N/A