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).

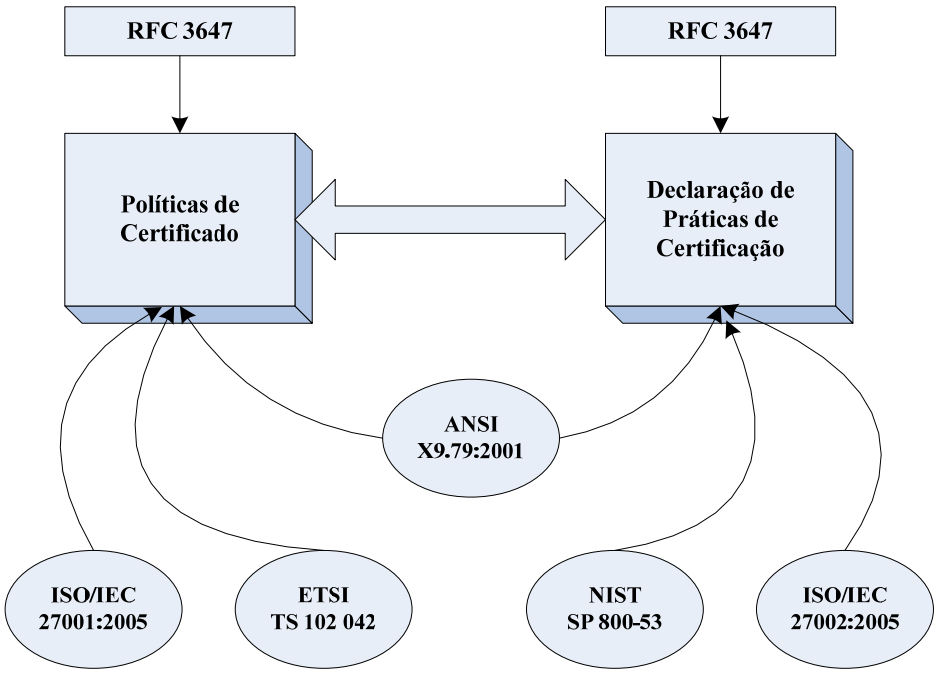

Figura 1. Relacionamento entre as referências e os documentos de PC e DPC

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.

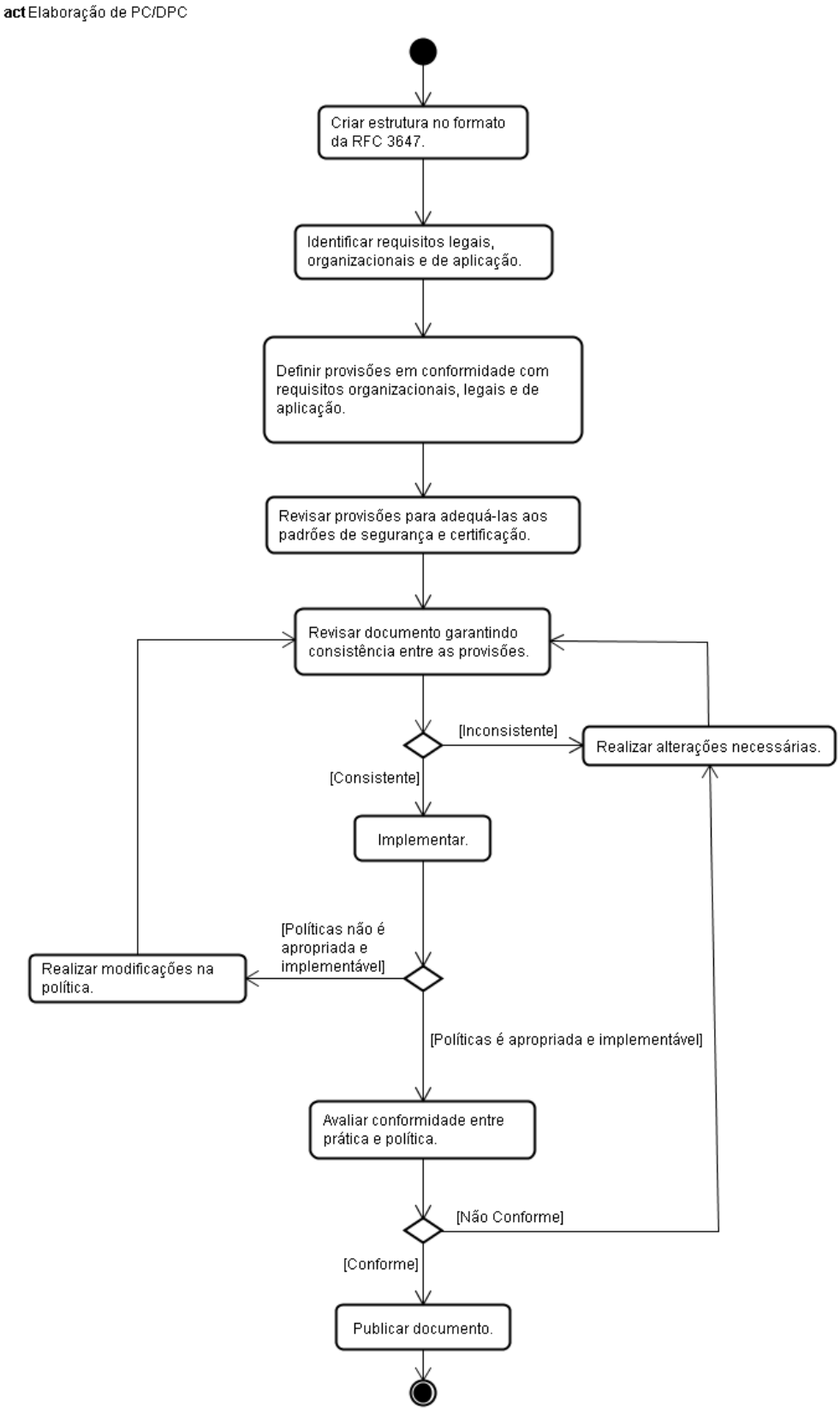

Figura 2. Passos para a elaboração de documentos de PC/DPC

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