Declaração de Práticas de Certificação - DPC[1]

AC e-notariado

Versão 4.0

2018/2020

[1] Publicação *ostensiva*.

Controle de Versões			
Versão	**Data**	**Autor**	**Notas da Revisão**
1.0	23/03/2018	Renato Martini	Versão inicial
2.2	08/05	Marcos de Paola	Ajustes conforme reunião em Brasília em 08/05
3.0/3.1	20/09	Renato Martini	Alterações para contemplar os requisitos presentes no ambiente de cloud
4.0	06/07/2020	Renato Martini	Revisão e atualização geral

Sumário

1. Introdução

1.1 Conceituação Geral

Este documento descreve as práticas e os procedimentos empregados pela AUTORIDADE CERTIFICADORA DO E-NOTARIADO – AC CNB em decorrência do Provimento nº 74, de 31 de julho de 2018 e do Provimento nº 100 de 26 de maio de 2020 do Conselho Nacional de Justiça, e aprovadas pelo Conselho Federal do Colégio Notarial do Brasil, na execução dos seus serviços de identificação e certificação digital, assim como pelas AUTORIDADES NOTARIAIS (AN) e por demais pessoas que participam da prestação de serviços de certificação.

1.2 Identificação

Esta comumente chamada DPC é a "Declaração de Práticas de Certificação da Autoridade Certificadora do e-notariado", seja da AC *CNB* quanto de sua(s) AC(s) subsequente(s). Ela receberá um OID (*object identifier*) para cumprir suas funções, segundo o padrão PENs (*Private Enterprise Numbers*) estabelecido pela IANA[2] (*Internet Assigned Number Authority*). A Política de Certificação - PC a ser operada pela AC no âmbito do e-notariado detalha as atribuições comuns de uma correntemente chamada Autoridade de Registro (AR) serão desempenhadas exclusivamente por tabeliães ou oficiais de registro civil vinculados à AC CNB, doravante denominados "Autoridades Notariais". Portanto, nesta DPC a designação de "Autoridade Notarial (AN)" apresenta-se como equivalente a um Prestador de serviços de certificação em todos os seus fins e atribuições numa infraestrutura de chaves públicas. Por conseguinte, as Autoridade Notariais serão responsáveis pelos processos de recebimento, validação e encaminhamento de solicitações de emissão ou de revogação de certificados digitais notarizados definidos pelo art. 2º, inc. II do Provimento nº 100 e de identificação de seus solicitantes.

Endereços:
Colégio Notarial do Brasil - Conselho Federal
Centro Empresarial Varig, Setor Comercial Norte
Quadra 4, Bloco B, Sala 1404
Asa Norte, Brasília/DF | CEP 70714-020

CNPJ
nº 05.334.890/0001-91

Responsabilidade técnica:
Marcos de Paola & Renato Martini

[2] IANA Private Enterprise Numbers: http://www.iana.org/assignments/enterprise-numbers.

1.3 Aplicabilidade da DPC

Esta DPC refere-se à estrutura de ACs constituídas no e-notariado.

1.4 Dados de Contato

O endereço da página web da AC CNB, do e-notariado, é https://www.e-notariado.org.br, onde serão devidamente publicados os dados a seguir, referentes às Autoridades Notariais, os tabeliães e oficiais responsáveis pelos processos de recebimento, validação e encaminhamento de solicitação de emissão ou de revogação dos certificados digitais emitidos, assim como a identificação de seus solicitantes:

1. relação de todas as AN credenciadas, com informações sobre uma ou mais Políticas de Certificação a ser implementada

2. para cada AN credenciada, os seus endereços físicos autorizados pela AC

3. opcional data e descritivo de um eventual descredenciamento de uma AN

1.5 Titularidade do Certificado e Cadeia de Certificação

Somente ACs subsequentes podem ser titulares de certificados emitidos pela AC CNB. Resguardando-se às ACs subsequentes a emissão de certificados para as entidades finais, pessoas físicas. É vedada às ACs subsequentes a criação de DPCs próprias.

2. Disposições Gerais

2.1 Obrigações, Direitos e Garantias

Nas obrigações abaixo detalhadas, descrevem-se as obrigações gerais da AC, suas ANs e entidades. Assim como os requisitos específicos associados a tais obrigações a serem implementadas.

a) Obrigações da AC:

1. operar de acordo com a DPC

2. gerar e gerenciar os seus pares de chaves criptográficas e assegurar a proteção de suas chaves privadas

3. notificar ao CNB-CF e aos titulares quando houver o comprometimento de quaisquer chaves privadas geradas no sistema de AC e determinar a imediata revogação de tal certificado

4. distribuir o seu próprio certificado

5. emitir, expedir e distribuir os certificados de Autoridades Notariais (AN) vinculadas e de usuários finais

6. informar a emissão do certificado ao respectivo solicitante

7. revogar os certificados por ela emitidos

8. emitir, gerenciar e publicar suas LCRs

9. publicar na página web (https://www.e-notariado.org.br/notary/repository) esta DPC

10. oferecer os dados para a fiscalização e correição das ANs vinculadas e os prestadores de serviço que lhe sejam vinculados, em conformidade com o Provimento nº 100, art. 7º, §1.

11. manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada

12. não emitir certificado com prazo de validade que se estenda além do prazo de validade de seu próprio certificado

b) Obrigações da AN:

1. receber solicitações de emissão ou de revogação de certificados

2. confirmar a identidade do solicitante e a validade da solicitação

3. encaminhar a solicitação de emissão ou de revogação de certificado à AC utilizando protocolo de comunicação seguro

4. encaminhar a solicitação de emissão ou de revogação de certificado à AC

5. disponibilizar os certificados emitidos pela AC aos seus respectivos solicitantes

6. identificar e registrar todas as ações executadas, conforme as normas, práticas e regras estabelecidas CNB-CF

7. manter a conformidade dos seus processos, procedimentos e atividades com as normas, critérios, práticas e regras estabelecidas pela AC e pelo CNB-CF

8. manter e garantir a segurança da informação por elas tratada, de acordo com o estabelecido nas normas, critérios, práticas e procedimentos definidos pelo CNB-CF e pela legislação nacional

9. garantir que todas as aprovações de solicitação de certificados sejam realizadas em cartórios autorizadas a assim operarem

c) Obrigações do Titular do Certificado

1. fornecer, de forma completa e precisa, todas as informações necessárias para sua identificação

2. garantir a proteção e o sigilo de suas chaves privadas, senhas e dispositivos criptográficos ou móveis

3. utilizar os seus certificados e chaves privadas de forma apropriada, conforme o previsto na PC correspondente

4. conhecer os seus direitos e obrigações, contemplados pela DPC, pela PC correspondente e por outros documentos aplicáveis do e-notariado

5. informar à AC qualquer comprometimento de sua chave privada e solicitar a imediata revogação do certificado correspondente

6. apresentar-se pessoalmente ao tabelião ou registrador civil (AN) para emissão de seu certificado

7. obedecer estritamente a esta DPC às PC aplicáveis, bem como respeitar a legislação aplicável e as obrigações contratuais assumidas perante a AC

8. reconhecer como próprios, autênticos, válidos e eficazes os documentos ou aplicações que contiverem o seu certificado

9. submeter à arbitragem ou conciliação eventuais repúdios de autenticidade ou incidentes de falsidade

d) Direitos da Terceira Parte (*Relying Party*)

1. Considera-se terceira parte, a parte que confia no teor, validade e aplicabilidade do certificado digital.

2. Constituem direitos da terceira parte:
   i. recusar a utilização do certificado para fins diversos dos previstos nesta DPC
   ii. verificar a qualquer tempo a validade do certificado. Um certificado emitido por AC é considerado válido quando: não constar da LCR da AC, não estiver expirado e puder ser verificado com o uso de certificado válido da AC

3. o não exercício desses direitos não afasta a responsabilidade da AC e do titular do certificado

e) Obrigações do Repositório

1. disponibilizar, logo após a sua emissão, os certificados emitidos pela AC

2. disponibilizar mecanismos para verificação do estado de revogação dos certificados, sendo eles: Lista de Certificados Revogados (LCR) e consulta via protocolo *Online Certificate Status Protocol* (OCSP)

3. implementar os recursos necessários para a garantia da segurança dos dados nele armazenados

2.2 Responsabilidades

a) Responsabilidades da AC

1. adotar as medidas de segurança e controle previstas nesta DPC, nas PCs e Política de Segurança que vier implementar, envolvendo seus processos, procedimentos e atividades

2. manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras do e-notariado e com a legislação vigente

3. manter e garantir a integridade, o sigilo e a segurança da informação por ela tratada

4. responder administrativa e judicialmente, nos termos da legislação vigente, quando agir com culpa

5. responder solidária e subsidiariamente por atos culposos das ANs vinculadas, que decorram especificamente das atividades de certificação inerentes a esta DPC

b) Responsabilidades da AN vinculada à AC

1. manter a conformidade dos seus processos, procedimentos e atividades com as normas, práticas e regras estabelecidas pela AC

2. manter e garantir a segurança da informação por ela tratada segundo as normas do e-notariado e da legislação vigente

3. responder administrativa e judicialmente, nos termos da legislação vigente, quando agir com culpa

c) Da Ausência de Responsabilidade

1. A AC do e-notariado não terá responsabilidade por eventuais fraudes decorrentes de pessoas portadoras de documentos de identificação não verdadeiros

2.3 Responsabilidade Financeira

a) Indenizações devidas pela terceira parte usuária

O usuário do Certificado Digital da AC do e-notariado (*Relying Party*) não é responsável perante esta AC e as Autoridades Notariais a ela vinculadas, exceto na hipótese de prática de ato ilícito.

b) Relações Fiduciárias

As indenizações decorrentes de danos a que comprovadamente der causa, seja pela AC ou pelas Autoridades Notariais a ela vinculadas, estarão descritas em instrumento específico.

c) Processos Administrativos

Os processos administrativos cabíveis, relativos às operações da AC e das Autoridades Notariais vinculadas à AC, seguirão a legislação específica na qual os procedimentos questionados se enquadrarem.

2.4 Legislação Cabível

Esta DPC aprovada pelo Conselho Federal do CNB obedece às leis da República Federativa do Brasil, atendendo aos requisitos da legislação em vigor, tais como o § 2º. do art. 10 da MP 2.200-2 de 24 de agosto de 2001, o art. 2º, inc. II da MP 983 de 16 de junho de 2020 e os Provimentos nº 74, de 31 de julho de 2018 e nº 100 de 26 de maio de 2020.

As ANs devem cumprir o disposto na Lei 8.935/94, no que for aplicável. Os certificados emitidos pelas ANs gozam outrossim da presunção de autenticidade como previsto no Código de Processo Civil, Lei 13.105 de 16 de março de 2015, art. 411, inc. I.

a) Da legislação

Esta DPC deve ser interpretada de acordo com as leis do Brasil. Esta escolha legal é feita para assegurar a interpretação uniforme desta DPC, independentemente do local de residência ou local de uso de certificados emitidos pela AC do e-notariado e suas ANs, ou ainda outros produtos e serviços. A lei brasileira aplica-se a todas as relações comerciais ou contratuais da AC nas quais esta DPC pode ser aplicada implícita ou explicitamente em relação aos produtos e serviços da AC onde a mesma atua como provedor ou fornecedor, beneficiário ou não.

b) Forma de interpretação e notificação

Caso uma ou mais disposições desta DPC vier a ser considerada ou declarada inválida, ilegal ou não aplicável, a AC tomará de imediato as medidas necessárias para adequar esta DPC ou a disposição em questão às exigências legais, sem prejuízo para o titular do certificado ou o seu usuário, mantidas válidas e eficazes todas as disposições.

c) Procedimentos de solução de disputa

Em caso de conflito entre esta DPC e outras declarações, políticas, planos, acordos, contratos ou documentos, esta DPC prevalecerá.

2.5 Tarifação

a) Tarifas de Serviço

Não se aplica.

b) Tarifas de emissão e renovação de certificados

Não se aplica.

c) Tarifas de acesso ao certificado

Não se aplica.

d) Tarifas de revogação ou de acesso à informação de status

Não se aplica.

e) Tarifas para outros serviços

Pelos demais serviços a AC cobrará o valor estabelecido nos termos do art. 8º, §3º do Provimento 100 supracitado.

f) Política de reembolso

Caso o certificado deva ser revogado por motivo de comprometimento da chave privada da AC ou de equipamento para uso da chave privada da AC, ou ainda quando constatada a emissão imprópria ou defeituosa, imputável à AC, esta emitirá outro certificado em substituição, sem cobrança ou ônus.

2.6 Publicação e Repositórios

a) Publicação de informação

A Autoridade Certificadora publicará e manterá disponível em seu sítio (https://www.e-notariado.org.br as seguintes informações, que serão mantidas e atualizadas em conformidade com a respectiva Política de Certificado:

1. seu próprio certificado
2. todos os certificados por ela emitidos
3. suas LCRs
4. consulta de estado de revogação de certificado via *Online Certificate Status Protocol* (OCSP) conforme RFC 6960
5. sua DPC
6. as PCs que implementar

b) Disponibilidade

Todas as informações, exceto consultas OCSP, serão mantidas disponíveis e atualizadas em no mínimo 99,5% (noventa e nova vírgula cinco por cento) do tempo por mês.

As consultas OCSP serão mantidas disponíveis em no mínimo 99% (noventa e nova por cento) do tempo por mês.

c) Controles de Acesso

Somente a AC, por seus funcionários competentes e designados especialmente para esse fim, pode alterar as informações constantes nesta DPC e nas PCs que implementa, após haver obtido a competente autorização do CNB-CF. Os controles de acesso para esta finalidade incluem identificação pessoal para acesso aos equipamentos utilização de senhas ou qualquer outra forma de autenticação forte. Do mesmo modo, somente a AC, por seus funcionários competentes e designados especialmente para esse fim, pode efetuar as necessárias atualizações de suas LCRs. O certificado da AC e os certificados emitidos pela mesma não podem ser modificados. Caso se faça necessário modificar os dados contidos nos mesmos, será necessária a revogação dos certificados. Não há restrições para o acesso para a leitura desta DPC, das PCs que implementa e das LCRs. Todas as informações disponibilizadas, conforme o item anterior desta DPC, estão disponíveis para leitura ostensivamente sem restrições.

d) Repositórios

A AC adota como repositório de LCR os seguintes endereços:

1. http://ac.e-notariado.org.br/crls/<idac>.crl
2. http://ac.e-notariado.com.br/crls/<idac>.crl (*failover*)

Onde <idac> corresponde a:

- No caso da AC raiz do e-notariado: “ac-raiz”;
- No caso da AC CNB: “ac-cnb”;
- No caso de ACs subsequentes, o ID de AC (exemplo: “*2Oficio*”)

O repositório de LCR atende os seguintes requisitos:

1. Disponibilidade – aquela definida no 2.2, item a
2. Protocolos de acesso – *HTTP*
3. Requisitos de segurança – obedece aos requisitos definidos no item 5

2.7 Fiscalização: conformidade e *compliance*

a) Da auditoria

As possíveis auditorias realizadas nas ACs e ANs do e-notariado têm por objetivo verificar se os processos, procedimentos e atividades dos prestadores de serviços estão em conformidade com suas respectivas DPC e PC e demais normas e procedimentos estabelecidos pelo CNB-CF, em consonância com o art. 8º, §1º, inc. III do Provimento 100.

b) Frequência de Auditoria

A AC poderá contratar auditorias independentes de conformidade das entidades a ela diretamente vinculadas, idealmente de forma anual, ou qualquer tempo segundo determinação do CNB-CF.

c) Escopo da Auditoria

As auditorias de conformidade verificam todos os aspectos relacionados com a emissão e o gerenciamento de certificados digitais, incluindo o controle dos processos de solicitação, identificação, autenticação, geração, publicação, distribuição, renovação e revogação de certificados.

Os tópicos cobertos pela auditoria de conformidade incluem, dentre outros:

1. Padrões de Segurança
2. Segurança física ou lógica
3. Administração dos serviços
4. Investigação de pessoal
5. PC e DPC utilizadas
6. Contratos
7. Considerações de sigilo
8. Qualquer outra recomendação expressa do CNB-CF

d) Comunicação de resultados e não conformidade

Todos os resultados e/ou relatórios da auditoria independente serão entregues ao CNB-CF para a aprovação e deliberação. Outrossim, a AC e as ANs ou qualquer entidade vinculada cumprirá, no prazo estipulado pelo Conselho Federal, as recomendações dos auditores para corrigir os casos de não conformidade com a legislação ou com as políticas, normas, práticas e regras estabelecidas.

2.8 Direitos de propriedade intelectual

Todos os direitos de propriedade intelectual de certificados, políticas, especificações de práticas e procedimentos, nomes e chaves criptográficas, e todos os documentos gerados para

a AC (eletrônicos ou não), de acordo com a legislação vigente, pertencem e continuarão sendo propriedade da AC do e-notariado.

2.9 Normas e Tipos de Sigilo

A chave privada de assinatura digital da estrutura de AC foi gerada e é mantida pela própria AC, que é responsável pelo seu sigilo. A divulgação ou utilização indevida de sua chave privada de assinatura é de sua inteira responsabilidade.

a) Tipos de informação sigilosas

Todas as informações coletadas, geradas, transmitidas e mantidas pela AC e a AN vinculada são consideradas sigilosas, exceto aquelas informações citadas no item b, *infra*. Como princípio geral, nenhum documento, informação ou registro fornecido à AC ou AN vinculada deverá ser divulgado.

b) Tipos de informações não sigilosas

Os seguintes documentos da AC e AN vinculada são considerados documentos não sigilosos:

1. os certificados e as LCR emitidos
2. informações corporativas que façam parte de certificados ou de diretórios públicos
3. esta DPC
4. versões públicas de Políticas de Segurança
5. extratos de conclusão de auditorias

c) Divulgação de informação de revogação de certificado

A AC divulga informações de revogação de certificados por ela emitidos, na sua página web descrita nesta DPC, através de sua lista de certificados revogados. A razões para revogação do certificado sempre serão informadas para o seu titular. A suspensão de certificados não será admitida na AC do e-notariado.

d) Quebra de sigilo por motivos legais

Como princípio geral, nenhum documento, informação ou registro que pertençam ou estejam sob a guarda da AC e sua rede de ANs vinculadas é divulgado a entidades legais ou seus funcionários, exceto quando:

1. exista uma ordem judicial corretamente constituída

2. estejam corretamente identificados o processo em que foi determinada e a autoridade judicial que determinou a quebra de sigilo

e) Informações a terceiros

Como diretriz geral nenhum documento, informação ou registro, sob a guarda da AC ou AN vinculada, será fornecido a terceiros, exceto quando o requerente o solicite através de instrumento devidamente constituído, seja autorizado para fazê-lo e esteja corretamente identificado.

f) Divulgação de informação por solicitação do titular

O titular do certificado, ou seu representante legal devidamente identificado, qualificado e autorizado, tem e terá sempre acesso às informações que lhe dizem respeito que estejam sob a guarda da AC e da AN em razão da solicitação e da emissão do certificado digital. O titular do certificado pode autorizar a AC ou a AN a divulgar tais informações a terceiros ou unicamente às pessoas que indique nessa autorização.
Esta autorização pode ser feita no ato da solicitação do certificado, no próprio formulário de solicitação, ou posteriormente, por e-mail ou outro documento legalmente aceito.

g) Outras circunstâncias de divulgação de informação

A AC e a AN podem divulgar informações que não sejam consideradas sigilosas pelo fato de:

1. estarem na posse legítima da AC ou da AN antes de seu fornecimento pelo solicitante ou titular do certificado ou o solicitante ou titular do certificado haver autorizado a sua divulgação.
2. posteriormente ao seu fornecimento pelo solicitante ou titular do certificado, terem sido obtidas ou puderem ter sido obtidas legalmente de um terceiro com direitos legítimos para sua divulgação sem quaisquer restrições.
3. terem sido requisitadas por determinação judicial ou governamental, obrigando-se a AC, nesse caso, a comunicar previamente, se possível, e de imediato ao solicitante ou titular do certificado a existência de tal determinação.

3. Processo de Identificação e Autenticação

3.1 Registro Geral e Inicial

Descrição da DPC para os requisitos e os procedimentos gerais a serem utilizados pela AN vinculada à AC, que será responsável pela a realização dos seguintes processos:

a) Validação da solicitação de certificado

Compreende todas as etapas abaixo, realizadas por definição (Provimento nº 100, art. 2º, inc. II) mediante a presença física do interessado, com base nos documentos de identificação citados anteriormente:

1. confirmação da identidade de um indivíduo: comprovação de que a pessoa que se apresenta como titular ou responsável pelo certificado é realmente aquela cujos dados constam na documentação que se apresenta. A Autoridade Notarial - AN efetua então a identificação e autenticação dos dados e documentos do Titular do Certificado por ocasião do ato notarial de identificação. Tais informações devem corresponder àquelas exigidas para o preenchimento do "Cartão de Assinatura" para reconhecimento de firma pelo tabelião (Autoridade Notarial). Já nos casos em que envolver certificado para "titular pessoa física", poder-se-á aceitar procuração desde que autorizada pelo tabelião.

2. nos casos de falecimento de um ou dos responsáveis legais por quaisquer empresas de um modo geral, desde que haja decisão judicial ou escritura notarial com nomeação de inventariante e termo de compromisso de inventariante assinado, e nomeação expressa deste como administrador, será admitida a pessoa nomeada na qualidade de responsável legal do certificado digital para todos os fins legais e administrativos.

3. emissão do certificado: conferência dos dados da solicitação de certificado com os constantes dos documentos apresentados e liberação da emissão do certificado no sistema da AC.

b) Verificação da solicitação de certificado

Confirmação da validação realizada, observando que são executados, obrigatoriamente:

1. por autorização expressa do tabelião ou de seus prepostos
2. em uma AN vinculada diretamente à AC do e-notariado
3. somente após se ter entregue na AN, de cópia da documentação apresentada para emissão do certificado
4. antes do início da validade do certificado

c) Validação em diligência

Será facultado ao agente de registro a validação em diligência, segundo autorização do tabelião, desde que utilizado ambiente computacional seguro, passível de controle, registrado no inventário de hardware e softwares da AN.

d) Etapas da Validação

Todas as etapas dos processos de validação da solicitação de certificado deverão ser registradas e assinadas digitalmente pelos executantes, de modo a possibilitar a reconstrução completa dos processos e procedimentos realizados. São mantidos ainda arquivos com as cópias de todos os documentos utilizados para confirmação da identidade de uma organização e/ou de um indivíduo. Tais cópias são mantidas em papel e/ou em forma digitalizada no dossiê documental formado para efeito da emissão do certificado.

e) Tipos de Nomes

Os tipos de nomes admitidos para os titulares de certificados da AC são:

1. Certificados de pessoa física, o campo "*Common Name*" (CN) é composto do nome do Titular do Certificado.
2. Certificados de pessoa jurídica, o campo "*Common Name*" (CN) é composto do nome empresarial da pessoa jurídica.
3. Certificados de equipamento, o campo "*Common Name*" (CN) é composto do "*Domain Name System*" (DNS) do site.
4. Certificados para assinatura de código, o campo "*Common Name*" (CN) é composto do nome empresarial da pessoa jurídica mais a área responsável pelo certificado.
5. Certificados de Aplicação, o campo "*Common Name*" (CN) é composto do nome da Aplicação.

f) Formação e Unicidade de Nomes

Para identificação dos titulares dos certificados emitidos, a AC faz uso de nomes significativos que possibilitam determinar a identidade da pessoa ou organização a que se referem. Os requisitos e procedimentos específicos, quando aplicáveis, estão detalhados nas PCs implementadas. No campo "*Distinguished Name*" (DN) devem ser únicos e não ambíguos, para cada titular de certificado, no âmbito da AC emitente. Números ou letras adicionais poderão ser incluídos ao nome de cada entidade para assegurar a unicidade do campo. O CNB-CF reserva-se por sua vez o direito de tomar todas as decisões referentes a disputas decorrentes da igualdade de nomes das AC de nível imediatamente subsequente ao seu. Durante o processo de confirmação de identidade, a AC solicitante deve provar o seu direito de uso de um nome específico (DN) em seu certificado. Os processos de tratamento, reconhecimento e confirmação

de autenticidade de marcas registradas serão executados de acordo com a legislação em vigor.

3.2 Geração de novo par de chaves antes da expiração do atual

Antes da expiração do certificado, o solicitante pode solicitar um novo certificado, enviando à Autoridade Notarial - AN uma solicitação, por meio eletrônico, usando a mesma plataforma móvel para o armazenamento do certificado, limitada a 2 (duas) ocorrências sucessivas. Nos demais casos ou quando o solicitante não utilizar o meio eletrônico, devem ser observados os mesmos requisitos e procedimentos exigidos para a solicitação inicial do certificado, na forma e no prazo estabelecidos na correspondente PC. A emissão de um novo certificado obedecerá ao estabelecido na correspondente PC implementada.

3.3 Geração de novo par de chaves após expiração ou revogação

Após a revogação do certificado, o solicitante poderá solicitar um novo certificado, enviando à Autoridade Notarial - AN uma solicitação, na forma, condições e prazo estabelecidos para a solicitação inicial de um certificado.

3.4 Solicitação de Revogação

A solicitação de revogação de certificado pode ser feita através de formulário específico, permitindo a identificação inequívoca do solicitante. A confirmação da identidade do solicitante é feita com base na confrontação de dados entre a solicitação de revogação e a solicitação de emissão. Os procedimentos detalhados de solicitação de revogação e de revogação estão descritos na correspondente PC.

4. Requisitos e Procedimentos operacionais

4.1 Solicitação de Certificado

A solicitação de emissão de um Certificado Digital deve ser feita perante a Autoridade Notarial – AN, seguindo procedimentos mínimos necessários descritos na Política de Certificação correspondente.

Os procedimentos de solicitação incluem a assinatura pelo solicitante de Termo de Titularidade contendo os termos e condições de uso do certificado. Ainda, o solicitante efetuará o fornecimento de todos os dados obrigatórios que permitam a comprovação dos atributos de identificação.

4.2 Emissão de Certificado

Somente após e na hipótese de validação conclusiva pela Autoridade Notarial - AN dos dados fornecidos pelo solicitante a AC procederá à emissão e assinatura do certificado. O certificado será considerado válido a partir do momento da sua emissão.

4.3 Aceitação de Certificado

O recebimento de um certificado pelo Titular de Certificado e o uso subsequente das chaves, constitui aceitação do certificado por parte do Titular. Também, no caso de certificados de equipamentos, aplicações, a aceitação é feita pela pessoa responsável pelo uso subsequente ao recebimento do certificado.

Aceitando um certificado, o Titular deste:

1. manifesta expressamente estar de acordo com as responsabilidades contínuas, obrigações e deveres impostas a ele pelo Termo de Responsabilidade e esta DPC da AC.
2. toma conhecimento e atesta que, para sua segurança, nenhuma pessoa deve ter acesso à chave privada e senhas associadas com o certificado.
3. afirma que as informações fornecidas durante o processo de solicitação são verdadeiras e foram publicadas dentro do certificado com precisão.

4.4 Revogação de Certificado

a) Circunstâncias para revogação

A revogação de um certificado refere-se à permanente inutilização do mesmo, o que se dá tipicamente nas seguintes circunstâncias:

1. quando constatada emissão imprópria ou defeituosa do mesmo.
2. quando for necessária a alteração de qualquer informação relevante constante no mesmo ou uma informação do certificado tornar-se inexata.
3. no caso de perda, roubo, modificação, acesso indevido ou comprometimento da chave privada correspondente ou da sua mídia armazenadora.
4. quando um titular de certificado organizacional deixa o emprego ou passa a não mais representar a pessoa jurídica em favor de quem o certificado foi expedido.
5. quando uma determinada AN interrompe suas atividades.
6. quando falecer o Titular de Certificado.
7. quando houver o descumprimento da DPC pela entidade vinculada.

8. o CNB-CF determinará a revogação do certificado da AC que deixar de cumprir a legislação vigente ou as políticas, normas, práticas e regras estabelecidas pelo e-notariado.

b) Quem pode solicitar a revogação

A revogação de um certificado somente poderá ser solicitada:

1. Pelo titular do certificado.
2. pelo responsável pelo certificado, no caso de certificado de equipamentos, aplicações.
3. pela AC e pela AN.
4. por determinação do CNB-CF.

c) Procedimento para a solicitação de revogação

Para solicitar a revogação é necessário o envio à AC e à AN de uma comunicação expressa, preenchido com os dados do solicitante, o número de série do certificado e a indicação do motivo da solicitação.

Como diretrizes gerais:

1. o solicitante da revogação de um certificado é identificado
2. as solicitações de revogação, bem como as ações delas decorrentes são registradas e armazenadas
3. as justificativas para a revogação de um certificado são documentadas
4. o processo de revogação de um certificado termina com a geração e a publicação de uma LCR que contém o certificado revogado

d) Prazo para solicitação de revogação

A solicitação de revogação deve ser imediata quando configuradas as circunstâncias definidas no item a, *supra*. Cada PC implementada pela AC estabelece o prazo para a aceitação do certificado por seu titular, dentro do qual a revogação desse certificado pode ser solicitada sem cobrança de tarifa pela AC.

e) Frequência de emissão de LCR

A AC emite uma nova LCR referentes a certificados de ACs Subsequentes a cada 30 (trinta) dias. A frequência máxima admitida para a emissão de LCR referente a certificados de AC é de 45 (quarenta e cinco) dias. Em caso de revogação de certificado de AC Subsequente, a AC deverá emitir nova LCR no prazo previsto no item c, *supra*,

"Procedimento para a solicitação de revogação" e notificar todas as ACs de nível imediatamente subsequente ao seu.

f) Requisitos para verificação de LCR

Todo certificado deve ter a sua validade verificada, na respectiva LCR, antes de ser utilizado. A autenticidade da LCR deve também ser confirmada por meio das verificações da assinatura da AC emitente e do período de validade da LCR.

g) Requisitos especiais para o caso de comprometimento de chave

Caso ocorra perda, roubo, modificação, acesso indevido ou comprometimento de chave privada ou de sua mídia armazenadora, o titular deverá notificar imediatamente a AC ou a Autoridade Notarial, solicitando a revogação de seu certificado, através de expressa comunicação.

4.5 Procedimentos de Auditoria de Segurança

a) Tipos de Evento Registrados

Todas as ações executadas pelo pessoal da AC, no desempenho de suas atribuições, são registradas de modo que cada ação esteja associada à pessoa que a realizou. A AC registra em arquivos para fins de auditoria todos os eventos relacionados à segurança do seu sistema de certificação, quais sejam:

1. iniciação e desligamento do sistema de certificação
2. tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da AC
3. mudanças na configuração da AC ou nas suas chaves
4. mudanças nas políticas de criação de certificados
5. tentativas de acesso (login) e de saída do sistema (logoff)
6. tentativas não autorizadas de acesso aos arquivos de sistema
7. geração de chaves próprias da AC ou de chaves de Titulares de Certificados
8. emissão e revogação de certificados
9. geração de LCR
10. tentativas de iniciar, remover, habilitar e desabilitar usuários de sistemas, e de atualizar e recuperar suas chaves
11. operações falhas de escrita ou leitura no repositório de certificados e da LCR, quando aplicável
12. operações descritas neste repositório, quando aplicável

b) Registros de eventos indiretos

A AC registra, eletrônica ou manualmente, informações de segurança não geradas diretamente pelo seu sistema de certificação, quais sejam:

1. registros de acessos físicos
2. manutenção e mudanças na configuração de seus sistemas
3. mudanças de pessoal e de perfis qualificados
4. relatórios de discrepância e comprometimento
5. registros de destruição de mídias de armazenamento contendo chaves criptográficas, dados de ativação de certificados ou informação pessoal de usuários
6. o ambiente de nuvem deve ser compatível com os itens *Identity and Access Management: Controls* IAM-01.1, IAM-01.2 e IAM-01.3 dos requisitos da Cloud Security Alliance

c) Registros de solicitação e revogação de certificados

A AN vinculada à AC, responsável pela DPC, registrará eletronicamente em arquivos de auditoria todos os eventos relacionados à validação e aprovação da solicitação, bem como, à revogação de certificados. Os seguintes eventos deverão obrigatoriamente estar incluídos em arquivos de auditoria:

1. data e hora das operações
2. validação e aprovação e o certificado gerado
3. a assinatura digital do executante

d) Período de Retenção para registros (*logs*) de Auditoria

A AC manterá os seus registros de auditoria pelo prazo de 2 (dois) meses e, subsequentemente, fará o armazenamento da maneira descrita no item 4.6.

e) Proteção de registro (log) de auditoria

O sistema de registro de eventos de auditoria inclui mecanismos para proteger os arquivos de auditoria contra leitura não autorizada, modificação e remoção, através das funcionalidades nativas dos sistemas operacionais. Mecanismos de proteção utilizados:

1. Os acessos lógicos são liberados através da ferramenta nativa do sistema operacional de modo a assegurar o uso apenas a usuários ou processos autorizados;
2. Os acessos lógicos aos registros de eventos de auditoria são registrados em logs do próprio sistema operacional.

3. Informações manuais de auditoria também são protegidas contra a leitura não autorizada, modificação e remoção.
4. Os mecanismos de proteção descritos neste item podem ser complementados pela Política de Segurança do e-notariado

f) Procedimentos para cópia de segurança (backup) de registro (log) de auditoria

A AC gera a cada semana cópia de backup de seus registros de auditoria, através de procedimentos utilizando conexão segura.

g) Sistema de coleta de dados de auditoria

O sistema de coleta de dados de auditoria é interno à AC e utiliza processos automatizados e manuais.

h) Avaliações de vulnerabilidade

Os eventos que indicam possível vulnerabilidade, detectados na análise periódica dos registros de auditoria da AC, são analisados detalhadamente e, dependendo de sua gravidade, registrados em separado. Ações corretivas decorrentes são implementadas pela AC e registradas para fins de auditoria.

4.6 Arquivamento de Registros

a) Tipos de eventos registrados

Os tipos de eventos arquivados pela AC são:

1. solicitações de certificados;
2. solicitações de revogação de certificados;
3. notificações de comprometimento de chaves privadas;
4. emissões e revogações de certificados;
5. emissões de LCR;
6. trocas de chaves criptográficas da AC;
7. informações de auditoria previstas no item 4.5 a, *supra*, “Tipos de Eventos Registrados”
8. o ambiente de nuvem deve obedecer e qualificar os itens *Infrastructure and Virtualization Security: Controls* IVS-01.1 até 01.5 dos requisitos da Cloud Security Alliance

b) Período de retenção para arquivo

Os períodos de retenção para cada evento arquivado são:

1. as LCR referentes a certificados de assinatura digital são retidas por, no mínimo, período igual ao do arquivamento dos respectivos certificados;
2. as demais informações são retidas por, no mínimo, 6 (seis) anos.

c) Proteção de arquivo

Os registros arquivados da AC são classificados e armazenados com requisitos de segurança compatíveis com essa classificação ou segundo orientação específica do CNB-CF.

d) Sistema de coleta de dados de arquivo

Todos os sistemas de coleta de dados de arquivo utilizados pela AC em seus procedimentos operacionais são automatizados ou manuais e internos.

e) Procedimentos para obter e verificar informação de arquivo

A verificação de informação de arquivo deve ser solicitada formalmente à AC ou à Autoridade Notarial - AN, identificando de forma precisa o tipo e o período da informação a ser verificada. O solicitante da verificação de informação deve ser devidamente identificado.

4.7 Troca de chave

Trinta dias antes da data de expiração do certificado digital, a Autoridade Notarial - AN poderá a seu critério comunicar ao seu titular, através de endereço eletrônico, a data de expiração do mesmo, apresentando-lhe procedimentos para a solicitação de novo certificado. Expirado o certificado do titular, a AC remove imediatamente este certificado de seu diretório, mantendo-o armazenado por, no mínimo, 30 (trinta) anos, para efeito de consulta histórica.

4.8 Comprometimento e Recuperação de Desastre

Os requisitos relacionados aos procedimentos de notificação e de tentativa de recuperação de desastres vão detalhados abaixo visando mecanismos de Continuidade de Negócios da AC para garantir a continuidade dos seus serviços críticos.

a) Recursos computacionais, software e dados corrompidos

A AC deverá registrar os itens infra descritos, que especificam as ações a serem tomadas no caso em que recursos computacionais, software e/ou dados são corrompidos, e que podem ser resumidas no seguinte:

1. é feita a identificação de todos os elementos corrompidos
2. o instante do comprometimento é determinado e é crítico para invalidar as transações executadas após aquele instante
3. é feita uma análise do nível do comprometimento para a determinação das ações a serem executadas, que podem variar de uma simples restauração de um backup de segurança até a revogação do certificado da AC

b) Certificado de entidade é revogado

Em caso de revogação dos certificados das ACs aqui referidas, as ações a serem tomadas podem ser resumidas da seguinte forma:

1. O CNB-CF e os Titulares de Certificados serão notificados por comunicação segura
2. A AC revoga os certificados por ela emitidos
3. A(s) AC(s) subsequente(s) solicita(m) um novo certificado à AC *CNB*
4. Iniciam-se os procedimentos para emissão dos novos certificados de usuários

c) Chave de entidade é comprometida

A AC deverá interromper suas atividades no caso de comprometimento de sua chave privada. Após a identificação da crise, são notificados os gestores do processo de certificação digital que acionam as equipes envolvidas, para ativar um plano contingência.

d) Atividades das Autoridades Notariais de Registro

Os procedimentos para o planejamento de recuperação de crises das ANs vinculadas para recuperação, total ou parcial das atividades das ANs, estão abaixo descritos:

1. identificação dos eventos que podem causar interrupções nos processos do negócio, por exemplo falha de equipamentos, inundações e incêndios
2. identificação e concordância de todas as responsabilidades e procedimentos de emergência
3. implementação dos procedimentos de emergência que permitam a recuperação e restauração nos prazos necessários. Atenção especial será dada à avaliação da recuperação das documentações armazenadas nas instalações técnicas atingidas pelo desastre
4. documentação dos processos e procedimentos acordados

5. treinamento adequado do pessoal nos procedimentos e processos de emergência definidos, incluindo o gerenciamento de crise
6. teste e atualização dos planos

4.9 Extinção da AC

Caso seja necessária a extinção dos serviços da estrutura de ACs, o CNB-CF executará os procedimentos para notificação dos usuários e para a transferência da guarda de seus dados e registros de arquivos incluem:

1. lavratura de Ata notarial com descritivo da extinção
2. notificação para o e-mail do titular do certificado
3. transferência progressiva do serviço e dos registros operacionais para um sucessor que tenha os mesmos requisitos de segurança da entidade extinta
4. preservação de quaisquer registros não transferidos a um sucessor
5. as chaves públicas dos certificados emitidos pela AC dissolvida serão armazenadas por outra AC após aprovação do CNB-CF
6. quando houver mais de uma AC interessada, assumirá a responsabilidade do armazenamento das chaves públicas aquela indicada pela AC e o CNB-CF
7. a AC, ao encerrar as suas atividades, transferirá, se for o caso, a documentação dos certificados digitais emitidos à AC que tenha assumido a guarda das respectivas chaves públicas
8. caso as chaves públicas não tenham sido assumidas por outra AC, os documentos referentes aos certificados digitais e as respectivas chaves públicas serão repassados ao CNB-CF

5. Controles de Segurança

6.1 Controle físico

O ambiente de nuvem deve obedecer estritamente aos itens da Datacenter Security, Controls DCS-01 até DCS-09 definido nos requisitos da Cloud Security Alliance. Devem igualmente serem compatíveis com os padrões internacionais SSAE16/ISAE 3402 e certificados ISO 27001.

6.2 Controles Procedimentais

Nos itens seguintes estão descritos os requisitos para a caracterização e o reconhecimento de perfis qualificados na AC, juntamente com as responsabilidades definidas para cada perfil. Para cada tarefa associada aos perfis definidos, é estabelecido o número de pessoas requerido para sua execução.

a) Perfis qualificados

A separação das tarefas para funções críticas é uma prática adotada, com o intuito de evitar que um funcionário utilize indevidamente o sistema de certificação sem ser detectado. As ações de cada empregado estão limitadas de acordo com o seu perfil. A AC estabelece um mínimo de 3 (três) perfis distintos para sua operação, distinguindo as operações cotidianas do sistema, a gestão e a auditoria dessas operações, bem como o gerenciamento de mudanças substanciais no sistema.
Antes de obterem qualquer tipo de acesso, todos os operadores do sistema de certificação da AC, serão autorizados em documento formal, com base nas necessidades de cada perfil, o tipo e o nível de acesso.
Quando um operador se desliga da AC, suas permissões de acesso são revogadas imediatamente. Quando há mudança na posição ou função que o empregado ocupa dentro da AC, são revistas suas permissões de acesso. Existe uma lista de revogação, com todos os recursos, antes disponibilizados, que o empregado deverá devolver à AC no ato de seu desligamento.

b) Número necessário de pessoas por tarefa

Controle multiusuário é requerido para a geração e a utilização da chave privada da AC do e-notariado, como se descreve no item 6.2, *infra.*

c) Identificação e autenticação para cada perfil

Profissionais que ocupam os perfis designados pela AC passam por um processo rigoroso de seleção. Todo funcionário da AC tem sua identidade e perfil verificados antes de:

1. ser incluído em uma lista de acesso aos sistemas que hospedam a AC
2. ser incluído em uma lista para acesso lógico ao sistema de certificação da AC
3. receber um certificado para executar suas atividades operacionais na AC
4. receber uma conta no sistema de certificação da AC

6.3 Controles de pessoal

Todos os operadores da AC, encarregados de tarefas operacionais, têm registrado um termo de responsabilidade, onde se encontram detalhados:

1. Os termos e as condições do perfil que ocupam
2. O compromisso de observar as normas, políticas e regras aplicáveis da AC
3. O compromisso de observar as normas, políticas e regras aplicáveis da CNB-CF
4. O compromisso de não divulgar informações sigilosas a que tenham acesso

a) Antecedentes, qualificação, experiência e requisitos de idoneidade

Todo o pessoal da AC e AN vinculada envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é admitido conforme o estabelecido pelo CNB e, quanto às ANs, pelo disposto na lei 8.935/94.

b) Procedimentos de Verificação de Antecedentes

Com o propósito de resguardar a segurança e a credibilidade da AC do e-notariado, toda a equipe envolvida em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados, é submetida aos seguintes processos, antes do começo das atividades:

1. Verificação de antecedentes criminais
2. Verificação de histórico de empregos anteriores
3. Comprovação de escolaridade e de residência

c) Requisitos de treinamento

Todo o pessoal da AC e da Autoridade Notarial - AN envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados recebe treinamento documentado, suficiente para o domínio dos seguintes temas:

1. princípios e mecanismos de segurança da AC e da Autoridade Notarial – AN
2. sistema de certificação em uso na AC
3. conhecimento de grafoscopia e documentoscopia
4. outros assuntos relativos a atividades sob sua responsabilidade

d) Frequência e requisitos para reciclagem técnica

Todo o pessoal da AC e da AN envolvido em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é mantido atualizado sobre eventuais mudanças tecnológicas nos sistemas da AC.

e) Sanções para ações não autorizadas

Na eventualidade de uma ação não autorizada, real ou suspeita, ser realizada por pessoa encarregada de processo operacional da AC, ela suspenderá o acesso desta pessoa ao seu sistema de certificação e tomará as medidas administrativas e legais cabíveis.

f) Requisitos para contratação de pessoal

Todo o pessoal das ANs envolvidas em atividades diretamente relacionadas com os processos de emissão, expedição, distribuição, revogação e gerenciamento de certificados é contratado conforme o estabelecido pela AN-Autoridade Notarial.

g) Documentação fornecida ao pessoal

A AC tornará disponível para todo o seu pessoal e para as Autoridades Notariais:

1. sua DPC
2. as PCs implementadas
3. as normas gerais de segurança que suplementem a DPC
4. documentação operacional relativa às suas atividades
5. todas as normas que se fizerem necessárias para a realização das atividades envolvidas

6. Controles Técnicos de Segurança

6.1 Geração e Instalação do Par de Chaves

a) Geração do par de chaves

O par de chaves da AC é gerado pelo próprio e-notariado, em ambiente de nuvem que deve suportar os itens EKM-02.4: Encryption & Key Management - Key Generation da Cloud Security Alliance, após o deferimento do pedido de credenciamento da mesma e a consequente autorização de funcionamento no âmbito do e-notariado.

b) Geração de chaves da entidade final

As chaves serão geradas em ambiente do próprio usuário. É responsabilidade exclusiva do titular do certificado a geração e a guarda da sua chave privada.

c) Entrega da chave pública para emissor de certificado

A AC do e-notariado disponibilizará cópia de sua chave pública, em formato PKCS#10. O representante autorizado da AC Subsequente entregará a chave pública da AC, em

cerimônia específica, em data e hora previamente estabelecidas pela AC. Os detalhes da cerimônia serão documentados para fins de auditoria.

d) Disponibilização de chave pública da AC para usuários

A página web https://ac.e-notariado.org.br disponibilizará o certificado digital da AC do e-notariado assim como todos os certificados das ACs subsequentes quando couber.

e) Tamanhos de chaves

O tamanho mínimo das chaves criptográficas associadas ao certificado de AC Subsequente é de RSA 4096 bits e ECDSA 512 bits.

f) Parâmetros técnicos de chaves

1. Geração de Chaves Assimétricas de AC

   Algoritmo RSA ou ECC-secp384r1 ou nistp384 (conforme FIPS 186-3) - Tamanho de chave RSA 4096

2. Geração de Chaves Assimétricas de Usuário Final

   Algoritmo RSA – Tamanho de chave RSA 2048

3. Assinaturas de certificados

Assinatura de Certificados de AC	**Assinatura de Certificados de Usuário Final**
Suíte de assinatura	Suíte de assinatura
sha512WithRSAEncryption sha512WithECDSAEncryption	sha256WithRSAEncryption sha256WithECDSAEncryption sha512WithRSAEncryption sha512WithECDSAEncryption

g) Geração de chave por hardware ou software

O processo de geração do par de chaves se dará em hardware, e obedecerá ao padrão FIPS 140-2, nível 2. Se em software, em ambiente móvel receberá a devida proteção naquele ambiente.

h) Propósitos de uso de chave (conforme campo "*Key usage*" na X.509 v3)

A chave privada de AC subsequente pode ser utilizada apenas para assinatura dos certificados por ela emitidos e para assinatura de sua LCR. A chave privada da AC é utilizada apenas para a assinatura dos certificados por ela emitidos e de sua LCR.

6.2 Proteção da Chave Privada

A chave privada da AC é gerada, armazenada e utilizada apenas em hardware (vide 6.1 *supra*). O acesso ao ambiente de computacional em *cloud* será controlado por meio de chave criptográfica de ativação.

a) Padrões para módulo criptográfico

HSM FIPS 140-2

b) Controle "n de m" para chave privada

A AC implementa o controle múltiplo para a ativação e desativação da sua chave privada através de controles do software de certificação. A AC implementará sistema que exigirá a presença no mínimo de 2 (dois) detentores da chave de ativação ("n") de um grupo de 5 (cinco) ("m") para a ativação da chave da AC.

c) Recuperação de chave privada (*key escrow*)

Não será permitido no e-notariado a recuperação (*escrow*) ou tutela de chaves privadas, isto é, não se permite que terceiros possam legalmente obter uma chave privada sem o consentimento de seu titular.

d) Cópia de segurança (*backup*) de chave privada

O e-notariado manterá a seu critério cópia de segurança de sua própria chave privada. A cópia de segurança de sua própria chave privada será armazenada cifrada, protegida com um nível de segurança não inferior àquele definido para a versão original da chave, e mantida pelo prazo de validade do certificado correspondente. A AC do e-notariado, assim como as ACs subsequentes, não manterá em hipótese alguma cópia de segurança da chave privada de Titular de Certificado de assinatura digital por ela emitido.

e) Inserção de chave privada em módulo criptográfico

A AC gera seus pares de chaves diretamente, sem inserções, no ambiente computacional onde as chaves serão utilizadas.

f) Método de ativação de chave privada

A ativação da chave privada da AC é implementada por meio de token criptográfico, protegido com senha, após a identificação de 2 dos detentores da chave de ativação da chave criptográfica. Os detentores da chave de ativação serão designados para essa função pelo CNB-CF. As senhas utilizadas obedecem à política de senhas estabelecida pela AC.

g) Método de desativação de chave privada

A chave privada da AC, armazenada em módulo criptográfico em ambiente de nuvem, é desativada quando não mais é necessária através de mecanismo disponibilizado pelo software de certificação que permite o apagamento de todas as informações contidas no módulo criptográfico. Este procedimento é implementado por meio de tokens criptográficos, simulação em software, ou outras ferramentas, protegidas com senha, após a identificação de 2 dos detentores da chave de ativação da chave criptográfica. Os detentores da chave de ativação são os Administradores do Sistema de Certificação da AC. As senhas utilizadas obedecem à política de senhas estabelecida pela AC.

h) Método de destruição de chave privada

Quando a chave privada da AC for desativada, em decorrência de expiração ou revogação, esta deve ser eliminada da memória do módulo criptográfico em ambiente de nuvem com alguma solução de *wiping* (NIST 800-88). Todas as cópias de segurança da chave privada da AC e os tokens criptográficos dos custodiantes serão eliminados. Os agentes autorizados para realizar estas operações são os administradores e os custodiantes das chaves de ativação da AC.

6.3 Outros Aspectos do Gerenciamento do Par de Chaves

a) Arquivamento de chave pública

A AC armazena as chaves públicas da própria AC e dos titulares de certificados, bem como as LCRs emitidas, após a expiração dos certificados correspondentes, permanentemente, para verificação de assinaturas geradas durante seu período de validade.

b) Períodos de uso para as chaves pública e privada

A chave privada da AC e dos titulares de certificados por ela emitidos, são utilizadas apenas durante o período de validade dos certificados correspondentes. A chave pública da AC pode ser utilizada durante todo o período de tempo determinado pela legislação aplicável, para verificação de assinaturas geradas durante o prazo de validade dos certificados correspondentes.
A cadeia de certificação do e-notariado deve respeitar o período máximo de validade admitido para o certificado, limitando-o à validade do certificado da AC que o emitiu.

6.4 Dados de Ativação

Os dados de ativação da chave privada da AC são únicos e aleatórios. Cada PC implementada garante que os dados de ativação da chave privada da entidade titular do certificado, se utilizados, são únicos e aleatórios.

6.5 Controles de Segurança Computacional

a) Requisitos técnicos específicos de segurança computacional

Os computadores servidores, utilizados pela AC, relacionados diretamente com os processos de emissão, expedição, distribuição, revogação ou gerenciamento de certificados, implementam, entre outras, as seguintes características:

1. controle de acesso aos serviços e perfis da AC
2. clara separação das tarefas e atribuições relacionadas a cada perfil qualificado da AC
3. acesso restrito aos bancos de dados da AC
4. uso de criptografia para segurança de base de dados, quando exigido pela classificação de suas informações
5. geração e armazenamento de registros de auditoria da AC
6. mecanismos internos de segurança para garantia da integridade de dados e processos críticos
7. mecanismos para cópias de segurança (backup)

b) Classificação da segurança computacional

A segurança computacional da AC segue as recomendações *Common Criteria*.

c) Controle de segurança para as Autoridades Notariais

Considerando-se que os equipamentos usados pela AN em serventias extrajudiciais, e que realizam tal papel, devem precipuamente se basear nos itens cabíveis definidos no Provimento nº 74 que "dispõe sobre padrões mínimos de tecnologia da informação". Assim, as estações de trabalho da AN, incluindo equipamentos portáteis, devem receber, pelo menos, as seguintes configurações de segurança:

1. controle de acesso lógico ao sistema operacional
2. exigência de uso de senhas fortes
3. diretivas de senha e de bloqueio de conta
4. logs de auditoria do sistema operacional ativados, registrando:
   i. iniciação e desligamento do sistema
   ii. tentativas de criar, remover, definir senhas ou mudar privilégios de sistema dos operadores da NA
   iii. mudanças na configuração da estação
   iv. tentativas de acesso (login) e de saída do sistema (logoff)
   v. tentativas não-autorizadas de acesso aos arquivos de sistema
   vi. tentativas de iniciar, remover, habilitar e desabilitar usuários e de atualizar e recuperar suas chaves
5. antivírus, antitrojan e antispyware instalados, atualizados e habilitados
6. *firewall* pessoal ativado, com permissões de acesso mínimas necessárias às atividades, podendo este ser substituído por firewall corporativo, para equipamentos instalados em redes que possuam esse dispositivo
7. proteção de tela acionada no máximo após dois minutos de inatividade e exigindo senha do usuário para desbloqueio
8. sistema operacional mantido atualizado, com aplicação de correções necessárias (*patches*, *hotfix*, etc.)
9. utilização apenas de softwares licenciados e necessários para a realização das atividades do usuário
10. impedimento de login remoto, via outro equipamento ligado à rede de computadores utilizada pela AN, exceto para as atividades de suporte remoto
11. utilização de data e hora de Fonte Confiável do Tempo
12. equipamentos de coleta biométrica

6.6 Controles Técnicos do Ciclo de Vida

a) Controles de desenvolvimento de sistemas

A AC do e-notariado adota o Sistema de Certificação Digital para o e-notariado, contratado e desenvolvido em *outsourcing*. Todas as adaptações são realizadas inicialmente em um ambiente de desenvolvimento e somente após a conclusão dos

testes é colocado em um ambiente de homologação. Finalizando o processo de homologação das alterações, o gerente técnico avalia e decide quando será a implementação no ambiente de produção.

b) Controle de gerenciamento de segurança

As alterações e adaptações consideradas emergenciais e críticas pelo gerente técnico devem ser aplicadas imediatamente, excluindo-se o processo descrito no item 6.6 a, *supra*.
Todavia, o gerenciamento de configuração, para a instalação e a contínua manutenção do sistema de certificação utilizado pela AC, deve envolver o teste de mudanças sempre planejadas no Ambiente de Desenvolvimento e Homologação isolados antes de sua implantação no ambiente de Produção, incluindo as seguintes atividades:

1. instalação de novas versões ou de atualizações nos produtos que constituem a plataforma do sistema de certificação
2. implantação ou modificação de Autoridades Certificadoras com customizações em nível de certificados, páginas web, scripts etc.
3. implantação de novos procedimentos operacionais relacionados com a plataforma de processamento incluindo módulos criptográficos
4. instalação de novos serviços na plataforma de processamento

c) Controles na geração da LCR antes de publicadas

Todas as LCRs geradas pela AC, antes de publicadas, são checadas quanto à consistência de seu conteúdo, comparando-o com o conteúdo esperado em relação a número da LCR, data/hora de emissão e outras informações relevantes.

6.7 Controles de Segurança de Rede

O ambiente de nuvem deve responder e atender aos itens Infrastructure and Virtualization Security, Controls IVS-01 até IVS-13 dos requisitos da Cloud Security Alliance.

6.8 Controles de Engenharia do Módulo Criptográfico

O ambiente de nuvem deve ser compatível com os itens Encryption and Key Management, Controls EKM-01 até EKM-04 dos requisitos da Cloud Security Alliance, com destaque ao padrão NIST FIPS 140-2 nível 2.

7. Perfis de Certificados e da Lista de Certificados Revogados – LCR

7.1 Diretrizes gerais

Nos seguintes itens desta DPC, são descritos os aspectos dos certificados e LCR emitidos pela AC.

a) Números de versão
Todos os certificados emitidos pela AC implementam a versão 3 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280. E apresentam obrigatoriamente as seguintes extensões:

1. a *Authority Key Identifier*, não crítica: o campo *keyIdentifier* contém o hash SHA-1 da chave pública da AC
2. *Subject Key Identifier*, não crítica: contém o hash SHA-1 da chave pública da AC titular do certificado
3. *Key Usage*, crítica: somente os bits *keyCertSign* e *CRLSign* estão ativados
4. *Certificate Policies*, não crítica:

   - o campo *policyIdentifier* deve conter os OIDs das PCs que a AC Subsequente, titular docertificado, implementa;
   - o campo *policyQualifiers* deve conter o endereço Web da DPC da AC: http://ac.e-notariado.org.br/policies/cnb.pdf

5. *basicConstraints*, crítica: contém o campo *CA=True* e, para ACs subsequentes, o campo *Path Length Constraint=0*
6. *CRL Distribution Points*, não crítica: contém o endereço Web onde se obtém a LCR da AC:
   - http://ac.e-notariado.org.br/crls/ac-cnb.crl
   - http://ac.e-notariado.com.br/crls/ac-cnb.crl

7. *Authority Information Access*, não crítica, contém:
   - Endereço web onde se obtém o certificado do emissor (certificado único codificado em DER):
     - http://ac.e-notariado.org.br/certs/ac-cnb.cer
     - http://ac.e-notariado.com.br/certs/ac-cnb.cer
   - Endereço web da consulta ao protocolo Online Certificate Status Protocol (OCSP):
     - http://ac.e-notariado.org.br/ocsp/cnb
     - http://ac.e-notariado.com.br/ocsp/cnb

8. *Subject Alternative Name*, não crítica: contém o código do cartório

b) Identificadores de algoritmos

Os certificados de AC deverão ser assinados com o uso do algoritmo sha512WithRSAEncryption.

c) Formatos de nomes

Os nomes da cadeia de certificação do e-notariado da AC titular de certificado, constante do campo "*Subject*", deverá adotar o "*Distinguished Name*" (DN) do padrão ITU X.500/ISO 9594, como exemplo, da seguinte forma:

Raiz:
C = **BR**
O = **Colégio Notarial do Brasil**
OU = **Colégio Notarial do Brasil – Conselho Federal – CNB-CF**
CN = **AC Raiz do e-notariado**

AC CNB:
C = **BR**
O = **Colégio Notarial do Brasil**
OU = **Colégio Notarial do Brasil – Conselho Federal – CNB-CF**
CN = **AC Colégio Notarial do Brasil**

ACs das serventias extrajudiciais:
C = **BR**
PostalCode = ***<CEP>***
S = ***<estado>***
L = ***<cidade>***
STREET = ***<logradouro> <número>***
O = **Colégio Notarial do Brasil**
OU = ***<Código Nacional de Serventia>***
CN = ***<nome fantasia que identifique a serventia>***

d) Configurações de nomes

As configurações aplicáveis para os nomes dos titulares de certificado emitidos pela AC são as seguintes:

1. São admitidos sinais de acentuação, trema ou cedilhas

2. São admitidos também sinais alfanuméricos e os caracteres especiais descritos na tabela abaixo:

Caractere	Código NBR9611 (hexadecimal)	Caractere	Código NBR9611 (hexadecimal)
(branco)	20	+	2B
!	21	,	2C
“	22	-	2D
#	23	.	2E
$	24	/	2F
%	25	:	3A
&	26	;	3B
'	27	=	3D
(	28	?	3F
)	29	@	40
*	2A	\	5C

3. Sintaxe e semântica dos qualificadores de política

   O campo *policyQualifiers* da extensão “*Certificate Policies*” deverá conter o endereço web (URL) da DPC da AC https://repositorio.e-notariado.org.br/dpc.pdf.

4. Semântica de processamento para extensões críticas

   Extensões críticas são interpretadas conforme a RFC 5280.

7.2 Perfil de LCR

a) Número de versão

As LCRs geradas pela AC implementam a versão 2 do padrão ITU X.509, de acordo com o perfil estabelecido na RFC 5280.

b) Extensões de LCR e de suas entradas

1. A AC adota as seguintes extensões de LCR definidas como obrigatórias:

   “*Authority Key Identifier*”, não crítica: contém o resumo SHA-1 da chave pública da AC; e “*CRL Number*”, não crítica: contém número sequencial para cada LCR emitida.

2. São adotadas outrossim como obrigatórias as seguintes extensões de LCR:

"*Authority Key Identifier*", não crítica: contém o resumo SHA-1 da chave pública da AC; e "*CRL Number*", não crítica: contém número sequencial para cada LCR emitida.

8. Gestão da DPC

Qualquer alteração nesta DPC da AC será submetida previamente à aprovação do Conselho Federal do CNB. Tais alterações estarão sempre disponíveis no seu repositório aqui indicado.

9. Referências

Requisitos Mínimos para as Declarações de Práticas de Certificação das Autoridades Certificadoras da ICP-Brasil. DOC-ICP-05, versão 4.2, 06 de julho de 2017.

Cloud Security Alliance Consensus Assessments Initiative (CAI): https://cloudsecurityalliance.org/download/consensus-assessments-initiative-questionnaire-v3-0-1/.

Microsoft Azure Responses to
Cloud Security Alliance Consensus Assessments Initiative Questionnaire v3.0.1: Version 1, Published March 2016.

Características Mínimas de Segurança para as AR da ICP-Brasil. DOC-ICP-03.01, versão 2.3, 08 de março de 2018.

Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework: RFC3647.

Template for a Certification Practice Statement (CPS) for the Resource PKI (RPKI): RFC7382.

A URN Namespace of Object Identifiers: RFC3061.

10. Acrônimos

LCR: Lista de certificados revogados

AN: Autoridade notarial

AC: Autoridade certificadora

AR: Autoridade de registro

IANA: Internet Assigned Number Authority

PC: Política de certificação

DPC: Declaração de práticas de certificação

https: protocolo "http" seguro

CN: Common Name

DN: Distinguished Name

RSA: Algoritmo Rivest-Shamir-Adleman

ECC: Criptografia de Curvas Elípticas (Elliptic Curves Cryptography)

HSM: Hardware Security Modules

FIPS: Federal Information Processing Standards

RFC: Request for Comments

ITU: International Telecommunication Union

SHA: secure hash algorithm

OID: object identifier

