



BOLETIM OFICIAL

SUMÁRIO

CONSELHO DE MINISTROS:

Decreto-Regulamentar nº 18/2007:

Regulamenta o Decreto-Lei nº 33/2007, de 24 de Setembro, que regula o uso da assinatura electrónica, o reconhecimento da sua eficácia jurídica, a actividade de certificação, bem como a contratação electrónica.

Resolução nº 46/2007:

Autoriza a alienação directa de 50% do prédio urbano nº 11968, situado em Alto Santo António, cidade do Mindelo, aos legítimos herdeiros do Sr. Pedro Neves e Sr.ª Etelvina Gomes Sant'Ana Neves.

CONSELHO DE MINISTROS

Decreto-Regulamentar nº 18/2007

de 24 de Dezembro

Com a aprovação do Decreto-Lei nº 33/2007, de 24 de Setembro, que regula o uso da assinatura electrónica, o reconhecimento da sua eficácia jurídica, a actividade de certificação, bem como a contratação electrónica, urge regulamentar, o presente diploma que visa aprovar as normas de carácter técnico e de segurança exigíveis às entidades certificadoras que emitem certificados qualificados, assim como alguns aspectos específicos relacionados com a credenciação das entidades certificadoras.

Prevê-se que, no exercício da sua actividade, a entidade certificadora utilize processos, sistemas e produtos relacionados com as assinaturas electrónicas de acordo com as melhores práticas internacionais existentes para com a actividade de certificação, nomeadamente, as normas e standards da União Internacional das Telecomunicações (UIT), as normas desenvolvidas no âmbito da Iniciativa Europeia de Normalização da Assinatura Electrónica (*European Electronic Signature Standardisation Initiative*, ou EESSI), publicadas pelo Instituto Europeu de Normalização para as Telecomunicações (*European Telecommunications Standards Institute*, ou ETSI), ou pelo Comité Europeu de Normalização (*Comité Européen de Normalisation*, ou CEN).

Aprovam-se regras precisas relativas aos vários serviços de certificação prestados pela entidade certificadora, como o registo, emissão, distribuição, gestão de revogação e fornecimento de dispositivos seguros de criação de assinaturas e validação cronológica, bem como o respectivo regime de subcontratação.

Prevêem-se ainda normas específicas relativas aos direitos e obrigações da entidade certificadora e dos requerentes e titulares dos certificados e estabelecem-se requisitos operacionais e de gestão, onde se incluem exigências particulares relativas à segurança, política de pessoal, auditorias, cessação da actividade e arquivo de informação.

Compreendendo o âmbito de aplicação do diploma todas as entidades certificadoras que emitem certificados qualificados, entidades essas que podem vir a solicitar a credenciação, prevê-se ainda em sede de regulamentação algumas exigências específicas para as entidades credenciadas que se prendem essencialmente com o reforço das garantias exigíveis face ao valor probatório que é conferido às assinaturas electrónicas emitidas por entidades certificadoras credenciadas.

Neste contexto e no âmbito da demonstração dos meios técnicos e humanos exigíveis às entidades certificadoras que solicitem credenciação junto da autoridade credenciadora, é exigida avaliação prévia da conformidade dos processos e dos componentes técnicos que utiliza no exercício da sua actividade de certificação com os requisitos técnicos e de segurança estabelecidos, efectuada por organismos acreditados, ficando sujeita a atribuição de credenciação à apresentação dos respectivos relatórios de avaliação e certificados de conformidade.

Estabelecendo o presente diploma requisitos de natureza essencialmente técnica, sem prejuízo da neutralidade das tecnologias assumida pelo Decreto-Lei nº 33/2007, de 24 de Setembro, os requisitos técnicos e de segurança ora estabelecidos estão baseados na utilização de criptografia assimétrica (criptografia de chave pública) como suporte das assinaturas electrónicas.

A actual solução de regulamentação de utilização da criptografia de chave pública não prejudica a necessária revisão das normas do presente diploma quando tal apareça justificado pela evolução da tecnologia que venha a verificar-se neste domínio.

Foi ouvida a Agência Nacional das Comunicações, ANAC.

Assim:

Ao abrigo do disposto no artigo 89º do Decreto-Lei nº 33/2007, de 24 de Setembro e,

No uso da faculdade conferida pela alínea b) do artigo 204º da Constituição, o Governo decreta o seguinte:

CAPÍTULO I

Disposições Gerais

Artigo 1.º

Objecto e âmbito

1. O presente diploma regula o Decreto-Lei n.º 33/2007, de 24 de Setembro, que regula o uso da assinatura electrónica, o reconhecimento da sua eficácia jurídica, a actividade de certificação, bem como a contratação electrónica.

2. Do presente diploma constam, designadamente, as regras técnicas e de segurança aplicáveis às entidades certificadoras na emissão de certificados qualificados destinados ao público.

Artigo 2.º

Definições

Para os efeitos do presente diploma, valem as definições constantes no artigo 3º do Decreto-Lei nº 33/2007, bem como as que se seguem:

- a) Entidade de registo ou unidade de registo, entidade que por via do estabelecimento de um acordo com uma entidade certificadora, esta delega a prestação de serviços de identificação e registo de utilizadores, bem como a gestão de pedidos de solicitação e de revogação de certificados;
- b) Validação cronológica ou estampado cronológico (*Time Stamping*), Constatação da data e hora de um documento electrónico mediante processos criptográficos, para datar os documentos de forma objectiva;
- c) Matérias classificadas, aquelas de carácter confidencial e cujo acesso é limitado a determinadas pessoas que estejam habilitadas com a adequada credencial de segurança pessoal, emitida pelas respectivas autoridades competentes, nos termos da lei;
- d) Dados de activação, Valores de dados, que não sejam chaves criptográficas, necessários para operar módulos criptográficos e que necessitam ser protegidos.

Artigo 3.º

Normas técnicas

1. A entidade certificadora deve utilizar obrigatoriamente, no exercício da sua actividade, processos, sistemas e produtos relacionados com as assinaturas electrónicas em conformidade com o disposto no presente diploma e com normas internacionais, tais como:

- a) As desenvolvidas no âmbito das normas da UIT, da Organização Internacional para a Padronização (*International Standard Organization*, ISO) e da Iniciativa Europeia de Normalização da Assinatura Electrónica (EESSI);
- b) Outras largamente reconhecidas como aplicáveis a produtos de assinatura electrónica.

2. A autoridade credenciadora publica, em aviso, na II Série do *Boletim Oficial*, as listas das normas a que se refere o número anterior.

3. As normas a que se refere a alínea a) do n.º 1 são as aprovadas pela autoridade credenciadora, que publica na II Série do *Boletim Oficial* as respectivas referências.

4. As normas previstas no n.º 1, relativas a processos, sistemas e produtos, aplicam-se a:

- a) Serviços e processos das entidadesificadoras respeitantes à gestão da infra-estrutura de chave pública, à gestão da segurança da informação e à gestão do ciclo de vida dos certificados qualificados;
- b) Sistemas de informação utilizados na emissão e gestão dos certificados qualificados;
- c) Módulos criptográficos para operações de assinatura;
- d) Aplicações de criação e de verificação de assinaturas;
- e) Dispositivos seguros de criação de assinatura;
- f) Serviços de validação cronológica.

5. Sempre que estejam envolvidas matérias classificadas, aplicam-se as regras de credenciação de segurança de matérias classificadas e respectiva credenciação, da competência da Agência Nacional das Comunicações (ANAC).

Artigo 4.º

Avaliação da conformidade

1. A conformidade com o disposto no artigo anterior dos processos, sistemas e produtos relacionados com as assinaturas electrónicas qualificadas é certificada, quando exigido, nos termos do presente diploma, pela ANAC.

2. A avaliação da conformidade dos produtos de assinatura electrónica qualificada é efectuada segundo os critérios comuns para a verificação e avaliação da segurança nas tecnologias da informação, para os níveis de avaliação de segurança e grau de robustez exigidos nas normas, especificações e outra documentação técnica aplicável nos termos do artigo 3.º.

3. Do certificado de conformidade referente à segurança dos produtos constam, obrigatoriamente:

- a) Os requisitos a que a certificação se aplica e em que plataforma foram testados;

b) Os algoritmos e parâmetros utilizados e respectivo prazo de validade;

c) O nível para que os produtos foram testados e o respectivo grau de robustez.

4. A conformidade das aplicações de criação e verificação de assinaturas e de validação cronológica pode ainda ser demonstrada através de declaração do respectivo fabricante do produto.

5. A declaração a que se refere o número anterior é emitida de acordo com os documentos orientadores de avaliação de conformidade (*Conformity Assessment Guidance*, EESSI) do CEN (*Comité Européen de Normalisation*), para o produto em causa, e contém a identificação do fabricante, do produto, dos requisitos com os quais garante a conformidade e das disposições da norma relativamente às quais esta se verifica.

Artigo 5.º

Procedimentos para a modificação de normas técnicas

1. A ANAC pode por sua iniciativa ou, a pedido dos interessados iniciar o procedimento para a elaboração e fixação de normas, com o objectivo de formular e modificar as normas estabelecidas pelo presente diploma.

2. Para o disposto no número anterior, a ANAC informa aos interessados sobre a abertura do procedimento da reformulação de normas e submete-a à consulta pública, nos termos do disposto no presente diploma.

3. Caso necessário, a ANAC pode fixar conjuntos alternativos de normas técnicas para a prestação de serviços com o objectivo de permitir o uso de diversas tecnologias e meios electrónicos, em conformidade com a lei e com o presente diploma.

Artigo 6.º

Subcontratação

1. A entidade certificadora pode subcontratar a prestação de serviços de certificação e o fornecimento dos respectivos componentes, incluindo o serviço de emissão de certificados, desde que a chave utilizada para gerar os certificados seja sempre identificada como pertencendo à entidade certificadora e que esta assuma e mantenha a inteira responsabilidade pelo cumprimento de todos os requisitos exigidos no presente diploma.

2. A entidade certificadora, quando solicitar ou utilizar os serviços ou as infraestruturas tecnológicas disponibilizados por terceiros, deve prever dentro do seu Plano de Contingência os procedimentos a seguir nas situações de interrupção destes serviços, de modo a permitir a continuidade da prestação de serviços de certificação sem nenhum prejuízo para os titulares.

3. O contrato celebrado entre a entidade certificadora e o prestador de serviços ou as infraestruturas, deve garantir a execução dos procedimentos mínimos sobre a cessação das actividades, constantes nas normas complementares elaboradas pela ANAC. A entidade certificadora credenciada ou que tenha iniciado o procedimento para obter a credenciação, deve fornecer à ANAC toda a informação estipulada no contrato, relacionada à prestação de serviços de certificação e à implementação do Plano de Cessação das Actividades e do Plano de Contingência.

4. É obrigatoriamente reduzido a escrito o contrato referido no numero anterior, onde se estabelecem as obrigações das partes e se identificam as funções da entidade certificadora prestadas pelo subcontratado.

5. A entidade certificadora é responsável por todos os serviços de certificação prestados por terceiros por ela subcontratados, designadamente os de registo, emissão, distribuição, gestão de revogação, fornecimento de dispositivos seguros de criação de assinaturas e validação cronológica.

CAPÍTULO II

Actividade da entidade certificadora

Secção I

Declaração de práticas e política de certificado

Artigo 7.º

Declaração de práticas de certificação

1. A entidade certificadora emite uma declaração de práticas de certificação em que constam os procedimentos utilizados para cumprimento dos requisitos identificados nas políticas de certificado, com a qual todos os serviços de certificação prestados têm de estar conformes, contendo, entre outros, os seguintes elementos:

- a) Descrição da estrutura de certificação;
- b) Descrição da infra-estrutura operacional;
- c) Procedimentos de validação da identidade e de outros dados pessoais e profissionais de requerentes e titulares;
- d) Procedimentos operacionais;
- e) Controlos de segurança física, de processos e de pessoal;
- f) Disposições sobre a emissão, utilização, actualização, renovação, suspensão e revogação dos certificados;
- g) Responsabilidades e obrigações do requerente, do titular, da entidade certificadora e dos destinatários;
- h) Disposições relativas à cessação de actividade;
- i) Método de validação cronológica utilizado;
- j) Período de validade da declaração de práticas de certificação.

2. A ANAC publica o manual contendo a estrutura da declaração de práticas de certificação que é revista, pelo menos uma vez por ano, e disponibilizado permanentemente, por via electrónica, para consulta dos requerentes, titulares e destinatários.

Artigo 8.º

Políticas de certificado

1. A ANAC define o conteúdo mínimo das políticas de certificado, de acordo com os padrões internacionais vigentes e legislação nacional e devem ainda conter, entre outras, as seguintes informações:

- a) Identificação da entidade certificadora;
- b) Política de administração dos certificados e detalhes dos serviços;

- c) Procedimentos de verificação de identidade dos titulares dos certificados;
- d) Obrigações da entidade certificadora, da unidade de registo e dos titulares dos certificados;
- e) Tratamento da informação administrada pelos titulares e observação da confidencialidade dessa informação;
- f) Alcance e limites da responsabilidade admitidos.

2. Para além do disposto no numero anterior, a entidade certificadora indica em cada certificado, através de um identificador único, a política que estabelece os termos, condições e âmbito de utilização do certificado e os requisitos que a declaração de práticas de certificação está obrigada a conter.

3. As políticas de certificado devem ser publicadas e actualizadas, de forma permanente, e devem estar acessíveis ao público, por via electrónica, e no sitio da *Internet* das entidades certificadora e credenciadora, respectivamente.

Secção II

Emissão e gestão das chaves

Artigo 9.º

Emissão das chaves da entidade certificadora

Os pares de chaves utilizados pela entidade certificadora na prestação de serviços de certificação são gerados:

- a) Num ambiente fisicamente seguro de acordo com as exigências estabelecidas no plano de segurança previsto no artigo 31.º e por pessoal que cumpra os requisitos estabelecidos no artigo 33.º;
- b) Recorrendo a um algoritmo e comprimento de chave apropriado, de acordo com o disposto no artigo 13.º;
- c) Recorrendo a um dispositivo seguro de criação de assinatura certificado nos termos do artigo 4.º;
- d) Por um mínimo de dois trabalhadores presentes física e conjuntamente no local.

Artigo 10.º

Gestão das chaves da entidade certificadora

1. As chaves privadas da entidade certificadora são:
 - a) Mantidas num dispositivo seguro de criação de assinatura e certificado nos termos do artigo 4.º;
 - b) Objecto de cópia de segurança, armazenada e reposta por pessoal autorizado e em ambiente físico seguro, de acordo com o procedimento descrito no plano de segurança, em condições de protecção igual ou superior às chaves em utilização;
 - c) Únicas e confidenciais durante a geração e a transmissão para um dispositivo seguro de criação de assinatura, não podendo ser armazenadas fora desse dispositivo;
 - d) Utilizadas dentro de áreas físicas seguras de acordo com o estabelecido no plano de segurança;
 - e) Utilizadas dentro do seu período de validade.

2. A entidade certificadora não pode usar as chaves privadas utilizadas na emissão de certificados e listas de revogação para outra finalidade.

3. No termo do seu período de validade, a cópia da chave privada é destruída de modo irreversível ou arquivada de forma a não poder ser reutilizada.

4. Na gestão das suas chaves, é da responsabilidade da entidade certificadora:

- a) Assegurar a integridade e autenticidade das chaves públicas e de qualquer parâmetro a elas associado durante a distribuição, assim como estabelecer um processo que permita autenticar a sua origem;
- b) Manter organizado um arquivo das chaves públicas, após o termo do seu período de validade;
- c) Garantir a segurança e integridade do equipamento criptográfico durante a sua vida útil e assegurar que o mesmo não é acedido ou alterado por pessoal não autorizado;
- d) Garantir que as chaves privadas armazenadas no equipamento criptográfico são destruídas quando da sua retirada de funcionamento;
- e) Assegurar que as operações de gestão das chaves privadas, de manipulação de dispositivos criptográficos e de informação do estado de suspensão e ou revogação são efectuadas por um mínimo de dois trabalhadores em simultâneo.

Artigo 11.º

Emissão das chaves de titulares

A entidade certificadora, na emissão das chaves para titulares, assegura que:

- a) O par de chaves do titular é gerado recorrendo a um algoritmo criptográfico apropriado, de acordo com o disposto no artigo 13.º;
- b) A chave privada entregue ao titular para criação de assinaturas é armazenada de forma segura antes da sua entrega, assegurando-se que a sua integridade não é comprometida;
- c) A chave privada entregue ao titular para criação de assinaturas é distinta da chave entregue para utilização em outras funções;
- d) Não é efectuada cópia de segurança nem de arquivo da chave privada do titular para criação de assinaturas.

Artigo 12.º

Dispositivos seguros de criação de assinaturas

A entidade certificadora, sempre que forneça dispositivos seguros de criação de assinaturas, assegura que:

- a) O dispositivo é preparado, armazenado e distribuído de forma segura e está certificado em conformidade com o disposto no artigo 4.º;
- b) No caso de o dispositivo ter associados dados de activação, estes são fornecidos de forma separada.

Artigo 13.º

Algoritmos criptográficos

Os algoritmos criptográficos utilizados na prestação de serviços de certificação e respectivos parâmetros associados são:

- a) Os constantes das listas publicadas pela ANAC na II série do *Boletim Oficial* e no seu *web site*;
- b) Os constantes em especificações técnicas emitidas para algoritmos e parâmetros, de acordo com a alínea a) do n.º 1 do artigo 3.º, quando não tenha sido publicada a lista a que se refere a alínea anterior.

Secção III

Validação cronológica

Artigo 14.º

Serviço de validação cronológica

1. A entidade certificadora assegura que a data e a hora da emissão, suspensão e revogação dos certificados possam ser determinadas através de serviços de validação cronológica, que ligam criptograficamente os dados com valores de tempo.

2. Nos serviços de validação cronológica, garante-se que:

- a) A origem e a validade de cada pedido de validação cronológica são determinadas;
- b) O pedido utiliza um algoritmo criptográfico reconhecido nos termos do artigo 13.º;
- c) A hora utilizada é definida a partir do tempo universal coordenado (*Coordinated Universal Time-UTC*) e certificada por um instituto nacional de medida, com incerteza inferior a 100 milissegundos (ms);
- d) Os dados incluídos no pedido são devolvidos sem alteração;
- e) A chave privada utilizada na assinatura da prova de validação cronológica:
 - i) É proibida a sua utilização para outra finalidade;
 - ii) É gerada recorrendo a um algoritmo e comprimento de chave apropriado, reconhecido nos termos do artigo 13.º;
 - iii) É gerada e armazenada num módulo criptográfico, certificado de acordo com o disposto no artigo 4.º;
- f) Em cada prova de validação cronológica são incluídos:
 - i) O valor tempo certificado;
 - ii) Um identificador único;
 - iii) Um indicador único da política de certificação cronológica adoptada;
 - iv) O grau de exactidão do valor tempo utilizado sempre que aquele seja superior ao indicado na política adoptada;
- g) A prova de validação cronológica é assinada criptograficamente antes da devolução da resposta ao pedido;
- h) É excluída da prova de validação cronológica, a identificação da entidade que a solicitou.

3. Os dados relacionados com a geração e a gestão das chaves utilizadas na validação cronológica, incluindo os dados associados à certificação da hora por um instituto nacional de medida, são registados e arquivados por um período mínimo de 20 anos.

Secção IV

Certificados qualificados

Artigo 15.º

Pedido

1. A entidade certificadora assegura que o pedido de emissão de certificado é efectuado por documento electrónico ao qual é aposta uma assinatura electrónica qualificada ou por documento escrito sobre suporte de papel, com assinatura autografada, e que o mesmo é requerido em obediência ao disposto nos artigos 16.º e 17.º.

2. A entidade certificadora verifica a identidade do requerente, por meio legalmente reconhecido, verificando, no caso de o pedido ser subscrito para outrem, os poderes bastantes do requerente para a referida subscrição.

Artigo 16.º

Pedido de emissão de certificado para pessoa singular

1. O pedido de emissão, quando requerido pela pessoa singular a constar como titular do certificado, contém, entre outros, os seguintes elementos:

- a) Nome completo;
- b) Indicação de eventual pseudónimo a constar como titular;
- c) Número do bilhete de identidade, data e entidade emitente ou qualquer outro elemento que permita a identificação inequívoca;
- d) Endereço e outras formas de contacto;
- e) Eventual indicação de uma qualidade específica em função da utilização a que este se destinar;
- f) Indicação quanto ao uso do certificado ser ou não restrito a determinados tipos de utilização, bem como eventuais limites do valor das transacções para as quais o certificado é válido;
- g) Outras informações relativas a poderes de representação, à qualificação profissional ou a outros atributos.

2. No caso de o pedido de emissão ser requerido por outrem que não a pessoa singular a constar como titular do certificado, o mesmo, para além dos elementos referidos no número anterior, contém, consoante seja requerido por pessoa singular ou colectiva, os seguintes elementos referentes ao requerente:

- a) Nome ou denominação legal;
- b) Número do bilhete de identidade, data e entidade emitente, ou qualquer outro elemento que permita a identificação inequívoca, ou número de pessoa colectiva;
- c) Residência ou sede;
- d) Objecto social, nome dos titulares dos corpos sociais e de outras pessoas com poderes para a obrigarem e número de matrícula na conservatória do registo comercial;
- e) Endereço e outras formas de contacto.

3. O pedido de inclusão no certificado de dados pessoais da pessoa singular a constar como seu titular tem de ser expressamente autorizado pela própria.

4. Na situação prevista no n.º 2 do presente artigo, o pedido é ainda acompanhado da declaração da pessoa singular a constar como titular do certificado de que se obriga ao cumprimento das obrigações enquanto titular.

Artigo 17.º

Pedido de emissão de certificado para pessoa colectiva

1. O pedido de emissão, quando requerido pela pessoa colectiva a constar como titular do certificado, é subscrito pelos seus representantes legais e contém, entre outros, os seguintes elementos:

- a) Denominação legal;
- b) Número de pessoa colectiva, sede, objecto social, nome dos titulares dos corpos sociais e de outras pessoas com poderes para a obrigarem e número de matrícula na conservatória do registo comercial;
- c) Nome completo, número do bilhete de identidade ou qualquer outro elemento que permita a identificação inequívoca das pessoas singulares que estatutária ou legalmente a representam;
- d) Endereço e outras formas de contacto;
- e) Indicação quanto ao uso do certificado ser ou não restrito a determinados tipos de utilização, bem como eventuais limites do valor das transacções para as quais o certificado é válido;
- f) Eventual referência a uma qualidade específica, em função da utilização a que o certificado estiver destinado;
- g) Outras informações relativas a poderes de representação, à qualificação profissional ou a outros atributos.

2. No caso de o pedido de emissão ser requerido por outrem que não a pessoa colectiva a constar como titular do certificado, ao mesmo, para além do disposto no número anterior, aplica-se, com as devidas adaptações, o previsto nas alíneas a) a e) do n.º 2 e no n.º 4, ambos do artigo 16.º.

Artigo 18.º

Registo

1. A entidade certificadora recebe o pedido, valida os seus dados e procede ao registo.

2. Do registo constam:

- a) A identificação da entidade que recebeu o pedido;
- b) Os dados constantes do pedido;
- c) Os documentos de prova que acompanham o pedido;
- d) A descrição dos métodos utilizados na verificação do pedido;
- e) A identificação do contrato referido no artigo 29.º;
- f) Outra informação útil à utilização do certificado.

3. Os dados do registo não podem ser utilizados para outros fins diferentes dos necessários à utilização do certificado.

4. A entidade certificadora mantém em arquivo, pelo prazo mínimo de 20 anos, os dados constantes do registo, os documentos que os comprovam e um exemplar do contrato.

5. Caso as entidades certificadoras cessem as suas actividades, devem transferir o arquivo disposto no número anterior para outra entidade certificadora ou para uma empresa especializada em arquivar dados electrónicos e que esteja devidamente credenciada pela ANAC. Esta situação deve constar tanto no registo da entidade certificadora como na política de certificação aprovada pela ANAC.

Artigo 19.º

Emissão

1. A entidade certificadora garante que, durante o processo de emissão, os dados de registo do titular são tratados de forma segura e que a chave pública constante do certificado está relacionada com a correspondente chave privada do titular.

2. A entidade certificadora atribui um identificador único para cada titular, para utilização no certificado.

3. A entidade certificadora assegura a protecção da confidencialidade e integridade dos dados de registo em todos os procedimentos de emissão.

4. O termo de validade do certificado não pode ultrapassar o termo de validade dos algoritmos utilizados e respectivos parâmetros.

5. O termo de validade do certificado complementar não pode ultrapassar o termo de validade do certificado com que esteja relacionado.

6. A entidade certificadora mantém o registo dos certificados emitidos, desde a data da respectiva emissão e durante o seu período de validade, e conserva-os por um período não inferior a 20 anos a partir da data em que termina aquele prazo.

7. A entidade certificadora só emite certificado para pessoa colectiva quando está em condições de garantir que a criação da assinatura, através de dispositivo de criação de assinatura, exige a intervenção de pessoas singulares que, estatutária ou legalmente, representam a pessoa colectiva titular desse certificado.

Artigo 20.º

Conteúdo e formato

1. O certificado qualificado contém, entre outras, as seguintes informações:

- a) Nome ou denominação do titular da assinatura e outros elementos necessários para uma identificação inequívoca, ou um pseudónimo claramente identificado como tal;
- b) Nome e outros elementos necessários para uma identificação inequívoca das pessoas singulares que estatutária ou legalmente representam o titular, quando este é uma pessoa colectiva;

c) Nome e assinatura electrónica avançada da entidade certificadora, bem como a indicação do país onde se encontra estabelecida;

d) Dados de verificação de assinatura correspondentes aos dados de criação de assinatura do titular;

e) Número de série;

f) Início e termo de validade;

g) Identificadores de algoritmos utilizados na verificação de assinaturas do titular e da entidade certificadora;

h) Indicação de o uso do certificado ser ou não restrito a determinados tipos de utilização, bem como eventuais limites do valor das transacções para as quais o certificado é válido;

i) Eventual referência a uma qualidade específica do titular da assinatura, em função da utilização a que o certificado estiver destinado;

j) Indicação de que é emitido como certificado qualificado;

k) Outras informações relativas a poderes de representação, à qualificação profissional ou a outros atributos, com a menção de se tratar de informações não confirmadas, se for o caso.

2. No caso de existir um certificado complementar, é assegurada a sua ligação ao certificado com o qual se relaciona, constando obrigatoriamente do certificado complementar as seguintes informações:

a) Indicação de que se trata de um certificado complementar;

b) Referência ao certificado no qual se baseia;

c) Designação dos algoritmos utilizados na verificação da assinatura da entidade certificadora;

d) Número de série do certificado complementar;

e) Identificação da entidade certificadora e país onde se encontra estabelecida;

f) Outras informações relativas a poderes de representação, à qualificação profissional ou a outros atributos, com a menção de se tratar de informações não confirmadas, se for o caso;

g) Assinatura electrónica avançada da entidade certificadora.

3. O formato dos certificados obedece às especificações técnicas emitidas pelo ETSI ou outras equivalentes reconhecidas nos termos do artigo 3.º.

4. A entidade certificadora assegura os mecanismos necessários para que a hierarquia de certificação seja estabelecida e os certificados emitidos possam ser reconhecidos.

5. A ANAC pode modificar os critérios para os conteúdos mínimos dos certificados, de acordo com a evolução tecnológica.

Artigo 21º

Incorporação de conteúdos adicionais

1. As entidades certificadoras devem introduzir nos certificados que emitem, os dados mencionados no número 1 do artigo anterior, bem como os que venham a ser estipulados pela ANAC.

2. Os atributos adicionais que as entidades certificadoras introduzem com a finalidade de definir limites ao uso do certificado, não devem dificultar ou impedir a leitura dos dados assinalados no número 1 do artigo anterior, nem o seu reconhecimento por terceiros.

Artigo 22º

Reconhecimento de certificado estrangeiro

1. As entidades certificadoras podem reconhecer os certificados emitidos por entidades certificadoras estrangeiras, sob a sua responsabilidade.

2. Para os efeitos do número anterior, as entidades certificadoras devem demonstrar à ANAC que os certificados por ela a serem reconhecidos, foram emitidos por um prestador de serviços de certificação não registado em Cabo Verde e que cumpra com as disposições referentes aos conteúdos mínimos dos certificados, estabelecidos na lei, no presente diploma e nas normas complementares emitidas pela ANAC.

3. A ANAC verifica o cumprimento das disposições legais e regulamentares e publica a informação sobre o reconhecimento no registo da entidade certificadora. Caso a entidade certificadora não observar o cumprimento dos dispositivos legais e regulamentares para o reconhecimento de certificados estrangeiros, a ANAC, mediante fundamentação, pode indeferir o pedido de reconhecimento.

4. Uma vez realizado o reconhecimento, a entidade certificadora, num prazo de 3 (três) dias úteis, deve comunicar tal situação à ANAC e publicar imediatamente, num prazo máximo de 24 (vinte e quatro) horas, no registo dos certificados da entidade certificadora.

5. O reconhecimento de certificados deve estar declarado nas práticas de certificação.

6. As entidades certificadoras estrangeiras devem obedecer o plano de segurança disposto no artigo 31º do presente diploma.

Artigo 23º

Distribuição

A entidade certificadora, na distribuição de certificado, deve utilizar sistemas seguros que permitam a sua conservação e disponibilização para efeitos de verificação, assegurando que:

- a) O certificado é disponibilizado, integralmente, ao titular para quem foi emitido;
- b) O certificado só é publicamente disponibilizado com o consentimento do titular;

c) São transmitidas ao destinatário as condições a que este se obriga, designadamente de:

- i) Verificar em cada comunicação ou transacção a validade, suspensão ou revogação do certificado;
- ii) Verificar se o certificado é utilizado de acordo com as condições emitidas pela entidade certificadora.

Artigo 24º

Renovação e actualização

Na renovação de certificados ou actualização devida a mudança de atributos do titular, a entidade certificadora deve:

- a) Verificar se toda a informação utilizada para comprovar a identidade e atributos do titular ainda se mantém válida;
- b) Comunicar antecipadamente ao titular todas as alterações dos termos e condições de emissão do certificado;
- c) Assegurar que as chaves de assinatura sejam actualizadas antes do fim do seu período de validade e que as chaves públicas com elas relacionadas garantem, pelo menos, o mesmo nível de segurança que ofereciam no certificado inicial;
- d) Garantir que a emissão de um novo certificado, que faça uso da chave pública previamente certificada, só é efectuada se for garantida a segurança criptográfica dessa chave durante o prazo de validade do novo certificado.

Artigo 25º

Revogação e suspensão

A entidade certificadora utiliza os procedimentos de revogação e suspensão de certificados de acordo com o disposto nos artigos 68º e 69º do Decreto-Lei n.º 33/2007, e com a sua declaração de práticas de certificação e ainda assegura:

- a) Que os pedidos e informações relativos a suspensão ou revogação são processados assim que recebidos, não podendo ser superior a vinte e quatro horas o período entre a recepção e a publicitação do seu novo estado;
- b) Que o certificado só é suspenso durante o período de tempo definido no plano de segurança, que não pode ultrapassar três dias úteis, e que, findo esse período, se a suspensão não for levantada, o certificado é revogado com efeitos a partir da data da suspensão;
- c) Que as alterações no estado de validade de certificados são transmitidas ao titular;
- d) Que um certificado revogado não pode ser reutilizado;
- e) Um serviço permanentemente disponível de actualização do estado de suspensão e revogação de certificados.

Secção V

Direitos e obrigações

Subsecção I

Obrigações

Artigo 26.º

Obrigações da entidade certificadora

A entidade certificadora tem as seguintes obrigações:

- a) Comprovar, por si ou através de uma entidade de registo, a qual tenha delegado tal função, a identidade ou outro dado dos requerentes considerado relevantes para os procedimentos de verificação de identidade;
- b) Manter à disposição permanente do público as políticas de certificação e o manual de procedimentos, nos aspectos que não contenha informação confidencial, nos termos aprovados pela ANAC, para tal fim;
- c) Cumprir cabalmente com as políticas de certificação acordadas com o titular e com o constante no manual de procedimentos, considerando o incumprimento do disposto na presente alínea como falta grave;
- d) Garantir o cumprimento do acordo de prestação de serviço celebrado com o titular, relativo aos serviços para os quais solicitou autorização;
- e) Informar ao requerente de um certificado, numa linguagem clara e acessível, em língua portuguesa, sobre as características do certificado solicitado, as limitações, se houver, os preços dos serviços de certificação, uso, administração e outros associados, incluindo os encargos adicionais e as formas de pagamento, os níveis de serviço a prestar, as obrigações que o titular assume como usuário do serviço de certificação, seu endereço em Cabo Verde e os meios aos quais o titular pode recorrer para solicitar esclarecimentos e efectuar reclamações;
- f) Dispor de um serviço de atendimento permanente aos titulares de certificados e usuários, através de atendimento personalizado, via telefone ou Internet, que permita dar uma pronta resposta as informações solicitadas;
- g) Dispor de recursos financeiros adequados ao tipo de actividade de certificação que desenvolve, de acordo com os níveis de responsabilidade derivados da mesma;
- h) Garantir o acesso público, eficiente e gratuito dos titulares e usuários ao registo de certificados emitidos, suspensos, revogados, reactivados ou reconhecidos;
- i) Manter actualizados os registos de certificados emitidos, suspensos, revogados ou reactivados, por um período de quarenta (40) anos, contado a partir do encerramento, da revogação ou termino do prazo de cada certificado;
- j) Adoptar os procedimentos e medidas de seguro confiáveis, conforme estabelecido pela ANAC, para garantir que as chaves privadas dos titulares não permaneçam em seu poder nem possam ser utilizadas por terceiros nos casos em que presta serviços de geração de chaves;
- k) Informar imediatamente à ANAC nos casos de ocorrência de qualquer evento que possa comprometer a correcta prestação de serviços;
- l) Garantir a integridade da informação que mantenha sob o seu controlo;
- m) Respeitar o direito do titular do certificado e não receber publicidade de nenhum tipo por seu intermédio, salvo consentimento expresso deste;
- n) Publicar por meios electrónicos e, pelo menos, num dos jornais de maior circulação nacional o certificado de chave pública correspondente à política de certificação para a qual obteve autorização;
- o) Cumprir as normas e recomendações estabelecidas pela ANAC para a protecção de dados pessoais;
- p) Observar os requisitos estabelecidos na lei, no presente diploma e nas normas regulamentares estabelecidas pela ANAC que dispõem sobre a autorização obtida para a prestação de serviços de certificação;
- q) Quando a chave privada da entidade certificadora ou seu sistema de segurança tenha sido comprometido de forma a afectar a confiabilidade do certificado, o novo certificado deve substituir de forma gratuita aquele que deixou de ser seguro e deve cumprir os mesmos requisitos. A ANAC estabelece, nestes casos, o processo de substituição de certificados. Nas situações em que um certificado tenha deixado de ser seguro por razões atribuídas ao titular, a entidade certificadora não é obrigada a substituir o certificado;
- r) Enviar, quando solicitado pela ANAC, os relatórios sobre o estado das operações de certificação, no formato e prazo estabelecidos por esta;
- s) Responder aos pedidos de informação por parte dos usuários de certificados, no tocante a validade e alcance de um certificado emitido por ela; e
- t) Divulgar no seu *web site* as seguintes informações:
 - i) Preço dos serviços a prestar;
 - ii) Declaração de práticas de certificação;
 - iii) Termos, condições e âmbito de utilização dos seus certificados;
 - iv) Indicação de que a informação registada, necessária à utilização do certificado, não é utilizada para outro fim;

- v) Período de tempo durante o qual mantém em arquivo a informação prestada pelo requerente e a referente à utilização dos respectivos certificados;
- vi) Indicação de que, em caso de cessação da actividade, a informação referida na alínea anterior é transmitida, nos termos da lei, para outra entidade;
- vii) Os meios utilizados para resolução de conflitos;
- viii) Legislação aplicável à actividade de certificação;
- ix) Número do registo de entidades certificadoras atribuído pela autoridade credenciadora;
- x) Data e número da credenciação, se credenciada.

Artigo 27.º

Obrigações do titular

1. O titular do certificado toma as medidas necessárias a evitar danos a terceiros e a preservar a confidencialidade da informação transmitida e é obrigado a:

- a) Utilizar as chaves criptográficas dentro das limitações impostas pela respectiva política de certificado;
- b) Garantir o sigilo da chave privada;
- c) Utilizar algoritmo e comprimento de chave de acordo com o artigo 13.º, no caso de gerar as suas próprias chaves;
- d) Usar um dispositivo seguro de criação de assinatura, se a política de certificado assim o exigir;
- e) Gerar as chaves no interior do dispositivo seguro de criação de assinatura, se a política de certificado assim o exigir;
- f) Informar de imediato a entidade certificadora em caso de perda de controlo da chave privada, ou de incorrecção ou alteração da informação constante do certificado, durante o período de validade deste.

Artigo 28.º

Obrigações do requerente

1. As obrigações do requerente em nome próprio são as obrigações do titular referidas no artigo anterior.

2. Aquele que requer um certificado para outrem é responsável por informar o titular dos termos e condições de utilização dos certificados, bem como das consequências do respectivo incumprimento.

Artigo 29.º

Contrato

1. O contrato celebrado entre a entidade certificadora e o requerente deve ser reduzido a escrito, em linguagem clara e acessível, num suporte físico duradouro, e subscrito pelas partes com assinatura electrónica qualificada, quando em documento electrónico, ou com assinatura autografada, quando em suporte de papel.

2. As cláusulas do contrato celebrado entre a entidade certificadora e o requerente contêm:

- a) As obrigações da entidade certificadora resultantes do disposto nos itens i), iii), vii) e viii) da alínea t) do artigo 26.º;
- b) As obrigações do requerente referidas no artigo anterior.

3. O contrato celebrado entre a entidade certificadora e o requerente deve ser registado e arquivado pela entidade certificadora pelo prazo mínimo de 20 anos.

Subsecção II

Direitos

Artigo 30.º

Protecção do direito dos utilizadores

1. A ANAC pode elaborar normas complementares que dispõem sobre a protecção do direito dos utilizadores.

2. As entidades reguladas devem dispor de um operador para responder as chamadas telefónicas dos utilizadores 24 (vinte e quatro) horas por dia ou deve gravar electronicamente as queixas e as chamadas dos usuários. Pode ser feita a combinação de operadores e gravadoras. Nos casos em que se utilizam gravadoras, a companhia deve contactar o utilizador imediatamente ou, o mais tardar, até o próximo dia útil após a ligação.

3. As entidades reguladas devem prestar aos seus clientes, através de uma linha telefónica de acesso gratuito ou endereço electrónico, as seguintes informações:

- a) Número de inscrição no registo das entidades certificadoras;
- b) Receber e aceitar pedidos de revogação e de suspensão de certificados;
- c) Taxas e impostos aplicáveis;
- d) Data de expiração do prazo da licença, caso exista; e
- e) Consultas ou outra informação relevante para a utilização de serviço.

CAPÍTULO III

Requisitos operacionais e de gestão

Artigo 31.º

Implementação da segurança

1. A entidade certificadora assegura que as instalações, procedimentos, pessoal, equipamentos e produtos obedecem a todas as normas de segurança aplicáveis ao exercício da sua actividade, devendo, designadamente:

- a) Ter um plano de segurança implementado de acordo com a norma internacional ISO/IEC 17799;
- b) Utilizar sistemas e produtos fiáveis, protegidos contra modificações;
- c) Ter um auditor de segurança;
- d) Elaborar relatórios de incidentes causados por falhas de segurança ou operação e desencadear atempadamente as respectivas medidas correctivas.

2. A entidade certificadora assegura que os procedimentos utilizados para garantir os níveis de segurança operacional, física e dos sistemas, de acordo com as normas adoptadas, se encontram documentados, implementados e actualizados, e mantém um inventário de bens com a respectiva classificação, de forma a caracterizar as suas necessidades de protecção.

3. A ANAC procede a uma avaliação de segurança da entidade certificadora, antes do início de actividade, sempre que estiverem envolvidas matérias classificadas.

Artigo 32.º

Plano de segurança

1. O plano de segurança contém, no mínimo:

- a) Descrição da estrutura organizacional e funcional e da actividade de certificação;
- b) Especificação dos processos de avaliação e de garantia da idoneidade e capacidade técnica do pessoal em funções;
- c) Especificação dos requisitos de segurança física, lógica e operacional;
- d) Requisitos de disponibilidade da informação, incluindo redundância de sistemas e planos de contingência;
- e) Indicação do período de tempo máximo para actualização do estado de revogação e ou suspensão de certificados;
- f) Indicação do período de tempo máximo em que um certificado se pode manter no estado de suspensão;
- g) Requisitos de protecção da informação, incluindo distinção dos vários níveis de segurança e perfis de acesso implementados;
- h) Definição das funções que conferem acesso aos actos e instrumentos de certificação, respectivos requisitos de segurança e perfis de acesso;
- i) Descrição dos produtos de assinatura electrónica utilizados e identificação das respectivas certificações de conformidade;
- j) Descrição e avaliação de outros riscos de segurança;
- k) Indicação dos responsáveis pela sua implementação;
- l) Indicação do processo de revisão periódica estabelecido.

2. No caso de estarem envolvidas matérias classificadas, o plano de segurança deve obter a aprovação da ANAC.

Artigo 33.º

Plano de contingência

1. A entidade certificadora, para fazer face à eventual ocorrência de desastres ou incidentes que ponham em

causa o funcionamento normal de prestação de serviços de certificação, implementa um plano de contingência que contemple:

- a) A possibilidade de adulteração ou acesso não autorizado às chaves privadas da entidade certificadora;
- b) Um planeamento que assegure a retoma das operações num espaço de tempo previamente definido;
- c) A forma como requerentes, titulares, destinatários e outras entidades certificadoras com as quais exista acordo são informados de qualquer acontecimento que ponha em causa a utilização segura de certificados e do estado de revogação;
- d) A manutenção da integridade e autenticidade da informação relativa ao estado de revogação.

2. A entidade certificadora assegura que os serviços de distribuição, revogação e estado de revogação de certificados se mantêm permanentemente disponíveis em caso de acidente, bem como procedimentos que permitam a continuação dos serviços em sistemas de recuperação alternativos, e garante que a migração dos sistemas primários para os sistemas de recuperação não põe em risco a segurança dos sistemas.

3. No caso de estarem envolvidas matérias classificadas, o plano de contingência deve obter a aprovação da ANAC.

Artigo 34.º

Política de pessoal

1. A entidade certificadora adopta regras de selecção e contratação do seu pessoal que reforçam e respeitam as disposições de segurança exigidas para o exercício da sua actividade, nomeadamente que:

- a) Para funções de gestão de infra-estruturas de chave pública, emprega pessoal especializado com conhecimentos específicos em tecnologia de assinatura electrónica e com conhecimentos de comportamentos de segurança;
- b) Todo o pessoal que desempenha funções relacionadas com os processos de certificação está livre de conflitos de interesse que possam prejudicar a sua imparcialidade;
- c) As funções relacionadas com os processos de certificação não são desempenhadas por pessoas que se encontram em situação indicadora de inidoneidade;
- d) No âmbito da sua estrutura organizativa contempla, pelo menos, os seguintes cargos e funções necessários à operação dos sistemas:

- i) Administrador de sistemas: autorizado a instalar, configurar e manter os sistemas, tendo acesso controlado a configurações relacionadas com a segurança;

- ii) Operador de sistemas: responsável por operar diariamente os sistemas, autorizado a realizar cópias de segurança e reposição de informação;
- iii) Administrador de segurança: responsável pela gestão e implementação das regras e práticas de segurança;
- iv) Administrador de registo: responsável pela aprovação da emissão, suspensão e revogação de certificados;
- v) Auditor de sistemas: autorizado a monitorizar os arquivos de actividade dos sistemas.

2. Os postos de trabalho ou funções referidos nas subalíneas i), iii) e v) da alínea d) do número anterior não podem ser assegurados pela mesma pessoa.

4. No caso de conter matéria classificada, a política de pessoal deve obter aprovação por parte da ANAC.

Artigo 35.º

Auditorias

1. O auditor de segurança é uma pessoa singular ou colectiva, independente da entidade certificadora, de reconhecida idoneidade, experiência e qualificações comprovadas na área da segurança de informação, na execução de auditorias de segurança e na utilização da norma ISO/IEC 17799, devidamente credenciada pela ANAC.

2. A entidade certificadora comprova através do relatório anual de auditoria de segurança, efectuada por auditor de segurança acreditado, que realizou uma avaliação de riscos e identificou e implementou os controlos necessários à segurança da informação.

3. As auditorias de segurança são efectuadas tendo por base a norma ISO/IEC 17799, devendo o respectivo relatório de auditoria ser enviado à autoridade credenciadora até 31 de Março de cada ano civil.

O auditor de segurança garante que os membros da sua equipa não actuam de forma parcial ou discriminatória e não prestaram serviços de consultoria à entidade certificadora nos últimos três anos nem mantêm com esta qualquer outro acordo ou vínculo contratual.

4. Em caso de subcontratação, o auditor deve:

- a) Informar previamente a entidade certificadora e obter a concordância desta para a subcontratação;
- b) Garantir a existência de contrato reduzido a escrito no qual estão claramente identificadas as funções subcontratadas e em que se estabelecem as obrigações entre as partes, nomeadamente no que respeita à confidencialidade e à independência de interesses comerciais ou outros, assim como à inexistência de qualquer tipo de vínculo com a entidade certificadora a ser auditada;
- c) Garantir que está apto a comprovar a competência técnica, idoneidade e isenção da entidade

subcontratada, bem como a sua credenciação de segurança pela Agência ANAC, nos casos legalmente exigíveis, e que esta cumpre o disposto no número anterior;

- d) Assumir a completa responsabilidade pelo trabalho subcontratado e pelo relatório final da auditoria.

Artigo 36.º

Cessação da actividade

1. Em caso de cessação de actividade, a entidade certificadora garante a continuidade da informação relativa a processos de certificação e, em particular, a manutenção do arquivo da informação necessária ao fornecimento de meios de prova em processos judiciais, nos termos do artigo seguinte.

2. Antes de cessar a sua actividade, a entidade certificadora deve:

- a) Comunicar a cessação de actividade nos termos do disposto nos números 1 e 2 do artigo 64.º do Decreto-Lei n.º 33/2007;
- b) Comunicar a cessação da actividade à ANAC para efeitos do cancelamento das credenciações de segurança;
- c) Cessar todas as relações contratuais com terceiros autorizados a actuarem em seu nome na execução de funções relativas à emissão de certificados;
- d) Destruir ou impedir a utilização, de modo definitivo, das chaves privadas;
- e) Garantir que a entidade a quem é transmitida toda a documentação se obriga à sua manutenção durante o período de tempo legalmente exigido.

Artigo 37.º

Arquivo de informação

1. A documentação referente ao funcionamento dos serviços de certificação, incluindo avarias, situações operacionais especiais e a informação respeitante ao registo, é mantida em ficheiro electrónico e conservada pelo período mínimo de 20 anos.

2. Para efeitos do disposto no número anterior, a entidade certificadora assegura:

- a) A confidencialidade e integridade da informação conservada em arquivo, relativa a certificados qualificados;
- b) Que a data e hora precisa de eventos relacionados com a gestão de chaves e de certificados é registada;
- c) Que todos os eventos documentados na declaração de práticas de certificação são registados de forma que não permita a sua alteração ou destruição;
- d) O arquivo da informação dos eventos relativos a:
 - i) Registo, incluindo alterações;

- ii) Ciclo de vida do par de chaves da entidade certificadora e de todas as chaves de titulares que são geridas pela entidade certificadora;
- iii) Ciclo de vida dos certificados qualificados;
- iv) Ciclo de vida de chaves geradas por dispositivos seguros fornecidos;
- v) Fornecimento de dispositivos seguros de criação de assinatura;
- vi) Pedidos relacionados com a revogação de certificados.

3. A documentação constante do ficheiro electrónico é certificada por meio de assinatura electrónica qualificada com validação cronológica.

4. A entidade certificadora conserva em ficheiro manual todos os documentos relativos às relações contratuais estabelecidas com os requerentes, comprovativos de identidade e poderes de representação e relações contratuais estabelecidas com subcontratados e os documentos relativos à idoneidade e habilitações profissionais das pessoas que exercem funções relacionadas com serviços de certificação.

5. A documentação referida no número anterior é guardada, no mínimo, pelo período de 20 anos.

CAPÍTULO IV

Credenciação

Artigo 38.º



Recursos das entidadesificadoras

1. Para o desenvolvimento adequado das actividades às quais são atribuídas as licenças às entidadesificadoras, estas devem contar com uma equipa de profissionais, estrutura física, tecnologia e recursos financeiros, assim como os procedimentos e sistemas de segurança que permitam, nomeadamente:

- a) Gerar, em um ambiente seguro, as assinaturas digitais próprias e todos os serviços que solicitem a autorização;
- b) Cumprir com o estipulado nas políticas e procedimentos de certificação;
- c) Garantir a confiabilidade dos sistemas de acordo com os padrões aprovadas pela ANAC;
- d) Emitir certificados que cumpram com:
 - i) O disposto no artigo 67º do Decreto-Lei nº 33/2007;
 - ii) As normas tecnológicas aprovadas pela ANAC;
 - iii) A política de certificação correspondente;
- e) Garantir a existência de sistemas de segurança nas suas instalações, de forma a assegurar o acesso restrito às equipas que operam os sistemas da entidade certificadora;
- f) Proteger o acesso à chave privada mediante a criação de mecanismos que impeçam o acesso à chave de pessoas não autorizadas;

- g) Proteger o acesso e o uso da chave privada mediante procedimentos que exijam a participação de mais de uma pessoa;
- h) Registrar as transacções realizadas afim de identificar o autor e o momento de cada uma das operações;
- i) Utilizar os sistemas que cumpram as funções de certificação exclusivamente com esse propósito, sem que a eles sejam dadas nenhuma outra função;
- j) Proteger todos os sistemas utilizados directa ou indirectamente na actividade de certificação com procedimentos de autenticação e de segurança de alto nível de protecção, que devem ser actualizados de acordo com os avanços tecnológicos para garantir a correcta prestação dos serviços de certificação;
- k) Garantir a continuidade das operações mediante um Plano de Contingência actualizado e aprovado.

2. Os critérios de avaliação dispostos no número anterior são estabelecidos pela ANAC, de acordo com os padrões internacionais e os regulamentos que dispõem sobre a matéria.

Artigo 39.º

Credenciação de entidadesificadoras

1. As entidadesificadoras que apresentam garantias do cumprimento de todos os requisitos técnicos e de segurança referidos no presente diploma e no Decreto-Lei n.º 33/2007, assim como da utilização nas suas operações de certificação de assinaturas electrónicas qualificadas, de processos, sistemas e produtos avaliados e certificados nos termos do artigo 4.º, podem solicitar a credenciação, ou a sua renovação, em formulário próprio, disponibilizado pela autoridade credenciadora, instruído com os documentos referidos no artigo 46º no Decreto-Lei n.º 33/2007.

2. O pedido, quando apresentado em suporte de papel, é entregue directamente ou remetido pelo correio, sob registo, caso o mesmo seja apresentado por via electrónica, em documento electrónico com aposição de assinatura electrónica qualificada. Os documentos destinados à instrução do mesmo são remetidos à autoridade credenciadora no prazo de três dias subsequentes ao envio.

3. Os documentos referidos no n.º 1 que já tiverem sido apresentados à autoridade credenciadora para efeitos de inscrição no registo das entidadesificadoras e se encontrem dentro do seu prazo de validade podem ser substituídos por declaração da entidade certificadora onde se declare que os mesmos não sofreram alteração desde a sua apresentação.

4. O pedido de credenciação, ou de renovação, é ainda instruído com cópias autenticadas, redigidas em português ou acompanhadas de tradução legalizada, dos certificados e relatórios de avaliação de conformidade a que se refere o n.º 1.

Artigo 40.º

Entidades certificadoras credenciadas

As entidades certificadoras credenciadas, além do cumprimento de todas as disposições aplicáveis às entidades certificadoras que emitem certificados qualificados, devem:

- a) Prestar os serviços autorizados pela ANAC de forma contínua, de acordo com os termos, condições e prazos estabelecidos na lei, no presente diploma, nas deliberações emanadas pela ANAC e na respectiva autorização;
- b) Cumprir com os requisitos económicos, técnicos e jurídicos mínimos que tenham sido estabelecidos pela ANAC e que motivaram a autorização, assim como observar o cumprimento de qualquer outro requisito estabelecido pela ANAC;
- c) Cumprir com as políticas de Certificação para as quais obteve autorização, com o Manual de Procedimentos, com o Plano de Seguros, com o Plano de Cessação de Actividades e com o Plano de Contingência aprovados pela ANAC, assim como com as normas complementares ditadas pela ANAC, em matéria de procedimentos tecnológicos, procedimentos de certificação, segurança e confidencialidade da informação, protecção de dados pessoais dos titulares de certificados, e qualquer outra norma emitida pela ANAC;
- d) Informar os requerentes dos efeitos legais conferidos a uma assinatura electrónica qualificada e da força probatória dos documentos aos quais a mesma tenha sido aposta, assim como sobre a necessidade de voltar a assinar os documentos nos casos em que estes sejam necessários, na forma assinada, por um período de tempo superior à validade dos algoritmos e parâmetros associados utilizados na geração e verificação da assinatura;
- e) Garantir que a referência à credenciação é incluída nos certificados qualificados que emite ou comunicada de outra forma adequada;
- f) Assegurar, dentro do horário de serviço, um prazo máximo de três horas para a actualização das listas de revogação a partir da entrada da respectiva informação, garantindo que fora do horário de serviço são tomadas as medidas adequadas para que um pedido de revogação de um certificado qualificado seja registado por meio de um dispositivo automático que possibilite a suspensão automática e imediata do certificado;
- g) Assegurar que uma interrupção contínua dos serviços de revogação superior a trinta minutos durante o período normal de funcionamento é documentada como avaria.

CAPÍTULO V

Entidades ou unidades de registo

Artigo 41.º

Funções e obrigações das unidades de registo

Sem prejuízo do disposto na regulamentação emanada pela ANAC, as entidades de registo têm como funções e obrigações o seguinte:

- a) Recepção de pedidos de emissão de certificados;
- b) Validação de entidades e autenticação dos dados dos requerentes de certificados;
- c) Validação de outros dados de requerentes de certificados que se lhes apresentam, cuja a verificação é delegada à entidade certificadora para a homologação de certificados com competências determinadas, como por exemplo, a qualidade de representante de uma pessoa jurídica, qualidade de funcionário de uma organização, qualidade de membro de um grupo profissional, ente outros;
- d) Remissão dos pedidos aprovados para a entidade certificadora a qual se encontra vinculada;
- e) Recepção e validação dos pedidos de suspensão ou revogação de certificados e sua remissão à entidade certificadora; e
- f) Colaboração para a realização de inspecções e auditorias por parte da entidade certificadora, da ANAC e seus auditores.

Artigo 42.º

Delegação de competência

1. As entidades certificadoras podem delegar às entidades de registo as competências para a validação da **entidade** e de outros dados dos requerentes de certificados, assim como a realização de registo e os trâmites que os mesmos são formulados.

2. Para efectuar esta delegação, tanto as entidades certificadoras como as entidades de registo, devem cumprir com as normas e procedimentos estabelecidos na lei, no presente diploma e nas disposições emanadas pela ANAC.

3. As entidades certificadoras devem receber a autorização da ANAC para efectuar a delegação de competências referida no nº 1.

Artigo 43.º

Responsabilidade da entidade certificadora em relação à Entidade de Registo

1. Uma entidade de registo pode constituir-se como uma única unidade ou como várias unidades dependentes hierarquicamente entre si, podendo delegar a sua operação a outras Entidades de Registo, sempre que houver aprovação da entidade certificadora e a respectiva autorização da ANAC.

2. A entidade certificadora é responsável, de acordo com o estabelecido na lei, nos casos em que delegue parte de suas funções a entidade de registo, sem prejuízo do direito da entidade certificadora reclamar junto das entidades de registo as indemnizações pelos danos e prejuízos que sofrerem pelos actos e omissões desta.

Artigo 44.º

Titulares das entidades de registo

Podem cumprir as funções de entidade de registo, os serviços de Registo Civil, Cartório e Notariado, as associações profissionais, para os seus membros, as câmaras de Comércio, para os seus membros, as entidades bancárias, para os seus clientes e em relação às entidades certificadora pertencentes a organismos públicos, aqueles que cumpram com os requisitos estabelecidos pela ANAC. Esta enumeração pode ser modificada pela ANAC no âmbito da sua faculdade de regulação.

Artigo 45.º

Supervisão das entidades de registo pela ANAC

1. As entidades de registo estão sujeitas aos regulamentos e à inspecção da ANAC como órgão de supervisão e de controlo em matéria de assinatura digital.

2. A ANAC autoriza o funcionamento de entidades de registo mediante a observância das regras previamente estabelecidas.

3. As entidades de registo estão sujeitas às mesmas obrigações que as entidades certificadoras, nas seguintes matérias:

- a) Conservação de dados dos titulares de certificados;
- b) Protecção dos direitos do consumidor;
- c) Confidencialidade da informação;
- d) Protecção de dados pessoais; e
- e) Em qualquer outro aspecto estabelecido pela ANAC, mediante normas que complementam o presente diploma.

Artigo 46.º

Segurança dos documentos a longo prazo

A nova assinatura referida na alínea a) do artigo anterior deve ser gerada com os algoritmos e parâmetros associados adequados e incluir as assinaturas anteriores, assim como validação cronológica.

Artigo 47.º

Publicitação

A autoridade credenciadora assegura que se encontra disponível para acesso geral, a qualquer momento, por via electrónica, a informação relativa à identificação das entidades certificadoras credenciadas.

Artigo 48.º

Entrada em vigor

O presente diploma entra em vigor no dia seguinte ao da sua publicação.

Visto e aprovado em Conselho de Ministros

José Maria Pereira Neves - Manuel Inocêncio Sousa

Promulgado em 14 de Dezembro de 2007

Publique-se

O Presidente da República, PEDRO VERONA RODRIGUES PIRES

Referendado em 17 de Dezembro de 2007

O Primeiro-Ministro, *José Maria Pereira Neves*

Resolução nº 46/2007

de 24 de Dezembro

Considerando que por óbito do Sr. Pedro Neves e esposa D^a Etelvina Gomes Sant'Ana Neves, foi declarado vaga, para o Estado, 50% da herança do casal, por falta de parentes sucessíveis daquela;

Considerando a decisão do Tribunal Judicial da Comarca de São Vicente que reconhece o Estado de Cabo Verde como herdeiro de metade do prédio urbano situado em Alto Santo António da Cidade de Mindelo, descrita na matriz predial sob o número 2310, que pertencia a Etelvina Gomes Sant'Ana Neves;

Considerando, ainda, as solicitações dos herdeiros no sentido do Estado vender a parte que lhe cabe na herança da residência;

Ao abrigo do disposto no artigo 113.º do Decreto-Lei nº 2/97, de 21 de Janeiro, que aprovou o regime jurídico dos bens patrimoniais e,

No uso da faculdade conferida pelo nº 2 do artigo 260.º da Constituição da República, o Governo aprova a seguinte resolução:

Artigo 1.º

É autorizada a alienação directa de 50% do prédio urbano nº 11968, descrito na Conservatória a fls. 82 do Livro B-32.º, inscrito na matriz predial sob o nº 2310, situado em Alto Santo António, Cidade de Mindelo, aos legítimos herdeiros do Sr. Pedro Neves e Sr.^a Etelvina Gomes Sant'Ana Neves.

Artigo 2.º

O preço base de licitação é determinado ao abrigo do disposto no nº 1 do artigo 54.º da Portaria nº 61/98, de 2 de Novembro, que regulamenta o processo de alienação dos bens móveis, semoventes e imóveis que integram o património do Estado

Artigo 3.º

As receitas arrecadas entram directamente no cofre do Estado.

Artigo 4.º

A presente resolução entra em vigor no dia seguinte ao da sua publicação.

Vista e aprovada em Conselho de Ministros

José Maria Pereira Neves

Publique-se.

O Primeiro-Ministro, *José Maria Pereira Neves*

24 DE AGOSTO DE 1842 - 24 DE AGOSTO DE 2007

INCV 165 ANOS

AO SERVIÇO DE CABO VERDE



BOLETIM OFICIAL

Registo legal, nº 2/2001, de 21 de Dezembro de 2001



Av. Amílcar Cabral/Calçada Diogo Gomes, cidade da Praia, República Cabo Verde.

C.P. 113 • Tel. (238) 612145, 4150 • Fax 61 42 09

Email: incv@gov1.gov.cv

Site: www.incv.gov.cv

AVISO

Por ordem superior e para constar, comunica-se que não serão aceites quaisquer originais destinados ao Boletim Oficial desde que não tragam aposta a competente ordem de publicação, assinada e autenticada com selo branco.

Sendo possível, a Administração da Imprensa Nacional agradece o envio dos originais sob a forma de suporte electrónico (Disquete, CD, Zip, ou email).

Os prazos de reclamação de faltas do Boletim Oficial para o Concelho da Praia, demais concelhos e estrangeiro são, respectivamente, 10, 30 e 60 dias contados da sua publicação.

Toda a correspondência quer oficial, quer relativa a anúncios e à assinatura do Boletim Oficial deve ser enviada à Administração da Imprensa Nacional.

A inserção nos Boletins Oficiais depende da ordem de publicação neles aposta, competentemente assinada e autenticada com o selo branco, ou, na falta deste, com o carimbo a óleo dos serviços donde provenham.

Não serão publicados anúncios que não venham acompanhados da importância precisa para garantir o seu custo.

ASSINATURAS

Para o país:

	Ano	Semestre
I Série	8.386\$00	6.205\$00
II Série.....	5.770\$00	3.627\$00
III Série	4.731\$00	3.154\$00

Para países estrangeiros:

	Ano	Semestre
I Série	11.237\$00	8.721\$00
II Série.....	7.913\$00	6.265\$00
III Série	6.309\$00	4.731\$00

Os períodos de assinaturas contam-se por anos civis e seus semestres. Os números publicados antes de ser tomada a assinatura, são considerados venda avulsa.

AVULSO por cada página 15\$00

PREÇO DOS AVISOS E ANÚNCIOS

1 Página	8.386\$00
1/2 Página	4.193\$00
1/4 Página	1.677\$00

Quando o anúncio for exclusivamente de tabelas intercaladas no texto, será o respectivo espaço acrescentado de 50%.

PREÇO DESTE NÚMERO — 240\$00