BOLETIM DA REPÚBLICA

PUBLICAÇÃO OFICIAL DA REPÚBLICA DE MOÇAMBIQUE

IMPRENSA NACIONAL DE MOÇAMBIQUE, E. P.

AVISO

A matéria a publicar no «Boletim da República» deve ser remetida em cópia devidamente autenticada, uma por cada assunto, donde conste, além das indicações necessárias para esse efeito, o averbamento seguinte, assinado e autenticado: **Para publicação no «Boletim da República».**

SUMÁRIO

CONSELHO DE MINISTROS

Decreto n.º 59/2019

de 3 de Julho

Havendo necessidade de criar e regulamentar o Sistema de Certificação Digital de Moçambique que visa garantir a autenticidade, integridade e validade jurídica de documentos em formato electrónico, ao abrigo dos artigos 54 e 55, conjugado com o artigo 74 da Lei n.º 3/2017, de 9 de Janeiro, Lei de Transações Electrónicas o Conselho de Ministros, decreta:

Artigo 1. É criado o Sistema de Certificação Digital de Moçambique e aprovado o Regulamento do Sistema de Certificação Digital de Moçambique, em anexo, que é parte integrante do presente Decreto.

Art. 2. O presente Decreto entra em vigor na data da sua publicação.

Aprovado pelo Conselho de Ministros, aos 2 de Abril de 2019.

Publique-se.

O Primeiro-Ministro, *Carlos Agostinho do Rosário.*

Regulamento do Sistema de Certificação Digital de Moçambique (SCDM)

CAPÍTULO I

Disposições Gerais

ARTIGO 1

(Definição)

1. Sistema de Certificação Digital de Moçambique abreviadamente designado por SCDM é um sistema que engloba as actividades de certificação digital de entidades públicas e privadas.

2. Para efeitos do presente Regulamento, são adoptadas outras definições que constam do glossário em anexo, que dele faz parte integrante.

ARTIGO 2

(Objecto)

O SCDM, visa garantir um ambiente electrónico seguro de transacções electrónicas no País.

ARTIGO 3

(Âmbito)

O SCDM é de âmbito nacional e aplica-se as pessoas singulares, colectivas públicas ou privadas.

ARTIGO 4

(Sistema de Certificação Digital de Moçambique)

1. O SCDM estabelece uma estrutura de confiança electrónica, de forma que as entidades certificadoras que lhe estão subordinadas disponibilizem serviços que garantam:

a) A realização de transacções electrónicas seguras;

b) A autenticação segura;

c) A autenticidade, integridade, confidencialidade, validade jurídica e não repúdio das assinaturas electrónicas de transacções ou informações em documentos electrónicos.

2. O SCDM reconhece, para efeitos de filiação na Autoridade Certificadora Raiz do Estado, as entidades certificadoras dos sectores público e privado.

3. O SCDM é ainda integrado, através de registo junto da Autoridade Credenciadora, pelas Entidades Certificadoras privadas, que emitam certificados qualificados.

CAPÍTULO II

Organização e Funcionamento do SCDM

ARTIGO 5

(Estrutura do SCDM)

1. O SCDM estrutura-se de seguinte modo:

a) Comité Gestor (CG);
b) Autoridade Certificadora Raiz do Estado (ACR);
c) Entidades Certificadoras (EC);
d) Entidades de Registo (ER) vinculadas às Entidades Certificadoras.

2. Para além dos órgãos indicados no número 1, do presente artigo, o Comité Gestor pode criar um Comité Técnico e definir a respectiva composição, periodicidade de reuniões e os termos de apoio logístico.

SECÇÃO I

Comité Gestor

ARTIGO 6

(Composição)

1. O Comité Gestor do SCDM é o órgão responsável pela gestão e administração do SCDM.

2. O Comité Gestor remete para aprovação pelo Conselho de Ministros as matérias por si apreciadas, e é presidido pelo Primeiro-Ministro e tem como Vice-Presidente o Ministro que superintende a área de tecnologias de informação e comunicação.

3. Compõem igualmente o Comité Gestor:

a) O Ministro que superintende a área das finanças;
b) O Ministro que superintende a área de Defesa;
c) O Ministro que superintende a área da Ordem e Segurança;
d) O Ministro que superintende a área da Administração Estatal e Função Pública;
e) O Ministro que superintende a área da Justiça;
f) O Ministro que superintende a área de Indústria e Comércio;
g) O Director-geral do Instituto Nacional de Tecnologias de Informação e Comunicação (INTIC).

4. Faz ainda parte da composição um representante de cada Entidade Certificadora pública integrada no SCDM que não esteja representada por nenhuma das entidades referidas nas alíneas anteriores. O Comité Gestor pode ainda integrar um representante das Entidades de Certificação de natureza privada, a ser designado pelo Presidente do Comité Gestor.

ARTIGO 7

(Competências)

1. Compete ao Comité Gestor do SCDM:

a) Elaborar e propor ao Conselho de Ministros, de acordo com a lei e tendo em conta as melhores práticas a nível de normas ou especificações internacionalmente reconhecidas, as políticas e as práticas de certificação a observar pelas Entidades Certificadoras, de Registo e demais prestadores de serviços de suporte que integram o SCDM;
b) Garantir que as declarações de práticas de certificação das várias Entidades Certificadoras que integram o SCDM, incluindo a Autoridade Certificadora Raiz do Estado, estejam em conformidade com a política de certificação do SCDM;
c) Propor ao Conselho de Ministros os critérios para aprovação dos pedidos das Entidades Certificadoras de integração no SCDM;
d) Propor ao Conselho de Ministros a admissão no SCDM de Entidades Certificadoras públicas;
e) Aferir a conformidade dos procedimentos seguidos pelas Entidades Certificadoras integradas no SCDM com as políticas e práticas aprovadas, sem prejuízo das competências legalmente cometidas à Autoridade Credenciadora;
f) Submeter a proposta de exclusão do SCDM das Entidades Certificadoras que não se mostrem em conformidade com as políticas e práticas aprovadas, comunicando tal facto à Autoridade Credenciadora;
g) Solicitar auditorias e outras acções de fiscalização às Entidades Certificadoras, assim como aos seus prestadores de serviço de suporte, sempre que suspeite do incumprimento das políticas e práticas por si aprovadas;
h) Propor ao Conselho de Ministros a actualização das políticas e práticas estabelecidas para o SCDM, de modo a garantir a sua compatibilidade e promover a actualização tecnológica e a sua conformidade com as políticas de segurança;
i) Pronunciar-se sobre as melhores práticas internacionais no exercício das actividades de certificação digital e propor a sua aplicação;
j) Representar institucionalmente o SCDM.

2. Compete, ainda, ao Comité Gestor do SCDM a promoção das actividades necessárias ao reconhecimento e interoperabilidade, nos termos previstos no artigo 50 da Lei n.° 3/2017, de 9 de Janeiro.

ARTIGO 8

(Funcionamento)

1. O Comité Gestor do SCDM reúne, de forma ordinária, duas vezes por ano e de forma extraordinária por convocação do seu presidente.

2. O apoio técnico, logístico e administrativo ao Comité Gestor do SCDM, bem como os encargos inerentes ao seu funcionamento, é da responsabilidade da entidade à qual é cometida a função de operação da Autoridade Certificadora Raiz do Estado.

3. O Comité Gestor do SCDM será secretariado pelo INTIC, a quem compete a preparação de reuniões, deliberações, envio de convocatórias e documentação das deliberações.

4. Compete à Vice-presidência do Comité Gestor:

a) Coadjuvar o Presidente do Comité Gestor nas suas actividades;
b) Substituir o Presidente nas suas ausências e impedimentos;
c) Assegurar o funcionamento do Secretariado do Comité Gestor;
d) Orientar a preparação das sessões do Comité Gestor, assegurando correspondentes reuniões preparatórias, visando a correcta integração, auscultação e acolhimento das contribuições e aconselhamentos das componentes técnicas dos temas em agenda;
e) Exercer as demais competências que lhe forem delegadas pelo Presidente.

SECÇÃO II

Autoridade Certificadora Raiz do Estado

ARTIGO 9

(Gestão e operação)

1. A Autoridade Certificadora Raiz do Estado é administrada pelo INTIC e é dirigida pelo seu Director-Geral, devendo assegurar:

a) A articulação entre a Autoridade Certificadora Raiz do Estado e o Comité Gestor do SCDM e entre aquela e as Entidades Certificadoras integradas no SCDM;
b) A administração de sistemas, com autorização para instalar, configurar e manter o sistema;
c) A operação de sistemas, com a responsabilidade de operá-los diariamente, com autorização para realizar cópias de segurança e reposição de informação;
d) A administração de segurança, com a responsabilidade pela gestão e implementação das regras e práticas de segurança;
e) A administração de registo, com a responsabilidade pela aprovação da emissão, pela suspensão e pela revogação de certificados;
f) A auditoria de sistemas, autorizando a monitorizar os arquivos de actividade dos sistemas.

2. As funções de administração de sistemas, de administração de segurança e de auditoria de sistemas devem ser desempenhadas por pessoas diferentes.

ARTIGO 10

(Competências)

1. A Autoridade Certificadora Raiz do Estado é um órgão certificador de topo da cadeia de certificação do SCDM que executa as políticas de certificados e directrizes aprovadas pelo Comité Gestor do SCDM.

2. Compete à Autoridade Certificadora Raiz do Estado:

a) Fazer o registo, a credenciação e fiscalização das Entidades Certificadoras;
b) Admitir a integração das Entidades Certificadoras que obedeçam aos requisitos estabelecidos no presente Decreto;
c) Prestar os serviços de certificação às Entidades Certificadoras no nível hierárquico imediatamente inferior ao seu na cadeia de certificação;
d) Garantir o cumprimento e a implementação enquanto Autoridade Certificadora de todas as regras e procedimentos estabelecidos no documento de políticas de certificação e na declaração de práticas de certificação do SCDM;
e) Implementar as políticas e práticas aprovadas para o efeito pelo Comité Gestor do SCDM;
f) Gerir toda a infra-estrutura e os recursos que compõem e garantem o funcionamento da Autoridade Certificadora Raiz do Estado, nomeadamente o pessoal, os equipamentos e as instalações;
g) Gerir todas as actividades relacionadas com a gestão do ciclo de vida dos certificados por si emitidos para as Entidades Certificadoras de nível imediatamente inferior ao seu;
h) Garantir que o acesso às suas instalações principal e alternativa é efectuado apenas por pessoal devidamente autorizado e credenciado;
i) Gerir o recrutamento de pessoal tecnicamente habilitado para a realização das tarefas de gestão e operação da Autoridade Certificadora Raiz do Estado;
j) Comunicar qualquer incidente, nomeadamente anomalias ou falhas de segurança, ao Comité Gestor do SCDM.

3. A Autoridade Credenciadora pode, no exercício das suas competências, solicitar outras Entidades Públicas ou Privadas toda a colaboração que julgar necessária.

ARTIGO 11

(Serviços)

1. A Autoridade Certificadora Raiz do Estado disponibiliza os seguintes serviços:

a) Processo de registo das Entidades Certificadoras integradas no SCDM;
b) Geração de certificados e gestão do seu ciclo de vida;
c) Disseminação dos certificados, das políticas e das práticas de certificação;
d) Gestão de revogação de certificados;
e) Disponibilização da informação do estado e do motivo da revogação referida na alínea anterior.

2. A Autoridade Certificadora Raiz do Estado emite exclusivamente certificados para as entidades certificadoras que lhe estejam subordinadas, não podendo emitir certificados destinados a utilizadores finais.

3. A Autoridade Certificadora Raiz do Estado poderá autorizar que uma AC ou uma AR contrate empresas prestadoras de serviços de suporte (PSS) para disponibilizar:

a) Infra-estruturas físicas e lógicas;
b) Recursos humanos especializados;
c) Realizar auditorias operacionais em entidades a elas subordinadas.

ARTIGO 12

(Filiação na Autoridade Certificadora Raiz do Estado)

1. Podem filiar-se à Autoridade Certificadora Raiz do Estado as Entidades Certificadoras referidas no número 1 do artigo 5 do presente Decreto.

2. As Entidades Certificadoras filiadas à Autoridade Certificadora Raiz do Estado não podem emitir certificados de nível imediatamente subsequente ao seu, excepto nos casos de acordos de certificação lateral ou cruzada promovidos e aprovados pelo Comité Gestor do SCDM.

3. A Autoridade Certificadora Raiz do Estado não deve ter, na mesma hierarquia de confiança, Entidades Certificadoras subordinadas que emitam certificados de autenticação da página web e certificados de utilizadores finais.

SECÇÃO III

Entidades Certificadoras

Sub Secção I

Funcionamento das Entidades Certificadoras

ARTIGO 13

(Competência da Entidade Certificadora)

Compete às Entidades Certificadoras que integram o SCDM, sejam elas públicas ou privadas que emitam certificados qualificados, obedecer as regras técnicas e de segurança constantes do presente regulamento.

ARTIGO 14

(Requisitos das Entidades Certificadoras)

1. Podem solicitar credenciação, em formulário próprio disponibilizado pela Autoridade Credenciadora, instruído com os documentos indicados pela mesma, as Entidades Certificadoras que cumpram os requisitos técnicos e de segurança referidos no artigo 59 da Lei n.º 3/2017, de 9 de Janeiro, e no presente Decreto.

2. A Entidade Certificadora do SCDM pode atribuir os serviços de registo a terceiros, denominados como Entidades de Registo, com as quais a Autoridade Certificadora acorde, por escrito, a prestação de serviços de identificação e registo de utilizadores de certificados, bem como a gestão de pedidos de revogação de certificados.

3. A Entidade Certificadora procede ao registo junto da Autoridade Credenciadora de todas as Entidades de registo que utilize na sua actividade.

ARTIGO 15

(Normas Técnicas da Entidade Certificadora)

1. Os processos, sistemas e produtos utilizados pela Entidade Certificadora no exercicio da sua actividade, devem estar em conformidade com o disposto no presente diploma e com as normas, especificações e outra documentação técnica a aprovar pela Entidade Reguladora de TIC, através de instruções a divulgar através do *Boletim da República* e na respectiva página *web*.

2. As normas técnicas a aprovar pela Entidade Reguladora de TIC, devem ser reconhecidas a nível internacional como aplicáveis aos processos, sistemas e produtos, regulados no presente Decreto, nomeadamente:

a) À gestão da segurança da informação e à gestão do ciclo de vida dos certificados;
b) Serviços e processos das Entidades Certificadoras respeitantes à gestão da segurança da informação;
c) Serviços e processos das Entidades Certificadoras respeitantes à gestão do ciclo de vida dos certificados;
d) Sistemas de informação utilizados na emissão e gestão dos certificados, incluindo os certificados qualificados;
e) Módulos criptográficos para operações de assinatura;
f) Aplicações de criação e de verificação de assinaturas;
g) Dispositivos seguros de criação de assinaturas.

3. Sempre que estejam envolvidas informação classificadas, aplicam-se as normas vigentes na Administração pública sobre informação classificada.

Sub Secção II

Critérios de avaliação e Contratação

ARTIGO 16

(Avaliação da Conformidade)

1. A conformidade com as normas técnicas indicadas no artigo anterior é certificada por auditorias, iniciais e periódicas, a contratar pela Entidade Certificadora, cujo resultado deve ser a ela submetido.

2. A Autoridade Credenciadora divulga os critérios de avaliação de conformidade a serem verificados nas auditorias.

3. 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 constantes das normas ISO/IEC 15408, para os níveis de avaliação de segurança e grau de robustez exigidos nas normas, especificações e outra documentação técnica aplicável nos termos do artigo anterior.

ARTIGO 17

(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 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.

3. É obrigatório a celebração de um contrato redigido a escrito entre a Entidade Certificadora e qualquer prestador de serviços, onde se estabelecem as obrigações das partes e as funções.

SECÇÃO IV

Entidades de Registo Vinculadas às Entidades Certificadoras

ARTIGO 18

(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 terão de estar conforme.

2. A declaração de práticas de certificação deve conter, 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.

3. A declaração de práticas de certificação é revista uma vez por ano, e está permanentemente disponível, por via electrónica, para consulta dos requerentes, titulares e destinatários.

ARTIGO 19

(Política de Certificado)

1. 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.

2. A política de certificado está permanentemente disponível, por via electrónica, para consulta dos requerentes, titulares e destinatários.

ARTIGO 20

(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 26, e por pessoal que cumpra os requisitos estabelecidos no artigo 29 do presente Decreto;

b) Recorrendo a um algoritmo e comprimento de chave apropriado, de acordo com o disposto no artigo 23 do presente Decreto;

c) Recorrendo a um dispositivo seguro de criação de assinatura, avaliado de acordo com o disposto no número 3 do artigo 15 do presente Decreto;

d) Por um mínimo de 2 (dois) trabalhadores presentes física e conjuntamente no local.

ARTIGO 21

(Credenciação de Entidade Certificadora de SCDM)

1. A Autoridade Credenciadora deve responder os pedidos de credenciação num prazo máximo de 3 (três) meses.

2. A credenciação é válida por um período de 4 (quatro) anos, findo o qual pode ser renovado mediante a verificação do cumprimento dos requisitos.

3. A Autoridade Credenciadora assegura que se encontra disponível para acesso geral, a qualquer momento, por via electrónica, a informação relativa a identificação das Entidades Certificadoras do SCDM.

ARTIGO 22

(Gestão das Chaves da Entidade Certificadora)

1. As chaves privadas da Entidade Certificadora são:

a) Mantidas num dispositivo seguro de criação de assinatura;

b) Objecto de cópia de segurança, armazenada e reposta por pessoal autorizado e em ambiente físico seguro, de acordo com 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 a Entidade Certificadora é responsável por:

a) Assegurar a integridade e autenticidade das chaves públicas e de qualquer parâmetro a elas associado durante a distribuição, e estabelecer um processo que permita autenticar a sua origem;

a) Manter organizado um arquivo das chaves públicas, após o termo do seu período de validade;

b) Garantir a segurança e integridade do equipamento criptográfico durante a sua vida útil, e assegurar que o mesmo não seja acedido ou alterado por pessoal não autorizado;

c) Garantir que as chaves privadas armazenadas no equipamento criptográfico são destruídas quando da sua retirada de funcionamento;

d) 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.

5. A Entidade Certificadora deve ter ao seu dispor somente as chaves públicas.

6. As chaves privadas são pessoais e intransmissíveis devendo apenas estar na posse e disponibilidade do utilizador.

ARTIGO 23

(Emissão das Chaves de Titulares)

1. 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 25 do presente Decreto;

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 seja efectuada cópia de segurança nem de arquivo da chave privada do titular para criação de assinaturas.

ARTIGO 24

(Dispositivos Seguros de Criação de Assinaturas)

No fornecimento dos dispositivos seguros de criação de assinaturas, a Entidade Certificadora, assegura que:

a) O dispositivo é preparado, armazenado e distribuído de forma segura;

b) No caso de o dispositivo ter associado dados de activação, estes são fornecidos de forma separada.

ARTIGO 25

(Algoritmos Criptográficos)

1. Os algoritmos criptográficos utilizados na prestação de serviços de certificação e respectivos parâmetros associados são os que constam da lista aprovada pela Autoridade Credenciadora, que os divulgará na página *web* respectiva e no *Boletim da República*.

2. Sempre que algum dos algoritmos indicados na lista referida no número 1 do presente artigo estiver em risco de segurança, a Autoridade Credenciadora notifica as Entidades Certificadoras do SCDM, que deverão adoptar as medidas adequadas, nomeadamente o aumento do comprimento das chaves ou a cessação da respectiva utilização.

ARTIGO 26

(Implementação da Segurança)

1. A Entidade Certificadora assegura que as instalações, procedimentos, pessoal, equipamentos e produtos obedecem às

normas de segurança aplicáveis ao exercício da sua actividade, devendo designadamente:

a) Ter um plano de segurança implementado de acordo com as normas aprovadas pela Autoridade Credenciadora;
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 mantêm um inventário de bens com a respectiva classificação, de forma a caracterizar as suas necessidades de protecção.

3. Sempre que estiverem envolvidas informações classificadas, a entidade competente para fiscalizar o cumprimento dos deveres antes do início de actividade da Entidade Certificadora, procede uma avaliação de segurança.

ARTIGO 27

(Plano de Segurança)

1. O plano de segurança contém, obrigatoriamente:

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

2. No caso de estarem envolvidas matérias classificadas, o plano de segurança deve obter a aprovação da entidade competente para a respectiva fiscalização.

ARTIGO 28

(Plano de Contingência)

1. A Entidade Certificadora implementa um plano de contingência para fazer face à eventual ocorrência de desastres ou incidentes que ponham em causa o funcionamento normal dos serviços de certificação, 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 informadas 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 de certificados se mantêm permanentemente disponíveis, em caso de acidente.

3. A Entidade Certificadora assegura procedimentos que permitem a continuação dos serviços em sistemas de recuperação alternativos, e garante que a migração dos sistemas primários para os sistemas de recuperação não ponha em risco a segurança dos sistemas.

ARTIGO 29

(Política de Pessoal)

1. A Entidade Certificadora adopta regras de selecção e contratação de pessoal que reforce e respeite as disposições de segurança exigidas para o exercício da sua actividade.

2. Para funções de gestão de infra-estruturas de chave pública, a Entidade Certificadora emprega pessoal especializado com conhecimentos específicos em tecnologia de assinatura digital e com conhecimentos de comportamentos de segurança.

3. O pessoal que desempenha funções relacionadas com os processos de certificação, observa o principio da imparcialidade, devendo encontrar-se livre de possíveis conflitos de interesse.

4. As funções relacionadas com os processos de certificação são desempenhadas por pessoas que não se encontrem em situação indiciadora de falta de idoneidade.

5. No âmbito da sua estrutura organizativa contempla, pelo menos, as funções indicadas no n.º 1 do artigo 9 e n.º 2 do artigo 10 do presente Decreto e assegura a segregação de funções ali imposta.

6. Os membros dos órgãos de administração e fiscalização e qualquer pessoal das Entidades Certificadoras com acesso aos actos e instrumentos de certificação, os sócios da sociedade e, tratando-se de sociedade anónima, os accionistas com participações significativas serão sempre pessoas de reconhecida idoneidade.

7. Entre outras circunstâncias atendíveis, considera-se indiciador de falta de idoneidade o facto de a pessoa ter sido:

a) Condenada, no País ou no estrangeiro, por qualquer crime punível com pena de prisão superior a um ano ou por crime de natureza patrimonial, crime com uso de meios informáticos ou crime contra o Estado;
b) Declarada, por sentença nacional ou estrangeira, falida ou insolvente ou julgada responsável por falência ou insolvência de empresa por ela dominada ou de cujos órgãos de administração ou fiscalização tenha sido membro;
c) Sujeita a sanções, no País ou no estrangeiro, pela prática de infracções às normas legais ou regulamentares que regem as actividades de produção, autenticação, registo e conservação de documentos, e designadamente as do notariado, dos registos públicos, do funcionalismo judicial, das bibliotecas públicas e da certificação de assinaturas electrónicas.

8. A falta dos requisitos de idoneidade previstos no presente artigo constitui fundamento de recusa e de revogação da credenciação nos casos em que já tenha sido emitida.

ARTIGO 30

(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 das normas aplicáveis e devidamente credenciada pela Autoridade Credenciadora.

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

3. O relatório de auditoria respectivo, deve ser enviado à Autoridade Credenciadora até 31 de Março de cada ano civil.

4. 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.

5. 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 estabelece 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 Autoridade Credenciadora, 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 31

(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 à Autoridade Credenciadora, com a antecedência mínima de três meses;

b) Cessar todas as relações contratuais com terceiros autorizados a actuarem em seu nome na execução de funções relativas à emissão de certificados;

c) Destruir, ou impedir a utilização, de modo definitivo, das chaves privadas;

d) Garantir que a entidade a quem é transmitida toda a documentação se obriga à sua manutenção durante o período de tempo legalmente exigido.

ARTIGO 32

(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 aos 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 ao:

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. Pedido relacionado 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 todos os documentos relativos às relações estabelecidas com os requerentes, comprovativos de identidade e poderes de representação, 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.

SECÇÃO V

Comité Técnico

ARTIGO 33

(Funcionamento do Comité Técnico)

1. O Comité Técnico é um órgão de apoio do Comité Gestor.

2. O Comité Gestor define a composição, periodicidade de reuniões e o apoio logístico ao Comité Técnico.

3. Os membros do Comité Técnico têm direito a auferir, pelo desempenho das suas funções, senhas de presença ou eventuais ajudas de custo, nos termos legais.

ARTIGO 34

(Perfil do Comité Técnico)

Os membros do Comité Técnico tem obrigatoriamente um perfil que revele habilitações académicas ou profissionais

especialmente relevantes no domínio da informática, governo electrónico e/ou segurança de informação, que os habilite a assessorar tecnicamente o Comité Gestor.

CAPÍTULO III

Serviços Acessórios

ARTIGO 35

(Serviço de Validação Cronológica)

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

2. Os serviços de validação cronológica devem garantir 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 25 do presente Decreto;

c) A hora utilizada é a hora oficial de Moçambique, certificada por meios adequados;

d) Os dados incluídos no pedido são devolvidos sem alteração.

3. Os serviços de validação cronológica devem garantir igualmente que chave privada utilizada na assinatura da prova de validação cronológica:

a) Não seja utilizada para outra finalidade;

b) Seja gerada recorrendo a um algoritmo e comprimento de chave apropriado, reconhecido nos termos do artigo 24 do presente Decreto;

c) Seja gerada e armazenada num módulo criptográfico, avaliado de acordo com o disposto no número 3 do artigo 16 do presente Decreto.

4. Em cada prova de validação cronológica são incluídos:

a) O valor tempo certificado;

b) Um identificador único;

c) Um indicador único da política de certificação cronológica adoptada;

d) O grau de exactidão do valor tempo utilizado sempre que aquele seja superior ao indicado na política adoptada.

5. A prova de validação cronológica é assinada criptograficamente antes da devolução da resposta ao pedido.

6. Não está incluída, na prova de validação cronológica, a identificação da entidade que a solicitou.

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

ARTIGO 36

(Preservação de Longo Prazo)

1. Entidades Certificadoras devem informar os requerentes de certificados que para assegurar a preservação de longo prazo dos documentos electrónicos aos quais tenham sido apostas assinaturas electrónicas, será necessária a periódica aplicação de mecanismos que assegurem a sua integridade.

2. A preservação de longo prazo é feita mediante aplicação de validação cronológica e da utilização de algoritmos cuja segurança perdure para além do prazo pelo qual seriam considerados seguros os algoritmos utilizados inicialmente.

CAPÍTULO IV

Actividade de Emissão e Gestão de Certificados Qualificados

ARTIGO 37

(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 autógrafa.

2. A Entidade Certificadora verifica a identidade do requerente, por meio legalmente reconhecido, verifica igualmente, nos casos em que o pedido se referir ao certificado cujo titular seja um terceiro, com poderes bastantes do requerente para apresentar tal pedido.

ARTIGO 38

(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 uma 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 para além dos elementos referidos no número anterior, deve conter 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 o 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, terá de ser expressamente autorizado por esta.

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, em que se obriga ao cumprimento das obrigações enquanto titular.

ARTIGO 39

(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 o 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 para além do disposto no número anterior, aplica-se, com as devidas adaptações, o previsto nas alíneas *a*) e *e*) do n.º 2 e n.º 4 do artigo anterior.

ARTIGO 40

(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 45 do presente Decreto;
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.

ARTIGO 41

(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 a 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 os respectivos parâmetros.

5. 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.

6. A Entidade Certificadora só emite certificado para pessoas colectivas quando estas garantem que a utilização do mesmo exige a intervenção de pessoas singulares que, estatutária ou legalmente, representam a pessoa colectiva titular desse certificado.

ARTIGO 42

(Conteúdo e formato do certificado qualificado)

1. O certificado qualificado contém 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 qualificada 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 do 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. O formato dos certificados obedece às especificações técnicas indicadas pela Autoridade Credenciadora nos termos do disposto no artigo 15.

3. A Entidade Certificadora assegura os mecanismos necessários para que a hierarquia de certificação seja estabelecida e os certificados emitidos possam ser reconhecidos.

ARTIGO 43

(Distribuição)

A Entidade Certificadora, na distribuição de certificados, deve utilizar sistemas seguros que permitam a sua conservação e disponibilização para efeitos de verificação, assegurando que:

a) O certificado seja disponibilizado, integralmente, ao titular para quem foi emitido;
b) O certificado só seja publicamente disponibilizado com o consentimento do titular;
c) Sejam transmitidas ao destinatário as condições a que este se obriga;
d) Se verifique em cada comunicação ou transacção a validade, suspensão ou revogação do certificado;
e) Se Verifique se o certificado é utilizado de acordo com as condições emitidas pela Entidade Certificadora.

ARTIGO 44

(Renovação e Actualização)

Na renovação de certificados ou actualização devido à 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 serão 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 sua segurança criptográfica durante o prazo de validade do novo certificado.

ARTIGO 45

(Revogação e Suspensão)

A Entidade Certificadora utiliza os procedimentos de revogação e suspensão de certificados de acordo com o disposto no artigo 59 da Lei de Transacções Electrónicas e de acordo com os termos da declaração de práticas de certificação, e assegura:

a) Que os pedidos e informações relativos à suspensão ou revogação são processados num período inferior a 24 horas após 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 poderá 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 de 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.

ARTIGO 46

(Obrigação de Informação)

No exercício da sua actividade, a Entidade Certificadora divulga a seguinte informação:

a) Preço dos serviços a prestar, se aplicável;

b) Declaração de práticas de certificação;

c) Termos, condições e âmbito de utilização dos seus certificados;

d) Existência de um meio de comunicação, permanentemente disponível, através do qual se procede ao pedido de suspensão e, ou, revogação do certificado;

e) Período de tempo durante o qual mantém, em arquivo, a informação prestada pelo requerente e a referente à utilização dos respectivos certificados;

f) Os mecanismos utilizados para resolução de conflitos;

g) Legislação aplicável à actividade de certificação;

h) Data e número da credenciação.

ARTIGO 47

(Obrigações do Titular)

O titular do certificado toma as medidas necessárias para evitar danos a terceiros e 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 24 do presente Decreto, no caso de gerar as suas próprias chaves;

d) Usar um dispositivo seguro de criação de assinatura, nos termos da política de certificado;

e) Gerar as chaves no interior do dispositivo seguro de criação de assinatura, nos termos da política de certificado;

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 48

(Obrigações do Requerente)

1. As obrigações do requerente em nome próprio são as obrigações 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 49

(Relações Contratuais Relativas à Emissão de Certificados)

1. As Entidades Certificadoras privadas devem celebrar contratos com os requerentes de certificados, reduzidos a escrito, em linguagem clara e acessível, num suporte físico duradouro, e subscritos pelas partes com assinatura electrónica qualificada, quando em documento electrónico, ou com assinatura autógrafa, 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 nas alíneas *a*), *c*), *h*) e *i*) do artigo 46 do presente Decreto;

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.

CAPÍTULO V

Taxas, Fiscalização e Multas

ARTIGO 50

(Taxas)

1. É fixado em 40 (quarenta) salários mínimos praticados no sector Público, pelo acto de registo da entidade certificadora.

2. É fixada em 75 (setenta e cinco) salários mínimos praticados no sector Público, devidos pela credenciação da entidade certificadora.

3. É fixada em 60 (sessenta) salários mínimos praticados no sector Público, devidos pela renovação da credenciação da entidade certificadora.

4. As taxas fixadas nos números anteriores são pagas pela entidade certificadora, no prazo máximo de trinta dias após notificação pela Autoridade Credenciadora, do acto de registo, da atribuição da credenciação ou da sua renovação.

5. Compete ao Ministro que superintendente a área de Finanças sob proposta do Ministro que superintende a área das TIC, por diploma Ministerial, actualizar o valor das taxas previstas nos números 1, 2 e 3 do presente artigo.

ARTIGO 51

(Fiscalização)

As entidades certificadoras fornecem à Autoridade Credenciadora, de modo pronto e exaustivo, todas as informações que lhes solicite para fins de fiscalização da sua actividade e disponibiliza para os mesmos fins a inspecção dos seus estabelecimentos e o exame local de documentos, objectos, equipamentos periféricos e aplicativos informáticos e procedimentos operacionais, no decorrer dos quais a Autoridade Credenciadora poderá fazer as cópias e registos que sejam necessários.

ARTIGO 52

(Sanções)

1. As infracções e às disposições do presente regulamento, são puníveis com multas que têm a seguinte graduação:

a) A violação do disposto no número 1 do artigo 49 do presente regulamento é punível, com multa de até 35 salários mínimos praticados no sector público;

b) A violação do disposto no número 2 do artigo 49 do presente regulamento é punida, com multa de até 30 salários mínimos praticados no sector público;

c) A violação do disposto no número 3 do artigo 49 do presente regulamento é punida, com multa de até 50 salários mínimos praticados no sector Público.

2. As multas fixadas nos termos do presente regulamento são cobradas ao dobro dos seus valores em caso de reincidência nas infracções.

3. As multas referenciadas acima, devem ser pagas no prazo de 30 (trinta) dias a contar da data da notificação.

CAPÍTULO VI

Disposições Finais

ARTIGO 53

(Acordos de Sistemas de Certificação)

1. A Autoridade Certificadora Raiz do Estado promove os contactos a nível regional e internacional com vista a obter o reconhecimento do SCDM junto de outros sistemas de certificação, de base pública ou privada.

2. Os acordos tendentes ao reconhecimento devem ter por base o reconhecimento mútuo de boas práticas de certificação e com objectivo de facilitar a utilização dos certificados emitidos no âmbito do SCDM nos sistemas informáticos mais comuns.

ARTIGO 54

(Interoperabilidade de Sistemas de Certificação)

Estabelecidos os acordos de interoperabilidade sobre sistemas de Certificação com base em certificação cruzada, com outras infra-estruturas de chaves públicas, de natureza privada ou pública, nacionais ou internacionais, a Autoridade Certificadora Raiz do Estado deverá:

a) Receber aprovação do Comité Gestor sobre a atribuição e a revogação de certificados emitidos com base em certificação cruzada;

b) Definir os termos e condições para o início, a suspensão ou a finalização dos procedimentos de interoperabilidade com outras infra-estruturas de chaves públicas.

ANEXO

Glossário

A

Assinatura digital - é um método de autenticação de informação digital tipicamente tratada como substituta à assinatura física, que permite identificar o remitente e autenticar o conteúdo que elimina a necessidade de ter uma versão em papel do documento que necessita ser assinado.

Assinatura electrónica – é o resultado de um processamento electrónico de dados susceptíveis de constituir objecto de direito individual e exclusivo e de ser utilizado para dar a conhecer a autoria de um documento electrónico.

Assinatura electrónica qualificada – assinatura electrónica baseada num certificado qualificado e criada através de um dispositivo seguro de criação de assinatura, que:

i. Identifica de forma unívoca o titular como autor do documento;

ii. A sua aposição ao documento depende apenas da vontade do titular;

iii. É criada com meios que o titular pode manter sob seu controlo exclusivo;

iv. A sua conexão com o documento permite detectar toda e qualquer alteração superveniente do conteúdo deste.

Aplicativos informáticos - são o conjunto de ferramentas desenhadas para realizar tarefas e trabalhos específicos no seu computador.

Auditor de Segurança – uma entidade credenciada pela Autoridade Credenciadora, a quem compete verificar a conformidade das actividades das Entidades Certificadoras com os requisitos estabelecidos no presente diploma, elaborando relatórios para instrução dos pedidos de credenciação.

Autoridade Credenciadora – entidade a quem compete a avaliação e certificação da conformidade dos processos e sistemas e produtos de assinatura electrónica assim como a supervisão das Entidades Certificadoras públicas e privadas.

C

Certificado – atestado electrónico que liga determinados dados a uma pessoa singular, a uma pessoa colectiva ou à uma página *web*.

Certificado qualificado – certificado que cumpre com os requisitos estabelecidos e emitidos por provedores de serviços de certificação credenciados, nos termos previstos no presente Decreto.

Chave privada – elemento de par de chaves assimétricas destinado a ser conhecido apenas pelo seu titular.

Chave pública – elemento de par de chaves assimétricas destinado a ser divulgado.

Credenciação – acto pelo qual é reconhecido a uma entidade que exerça a actividade de Entidade Certificadora o preenchimento dos requisitos definidos no presente diploma.

D

Dispositivo seguro de criação de assinatura – dispositivo de criação de assinatura que assegura, através de meios técnicos e processuais adequados, que:

i. Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura só possam ocorrer uma única vez e que a confidencialidade desses dados se encontre assegurada;

ii. Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura não possam, com um grau razoável de segurança, ser deduzidos de outros dados e que a assinatura esteja protegida contra falsificações realizadas através das tecnologias disponíveis;

iii. Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura possam ser eficazmente protegidos pelo titular contra a utilização ilegítima por terceiros;

iv. Os dados que careçam de assinatura não sejam modificados e possam ser apresentados ao titular antes do processo de assinatura.

E

Entidade Certificadora – uma entidade que realiza actividades de certificação digital.

Entidade de Registo – uma entidade a qual uma Entidade Certificadora delega a actividade de recolha e registo dos dados a incluir em certificados.

Equipamentos periféricos – são aparelhos ou placas de expansão que enviam ou recebem informações do computador, tais como: computadores, impressoras, discos, entre outros.

T

Titular – a pessoa singular ou colectiva identificada num certificado como a detentora de um certificado.

V

Validação cronológica – declaração de Entidade Certificadora que atesta a data e hora da criação, expedição ou recepção de um documento electrónico.

Decreto n.º 60/2019

de 3 de Julho

Havendo necessidade de aprovar o subsídio especial remuneratório dos Funcionários e Agentes do Estado de Carreira de Regime Geral e Especial não Diferenciada que exercem funções técnico-administrativas nos Tribunais, no Conselho Constitucional e no Ministério Público, e nos respectivos órgãos de gestão e disciplina, ao abrigo da alínea *f*) do artigo 203 da Constituiçao da República de Moçambique, o Conselho de Ministros decreta:

Artigo 1. É fixado o subsídio especial em 75%, a incidir sobre o salário base da função ou categoria profissional dos Funcionários e Agentes do Estado de Carreira de Regime Geral e Especial não Diferenciada que exercem funções técnico-administrativas nos Tribunais, no Conselho Constitucional e no Ministério Público e nos respectivos órgãos de gestão e disciplina.

Art. 2. O Presente Decreto entra em vigor a partir de 1 de Janeiro de 2020.

Aprovado pelo Conselho de Ministros, aos 21 de Maio de 2019.

Publique-se.

O Primeiro Ministro, *Carlos Agostinho do Rosário*.

Preço — 60,00 MT

Imprensa Nacional de Moçambique, E.P.