# ANEXO I

# REGULAMENTO DE CREDENCIAÇÃO DE ORGANISMOS DE CERTIFICAÇÃO

## PREÂMBULO

A Agência Reguladora Multissectorial da Economia – ARME, nos termos do n.º 1, do artigo 1.º, do Decreto-lei n.º 50/2018, de 20 de setembro, que cria a ARME e aprova os seus Estatutos, é uma autoridade administrativa independente, de base institucional, dotada de funções reguladoras, incluindo a de regulamentação, supervisão e sancionamento de infrações, que tem por finalidade principal a atividade administrativa de regulação técnica e económica dos setores das comunicações eletrónicas, energia, água e transportes coletivos urbanos e interurbanos de passageiros, segundo o n.º 1, do artigo 2.º, do Decreto-lei n.º 50/2018, de 20 de outubro.

O Decreto-lei n.º 50/2018, de 20 de setembro, na alínea *f)*, do seu artigo 15.º, atribui aos órgãos da ARME, no âmbito da sua competência de supervisão, como entidade reguladora do setor das comunicações eletrónicas, a competência de supervisionar as entidades de certificação.

Assim, definiu-se no artigo 82.º, do Decreto-lei n.º 27/2023, de 20 de outubro, que estabelece as normas aplicáveis aos serviços de confiança, nomeadamente às transações eletrónicas, e institui um quadro legal para as assinaturas eletrónicas, os selos eletrónicos, os selos temporais, os documentos eletrónicos, os serviços de certificados para autenticação de sítios *Web,* arquivo eletrónico, o certificado eletrónico de atributos, a gestão de dispositivos de criação de assinaturas e de selos eletrónicos à distância, e os livros-razão eletrónicos, que as funções de autoridade credenciadora são atribuídas à Entidade Reguladora do Sector das Comunicações Eletrónicas, ou seja, à ARME.

Para a prossecução destas atribuições, no âmbito da sua competência como Entidade Reguladora do Sector das Comunicações Eletrónicas, incluindo, principalmente, as funções como autoridade credenciadora, a ARME deve emitir e publicar no seu sítio da *Internet* e no *Boletim Oficial* as normas de acreditação de auditor de segurança, nos termos do n.º 5, do artigo 27.º, e do artigo 99.º, do Decreto-Lei n.º 27/2023, de 20 de outubro.

No quadro regulatório definido pela legislação de referência no que respeita às atividades de credenciação e certificação no âmbito da Infraestrutura de Chaves Públicas de Cabo Verde – ICP – CV, compete à ARME, designadamente, definir quais são as regras que devem ser observadas pelos organismos que pretendam realizar as avaliações de

conformidade dos prestadores qualificados de serviços de confiança, bem como estabelecer o procedimento de credenciação desses organismos.

Cabo Verde se beneficia se os seus serviços forem reconhecidos internacionalmente, logo, é necessário que a avaliação de conformidade dos prestadores desses serviços seja realizada por organismos de certificação que estejam acreditados por organismos de acreditação que façam parte de programas de acordos multilaterais de reconhecimento mútuo de acreditação.

No que respeita à acreditação, dois grupos internacionais são considerados chaves, a Cooperação Internacional de Acreditação de Laboratórios – ILAC, e o Foro Internacional de Acreditação – IAF, ambos com o objetivo de garantir uma maior segurança e confiança no comércio internacional.

Atualmente, nem a ARME, nem outros organismos de Cabo Verde não integram programas de acordos de reconhecimento multilaterais de acreditação. Neste sentido, são aceites acreditações concedidas por organismos de acreditação de outros países, desde que façam parte dos referidos programas.

A avaliação de conformidade de entidades certificadoras que emitem certificados qualificados para *sites* de *internet* e para a assinatura de *e-mails*, também conhecidos como certificados publicamente confiáveis, deve ser realizada por organismos de certificação que estejam credenciados no Programa *WebTrust*, do *CPA Canada*, ou no *Accredited Conformity Assessment Bodies' Council – ACAB*, visto que, os relatórios de auditoria emitidos são aceites pela Adobe e pelo Programa de Raízes Confiáveis do Mozilla, que serve de base para diferentes desenvolvedores de *software* para criação de suas listas de confiança.

Neste sentido, o regulamento de credenciação de organismos de certificação tem por objeto define as normas previstas no n.º 5, do artigo 27.º, do Decreto-lei n.º 27/2023 de 20 de outubro, necessárias para a credenciação de organismos de certificação que realizam avaliações de conformidade aos prestadores dos serviços de transações eletrónicas, as assinaturas eletrónicas, os selos eletrónicos, os selos temporais, os documentos eletrónicos, arquivo eletrónico, o certificado eletrónico de atributos, a gestão de dispositivos de criação de assinaturas e de selos eletrónicos à distância, e os livros-razão eletrónicos; ou serviços de certificados para autenticação de sítios *Web*.

CAPÍTULO I

**Disposições Gerais**

Artigo 1.º

**Objeto**

O presente regulamento define as normas previstas no n.º 5, do artigo 27.º, do Decreto-lei n.º 27/2023 de 20 de outubro, necessárias para a credenciação de organismos de certificação que realizam avaliações de conformidade aos prestadores dos seguintes serviços de confiança:

a) Transações eletrónicas, as assinaturas eletrónicas, os selos eletrónicos, os selos temporais, os documentos eletrónicos, arquivo eletrónico, o certificado eletrónico de atributos, a gestão de dispositivos de criação de assinaturas e de selos eletrónicos à distância, e os livros-razão eletrónicos; ou

b) Serviços de certificados para autenticação de sítios *Web*.

Artigo 2.º

**Âmbito**

O presente regulamento aplica-se a todas as pessoas coletivas que pretendam ser credenciadas para realização de avaliações de conformidade dos prestadores qualificados de serviços de confiança, no âmbito do Decreto-lei n.º 27/2023, de 20 de outubro.

Artigo 3.º

**Siglas e definições**

1. No presente regulamento são utilizadas as seguintes siglas:

*a)* ARME: Agência Reguladora Multissetorial da Economia;

*b)* CAB: Certification Authority Browser;

*c)* CISA: Certified Information System Auditor;

*d)* CISM: Certified Information Security Manager;

*e)* CISSP: Certified Information Systems Security Professional;

*f)* EA: Cooperação Europeia para Acreditação;

*g)* EC: Entidade Certificadora;

*h)* ETSI: European Telecommunications Standards Institute;

*i)* IAF: Fórum Internacional de Acreditação ICP Infraestrutura de Chaves Públicas;

*j)* IGPQI: Instituto de Gestão da Qualidade e da Propriedade intelectual;

*k)* IPAC: Instituto Português de Acreditação;

*l)* ISO/IEC: Internacional Organization for Standardization / International Electrotechnical Commission.

2. Para efeito do presente regulamento, entende-se por:

*a)* Acreditação: a atividade de acreditação consiste na avaliação e reconhecimento da competência técnica de entidades para efetuar atividades específicas de avaliação da conformidade (e.g. ensaios, calibrações, certificações e inspeções). A acreditação integra-se num sistema geral que inclui a avaliação da conformidade e a fiscalização do mercado e visa avaliar e garantir a conformidade com os requisitos aplicáveis.

*b)* Avaliação de conformidade: a avaliação da conformidade consiste na demonstração que um dado bem, produto, processo ou serviço cumpre com os requisitos que lhe são aplicáveis, através da realização de ensaios, calibrações, inspeções e verificações.

*c)* Organismo de acreditação: o organismo a proceder à acreditação com poderes de autoridade pública;

*d)* Organismo de certificação: é o organismo que efetua actividades de avaliação da conformidade, nomeadamente a calibração, ensaio, certificação e inspeção.

## CAPÍTULO II

## Procedimento de Credenciação de Organismos de Certificação

### Artigo 3.º

### Condições do organismo de certificação

1. As pessoas colectivas, que pretendam exercer as funções de organismo de certificação no âmbito do Decreto-lei n.º 27/2023, são credenciadas pela Autoridade Credenciadora se preencherem, cumulativamente, as seguintes condições:

*a)* O organismo de certificação ser uma pessoa coletiva, independente do Prestador Qualificado de Serviço de Confiança, de reconhecida idoneidade, experiência e qualificações comprovadas na área da segurança de informação, na execução de auditorias de segurança e na utilização das normas internacionais aplicáveis à auditoria de segurança da informação e avaliações de conformidade;

*b)* O organismo de certificação que solicita a credenciação à Autoridade Credenciadora deve estar registado e acreditado por organismo de acreditação que participa de programas de acordos de reconhecimento multilaterais, como EA ou IAF:

*i.* Este registo e a acreditação devem ser comprovadas por meio de apresentação de certificado de acreditação emitido pelo organismo oficial de acreditação do país que o atribuiu e dentro do prazo de validade, bem como devem ser

apresentados os meios de prova de que o organismo de acreditação encontra-se inscrito na EA ou na IAF;

*ii.* O certificado deve ser emitido em língua oficial do organismo nacional de acreditação e em inglês, e publicado no *site* do organismo nacional de acreditação e mantido atualizado. Nos casos em que a língua oficial do organismo nacional de acreditação não seja a portuguesa, o certificado deve ser acompanhado de tradução para o português realizado por tradutor juramentado;

*iii.* O âmbito do certificado de acreditação deve estar adequado ao tipo de credenciação solicitado à Autoridade Credenciadora.

*e)* Para realizar auditorias aos Prestadores de Serviços de Confiança que emitem certificados qualificados e/ou certificados publicamente confiáveis, também pode ser aceite a candidatura de organismo de certificação que esteja devidamente acreditado pelo programa *WebTrust* da CPA Canada e pela Accredited Conformity Assessment Bodies' Council.

*f)* A acreditação referida na alínea e) deve ser comprovada por meio de apresentação de:

*i.* Documento "*WebTrust for Certification Authorities - Practitioner Enrollment And Renewal Application*" devidamente assinado pelo CPA Canada, ainda dentro do prazo de validade; e

*ii.* Comprovativo do CPA Canada onde conste o nome do organismo de certificação como habilitado para atuar em Cabo Verde; ou

*iii.* Certificado de acreditação na *Accredited Conformity Assessment Bodies' Council* (ACAB'c), ou comprovativo de que se encontra inscrito na lista da CAB-member List.

*a)* O organismo de certificação deve emitir e assinar um termo que garante que os membros da sua equipa não atuam 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.

*b)* Não pode ser realizada subcontratação, devendo a avaliação de conformidade ser realizada pela própria empresa que se credenciou junto da Autoridade Credenciadora.

*c)* As avaliações de conformidade são efetuadas tendo por base as diretrizes constantes no documento "Regras para Avaliação de Conformidade de Prestadores Qualificados de Serviços de Confiança", publicado pela Autoridade Credenciadora.

2. O organismo de certificação deve ainda atender às seguintes condições:

*a)* Não estar em estado de falência, liquidação ou de cessação de atividade, ou ter pendentes processos correspondentes;

*b)* Não ter sido condenado, por sentença transitada em julgado, por qualquer delito que afete a honra profissional, nomeadamente fraude, ou ter sofrido punição disciplinar por falta grave em matéria profissional;

*c)* Não enviar, de forma consciente ou intencional, informação falsa, incompleta ou omissa com indução de dolo à Autoridade Credenciadora;

*d)* Dispor de pelo menos um auditor qualificado para conduzir as avaliações de conformidade, conforme o artigo 4.º.

Artigo 4.º

**Requisitos e competências dos auditores**

1. Para realizar as avaliações de conformidade dos Prestadores de Serviços de Confiança, os Organismos de Certificação deverão designar auditores que preencham, obrigatoriamente, os seguintes requisitos:

*a)* Possuir formação académica de nível superior ou sua equiparação mediante valorização de currículo profissional;

*b)* Ter, no mínimo, quatro anos de experiência de trabalho, a tempo inteiro, em assuntos relacionados com tecnologias de informação, em que pelo menos 2 (dois) desses anos tenham sido desenvolvidos em cargos ou funções relacionadas com segurança da informação;

*c)* Possuir conhecimentos, no âmbito da segurança da informação, sobre a condução de análises de risco, de forma a identificar os ativos, ameaças e vulnerabilidades a que estão sujeitas os prestadores de serviços de confiança, no sentido de compreender o impacto, consequente minimização e controlo dos riscos;

*d)* Ter conhecimentos atualizados nos assuntos relacionados com as tecnologias em que se baseiam as Infraestruturas de Chaves Públicas e demais serviços de confiança;

*e)* Ter conhecimentos atualizados nos assuntos relacionados com a gestão da segurança da informação e análise e avaliação de sistemas, bem com base, entre outros, nos requisitos da norma ISO/IEC 27001;

*f)* Ser fiável e possuir qualidades de lealdade funcional, competência profissional e idoneidade cívica;

*g)* Ter capacidade para detectar e analisar incidentes de segurança nos registos das operações realizadas pelo prestador de serviço de confiança, durante a sua actividade;

*h)* Conhecer, compreender e interpretar de forma adequada os princípios e processos relativos à análise, avaliação e gestão do risco;

*i)* Estar apto para a preparação, distribuição de tarefas e condução de equipas de auditoria, bem como no âmbito da revisão da documentação e avaliação da auditoria;

*j)* Possuir experiência na elaboração e apresentação de relatórios finais de auditoria;

*k)* Ter exercido atividade de auditor em pelo menos quatro auditorias de entidade certificadoras; e

*l)* Conhecer e interpretar a legislação nacional que estabelece as regras para os serviços de confiança.

2. As certificações internacionalmente exigidas, são uma das seguintes:

*a)* CISA-Certified Information System Auditor;

*b)* CISM-Certified Information Security Manager;

*c)* CISSP-Certified Information Systems Security Professional;

*d)* ISSO/IEC 27001 Lead Auditor.

Artigo 5.º

**Pedido de credenciação**

1. O pedido de credenciação de Organismos de Certificação e os documentos requeridos no n.º 3 devem ser encaminhados para o endereço da sede da Autoridade Credenciadora e para o e-mail xxxx@arme.cv, em formato pdf assinado digitalmente.
2. São aceites apenas os processos que reúnam os requisitos mínimos de candidatura constantes neste regulamento, os quais devem ser devidamente comprovados.
3. O pedido de credenciação deverá ser instruído dos seguintes documentos:

*a)* Carta, em papel timbrado do organismo de certificação, dirigido à Autoridade Credenciadora, a solicitar a credenciação como organismo de certificação nos termos do Decreto Lei n.º 27/2023 de outubro;

*b)* Formulário disponbilizado pela autoridade credenciadora, devidamente preenchido;

*c)* Certidão da Conservatória do Registo Comercial ou fotocópia autenticada;

*d)* Fotocópia da Declaração do número de identificação fiscal;

*e)* Fotocópia do contrato social ou estatutos da empresa e suas posteriores alterações, onde conste nomeadamente o objecto social;

*f)* Alvará (fotocópia), se a atividade assim o exigir;

g) Currículo da pessoa coletiva (trabalhos realizados que entender evidenciar em seu abono);

h) Certidões ou outros documentos comprobatórios do cumprimento do disposto nos pontos *i* e *ii*, da alínea l), do artigo 3.º;

i) Declaração, a referir o cumprimento do disposto no ponto iii, da alínea l), do artrigo 3.º;

j) Individualmente, devem ser entregues, por cada membro da equipa de auditoria, os seguintes elementos:

   *i.* Uma fotografia a cores;

   *ii.* Fotocópia do documento de identificação;

   *iii.* Declaração, que garante que o candidato é fiável e possui qualidades de lealdade funcional e idoneidade cívica para exercer as funções de auditor de segurança, assinada pela entidade máxima da empresa;

   *iv.* Currículo detalhado;

   *v.* Outros elementos e/ou referências considerados relevantes para a demonstração da aptidão para o exercício da função de auditor.

k) O membro da equipa que desempenhe a função de auditor coordenador deve ter, pelo menos, 5 anos de experiência, dez auditorias realizadas e apresentar, adicionalmente, documentos comprovativos do exercício da atividade de auditor onde conste, para cada uma das auditorias:

   *i.* A identificação da entidade auditada;

   *ii.* A identificação da sua função; e

   *iii.* A data, duração e âmbito da auditoria.

4. Considera-se documentação adequada para comprovação da atividade de auditor, entre outros, declarações da(s) entidade(s) que foram alvo das auditorias, ou outra à consideração do avaliado desde que permita aferir a validade das auditorias.

5. Todas as referências e elementos incluídos nos *Curriculum* devem ser acompanhados dos respetivos comprovativos.

6. No caso de se tratar de uma empresa estrangeira que não tenha filial ou representante legal no país, as exigências estabelecidas serão atendidas mediante a apresentação de documentos equivalentes autenticados por Apostila de Haia e traduzidos por tradução.

7. Documentos complementares podem ser solicitados pela Autoridade Credenciadora, que neste caso, define novo prazo para envio dos documentos.

8. Se a solicitação do número anterior não for atendida em até 15 (quinze) dias, o processo será arquivado, mediante despacho fundamentado da Autoridade Credenciadora.

9. Os documentos apresentados pela candidata para credenciação constituirá processo específico, e será mantida por prazo não inferior a 5 (cinco) anos, podendo ser consultada por interessados.

10. Sobre o pedido de credenciação ou de renovação, a Autoridade Credenciadora, por meio de decisão fundamentada, pode:

    *a)* Deferir o pedido;

    *b)* Notificar a candidata para, no prazo máximo de 15 (quinze) dias corridos, complementar a documentação apresentada;

    *c)* Indeferir o pedido se, vencido o prazo da alínea b), não forem cumpridas as exigências constantes da notificação; e

    *d)* Indeferir o pedido que não atenda aos requisitos técnicos estabelecidos.

11. A credenciação será publicada no Boletim Oficial da República e será renovada a cada três (3) anos, a contar da data da publicação da respectiva credenciação ou renovação.

12. A Autoridade Credencidadora publica em seu sítio na internet a lista de organismos de certificação credenciados para realização de avaliações de conformidade nos moldes do Decreto Lei n.º 27/2023 de outubro, na página Registo de Organismos de Certificação Credenciados.

13. Nas renovações, mediante solicitação à Autoridade Credenciadora, o organismo de certificação anexa a mesma documentação apresentada para a credenciação inicial, podendo, os documentos que não sofreram alteração desde o último deferimento, ser substituídos por declaração expressa do responsável legal, sob as penas da lei, de que não houve alteração.

14. Qualquer alteração ocorrida, quer seja em atos constitutivos, estatuto, contrato social, organograma ou vinculação da entidade, quer seja dos dirigentes ou da equipa técnica de auditores, é submetida imediatamente ao conhecimento da Autoridade Credenciadora, mediante formalização enviada por email para xxxx@arme.cv, a qual faz parte do processo de credenciação do respetivo organismo de certificação.

15. A apresentação de documentos para fins de credenciação ou revogação de credenciação será sempre por meio físico e eletrónico.

16. Nos casos em que ocorrem a alteração dos documentos, é responsabilidade dos organismos de certificação credenciados solicitar à autoridade credenciadora a atualização de seus dados de registo, observando o disposto no n.º 1 do artigo 5.º.

17. O organismo de certificação credenciado poderá solicitar a a revogação da credenciação à autoridade credenciadora, a qualquer momento.

18. Indeferido o pedido de credenciação ou de renovação de credenciação, a Autoridade Credenciadora notificará diretamente ao interessado, por meio de carta, procedendo aos ajustes correspondentes no Cadastro de Certificação Credenciados.

19. A Autoridade Credenciadora deverá, no prazo de 15 (quinze) dias corridos, a contar do deferimento do credenciação, da renovação ou da recepção do pedido de revogação da credenciação, atualizar o Cadastro de Organismos de Certificação Credenciados, disponível em seu *website*.

## CAPÍTULO III

## **Disposições Finais**

### Artigo 6.º

### **Entrada em vigor**

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