Sexta-feira, 21 de março de 2025

II Série
Número 53

BOLETIM OFICIAL

CONSELHO DE MINISTROS

Resolução n. º 12/2025

Sumário: Renovando os mandatos dos membros do Conselho da Administração do Laboratório de Engenharia Civil de Cabo Verde – Entidade Pública Empresarial.

De 21 de março

Ao abrigo do disposto nos artigos 11º e 13º do Estatuto Laboratório de Engenharia Civil de Cabo Verde, Entidade Pública Empresarial, aprovado pelo Decreto-Lei n.º 31/2014, de 27 de julho, alterado pelo Decreto-Lei n.º 22/2018, de 9 de maio; e

Nos termos do n.º 2 do artigo 265º da Constituição, o Governo aprova a seguinte Resolução:

Artigo 1º

Renovação dos mandatos

São renovados os mandatos dos membros do Conselho de Administração do Laboratório de Engenharia Civil de Cabo Verde, Entidade Pública Empresarial, nos cargos que se indicam:

a) Adlisa Maria Delgado - Presidente;

b) Manuel Vasconcelos Fernandes – Administrador Executivo;

c) Leinilda Jesus Dias Pereira – Administradora não Executiva.

Artigo 2º

Entrada em vigor

A presente Resolução entra em vigor no dia seguinte ao da sua publicação e produz efeitos a 1 de agosto de 2024.

Aprovada em Conselho de Ministro, aos 4 de março de 2025. — O Primeiro Ministro, *José Ulisses de Pina Correia e Silva.*

A2025/S2/BO53/13505
Resolução n. º 12/2025

CHEFIA DO GOVERNO
Secretaria-Geral do Governo

Republicação n.º 7/2025

Sumário: Retifica e republica-se na íntegra a publicação feita de forma inexata no Boletim Oficial n.º 47, II Série de 13 de março de 2025, referente ao Despacho n.º 10/2025, que autoriza a realização de despesa com a contratação da empreitada para a realização da obra de construção do aterro controlado da ilha de São Vicente.

Por ter sido publicado de forma inexata no Boletim Oficial n.º 47, II Série de 13-03-2025, o Despacho n.º 10/2025, autorizando a realização de despesa com a contratação da empreitada para a realização da obra de construção do aterro controlado da ilha de São Vicente, retifica-se e republica-se na parte que se interessa.

Secretária-geral do Governo, aos 19 de março de 2025. — A Secretária Geral do Governo, *Maria José Monteiro.*

Despacho n.º 10/2025

De 27 de fevereiro de 2025

Ao abrigo do disposto no artigo 42º, n.º 1, alínea d), do Decreto-Lei n.º 1/2009, de 5 de janeiro, aplicável por força do disposto no n.º 2 do artigo 3º da Lei n.º 88/VIII/2015, de 14 de abril, autorizo, o Ministério da Agricultura e Ambiente, através da Agência Nacional de Água e Saneamento, a realização da despesa com a contratação da empreitada para a realização da obra de construção do aterro controlado da ilha de São Vicente, no montante total de 34.592.000$00 (trinta e quatro milhões, quinhentos e noventa e dois mil escudos), acrescido de impostos à taxa legal em vigor.

A presente aquisição será financiada pelo Fundo do Ambiente de Cabo Verde.

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

Publique-se.

Gabinete do Primeiro-ministro, na Praia, aos 27 de fevereiro de 2025. — O Primeiro Ministro, *José Ulisses de Pina Correia e Silva.*

A2025/S2/BO53/13505
Republicação n.º 7/2025

MINISTÉRIO DA AGRICULTURA E AMBIENTE
Direção de Serviços de Gestão de Recursos Humanos, Financeiro e Patrimonial

Rescisão de Contrato de Trabalho n.º 21/2025

Sumário: Rescindindo, a seu pedido, o contrato de trabalho a termo celebrado entre o Ministério da Agricultura e Ambiente e Anilton dos Reis Vieira.

Rescisão de Contrato de Trabalho a Termo pelo Trabalhador

É rescindido, a seu pedido, nos termos do artigo 243º do Código Laboral, o Contrato de Trabalho a Termo celebrado em 02 de janeiro de 2015, entre o Ministério da Agricultura e Ambiente e o Senhor Anilton dos Reis Vieira, Apoio Operacional Nível III, com efeitos a partir de 05 de fevereiro de 2025.

Praia, aos 18 de março de 2025. — A Diretora de Serviço, *Edna Patrícia Francês Lima Tavares.*

A2025/S2/BO53/13505
Rescisão de Contrato de Trabalho n.º 21/2025

MINISTÉRIO DA AGRICULTURA E AMBIENTE
Direção de Serviços de Gestão de Recursos Humanos, Financeiro e Patrimonial

Extrato do Despacho n.º 285/2025

Sumário: Promovendo João Soares dos Reis Borges Gomes, Técnico Sénior Nível I, do Quadro de Pessoal do Ministério da Agricultura e Ambiente para Técnico Sénior Nível II.

Extrato do Despacho de S. Ex.ª do Ministro da Agricultura e Ambiente

De 27 de setembro de 2024

João Soares dos Reis Borges Gomes, Técnico Sénior Nível I, quadro definitivo do Ministério da Agricultura e Ambiente, é Promovido para Técnico Sénior Nível II, nos termos do artigo 37º, do Decreto-Lei n.º 9/2013, de 26 de fevereiro, conjugado com o n.º 2 do artigo 49º do Decreto-Lei n.º 59/2014, de 04 de novembro.

A despesa tem cabimento na rubrica 02.01.01.01.02 – Pessoal de quadro, no centro de custo 40.10.20.05.03 – DGASP- Implementação de Políticas e Promoção do Desenvolvimento Rural do Ministério da Agricultura e Ambiente.

Direção de Serviço de Gestão de Recursos Humanos, Financeiro e Patrimonial do Ministério da Agricultura e Ambiente, na Praia, aos 3 de fevereiro de 2025. — A Diretora de Serviço, *Edna Patrícia Francês Lima Tavares.*

A2025/S2/BO53/13505
Extrato do Despacho n.º 285/2025

MINISTÉRIO DA AGRICULTURA E AMBIENTE
Direção de Serviços de Gestão de Recursos Humanos, Financeiro e Patrimonial

Extrato do Despacho n.º 286/2025

Sumário: Promovendo Eneida Maria Pereira Rodrigues Silva, Técnico Sénior Nível II, do Quadro de Pessoal do Ministério da Agricultura e Ambiente para Técnico Sénior Nível III.

Extrato do Despacho de S. Ex.ª do Ministro da Agricultura e Ambiente

De 27 de setembro de 2024

Eneida Maria Pereira Rodrigues Silva, Técnico Sénior Nível II, quadro definitivo do Ministério da Agricultura e Ambiente, é Promovida para Técnico Sénior Nível III, nos termos do n.º 6 artigo 37º, do Decreto-Lei n.º 9/2013, de 26 de fevereiro, conjugado com o n.º 2 do artigo 49º do Decreto-Lei n.º 59/2014, de 04 de novembro.

A despesa tem cabimento na rubrica 02.01.01.01.02 – Pessoal de quadro, no centro de custo 40.10.20.05.03 – DGASP- Implementação de Políticas e Promoção do Desenvolvimento Rural do Ministério da Agricultura e Ambiente.

Direção de Serviço de Gestão de Recursos Humanos, Financeiro e Patrimonial do Ministério da Agricultura e Ambiente, na Praia, aos 3 de fevereiro de 2025. — A Diretora de Serviço, *Edna Patrícia Francês Lima Tavares.*

A2025/S2/BO53/13505
Extrato do Despacho n.º 286/2025

COMISSÃO NACIONAL DE ELEIÇÕES

Edital n.º 01/CNE/2025

Sumário: Eleições Presidenciais de 2021 - Prestação de Contas Eleitorais – Candidatura de Gilson Alves. Em cumprimento do disposto no artigo 133º do Código Eleitoral, a Comissão Nacional de Eleições publica as contas discriminadas de candidatura e campanha eleitoral.

Assunto: Eleições Presidenciais de 2021 - Prestação de Contas Eleitorais – Candidatura do Dr. Gilson João dos Santos Alves.

Em cumprimento do disposto no artigo 133º de Código Eleitoral, a Comissão Nacional de Eleições publica as contas discriminadas de candidatura e campanha eleitoral às eleições presidenciais realizadas de 17 de outubro de 2021, aprovadas pelo plenário da CNE, na reunião de 21 de fevereiro de 2025.

Prestação de contas eleitorais - contas regulares consolidadas (a)

DESIGNAÇÃO	Candidatura		TOTAL POR RUBRICA	
	Gilson João dos Santos Alves			
	Valor	%	Valor	%
FINANCIAMENTOS (b)				
Receitas				
Contribuições de partidos nacionais	-	0,0%	-	0,0%
Donativos de particulares	-	0,0%	-	0,0%
Donativos em espécies	-	0,0%	-	0,0%
Donativos de eleitores não residentes em CV	-	0,0%	-	0,0%

A2025/S2/BO53/13505
Edital n.º 01/CNE/2025

Crédito comerciais	111 476,00	6,9%	111 476,00	6,9%
Contribuições de candidatos	1 502 561,00	93,1%	1 502 561,00	93,1%
Outras receitas (Impostos Retidos)		0,0%	-	0,0%
Subtotal (1)	1 614 037,00	100,0%	1 614 037,00	100,0%
Empréstimos de bancos sediados em CV (2)	-	0,0%	-	0,0%
Total de financiamentos (3 = 1 + 2)	1 614 037,00	100,0%	1 614 037,00	100,0%
DESPESAS (c)				
Despesas com o pessoal		0,0%	-	0,0%
Aquisição de bens e serviços	1 614 037,00	100,0%	1 614 037,00	100,0%
Juros e outros encargos	-	0,0%	-	0,0%
Outras despesas correntes	-	0,0%	-	0,0%
Total de despesas (d)	1 614 037,00	100,0%	1 614 037,00	100,0%

(a) Candidatura que prestaram contas ou cujas contas apresentadas foram consideradas regulares (artigo 133º do CE)

(b) Conforme a classificação dada no artigo 124º do Código Eleitoral

(c) Conforme o n.º 1 do artigo 127º do Código Eleitoral

(d) Plafond das despesas para cada candidato - 80% do montante global da subvenção do Estado prevista: 766.349.122$00 (n.º 1 do artigo 128º do CE).

A2025/S2/BO53/13505
Edital n.º 01/CNE/2025

Membro Secretário da CNE, *Elba Helena Rocha Pires.*

A2025/S2/BO53/13505
Edital n.º 01/CNE/2025

AGÊNCIA REGULADORA MULTISSETORIAL DA ECONOMIA - ARME
Conselho de Administração

Deliberação n.º 20/CA/2025

Sumário: Aprovando o regulamento que estabelece as normas aplicáveis à credenciação de organismos de certificação responsáveis pela realização de avaliações de conformidade junto dos prestadores dos serviços de confiança.

De 26 de fevereiro de 2025

Preâmbulo

A Agência Reguladora Multissetorial 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, dotada de competências reguladoras, incluindo regulamentação, supervisão e sancionamento de infrações. A sua principal finalidade é a regulação técnica e económica dos setores das comunicações eletrónicas, energia, água e transportes coletivos urbanos e interurbanos de passageiros, conforme disposto no n.º 1 do artigo 2.º do referido decreto-lei.

No âmbito da sua competência de supervisão do setor das comunicações eletrónicas, a ARME tem a responsabilidade de supervisionar as entidades de certificação, nos termos da alínea f) do artigo 15.º dos Estatutos da ARME aprovados pelo Decreto-Lei n.º 50/2018, de 20 de setembro. Esta atribuição foi reforçada pelo artigo 82.º do Decreto-Lei n.º 27/2023, de 20 de outubro, que estabelece o quadro legal aplicável aos serviços de confiança, incluindo assinaturas eletrónicas, selos eletrónicos, selos temporais, documentos eletrónicos, certificados para autenticação de sítios Web, arquivo eletrónico e livros-razão eletrónicos. De acordo com esta legislação, a ARME é designada como a autoridade credenciadora responsável pela definição e implementação das normas de acreditação de auditores de segurança e organismos de certificação.

A evolução tecnológica e a crescente digitalização da economia e da sociedade exigem mecanismos eficazes para garantir a segurança, a autenticidade e a confiabilidade das transações eletrónicas. Neste contexto, os organismos de certificação desempenham um papel fundamental, assegurando a conformidade dos prestadores de serviços de confiança com os requisitos técnicos e regulamentares estabelecidos.

No quadro da Infraestrutura de Chaves Públicas de Cabo Verde (ICP-CV), torna-se essencial garantir que a avaliação de conformidade dos prestadores de serviços de confiança seja realizada por organismos de certificação devidamente acreditados. A credenciação desses organismos deve seguir padrões internacionais reconhecidos, assegurando que os serviços prestados em Cabo Verde sejam aceites globalmente. Para tal, as acreditações devem ser concedidas por organismos que integrem programas de acordos multilaterais de reconhecimento mútuo de acreditação, como

A2025/S2/BO53/13505
Deliberação n.º 20/CA/2025

os promovidos pela Cooperação Internacional de Acreditação de Laboratórios (ILAC) e pelo Fórum Internacional de Acreditação (IAF).

Relativamente aos organismos de acreditação integrados nesses programas, são reconhecidas acreditações emitidas por entidades estrangeiras de reputação internacional. Além disso, no caso específico das entidades certificadoras que emitem certificados qualificados para sítios *Web* e assinaturas de e-mails – conhecidos como certificados publicamente confiáveis –, a avaliação de conformidade deve ser realizada por organismos de certificação credenciados no Programa *WebTrust*, do CPA Canada, ou no *Accredited Conformity Assessment Bodie's Council* (ACAB'c). Estes programas são amplamente aceites por desenvolvedores de software e garantem que os certificados emitidos sejam reconhecidos globalmente.

Deste modo, o presente regulamento estabelece as normas necessárias para a credenciação de organismos de certificação que realizam avaliações de conformidade aos prestadores de serviços de confiança, assegurando a fiabilidade e segurança das transações eletrónicas em Cabo Verde. A implementação deste quadro normativo contribuirá para a proteção dos utilizadores, o fortalecimento da economia digital e o alinhamento do país com os melhores padrões internacionais.

Assim, nos termos da alínea *b)* do artigo 14.º, e da alínea *f)* do artigo 15.º dos Estatutos da ARME, aprovados pelo Decreto-Lei n.º 50/2018, de 20 de setembro, do artigo 82.º, da alínea *o)* do artigo 83.º, e do n.º 1 do artigo 99.º do Decreto-Lei n.º 27/2023 de 20 de outubro, o Conselho de Administração, em sua reunião ordinária de 16 de fevereiro de 2025, aprova o presente Regulamento, que estabelece as normas aplicáveis à credenciação de organismos de certificação responsáveis pela realização de avaliações de conformidade junto dos prestadores dos serviços de confiança.

Artigo 1.º

Aprovação

É aprovado o regulamento que estabelece as normas aplicáveis à credenciação de organismos de certificação responsáveis pela realização de avaliações de conformidade junto dos prestadores dos serviços de confiança nos termos do Decreto-Lei n.º 27/2023 de 20 de outubro.

Artigo 2.º

Entrada em vigor

A presente deliberação entra em vigor no dia seguinte ao da sua publicação em Boletim Oficial.

Feita na Cidade da Praia, aos 26 de fevereiro de 2025. — O Conselho de Administração, O Presidente, *Leonilde Santos*, os Administradores, *João Tomar* e *Carlos Ramos*.

A2025/S2/BO53/13505
Deliberação n.º 20/CA/2025

REGULAMENTO DE CREDENCIAÇÃO DE ORGANISMOS DE CERTIFICAÇÃO

CAPÍTULO I

Disposições Gerais

Artigo 1.º

Objeto

O presente regulamento estabelece as normas aplicáveis à credenciação de organismos de certificação responsáveis pela realização de avaliações de conformidade junto dos prestadores dos seguintes serviços de confiança:

a)Transações eletrónicas, assinaturas eletrónicas, selos eletrónicos, selos temporais, documentos eletrónicos, arquivo eletrónico, certificados eletrónicos de atributos, gestão de dispositivos de criação de assinaturas e de selos eletrónicos à distância, bem como livros-razão eletrónicos; e

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

Artigo 2.º

Âmbito

O presente regulamento é aplicável a todas as pessoas coletivas que pretendam obter credenciação para a realização de avaliações de conformidade dos prestadores qualificados de serviços de confiança, nos termos 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;

A2025/S2/BO53/13505
Deliberação n.º 20/CA/2025

g) EC: Entidade Certificadora;

h) ETSI:European Telecommunications Standards Institute;

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

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

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

a) "Acreditação", procedimento através do qual um organismo de acreditação reconhece, formalmente, que uma entidade é competente tecnicamente para efectuar uma determinada função específica, de acordo com normas internacionais ou nacionais, baseando-se, complementarmente, nas orientações emitidas pelos organismos internacionais de acreditação;

b) "Avaliação de conformidade", é o processo sistemático destinado a verificar se um bem, produto, processo ou serviço atende aos requisitos técnicos, regulatórios e normativos aplicáveis, por meio da realização de ensaios, calibrações, inspeções e auditorias;

c) "Organismo de acreditação": é a entidade com poderes de autoridade pública responsável por avaliar, reconhecer e supervisionar a competência técnica de organismos de avaliação da conformidade, garantindo que operem em conformidade com normas e regulamentos nacionais e internacionais;

d) "Organismo de certificação", é o organismo reconhecido pela autoridade credenciadora como sendo competente para avaliação e certificação da conformidade de prestadores qualificados de serviços de confiança e dos serviços de confiança qualificados prestados.

CAPÍTULO II

Procedimento de Credenciação de Organismos de Certificação

Artigo 4.º

Condições do organismo de certificação

1. As pessoas coletivas que pretendam exercer funções como organismos de certificação, nos termos do Decreto-Lei n.º 27/2023, de 20 de outubro, devem ser previamente credenciadas pela Autoridade Credenciadora, desde que preencham, cumulativamente, as seguintes condições:

a) O organismo de certificação deve ser uma pessoa coletiva independente do Prestador Qualificado de Serviço de Confiança dotada de reconhecida idoneidade, experiência e qualificações comprovadas na área da segurança da informação, na execução de auditorias de

A2025/S2/BO53/13505
Deliberação n.º 20/CA/2025

segurança e na aplicação das normas internacionais aplicáveis à auditoria de segurança da informação e à avaliação da conformidade;

b) O organismo de certificação que solicita a credenciação à Autoridade Credenciadora deve estar registado e acreditado por um organismo de acreditação que integre programas de acordos de reconhecimento multilaterais como os promovidos pela EA ou pela IAF:

i. Este registo e a acreditação devem ser comprovados mediante a apresentação de certificado de acreditação emitido pelo organismo oficial de acreditação do país de origem dentro do prazo de validade, devendo igualmente ser apresentados os meios de prova que atestem a inscrição do organismo de acreditação na EA ou na IAF;

ii. O certificado deve ser emitido na língua oficial do organismo nacional de acreditação e em inglês, devendo ser publicado no respetivo site e mantido atualizado, sendo que, nos casos em que a língua oficial do organismo nacional de acreditação não seja o português, deve ser acompanhado de tradução para português realizada por tradutor;

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

c) 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 um organismo de certificação que esteja devidamente acreditado pelo programa WebTrust da CPA Canada ou pelo Accredited Conformity Assessment Bodies' Council;

d) A acreditação referida na alínea c) 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.

e) O organismo de certificação deve emitir e assinar um termo que garanta que os membros da sua equipa não atuam de forma parcial ou discriminatória, não prestaram serviços de consultoria à entidade certificadora nos últimos três anos, nem mantêm com esta qualquer outro acordo ou vínculo contratual;

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

A2025/S2/BO53/13505
Deliberação n.º 20/CA/2025

a) Não se encontrar em estado de falência, liquidação ou cessação de atividade, nem ter processos correspondentes pendentes;

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

c) Não enviar, de forma consciente ou intencional, informações falsas, incompletas ou omissas, com a intenção de induzir a Autoridade Credenciadora em erro;

d) Dispor de, pelo menos, um auditor qualificado para a condução das avaliações de conformidade, nos termos do artigo 5.º;

e) Não pode ser realizada subcontratação; a avaliação de conformidade deve ser realizada pela própria empresa que se credenciou junto da Autoridade Credenciadora;

f) As avaliações de conformidade são efetuadas com base nas regras constantes no Regulamento de avaliação de conformidade Prestadores Qualificados de Serviços de, publicado pela Autoridade Credenciadora.

Artigo 5.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 cumpram, obrigatoriamente, os seguintes requisitos:

a) Possuir formação académica de nível superior ou equivalente, mediante a valorização do currículo profissional;

b) Ter, no mínimo, quatro anos de experiência profissional a tempo inteiro em áreas relacionadas com tecnologias de informação, dos quais pelo menos dois anos tenham sido dedicados a 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 os prestadores de serviços de confiança estão expostos, visando compreender o impacto, bem como a minimização e controlo dos riscos subsequentes;

d) Ter conhecimentos atualizados sobre os assuntos relacionados com as tecnologias subjacentes às Infraestruturas de Chaves Públicas e demais serviços de confiança;

e) Ter conhecimentos atualizados sobre a gestão da segurança da informação, análise e avaliação

A2025/S2/BO53/13505
Deliberação n.º 20/CA/2025

de sistemas, com base, nomeadamente, 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 serviços de confiança durante a sua atividade;

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

i) Estar apto para a preparação, distribuição de tarefas e condução de equipas de auditoria, bem como para a revisão da documentação e avaliação da auditoria;

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

k) Ter exercido a atividade de auditor em, pelo menos, quatro auditorias realizadas a entidades certificadoras; e

l) Conhecer e interpretar a legislação nacional que estabelece as regras aplicáveis aos serviços de confiança.

2. A certificação exigida internacionalmente é 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 6.º

Pedido de credenciação

1. O pedido de credenciação dos Organismos de Certificação e os documentos exigidos no n.º 3 devem ser encaminhados para o endereço da sede da Autoridade Credenciadora e para o e-mail autoridadecredenciadora@arme.cv, em formato PDF assinado digitalmente.

2. São aceites apenas os processos que cumpram os requisitos de candidatura estabelecidos neste regulamento, os quais devem ser devidamente comprovados.

3. O pedido de credenciação deve ser acompanhado dos seguintes documentos:

A2025/S2/BO53/13505
Deliberação n.º 20/CA/2025

a) Carta em papel timbrado do organismo de certificação, dirigida à Autoridade Credenciadora, solicitando a credenciação como organismo de certificação, nos termos do Decreto-Lei n.º 27/2023, de 20 de outubro;

b) Formulário disponibilizado pela Autoridade Credenciadora, devidamente preenchido;

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

d) Fotocópia da Declaração de Número de Identificação Fiscal;

e) Fotocópia do contrato social ou estatutos da empresa, com as suas posteriores alterações, onde conste, nomeadamente, o objeto social;

f) Fotocópia do alvará, se a atividade o exigir;

g) Currículo da pessoa coletiva, com os trabalhos realizados que se considere relevante evidenciar em seu abono.

h) Certidões ou outros documentos comprobatórios do cumprimento do disposto nos pontos i e ii, da alínea d), do artigo 4.º;

i) Declaração, a referir o cumprimento do disposto nnas alíneas a) a f) do n.º 2 do artigo 4.º;

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

i. Fotografia a cores;

ii. Fotocópia do documento de identificação;

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

iv. Currículo detalhado;

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

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

a) A identificação da entidade auditada;

A2025/S2/BO53/13505
Deliberação n.º 20/CA/2025

b) A identificação da sua função; e

c) A data, duração e âmbito da auditoria.

5. Considera-se documentação adequada para comprovação da atividade de auditor, entre outros, declarações da(s) entidade(s) auditadas ou outros documentos à consideração do avaliado, desde que permitam aferir a validade das auditorias.

6. Todas as referências e elementos incluídos no currículo devem ser acompanhados dos respetivos comprovativos.

7. No caso de tratar-se de uma empresa estrangeira que não possua filial ou representante legal no país, as exigências estabelecidas serão cumpridas mediante a apresentação de documentos equivalentes, autenticados por Apostila de Haia e traduzidos por tradutor oficial.

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

9. Se a solicitação do número anterior não for atendida no prazo de 15 (quinze) dias, o processo será arquivado, mediante despacho fundamentado da Autoridade Credenciadora.

10. Os documentos apresentados pela candidata para credenciação constituirão um processo específico, que será mantido por um prazo não inferior a 5 (cinco) anos, podendo ser consultado por interessados.

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

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 renovada a cada 3 (três) anos, a contar da data da publicação da respetiva credenciação ou renovação.

12. A Autoridade Credenciadora publicará, em seu sítio na internet, a lista de organismos de certificação credenciados para a realização de avaliações de conformidade nos termos do Decreto-Lei n.º 27/2023, de outubro, na página "Registo de Organismos de Certificação

A2025/S2/BO53/13505
Deliberação n.º 20/CA/2025

Credenciados".

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

14. Qualquer alteração ocorrida, quer em atos constitutivos, estatuto, contrato social, organograma ou vinculação da entidade, quer nos dirigentes ou na equipa técnica de auditores, deverá ser imediatamente submetida ao conhecimento da Autoridade Credenciadora, mediante formalização enviada por e-mail para autoridadecredenciadora@arme.cv, a qual fará 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 efetuada por meio físico e eletrónico.

16. Nos casos em que ocorram alterações nos 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 pode solicitar a revogação da credenciação à Autoridade Credenciadora a qualquer momento.

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

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

CAPÍTULO III

Disposições Finais

Artigo 7.º

Entrada em vigor

O presente regulamento entra em vigor no dia seguinte à sua publicação em Boletim Oficial.

Feita na Cidade da Praia, aos 26 de fevereiro de 2025. — O Conselho de Administração, O Presidente, *Leonilde Santos* e os Administradores, *João Tomar* e *Carlos Ramos*.

A2025/S2/BO53/13505
Deliberação n.º 20/CA/2025

A2025/S2/BO53/13505
Deliberação n.º 20/CA/2025

AGÊNCIA REGULADORA MULTISSETORIAL DA ECONOMIA - ARME
Conselho de Administração

Deliberação n.º 21/CA/2025

Sumário: Aprovando o regulamento que estabelece os procedimentos e a metodologia aplicáveis às avaliações de conformidade dos prestadores de serviços de confiança, nos termos do Decreto-Lei n.º 27/2023, de 20 de outubro, com vista à atribuição e manutenção do estatuto de qualificado.

De 26 de fevereiro de 2025

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 regulamentação, supervisão e sancionamento de infrações. A ARME tem como 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, conforme o n.º 1 do artigo 2.º do Decreto-Lei n.º 50/2018, de 20 de setembro.

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 regras técnicas e de segurança aplicáveis ao exercício da atividade de prestação de serviço de confiança, nos termos do artigo 99.º do Decreto-Lei n.º 27/2023, de 20 de outubro.

A alínea *xx)* do artigo 3.º do Decreto-Lei n.º 27/2023, de 20 de outubro, define os prestadores qualificados de serviços de confiança como entidades que fornecem serviços eletrónicos de

A2025/S2/BO53/13505
Deliberação n.º 21/CA/2025

criação, verificação e validação de assinaturas eletrónicas, selos eletrónicos ou selos temporais, serviços de envio registado eletrónico e certificados relacionados com estes serviços; criação, verificação e validação de certificados para a autenticação de sítios web; conservação das assinaturas, selos ou certificados eletrónicos relacionados com esses serviços; arquivo eletrónico de documentos eletrónicos; gestão de dispositivos de criação de assinaturas e de selos eletrónicos à distância; e registo de dados eletrónicos num livro-razão eletrónico.

Para que os serviços de confiança possam ser prestados continuamente por prestadores qualificados de serviços de confiança dentro da Infraestrutura de Chaves Públicas de Cabo Verde, é necessário implementar um sistema de avaliação de conformidade que garanta que esses serviços cumprem os requisitos normativos nacionais e internacionais aplicáveis.

O regulamento de avaliação de conformidade de prestadores qualificados de serviços de confiança tem como objetivo uniformizar os procedimentos e a metodologia a empregar nas avaliações de conformidade dos prestadores de serviços de confiança, no âmbito do Decreto-Lei n.º 27/2023, de 20 de outubro, com o objetivo de atribuição e manutenção do estatuto de qualificado, e mediante as seguintes normas internacionais de referência: ISO/IEC 17021; ISO/IEC 17065; ETSI EN 319 403-1; ETSI EN 319 403-2; ETSI EN 319 403-3; WEBTRUST FOR CA; WEBTRUST NS; WEBTRUST SSL; WEBTRUST SSL EV; e WEBTRUST REPORT.

Assim, nos termos da alínea *b)* do artigo 14.º, e da alínea *f)* do artigo 15.º dos Estatutos da ARME, aprovados pelo Decreto-Lei n.º 50/2018, de 20 de setembro, do artigo 82.º, das alíneas *o)* e *q)* do artigo 83.º, e do n.º 1 do artigo 99.º do Decreto-Lei n.º 27/2023 de 20 de outubro, o Conselho de Administração, em sua reunião ordinária de 26 de fevereiro de 2025, aprova o presente Regulamento, que estabelece os procedimentos e a metodologia a empregar nas avaliações de conformidade dos prestadores de serviços de confiança (PSC), no âmbito do Decreto-Lei n.º 27/2023, de 20 de outubro, com o objetivo de atribuição e manutenção do estatuto de qualificado.

Artigo 1.º

Aprovação

É aprovado o regulamento que estabelece os procedimentos e a metodologia aplicáveis às avaliações de conformidade dos prestadores de serviços de confiança, nos termos do Decreto-Lei n.º 27/2023, de 20 de outubro, com vista à atribuição e manutenção do estatuto de qualificado.

A2025/S2/BO53/13505
Deliberação n.º 21/CA/2025

Artigo 2.º

Entrada em vigor

A presente deliberação entra em vigor no dia seguinte ao da sua publicação em Boletim Oficial.

Feita na Cidade da Praia, aos 26 de fevereiro de 2025. — O Conselho de Administração, A Presidente, *Leonilde Santos*, Os Administradores, *João Tomar* e *Carlos Ramos.*

REGULAMENTO DE AVALIAÇÃO DA CONFORMIDADE DE PRESTADORES QUALIFICADOS DE SERVIÇOS DE CONFIANÇA

CAPÍTULO I

Disposições Gerais

Artigo 1.º

Objeto

O presente Regulamento estabelece os procedimentos e a metodologia aplicáveis às avaliações de conformidade dos prestadores de serviços de confiança, nos termos do Decreto-Lei n.º 27/2023, de 20 de outubro, com vista à atribuição e manutenção do estatuto de qualificado.

Artigo 2.º

Âmbito

O presente Regulamento aplica-se a todos os organismos de certificação credenciados pela Autoridade Credenciadora para a realização de avaliações de conformidade dos prestadores de serviços de confiança, com vista à atribuição e manutenção do estatuto de prestador qualificado.

Artigo 3.º

Siglas e definições

1. No presente regulamento são utilizadas as seguintes siglas:

a) ETSI: European Telecommunications Standards Institute;

b) RFA: Relatório Final de Auditoria;

c) RPI: Relatório de Primeiras Impressões;

d) TI: Tecnologias de Informação

A2025/S2/BO53/13505
Deliberação n.º 21/CA/2025

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

a) "Acreditação", procedimento através do qual um organismo de acreditação reconhece, formalmente, que uma entidade é competente tecnicamente para efetuar uma determinada função específica, de acordo com normas internacionais ou nacionais, baseando-se, complementarmente, nas orientações emitidas pelos organismos internacionais de acreditação;

b)"Avaliação de conformidade", é o processo sistemático destinado a verificar se um bem, produto, processo ou serviço atende aos requisitos técnicos, regulatórios e normativos aplicáveis, por meio da realização de ensaios, calibrações, inspeções e auditorias.

c) "Organismo de acreditação", é a entidade com poderes de autoridade pública responsável por avaliar, reconhecer e supervisionar a competência técnica de organismos de avaliação da conformidade, garantindo que operem em conformidade com normas e regulamentos nacionais e internacionais;

d) "Organismo de certificação", é o organismo reconhecido pela Autoridade Credenciadora como sendo competente para avaliação e certificação da conformidade de prestadores qualificados de serviços de confiança e dos serviços de confiança qualificados prestados.

CAPÍTULO II

Avaliação de Conformidade

Artigo 4.º

Auditorias pré-operacionais e periódicas

1. A avaliação de conformidade do prestador qualificado de serviços de confiança é realizada através de auditoria pré-operacional, para efeitos de atribuição do respetivo estatuto, bem como por meio de auditorias anuais ou periódicas, contadas a partir da data de início da auditoria inicial, nos seguintes termos:

a) Realização de auditorias completas, pelo menos, a cada 24 meses;

b) Realização de auditorias de acompanhamento nos anos em que não ocorram auditorias completas.

2. A auditoria dos prestadores qualificados de serviços de fornecimento de certificados publicamente confiáveis deve ser realizada anualmente, de forma integral, em conformidade com as normas *ETSI EN 319 403-2* e *WEBTRUST SSL*.

3. As avaliações de conformidade são realizadas a expensas do prestador qualificado de serviços, por um organismo de certificação credenciado pela Autoridade Credenciadora nos termos do

A2025/S2/BO53/13505
Deliberação n.º 21/CA/2025

Regulamento de Credenciação de Organismos de Certificação.

4. A Autoridade Credenciadora publica no seu *website* a lista dos organismos de certificação credenciados, os quais devem realizar as avaliações de conformidade em observância dos requisitos estabelecidos no presente Regulamento.

5. Após a receção do relatório de auditoria, a Autoridade Credenciadora delibera sobre a atribuição ou manutenção do estatuto de prestador qualificado de serviços de confiança à entidade avaliada.

Artigo 5.º

Procedimentos de auditoria

O organismo de certificação pode desenvolver a sua própria metodologia de auditoria, desde que respeite os procedimentos estabelecidos nos padrões indicados na Tabela constante do anexo, que faz parte integrante do presente Regulamento.

Artigo 6.º

Plano da auditoria

1. O prestador de serviços de confiança que exerce a sua atividade, total ou parcialmente, em diversos locais, deve assegurar que todos operam sob um único sistema de gestão e que estão sujeitos a auditorias internas, de acordo com os procedimentos internos estabelecidos pelo próprio prestador de serviços.

2. Nos casos mencionados no número anterior, a avaliação deve ser realizada com base numa amostragem, a ser definida pelo organismo de certificação, devendo este considerar as seguintes informações como orientação:

a) Os resultados das auditorias internas realizadas anteriormente;

b) As vulnerabilidades, ameaças e riscos associados a cada local;

c) Os resultados das revisões realizadas pelo órgão ou grupo de gestão;

d) As diferenças e variações na dimensão e na atividade dos locais;

e) A complexidade do sistema de gestão do prestador de serviços de confiança;

f) A complexidade dos sistemas de informação de cada um dos locais;

g) A interação com sistemas de informação críticos do prestador de serviços de confiança; e

A2025/S2/BO53/13505
Deliberação n.º 21/CA/2025

h) As diferenças nos requisitos legais aplicáveis.

3. As informações mencionadas no número anterior devem ser consideradas para a definição da dimensão e composição da equipa de auditoria, bem como para o tempo necessário à sua execução.

Artigo 7.º

Tipos e fases da auditoria

1. As auditorias destinadas à avaliação da conformidade do prestador qualificado de serviços de confiança são as seguintes:

a) Auditorias pré-operacionais, ou auditorias de concessão;

b) Auditorias operacionais, ou auditorias de acompanhamento ou de renovação.

2. Para efeitos das auditorias referidas no número anterior, as fases são as seguintes:

a) Fase 1: Pré-avaliação;

b) Fase 2: Auditoria no local;

c) Fase 3: Elaboração do relatório final de auditoria (RFA).

Artigo 8.º

Fase de pré-avaliação

1. A Fase 1, ou fase de pré-avaliação, inclui a realização de uma ou mais reuniões preliminares com o representante da entidade a auditar, com o objetivo de estabelecer o plano para a Fase 2 da auditoria e obter um conhecimento detalhado da estrutura e da extensão do(s) serviço(s) prestado(s) pelo prestador qualificado de serviços de confiança.

2. Devem ser verificados, de acordo com a especificidade de cada entidade a auditar, os seguintes documentos, bem como outros que sejam considerados relevantes:

a) Lista de serviços eletrónicos de confiança e dos locais onde a organização opera;

b) Lista de contratados no âmbito dos serviços eletrónicos de confiança;

c) Listas de verificação preenchidas pelo prestador de serviços de confiança (PSC), no âmbito da autoavaliação;

d) Declaração de práticas;

A2025/S2/BO53/13505
Deliberação n.º 21/CA/2025

e) Políticas aplicáveis aos serviços;

f) Plano de segurança;

g) Política de segurança;

h) Plano de contingência e continuidade;

i) Análise de risco do PSC e dos serviços de confiança prestados;

j) Procedimentos internos;

k) Deliberações do grupo de gestão do PSC;

l) Actas de reuniões;

m) Relatórios de incidentes;

n) Relatórios de auditorias ou certificações, internas ou externas;

o) Certificações obtidas;

p) Exemplares dos vários tipos de certificados emitidos, quando aplicável;

q) Lista de revogação de certificados, quando aplicável;

r) Documentos relativos ao estatuto legal da entidade;

s) Seguro de responsabilidade civil;

t) Contratos com fornecedores de serviços de subcomponentes de confiança;

u) Documentos que comprovem a certificação de componentes incorporados no serviço avaliado, quando aplicável.

3. Os seguintes documentos podem ser incluídos na Fase 1 da auditoria, desde que sejam considerados relevantes.:

a) A verificação dos registos referentes à entidade legal;

b) Os acordos para cobertura de responsabilidades;

c) As relações contratuais entre o prestador de serviço de confiança e os eventuais contratados que operam ou fornecem serviços de subcomponentes;

d) As auditorias ou certificações internas/externas;

A2025/S2/BO53/13505
Deliberação n.º 21/CA/2025

e) A revisão da gestão de segurança e de outras investigações relacionadas com a auditoria preliminar das conformidades parciais ou das não conformidades autodeclaradas.

4. Os auditores devem acordar com o prestador de serviços de confiança o local e o momento em que a fase 1 da auditoria será realizada, seja no local, à distância ou através de uma combinação de ambas as modalidades.

5. A avaliação documental deve estar concluída antes do início da Fase 2, independentemente do local onde esta seja realizada.

6. Com base nos elementos recolhidos, o auditor elabora o documento Calendário e Plano de Auditoria, que serve de base para os trabalhos de avaliação a desenvolver na Fase 2.

7. O Calendário e Plano de Auditoria deve ser enviado à Entidade Auditada com antecedência, devendo incluir, no mínimo, para cada dia de auditoria, os seguintes elementos:

a) Os itens que serão objeto de apreciação;

b) O local onde a auditoria se realizará; e

c*)* As pessoas com funções de confiança que deverão estar presentes em cada um dos aspetos a avaliar.

8. Os resultados obtidos na Fase 1 são incluídos no RFA.

Artigo 9.º

Fase de auditoria no local

1. Na Fase 2, ou fase de auditoria no local, devem ser revistas as áreas sensíveis identificadas na Fase 1 e avaliada a resolução de eventuais problemas.

2. Os objetivos da auditoria no local são os seguintes:

a) Confirmar a conformidade do prestador de serviços de confiança com a sua política, objetivos e procedimentos;

b) Confirmar que os serviços de confiança implementados pelo prestador de serviços de confiança estão em conformidade com os requisitos regulamentares e normativos aplicáveis aos serviços a certificar.

3. A auditoria deve concentrar-se na recolha das seguintes evidências relacionadas com os serviços de confiança prestados pelo prestador de serviços de confiança.

a) Implementação dos requisitos dos serviços de confiança;

A2025/S2/BO53/13505
Deliberação n.º 21/CA/2025

b) Processos e procedimentos organizacionais relacionados com os serviços de confiança;

c) Processos e procedimentos técnicos associados aos serviços de confiança;

d) Interface dos componentes dos serviços de confiança;

e) Implementação de medidas de segurança da informação para os serviços de confiança, incluindo a proteção da rede de TI;

f) Produtos relacionados com os serviços de confiança como módulos criptográficos;

g) Segurança física dos locais relevantes do prestador de serviços de confiança.

4. Caso o serviço utilize componentes auditadas separadamente, deve ser garantido o cumprimento dos requisitos desses componentes, em particular no que diz respeito à segurança da informação.

5. O organismo de certificação apresenta o Relatório de Primeiras Impressões (RPI) e comunica, de forma verbal, as não conformidades identificadas durante o processo de auditoria, tanto na fase 1 como na fase 2.

6. O RPI pode ser transcrito num documento, classificado de forma adequada, e enviado à entidade auditada para a programação das ações ou intervenções necessárias indicadas.

7. Para a apresentação do RPI, devem estar presentes os responsáveis do Grupo de Gestão/Conselho Executivo do prestador de serviços de confiança auditado.

Artigo 10.º

Relatório final de auditoria

1. O Relatório Final de Auditoria (RFA) deve incluir as seguintes informações:

a) Relato da auditoria, incluindo um resumo da análise documental e da(s) norma(s), especificações publicamente disponíveis e/ou requisitos regulatórios que serviram de base para a realização da auditoria;

b) Relato da auditoria da análise de risco de segurança da informação do prestador de serviços de confiança;

c) Tempo total de auditoria utilizado, com especificação detalhada do tempo despendido na revisão documental, avaliação da análise de risco, auditoria no local e elaboração do relatório de auditoria;

d) Investigações de auditoria realizadas, justificação da sua seleção e metodologia aplicada,

A2025/S2/BO53/13505
Deliberação n.º 21/CA/2025

incluindo a metodologia de amostragem e os procedimentos de teste;

e) Áreas abrangidas pela auditoria, incluindo os requisitos de certificação, os locais auditados, os registos analisados e as metodologias de auditoria utilizadas;

f) Observações registadas, tanto positivas como negativas;

g) Detalhes das não conformidades identificadas, suportadas por evidências objetivas (quando aplicável) e referência ao requisito que não foi cumprido;

h) Comentários sobre a conformidade do prestador de serviços de confiança e dos serviços de confiança prestados com os critérios que fundamentaram a auditoria, acompanhados de uma declaração clara sobre eventuais não conformidades e, quando aplicável, comparação com os resultados de auditorias anteriores realizadas ao prestador de serviços de confiança e aos serviços de confiança em causa.

2. Podem também integrar o relatório de auditoria questionários preenchidos, listas de verificação, observações, registos ou anotações do auditor.

3. As informações relativas às amostras avaliadas durante a auditoria devem constar do relatório de auditoria ou de outra documentação de certificação.

4. O relatório deve avaliar a adequação da organização e dos procedimentos internos adotados pelo prestador de serviços de confiança para garantir a confiança nos serviços prestados.

5. Com o objetivo de fundamentar a decisão de confirmar que o prestador de serviços de confiança e os seus serviços fiduciários auditados cumprem os critérios de auditoria definidos, os auditores devem elaborar relatórios claros que contenham informações suficientes para sustentar essa decisão.

6. O RFA deve incluir as não conformidades, classificadas como de Baixo Impacto e de Alto Impacto, bem como Oportunidades de Melhoria, e deve ser classificado com o nível de segurança confidencial.

7. O relatório deve ser distribuído, no prazo de 10 (dez) dias úteis após a conclusão da Fase 2, da seguinte forma:

a) Um (1) exemplar para a entidade auditada;

b) Um (1) exemplar para a autoridade credenciadora.

8. Nas auditorias a Prestadores de Serviços de Confiança (PSC) que fornecem certificados publicamente confiáveis, o organismo de certificação deve emitir, igualmente, um relatório no formato definido nos seguintes documentos, consoante o esquema de acreditação do organismo

A2025/S2/BO53/13505
Deliberação n.º 21/CA/2025

de certificação e o tipo de serviço avaliado:

a) ETSI EN 319 403-2; ou

b) WebTrust for CA, WebTrust NS, WebTrust SSL, WebTrust SSL EV e WebTrust Report.

9. O Relatório Final de Auditoria (RFA) será analisado pela autoridade credenciadora, em conjunto com os demais documentos referenciados no Regulamento dos Requisitos para Prestadores Qualificados de Serviços de Confiança, com o objetivo de atribuir ou manter o estatuto de prestador qualificado de serviços de confiança da entidade auditada.

10. Os documentos utilizados como evidência no âmbito da auditoria devem ser conservados pelo organismo de avaliação da conformidade durante um período de cinco anos, devendo ser disponibilizados à autoridade credenciadora, sempre que solicitados.

Artigo 11.º

Plano de ações corretivas

1.Caso sejam identificadas não conformidades no Relatório Final de Auditoria (RFA), o prestador de serviços de confiança deve elaborar um Plano de Ações Corretivas, no qual constem, para cada não conformidade, os seguintes elementos:

a) Número da Não Conformidade;

b) Classificação (baixo impacto ou alto impacto);

c) Descrição da Não Conformidade;

d) Análise das causas e da sua extensão;

e) Ações Corretivas;

f) Prazo;

g) Responsável.

2. O Plano de Ações Corretivas deve ser assinado por, pelo menos, um dos membros do Grupo de Gestão ou do Conselho Executivo do PSC e enviado ao organismo de avaliação da conformidade e à Autoridade de Regulação e Monitorização de Entidades (ARME) no prazo máximo de 10 dias úteis após a receção do RFA.

3. As não conformidades classificadas como de alto impacto devem ser corrigidas no prazo acordado com o organismo de certificação, o qual avalia as ações corretivas e os respetivos prazos, fornecendo ao prestador de serviços de confiança informações sobre as tarefas de

A2025/S2/BO53/13505
Deliberação n.º 21/CA/2025

avaliação adicionais necessárias para verificar a correção das não conformidades.

4. As ações corretivas para não conformidades de baixo impacto devem ser implementadas da seguinte forma:

a) No prazo de 3 meses após a notificação ao prestador de serviços de confiança das não conformidades constantes do relatório de auditoria; ou

b) No prazo de 6 meses após a notificação ao prestador de serviços de confiança das não conformidades constantes do relatório de auditoria, desde que seja demonstrado que a complexidade da ação corretiva justifica um prazo mais alargado.

5. O prestador de serviços de confiança deve disponibilizar ao organismo de certificação a documentação necessária para avaliar a complexidade da ação corretiva referida no número anterior.

CAPÍTULO III

Disposições Finais

Artigo 12.º

Entrada em vigor

O presente regulamento entra em vigor no dia imediato ao da sua publicação em Boletim Oficial.

A2025/S2/BO53/13505
Deliberação n.º 21/CA/2025

Anexo

A tabela estabelece a correspondência entre os serviços de confiança e os padrões a serem utilizados pelos organismos de certificação para a realização da avaliação da conformidade.

Serviço de confiança definido no Decreto-Lei 23/2023	**Padrões para avaliação de conformidade**
Fornecimento de certificados qualificados de assinaturas eletrónicas (Art.º 53º)	ISO/IEC 17021-1 ISO/IEC 17065 ETSI EN 319 403-1 ETSI EN 319 403-3 OU WebTrust for CA WebTrust Network Security
Fornecimento de certificados qualificados de selos eletrónicos (Art.º 65º)	
Fornecimento de certificados qualificados de autenticação de sítios web (Art.º 73º)	ISO/IEC 17021-1 ISO/IEC 17065 ETSI EN 319 403-1 ETSI EN 319 403-2 ETSI EN 319 403-3 OU WebTrust for CA WebTrust Network Security WebTrust SSL WebTrust SSL EV

A2025/S2/BO53/13505
Deliberação n.º 21/CA/2025

Fornecimento de selos temporais qualificados (Art.º 69º)	ISO/IEC 17021-1 ISO/IEC 17065 ETSI EN 319 403-1 ETSI EN 319 403-3
Validação de assinaturas eletrónicas qualificadas (Art.º 55º)	
Validação dos selos eletrónicos qualificados (Art.º 68º)	
Preservação de assinaturas eletrónicas qualificadas (Art.º 56º)	
Preservação dos selos eletrónicos qualificados (Art.º 68º)	
Envio registado eletrónico (Art.º 72º)	
Fornecimento de certificado eletrónico qualificado de atributos (Art.º 77º)	
Gestão de dispositivos de criação de assinaturas e de selos eletrónicos à distância (Art.º 46.º e 66.º)	
Registo de dados eletrónicos num livrorazão eletrónico (Art.º 81º)	

Feita na Cidade da Praia, aos 26 de fevereiro de 2025. — O Conselho de Administração, O Presidente, *Leonilde Santos*, Os Administradores, *João Tomar* e *Carlos Ramos*.

A2025/S2/BO53/13505
Deliberação n.º 21/CA/2025

A2025/S2/BO53/13505
Deliberação n.º 21/CA/2025

AGÊNCIA REGULADORA MULTISSETORIAL DA ECONOMIA - ARME
Conselho de Administração

Deliberação n.º 22/CA/2025

Sumário: Aprovando o regulamento que estabelece requisitos de segurança física aplicáveis aos prestadores qualificados de serviços de confiança que prestam serviços de confiança no âmbito da Infraestrutura de Chaves Públicas de Cabo Verde (ICP-CV).

De 26 de fevereiro de 2025

Preâmbulo

A Agência Reguladora Multissectorial da Economia (ARME), criada pelo Decreto-Lei n.º 50/2018, de 20 de setembro, e dotada de funções reguladoras, supervisão e sancionamento de infrações, assume um papel central na regulação técnica e económica dos setores das comunicações eletrónicas, energia, água e transportes coletivos urbanos e interurbanos de passageiros. No exercício das suas competências, a ARME é responsável por supervisionar as entidades de certificação no âmbito do setor das comunicações eletrónicas, conforme estabelecido na alínea f) do artigo 15.º do referido diploma legal.

O Decreto-Lei n.º 27/2023, de 20 de outubro, que estabelece as normas aplicáveis aos serviços de confiança, incluindo transações eletrónicas, assinaturas eletrónicas, selos eletrónicos, selos temporais, documentos eletrónicos, serviços de certificados para autenticação de sítios *web*, arquivo eletrónico, certificado eletrónico de atributos, gestão de dispositivos de criação de assinaturas e selos eletrónicos à distância, e livros-razão eletrónicos, atribui à ARME, na qualidade de Entidade Reguladora do Sector das Comunicações Eletrónicas, as funções de autoridade credenciadora. Esta atribuição confere à ARME a competência para credenciar, controlar e supervisionar os prestadores qualificados de serviços de confiança, garantindo o cumprimento dos requisitos legais e regulamentares aplicáveis, bem como para atribuir ou retirar o estatuto de qualificado aos prestadores e aos serviços por eles prestados.

No âmbito das suas competências, a ARME deve emitir e publicar, no seu sítio da *Internet* e no Boletim Oficial, as regras técnicas e de segurança aplicáveis ao exercício da atividade de prestação de serviços de confiança, conforme previsto no artigo 99.º do Decreto-Lei n.º 27/2023, de 20 de outubro. Estas regras visam assegurar a integridade, confidencialidade e disponibilidade dos serviços de confiança, bem como a proteção dos dados pessoais e das informações sensíveis tratadas no âmbito destas atividades.

O presente regulamento, que define os requisitos mínimos de segurança física das instalações dos prestadores qualificados de serviços de confiança, insere-se neste quadro regulatório e tem como objetivo principal estabelecer um conjunto de medidas e procedimentos destinados a garantir a proteção física das instalações, equipamentos e informações sensíveis destes prestadores. A

A2025/S2/BO53/13505
Deliberação n.º 22/CA/2025

adoção destas medidas é essencial para prevenir riscos e ameaças que possam comprometer a integridade e a continuidade dos serviços de confiança, bem como para assegurar a conformidade com as normas internacionais de referência no domínio da certificação digital, nomeadamente as normas WEBTRUST FOR CA, ETSI EN 319 401, ETSI EN 319 411-1, ETSI EN 319 411-2, ISO/IEC 27001 e ISO/IEC 27002.

O regulamento está estruturado em capítulos que abordam, de forma detalhada, os requisitos de segurança física aplicáveis às instalações dos prestadores qualificados de serviços de confiança, com especial enfoque nas entidades certificadoras. Estes requisitos incluem a definição de perímetros de segurança, controlos de acesso físico, proteção contra catástrofes naturais e falhas de serviços públicos, medidas de prevenção de roubo e intrusão, e a implementação de sistemas de videovigilância e alarmística. Adicionalmente, o regulamento estabelece procedimentos para a gestão de equipamentos, a proteção de informações sensíveis e a recuperação de desastres, garantindo a resiliência e a continuidade das operações em situações de crise.

Assim, nos termos da alínea *b)* do artigo 14.º, e da alínea *f)* do artigo 15.º dos Estatutos da ARME, aprovados pelo Decreto-Lei n.º 50/2018, de 20 de setembro, do artigo 82.º e do n.º 1 do artigo 99.º do Decreto-Lei n.º 27/2023 de 20 de outubro, o Conselho de Administração, em sua reunião ordinária de 26 de fevereiro de 2025, aprova o presente Regulamento, que estabelece os requisitos de segurança física aplicáveis aos prestadores qualificados de serviços de confiança que prestam serviços de confiança no âmbito da Infraestrutura de Chaves Públicas de Cabo Verde (ICP-CV).

Artigo 1.º

Aprovação

É aprovado o regulamento que estabelece os requisitos de segurança física aplicáveis aos prestadores qualificados de serviços de confiança que prestam serviços de confiança no âmbito da Infraestrutura de Chaves Públicas de Cabo Verde (ICP-CV).

Artigo 2.º

Entrada em vigor

A presente deliberação entra em vigor no dia seguinte ao da sua publicação em Boletim Oficial.

Feita na Cidade da Praia, aos 26 de fevereiro de 2025. — O Conselho de Administração, A Presidente, *Leonilde Santos* e os Administradores, *João Tomar* e *Carlos Ramos*.

A2025/S2/BO53/13505
Deliberação n.º 22/CA/2025

REGULAMENTO DOS REQUISITOS DE SEGURANÇA FÍSICA DE INSTALAÇÕES DE PRESTADORES QUALIFICADOS DE SERVIÇOS DE CONFIANÇA

CAPÍTULO I

Disposições Gerais

Artigo 1.º

Objeto

O presente regulamento estabelece as regras aplicáveis aos requisitos de segurança física aplicáveis aos prestadores qualificados de serviços de confiança da Infraestrutura de Chaves Públicas de Cabo Verde (ICP-CV).

Artigo 2.º

Âmbito

O presente regulamento aplica-se aos prestadores qualificados de serviços de confiança que prestam serviços de confiança, nos termos do disposto no Decreto-Lei n.º 27/2023, de 20 de outubro.

Artigo 3.º

Objetivos

1. A implementação e manutenção dos controlos de segurança física por parte da entidade certificadora têm os seguintes objetivos:

a) Limitar o acesso físico às instalações e equipamentos da entidade certificadora a pessoas autorizadas;

b) Garantir que as instalações e os equipamentos da entidade certificadora estão protegidos contra ameaças ambientais;

c) Evitar a perda, dano ou comprometimento de bens, bem como a interrupção das atividades comerciais;

d) Evitar o comprometimento da informação e das instalações de tratamento da informação.

2. O fator de segurança descrito na alínea a) requer, pelo menos, duas autorizações para permitir o acesso a informações, áreas ou à realização de ações críticas, garantindo uma camada adicional de proteção, de modo a assegurar que uma pessoa com acesso autorizado só consiga aceder se outra pessoa, igualmente autorizada, o aprovar.

A2025/S2/BO53/13505
Deliberação n.º 22/CA/2025

Artigo 4.º

Siglas e definições

1. No presente regulamento são utilizadas as seguintes siglas:

a) ARME: Agência Reguladora Multissetorial da Economia;

b) EC: Entidade Certificadora;

c) ETSI: European Telecommunications Standards Institute;

d) HVAC: Heating, Ventilation and Air Conditioning;

e) ISO/IEC: International Organization for Standardization / International Electrotechnical Commission;

f) PQSC: Prestador Qualificado de Serviços de Confiança;

g) PSC: Prestador de Serviços de Confiança;

h) UPS: Uninterruptible Power Supply;

i) UR: Unidade de Registo.

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

a) "Entidade certificadora", é uma entidade ou pessoa coletiva credenciada que presta serviço de confiança, designadamente cria ou fornece meios para a criação, verificação e validação de assinaturas eletrónicas, selos eletrónicos ou selos temporais, serviços de envio registado eletrónico e certificados relacionados com estes serviços ou na criação, verificação e validação de certificados para a autenticação de sítios *Web* ou na preservação das assinaturas, selos ou certificados eletrónicos relacionados com esses serviços;

b) "Prestador de serviços de confiança", a pessoa coletiva que preste um ou mais do que um serviço de confiança quer como prestador qualificado quer como prestador não qualificado de serviços de confiança;

c) "Prestador qualificado de serviços de confiança", o prestador de serviços de confiança que preste um ou mais do que um serviço de confiança qualificado e ao qual é concedido o estatuto de qualificado pela autoridade credenciadora;

d) "Serviço de confiança", um serviço eletrónico geralmente prestado mediante pagamento, nos termos do Decreto-Lei n.º 27/2023 de 20 de outubro.

A2025/S2/BO53/13505
Deliberação n.º 22/CA/2025

Artigo 5.º

Requisitos das Instalações relacionadas com a criação e gestão de certificados

1. A entrada no edifício deve ser realizada exclusivamente através de pontos de acesso limitados e controlados.

2. Devem ser estabelecidos perímetros de segurança em torno das instalações relacionadas com a criação e gestão de certificados.

3. As instalações relacionadas com a criação e gestão de certificados devem estar localizadas num ambiente fisicamente seguro, com, pelo menos, quatro níveis de segurança para aceder aos ativos, sistemas e informações sensíveis, conforme descrito no anexo, que constitui parte integrante do presente regulamento.

4. Os sistemas devem estar fisicamente separados de outros sistemas, mesmo que pertençam à mesma organização, de modo a garantir que apenas o pessoal autorizado tenha acesso adequado.

5. O processo de criação e gestão de certificados deve ser realizado num ambiente capaz de proteger fisicamente os sistemas e os dados envolvidos contra riscos associados a acessos não autorizados.

6.No caso de instalações partilhadas com outras organizações, estas devem estar localizadas fora do perímetro de segurança relacionado com a criação e gestão de certificados.

7. As funções relacionadas com as operações de criação e gestão de certificados podem ser suportadas na mesma área, desde que o acesso seja restrito ao pessoal autorizado para o efeito.

8.As chaves de acesso devem ser mantidas fisicamente separadas, de forma a garantir que apenas o pessoal de confiança e devidamente autorizado tenha acesso às mesmas.

9.Todos os colaboradores devem utilizar uma identificação visível durante o período de permanência nas instalações.

Artigo 6.º

Controlos de segurança para visitantes

1. Todas as entradas físicas devem estar sujeitas a controlo e supervisão, de modo a restringir o acesso ao edifício ou às instalações operacionais da entidade certificadora apenas ao pessoal autorizado.

2. Todos os visitantes devem ser acompanhados por pessoal autorizado durante a sua permanência no edifício e nas instalações operacionais da entidade certificadora, devendo ser

A2025/S2/BO53/13505
Deliberação n.º 22/CA/2025

registadas a data e hora de entrada e de saída.

3. Os fornecedores, após autorização, devem ter acesso às instalações operacionais da entidade certificadora apenas quando estritamente necessário.

Artigo 7.º

Controlos de segurança física para instalações da entidade certificadora

1. Controlo de acesso físico:

a) Barreiras físicas robustas, com paredes sólidas que se estendam desde o piso real até ao teto real;

b) Portas corta-fogo nos perímetros de segurança;

c) O acesso às instalações operacionais da entidade certificadora deve ser restrito a pessoal autorizado e protegido através da utilização de controlos de autenticação multifator;

d) Os direitos de acesso às instalações operacionais da entidade certificadora devem ser revistos e atualizados de forma regular;

e)Todas as entradas e saídas das instalações operacionais da entidade certificadora devem ser devidamente registadas.

2. Proteção contra catástrofes naturais e colapso de estruturas de canalização:

a) Sistema de deteção de inundações;

b) Sistema de proteção contra descargas atmosféricas;

c) Sistema de proteção contra emissões de radiação eletromagnética;

d) Sistema de climatização (HVAC), suportado por gerador e dotado de capacidade para controlo de temperatura, humidade e alarmística;

e) Sistema de deteção e extinção automática de incêndios.

3. Proteção contra falhas de serviços públicos de apoio:

a) Energia: implementação de sistemas de UPS (Uninterruptible Power Supply) e Implementação de uma fonte de energia alternativa (gerador), que garanta o abastecimento contínuo de energia às instalações e sistemas críticos em caso de falha de energia;

b) Telecomunicações: através da contratação de um serviço de acesso à Internet com redundância

A2025/S2/BO53/13505
Deliberação n.º 22/CA/2025

ao nível dos equipamentos e das linhas de comunicação.

4. Proteção contra roubo:

a) Sistema de videovigilância para monitorização das entradas, saídas e atividades nas instalações operacionais do prestador de serviços de confiança;

b) As instalações relacionadas com a criação ou gestão de certificados devem estar fisicamente trancadas e protegidas com sistema de alarme quando desocupadas;

c) Sistema de alarme nas portas e, quando aplicável, nas janelas, para monitorização em caso de permanência aberta;

d) Sistema de deteção de intrusões implementado em todas as portas externas das instalações relacionadas com a criação ou gestão de certificados, o qual deve ser testado regularmente.

5. Recuperação de desastres através da implementação de um site redundante numa localização que não esteja exposta aos mesmos riscos da localização original.

Artigo 8.º

Controlos para segurança de equipamentos

1. Devem ser implementados controlos para proteger os equipamentos e as informações relacionados com o serviço, no caso de serem retirados da organização sem autorização.

2. Deve ser elaborado e mantido um inventário dos ativos e equipamentos relativos às instalações operacionais da entidade certificadora.

3. Os equipamentos devem estar localizados de forma a minimizar os riscos associados a ameaças ambientais e a acessos não autorizados.

4. Os equipamentos devem estar protegidos contra falhas de energia e outras anomalias elétricas, através da utilização de sistemas de UPS (*Uninterruptible Power Supply*) e geradores.

5. A cablagem de energia elétrica e de telecomunicações que suporta o funcionamento das instalações operacionais do prestador de serviços de confiança deve estar protegida contra interceções e danos.

6. Todos os equipamentos devem ser submetidos a um processo de manutenção, de acordo com as instruções do fabricante.

7. Todos os equipamentos que armazenam informação devem ser verificados cuidadosamente antes de serem eliminados ou reutilizados, com o objetivo de prevenir o acesso a

A2025/S2/BO53/13505
Deliberação n.º 22/CA/2025

informação sensível por parte de pessoas não autorizadas.

Artigo 9.º

Controlos gerais

1. As informações comerciais, sensíveis ou críticas devem ser guardadas sob chave quando não estiverem a ser utilizadas e sempre que as instalações da prestadora de serviços de confiança se encontrem desocupadas.

2. Os postos de trabalho devem ser desligados, bloqueados com palavra-passe ou protegidos através de fechadura com chave, ou outros controlos equivalentes, quando não estiverem a ser utilizados (por exemplo, mediante a aplicação de uma política de ecrã limpo).

3. Qualquer movimentação de materiais e equipamentos de ou para as instalações da Unidade de Registo carece de autorização prévia.

Artigo 10.º

Entrada em vigor

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

Anexo

Níveis de segurança para aceder os ativos, sistemas e informação sensíveis

(a o que refere o n.º 3 do artigo 5.º do presente regulamento)

NÍVEL	DESCRIÇÃO
Nível 1	Está localizado após a primeira barreira de acesso às instalações da prestadora de serviços qualificados de confiança. Para aceder a área de nível 1, todo o pessoal deve ser identificado e registado pelos seguranças. A partir desse nível, pessoas não relacionadas com as operações da prestadora de serviços qualificados de confiança devem estar devidamente identificadas e serem acompanhadas. Nenhum tipo de processo operacional ou administrativo da entidade certificadora deve ser realizado nesse nível.

A2025/S2/BO53/13505
Deliberação n.º 22/CA/2025

Nível 2	É o nível adjacente ao nível 1, sendo o primeiro nível interno e requer, da mesma forma que o nível 1, a identificação individual das pessoas que nele entram. É o nível mínimo de segurança requerido para a realização de qualquer atividade operacional ou administrativa da entidade certificadora. A transição do primeiro para o segundo nível deve exigir a identificação através de meio eletrónico, bem como o uso de crachá.
Nível 3	É o nível adjacente ao nível 2 e é o primeiro nível que deve conter material e atividades sensíveis da operação da entidade certificadora. Quaisquer atividades relativas ao ciclo de vida dos certificados digitais devem estar localizadas a partir desse nível. Pessoas que não estejam envolvidas com as respetivas atividades não devem ter permissão para aceder a este nível. Caso seja necessário o acesso por parte de pessoas não autorizadas, as mesmas não podem permanecer neste nível se não estiverem acompanhadas por alguém que tenha o acesso autorizado. Devem ser controladas as entradas e as saídas de cada pessoa autorizada, de forma a considerar dois tipos de mecanismos de controlo para a entrada, como, por exemplo, cartão eletrónico e identificação biométrica (duplo fator de autenticação). O uso de telemóveis e outros equipamentos de comunicação/tecnologia, exceto os equipamentos necessários para a operação da entidade certificadora, não devem ser permitidos a partir do nível 3.

A2025/S2/BO53/13505
Deliberação n.º 22/CA/2025

Nível 4	É o nível adjacente ao nível 3, sendo onde devem ocorrer as atividades sensíveis de operação da entidade certificadora, como, por exemplo, a emissão e revogação de certificados. Todos os sistemas e equipamentos necessários para estas atividades devem estar localizados a partir desse nível, inclusive os sistemas de unidade de registo. O nível 4 deve possuir requisitos de controlo de acesso semelhante ao nível 3 e, adicionalmente, cada acesso ao seu ambiente deve ser acompanhado por duas pessoas autorizadas (dupla custódia), sendo obrigatória a permanência de duas pessoas autorizadas enquanto o ambiente estiver ocupado. Os cofres existentes devem estar localizados no interior do nível 4.

Feita na Cidade da Praia, aos 26 de fevereiro de 2025. — O Conselho de Administração, A Presidente, *Leonilde Santos*, os Administradores, *João Tomar* e *Carlos Ramos*.

A2025/S2/BO53/13505
Deliberação n.º 22/CA/2025

AGÊNCIA REGULADORA MULTISSETORIAL DA ECONOMIA - ARME
Conselho de Administração

Deliberação n.º 23/CA/2025

Sumário: Aprovando o regulamento que estabelece as condições de elegibilidade de prestadores de serviços de confiança, para obterem e manterem o estatuto de qualificados, no âmbito do Decreto-Lei n.º 27/2023, de 20 de outubro.

De 26 de fevereiro de 2025

Preâmbulo

A Agência Reguladora Multissetorial 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, constitui-se como uma autoridade administrativa independente, de base institucional, dotada de competências reguladoras, incluindo a regulamentação, supervisão e sancionamento de infrações. A sua finalidade principal consiste na regulação técnica e económica dos setores das comunicações eletrónicas, energia, água e transportes coletivos urbanos e interurbanos de passageiros, conforme estabelecido no n.º 1 do artigo 2.º do referido diploma legal.

No âmbito das suas atribuições, a ARME assume, entre outras, a competência de supervisionar as entidades de certificação, nos termos da alínea f) do artigo 15.º do Decreto-Lei n.º 50/2018, de 20 de setembro. Esta competência é particularmente relevante no contexto da regulação do setor das comunicações eletrónicas, onde a segurança e a confiança nas transações eletrónicas assumem um papel central.

O Decreto-Lei n.º 27/2023, de 20 de outubro, que estabelece as normas aplicáveis aos serviços de confiança, nomeadamente no que diz respeito às transações eletrónicas, veio instituir um quadro legal abrangente para a regulação de diversas modalidades de serviços de confiança, tais como assinaturas eletrónicas, selos eletrónicos, selos temporais, documentos eletrónicos, serviços de certificados para autenticação de sítios *web*, arquivo eletrónico, certificados eletrónicos de atributos, gestão de dispositivos de criação de assinaturas e selos eletrónicos à distância, e livros-razão eletrónicos. No artigo 82.º deste diploma, atribui-se à ARME, enquanto Entidade Reguladora do Setor das Comunicações Eletrónicas, as funções de autoridade credenciadora no âmbito dos serviços de confiança.

Para a prossecução destas atribuições, a ARME deve emitir e publicar, no seu sítio da Internet e no Boletim Oficial, as regras técnicas e de segurança aplicáveis ao exercício da atividade de prestação de serviços de confiança, nos termos do artigo 99.º do Decreto-Lei n.º 27/2023, de 20 de outubro. Estas regras visam assegurar que os prestadores de serviços de confiança cumpram os requisitos legais e técnicos necessários para a atribuição e manutenção do estatuto de prestador qualificado, garantindo assim a confiança e a segurança dos serviços prestados no âmbito da

A2025/S2/BO53/13505
Deliberação n.º 23/CA/2025

Infraestrutura de Chaves Públicas de Cabo Verde (ICP-CV).

O presente regulamento define as condições de elegibilidade para que os prestadores de serviços de confiança possam obter e manter o estatuto de prestador qualificado, em conformidade com o disposto no Decreto-Lei n.º 27/2023, de 20 de outubro. Para tal, estabelece-se um conjunto de requisitos técnicos, organizacionais e de segurança que os prestadores devem cumprir, alinhados com as normas internacionais de referência aplicáveis, nomeadamente as normas ETSI, ISO/IEC, IETF RFC, entre outras.

A atribuição do estatuto de prestador qualificado de serviços de confiança pressupõe a verificação do cumprimento dos requisitos legais previstos no artigo 26.º do Decreto-Lei n.º 27/2023, de 20 de outubro, e a realização de auditorias de conformidade por organismos credenciados. Este estatuto tem uma duração de três anos, podendo ser renovado por igual período, desde que se mantenham as condições que justificaram a sua atribuição inicial.

O presente regulamento visa, assim, estabelecer um quadro normativo claro e rigoroso para a credenciação e supervisão dos prestadores de serviços de confiança, garantindo a qualidade, a segurança e a confiança dos serviços prestados no âmbito da ICP-CV, em conformidade com as melhores práticas internacionais e com a legislação aplicável.

Assim, nos termos da alínea *b)* do artigo 14.º, e da alínea *f)* do artigo 15.º dos Estatutos da ARME, aprovados pelo Decreto-Lei n.º 50/2018, de 20 de setembro, do artigo 82.º e do n.º 1 do artigo 99.º do Decreto-Lei n.º 27/2023 de 20 de outubro, o Conselho de Administração, em sua reunião ordinária de 26 de fevereiro de 2025, aprova o presente Regulamento, estabelece as condições de elegibilidade de prestadores de serviços de confiança, para obterem e manterem o estatuto de qualificados, no âmbito do Decreto-Lei n.º 27/2023 de 20 de outubro.

Artigo 1.º

Aprovação

É aprovado o regulamento que estabelece as condições de elegibilidade de prestadores de serviços de confiança, para obterem e manterem o estatuto de qualificados, no âmbito do Decreto-Lei n.º 27/2023 de 20 de outubro.

Artigo 2.º

Entrada em vigor

A presente deliberação entra em vigor no dia seguinte ao da sua publicação em Boletim Oficial.

Feita na Cidade da Praia, aos 26 de fevereiro de 2025. — O Conselho de Administração, O Presidente, *Leonilde Santos*, os Administradores, *João Tomar* e *Carlos Ramos*.

A2025/S2/BO53/13505
Deliberação n.º 23/CA/2025

REGULAMENTO DOS REQUISITOS PARA PRESTADORES QUALIFICADOS DE SERVIÇOS DE CONFIANÇA

Artigo 1.º

Objeto

O presente regulamento estabelece as condições de elegibilidade aplicáveis aos prestadores de serviços de confiança, nos termos do disposto no Decreto-Lei n.º 27/2023, de 20 de outubro, para a obtenção e manutenção do estatuto de prestador de serviços de confiança qualificado.

Artigo 2.º

Âmbito

O presente regulamento aplica-se aos prestadores de serviços de confiança que pretendam obter ou renovar o estatuto de prestador qualificado para um ou mais serviços de confiança, nos termos definidos no Decreto-Lei n.º 27/2023, de 20 de outubro.

Artigo 3.º

Siglas

1. No presente regulamento são utilizadas as seguintes siglas:

a) ARME: Agência Reguladora Multissetorial da Economia;

b) ETSI: European Telecommunications Standards Institute;

c) FIPS PUB: Federal Information Processing Standard Publications;

d) HSM: Hardware Security Module;

e) ISO/IEC: International Organization for Standardization / International Electrotechnical Commission;

f) QSCD: Dispositivos Qualificados de Criação de Assinaturas/Selos Eletrônicos;

g) RFC: Request for Comments.

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

a) "Prestador de serviços de confiança", a pessoa coletiva que preste um ou mais do que um serviço de confiança quer como prestador qualificado quer como prestador não qualificado de serviços de confiança;

A2025/S2/BO53/13505
Deliberação n.º 23/CA/2025

b) "Prestador qualificado de serviços de confiança", o prestador de serviços de confiança que preste um ou mais do que um serviço de confiança qualificado e ao qual é concedido o estatuto de qualificado pela autoridade credenciadora;

c) "Serviço de confiança", um serviço eletrónico geralmente prestado mediante pagamento, nos termos do Decreto-Lei n.º 27/2023, de 20 de outubro;

Artigo 3.º

Requisitos para prestadores qualificados de serviços de confiança

1. Os prestadores de serviços de confiança que pretendam fornecer serviços qualificados devem proceder à sua credenciação junto da autoridade credenciadora.

2. Para efeitos de credenciação, os prestadores de serviços de confiança devem preencher o formulário de Pedido de Credenciação de Prestador Qualificado de Serviços de Confiança, disponível no sítio eletrónico da autoridade credenciadora, e apresentar a documentação e os comprovativos exigidos nos termos do Decreto-Lei n.º 27/2023, de 20 de outubro.

3. Para obter o estatuto de prestador de serviços de confiança qualificado, os prestadores devem assegurar que as suas instalações, procedimentos, competências do pessoal, equipamentos e sistemas cumprem as normas de segurança aplicáveis ao exercício da sua atividade, observando os seguintes requisitos:

a) Estabelecer ou adaptar a sua atividade operacional de acordo com os requisitos definidos no Decreto-Lei n.º 27/2023, de 20 de outubro, e nos documentos constantes da tabela que integra o anexo ao presente regulamento, do qual faz parte integrante;

b) Elaborar uma Declaração de Práticas para cada tipo de serviço prestado, com o objetivo de informar os utilizadores e terceiras partes sobre a organização e execução das atividades do prestador, bem como sobre as características dos serviços de confiança prestados;

c) No caso de prestadores de serviços de confiança que emitam certificados digitais qualificados, elaborar uma Declaração de Práticas de Certificação e uma Política de Certificação, em conformidade com as normas e requisitos aplicáveis:

i. A Declaração de Práticas de Certificação deve observar obrigatoriamente a estrutura definida na IETF RFC 3647, descrevendo os processos que o prestador de serviços utilizará na criação e manutenção dos certificados.

ii. A Política de Certificação deve indicar os tipos de certificados emitidos pelo prestador, em conformidade com a norma ETSI 319 411-2, e descrever cada tipo em termos de qualidade.

A2025/S2/BO53/13505
Deliberação n.º 23/CA/2025

iii. A Política de Certificação pode constituir um documento autónomo ou integrar a Declaração de Práticas de Certificação.

iv. Os documentos referidos substituem a Declaração de Práticas no que diz respeito ao fornecimento de certificados digitais.

v. Caso o prestador ofereça outros serviços além da emissão de certificados digitais, deve elaborar uma Declaração de Práticas para cada um dos demais serviços prestados.

d) Elaborar o Plano de Segurança, nos termos previstos no artigo 25.º do Decreto-Lei n.º 27/2023, de 20 de outubro, em conformidade com as disposições da norma ISO/IEC 27001 e com os requisitos estabelecidos no artigo 6.º do presente regulamento;

e) Efetuar uma Avaliação de Riscos, de acordo com as disposições do documento ETSI EN 319 401 e da norma ISO/IEC 27005, a qual deve ser submetida ao órgão executivo do prestador de serviços para conhecimento e aprovação;

f) Elaborar e manter um Inventário de todos os ativos de informação, atribuindo uma classificação que seja consistente com a avaliação de riscos realizada, em conformidade com as disposições da norma ISO/IEC 27002. O inventário deve ser atualizado sempre que ocorram alterações nos ativos e revisto, no mínimo, anualmente;

g) Elaborar um Plano de Contingência, que inclua, no mínimo, os requisitos estabelecidos no artigo 7.º do presente regulamento;

h) Elaborar uma Política de Pessoal, responsável pelas funções de gestão dos serviços de confiança, que contenha, no mínimo, os requisitos descritos no artigo 8.º;

i) Elaborar um Plano de Cessação de Atividades que contenha, no mínimo, os requisitos descritos no artigo 9.º.

j) Utilizar sistemas e dispositivos fiáveis, de acordo com o disposto no artigo 10.º.

k) Desenvolver a atividade em instalações físicas adequadas, em conformidade com os requisitos definidos no Regulamento de Segurança Física de Instalações de Prestadores Qualificados de Serviços de Confiança.

l) No caso de prestadores de serviços que emitam certificados digitais, as respetivas atividades de registo devem ser executadas em ambiente físico.

m) Contratar os serviços de um Organismo de Avaliação de Conformidade credenciado pela autoridade credenciadora, para realização de auditoria pré-operacional, para fins de obtenção do estatuto de Prestador Qualificado de Serviços de Confiança, e auditoria operacional anual, para

A2025/S2/BO53/13505
Deliberação n.º 23/CA/2025

fins de manutenção do estatuto de qualificado, conforme definido no Regulamento de Avaliação de Conformidade.

Artigo 4.º

Pedido de credenciação

1.O candidato a prestador qualificado de serviços de confiança, para iniciar o processo de credenciação inicial, deve submeter à Agência Reguladora Multissetorial da Economia (ARME) os seguintes documentos:

a) Pedido de Credenciação de Prestador Qualificado de Serviços de Confiança, devidamente preenchido;

b) Estatutos da pessoa coletiva e, no caso de sociedades, contrato de sociedade;

c) Relação de todos os sócios, com especificação das respetivas participações, bem como dos membros dos órgãos de administração e de fiscalização. No caso de sociedades anónimas, deve ser apresentada a relação de todos os acionistas com participações significativas, diretas ou indiretas;

d) Declarações subscritas por todas as pessoas singulares e coletivas envolvidas, atestando que não se encontram em nenhuma das situações indiciadoras de falta de idoneidade;

e) Prova do substrato patrimonial e dos meios financeiros disponíveis, designadamente a realização integral do capital social;

f) Descrição da organização interna e Plano de Segurança, em conformidade com os requisitos estabelecidos no presente regulamento;

g) Demonstração dos meios técnicos e humanos exigidos pela autoridade credenciadora, incluindo certificados de conformidade dos produtos de serviços de confiança emitidos por organismos de certificação;

h) Programa geral da atividade prevista para os primeiros três anos de operação;

i) Descrição geral das atividades exercidas nos últimos três anos ou, no caso de entidades constituídas há menos tempo, desde a sua constituição, acompanhada do balanço e contas dos exercícios correspondentes;

j) Comprovação de contrato de seguro válido, que cubra adequadamente a responsabilidade civil decorrente da atividade de certificação;

k) Documentos técnicos referidos no n.º 3 do artigo 3.º do presente regulamento;

A2025/S2/BO53/13505
Deliberação n.º 23/CA/2025

l) Relatório da auditoria pré-operacional, que contemple a avaliação de conformidade de todos os serviços para os quais seja solicitado o estatuto de qualificado.

2. Os documentos apresentados são analisados pela autoridade credenciadora, que decide sobre a aceitação ou recusa do pedido de atribuição do estatuto de prestador qualificado de serviços de confiança.

3. O estatuto de prestador qualificado de serviços de confiança é válido por um período de três anos, podendo ser renovado por períodos de igual duração.

Artigo 5.º

Renovação da credenciação

1. A estrutura para os prestadores qualificados de serviços de confiança, que deve ser encaminhar à autoridade credenciadora para os prestadores de prestadores para os prestadores qualificados de serviços de confiança:

a) Pedido de Renovação de Credenciação de Prestador Qualificado de Serviços de Confiança, devidamente preenchido, de acordo com o formulário disponível no sítio da Internet da autoridade credenciadora;

b) Atualização dos documentos referidos no n.º 1 do artigo 4.º do presente regulamento;

c) Atualização dos documentos técnicos definidos no n.º 3 do artigo 3.º do presente regulamento;

d) Relatório de auditoria operacional, que inclua a última avaliação de conformidade de todos os serviços para os quais seja solicitada a renovação do estatuto de qualificado.

2. Os documentos apresentados são analisados pelos órgãos competentes da autoridade credenciadora, podendo o pedido de renovação do estatuto de prestador qualificado de serviços de confiança ser aceite ou recusado.

Artigo 6.º

Plano de segurança

1. O prestador qualificado de serviços de confiança deve elaborar um Plano de Segurança que inclua, no mínimo, as seguintes informações:

a) Descrição da estrutura organizacional e funcional, bem como da atividade de serviços de confiança prestada;

b) Especificação dos processos de avaliação e garantia da idoneidade e capacidade técnica do

A2025/S2/BO53/13505
Deliberação n.º 23/CA/2025

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) Requisitos de proteção da informação, com distinção dos níveis de segurança e dos perfis de acesso implementados;

f) Definição das funções que conferem acesso aos atos e instrumentos dos serviços de confiança, respetivos requisitos de segurança e perfis de acesso;

g) Descrição dos produtos de assinatura eletrónica utilizados, com identificação das respetivas certificações de conformidade, quando aplicável;

h) Descrição e avaliação de outros riscos de segurança;

i) Indicação dos responsáveis pela implementação do Plano de Segurança;

j) Indicação do processo de revisão periódica estabelecido.

3. A equipa que atua diretamente nos serviços de confiança deve ser formalmente informada sobre a existência e o conteúdo do Plano de Segurança.

Artigo 7.º

Plano de contingência

1. O prestador qualificado de serviços de confiança deve dispor de procedimentos que permitam assegurar a continuidade dos serviços em sistemas de recuperação alternativos, de modo a fazer face à eventual ocorrência de desastres ou incidentes que possam comprometer o funcionamento normal dos serviços prestados. Estes procedimentos devem garantir que a migração dos sistemas primários para os sistemas de recuperação não coloque em risco a segurança dos sistemas.

2. No caso do prestador de serviços de emissão de certificados e selos digitais, deve ser garantida a disponibilidade permanente dos serviços de distribuição, revogação e consulta do estado de revogação de certificados, mesmo em situações de incidentes.

3. O prestador qualificado de serviços de confiança deve implementar um Plano de contingência que inclua, no mínimo:

a) A possibilidade de adulteração ou acesso não autorizado às chaves privadas, próprias ou de terceiros sob sua custódia, quando aplicável;

A2025/S2/BO53/13505
Deliberação n.º 23/CA/2025

b) A invasão dos seus sistemas e da rede interna;

c) Incidentes de segurança física e lógica;

d) A indisponibilidade da infraestrutura;

e) Fraudes ocorridas no registo do utilizador, na emissão, expedição, distribuição, revogação e gestão de certificados, no caso de se tratar de um prestador qualificado de serviços de confiança que emita certificados digitais.

4. O Plano de contingência deve incluir os seguintes procedimentos:

a) Retoma das operações num prazo que minimize o impacto para os utilizadores;

b) Notificação aos requerentes, titulares, destinatários e demais entidades com as quais existam acordos, sobre qualquer ocorrência que comprometa a utilização segura dos serviços prestados;

c) Notificação às autoridades competentes, sempre que aplicável;

d) Revogação dos certificados afetados, sempre que necessário;

e) Procedimentos para a interrupção ou suspensão de serviços e para a investigação do incidente;

f) Análise e monitorização dos registos de auditoria;

g) Gestão do relacionamento com o público e com os meios de comunicação social, sempre que aplicável.

5. Todos os intervenientes no Plano de contingência devem receber formação específica para lidar com incidentes.

6. O plano deve ser atualizado e testado, no mínimo, uma vez por ano, bem como sempre que o prestador identifique alterações no seu ambiente ou sistema que possam gerar riscos para a segurança da informação.

Artigo 8.º

Política de pessoal

1. O prestador qualificado de serviços de confiança deve adotar as seguintes regras de seleção e contratação de funcionários, de modo a reforçar e respeitar as disposições de segurança exigidas para o exercício da sua atividade:

a) Para funções de gestão da infraestrutura que suporta os serviços de confiança, deve empregar pessoal especializado, com conhecimentos específicos em assinatura eletrónica, certificação

A2025/S2/BO53/13505
Deliberação n.º 23/CA/2025

digital e outras tecnologias relevantes para os serviços prestados, bem como em segurança da informação e proteção de dados pessoais;

b) Todo o pessoal que desempenha funções relacionadas com os processos que suportam os serviços de confiança deve estar livre de conflitos de interesse que possam comprometer a sua imparcialidade;

c) As funções relacionadas com os processos que suportam os serviços de confiança não podem ser desempenhadas por pessoas que se encontrem em situação indicadora de falta de idoneidade;

d) No âmbito da sua estrutura organizativa, deve contemplar, pelo menos, os seguintes cargos e funções necessários à operação dos sistemas que suportam os serviços de confiança:

i. Administrador de sistemas: responsável pela instalação, configuração e manutenção dos sistemas, com acesso controlado às configurações relacionadas com a segurança;

ii. Operador de sistemas: encarregado da operação diária dos sistemas, com autorização para realizar cópias de segurança e reposição de informação;

iii. Administrador de segurança: responsável pela gestão e implementação das regras e práticas de segurança;

iv. Auditor de sistemas: autorizado a monitorizar os registos de atividade dos sistemas;

v. Administrador de registo: responsável pela aprovação da emissão, suspensão e revogação de certificados, no caso de o prestador qualificado de serviços de confiança emitir certificados e selos digitais.

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

Artigo 9.º

Plano de cessação de atividades

1. O prestador qualificado de serviços de confiança deve dispor de um Plano de Cessação de Atividades atualizado, no qual conste que, antes de terminar os seus serviços, adotará as seguintes medidas:

a) Informará do término da sua atividade todos os assinantes e demais entidades com as quais mantém acordos ou outras formas de relações estabelecidas, incluindo as partes confiantes, outros prestadores de serviços de confiança e as autoridades competentes, designadamente os órgãos de supervisão;

A2025/S2/BO53/13505
Deliberação n.º 23/CA/2025

b) Revogará a autorização de todos os subcontratantes para atuar em nome do prestador na execução de quaisquer funções relacionadas com o processo de emissão de *tokens* de serviço de confiança;

c) Transferirá as obrigações para uma entidade confiável, de modo a garantir a manutenção de todas as informações necessárias para comprovar a operação do prestador por um período razoável, exceto se for demonstrado que o prestador não possui tais informações;

d) Destruirá ou retirará de uso as suas chaves privadas, incluindo cópias de *backup*, de forma a impossibilitar a sua recuperação;

e) Tomará as providências necessárias para transferir a prestação dos serviços de confiança aos seus clientes existentes para outro prestador qualificado.

2. O prestador qualificado de serviços de confiança deve celebrar um acordo que garanta a cobertura dos custos associados ao cumprimento dos requisitos mínimos previstos no número anterior, em caso de falência ou de impossibilidade de suportar esses custos por meios próprios, dentro dos limites estabelecidos pela legislação aplicável em matéria de insolvência.

3. O prestador qualificado de serviços de confiança deve declarar nas suas práticas as disposições adotadas para a cessação da sua atividade.

4. O prestador qualificado de serviços de confiança mantém ou transfere para uma entidade confiável as suas obrigações de disponibilizar a sua chave pública ou os seus *tokens* de serviço de confiança às partes interessadas, por um período razoável.

Artigo 10.º

Dispositivos e sistemas fiáveis

1. O prestador qualificado de serviços de confiança deve utilizar sistemas e dispositivos fiáveis para a realização das suas operações, com as seguintes características:

a) Os Dispositivos Seguros de Hardware (HSM) utilizados para operações que envolvem chaves criptográficas devem preencher os seguintes critérios:

i. Ter garantia de EAL 4 ou superior, de acordo com a norma ISO/IEC 15408, ou critérios de avaliação equivalentes reconhecidos a nível nacional ou internacional para a segurança das tecnologias de informação, desde que correspondam a um alvo de segurança ou perfil de proteção que cumpra os requisitos dos documentos aplicáveis ao serviço prestado, com base numa análise de risco e considerando medidas de segurança físicas e outras medidas de segurança não técnicas; ou

A2025/S2/BO53/13505
Deliberação n.º 23/CA/2025

ii. Cumprir os requisitos identificados na ISO/IEC 19790 ou FIPS PUB 140-2 nível 3 ou FIPS PUB 140-3 nível 3.

b) Os dispositivos criptográficos seguros devem ser operados na sua configuração, conforme descrito na documentação de orientação de certificação apropriada, ou numa configuração equivalente que atinja o mesmo objetivo de segurança.

c) Os Dispositivos Qualificados de Criação de Assinaturas/Selos Eletrónicos (QSCD), fornecidos pelo prestador aos titulares, no âmbito dos serviços de emissão de certificados digitais, quando aplicável.

d) Os algoritmos e parâmetros criptográficos utilizados nas diferentes operações e serviços executados pelo prestador qualificado de serviços de confiança devem refletir, com especial atenção, a durabilidade dos esquemas de assinatura relativamente à sua resistência a ataques, uma vez que isso afeta diretamente o período de validade que se pretende atribuir aos certificados e assinaturas criados.

e) Para tal, devem ser utilizadas as recomendações do Capítulo 8 do documento ETSI TS 119 312, considerando sempre a sua versão mais recente.

f) Os sistemas utilizados na execução dos processos críticos devem ser fiáveis e cumprir, no mínimo, os requisitos 7.4-04 a 7.4-10 do documento ETSI EN 319 401.

2. Os requisitos para os sistemas fiáveis podem ser garantidos através da utilização, por exemplo, de sistemas em conformidade com o CEN TS 419 261, o CEN EN 419 241-1 ou com um perfil de proteção adequado (ou perfis), definido de acordo com a norma ISO/IEC 15408.

Artigo 11.º

Entrada em vigor

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

Feita na Cidade da Praia, aos 26 de fevereiro de 2025. — O Conselho de Administração, O Presidente, *Leonilde Santos*, os Administradores, *João Tomar* e *Carlos Ramos*.

A2025/S2/BO53/13505
Deliberação n.º 23/CA/2025

AGÊNCIA REGULADORA MULTISSETORIAL DA ECONOMIA - ARME
Conselho de Administração

Deliberação n.º 24/CA/2025

Sumário: Aprovando o regulamento que estabelece as regras aplicáveis aos requisitos de segurança física aplicáveis às unidades de registo.

De 26 de fevereiro de 2025

Preâmbulo

A Agência Reguladora Multissectorial da Economia (ARME), criada pelo Decreto-Lei n.º 50/2018, de 20 de setembro, que aprova os seus Estatutos, é uma autoridade administrativa independente, de base institucional, dotada de funções reguladoras, incluindo a regulamentação, supervisão e sancionamento de infrações. Nos termos do n.º 1 do artigo 1.º do referido diploma, a ARME tem como 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, conforme estabelecido no n.º 1 do artigo 2.º do mesmo diploma.

No âmbito das suas competências, o artigo 15.º, alínea f), do Decreto-Lei n.º 50/2018, de 20 de setembro, atribui aos órgãos da ARME, enquanto entidade reguladora do setor das comunicações eletrónicas, a competência de supervisionar as entidades de certificação. Esta atribuição foi reforçada pelo Decreto-Lei n.º 27/2023, de 20 de outubro, que estabelece as normas aplicáveis aos serviços de confiança, nomeadamente no que diz respeito 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, o 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. O artigo 82.º deste diploma atribui à ARME, enquanto Entidade Reguladora do Sector das Comunicações Eletrónicas, as funções de autoridade credenciadora.

Para a prossecução destas atribuições, a ARME, no exercício das suas competências como Entidade Reguladora do Sector das Comunicações Eletrónicas e, em particular, no desempenho das funções de autoridade credenciadora, deve emitir e publicar no seu sítio da Internet e no Boletim Oficial as regras técnicas e de segurança aplicáveis ao exercício da atividade de prestação de serviços de confiança, nos termos do artigo 99.º do Decreto-Lei n.º 27/2023, de 20 de outubro.

Neste contexto, o presente Regulamento de Segurança Física de Instalações de Unidades de Registo tem como objeto definir os requisitos de segurança física aplicáveis às unidades de registo, visando a proteção contra potenciais riscos e ameaças que possam comprometer a sua

A2025/S2/BO53/13505
Deliberação n.º 24/CA/2025

integridade e operações. Este regulamento está alinhado com as disposições do Decreto-Lei n.º 27/2023, de 20 de outubro, e com as normas de referência internacional aplicáveis à atividade de certificação digital, nomeadamente: WEBTRUST FOR CA; ETSI EN 319 401; ETSI EN 319 411-1; ETSI EN 319 411-2; ISO/IEC 27001; e ISO/IEC 27002.

Assim, nos termos da alínea *b)* do artigo 14.º, e da alínea *f)* do artigo 15.º dos Estatutos da ARME, aprovados pelo Decreto-Lei n.º 50/2018, de 20 de setembro, do artigo 82.º e do n.º 1 do artigo 99.º do Decreto-Lei n.º 27/2023 de 20 de outubro, o Conselho de Administração, em sua reunião ordinária de 26 de fevereiro de 2025, aprova o presente Regulamento, que estabelece as regras aplicáveis aos requisitos de segurança física aplicáveis às unidades de registo.

Artigo 1.º

Aprovação

É aprovado o regulamento que estabelece que que estabelece as regras aplicáveis aos requisitos de segurança física aplicáveis às unidades de registo.

Artigo 2.º

Entrada em vigor

A presente deliberação entra em vigor no dia seguinte ao da sua publicação em Boletim Oficial.

Feita na Cidade da Praia, aos 26 de fevereiro de 2025. — O Conselho de Administração, A Presidente, *Leonilde Santos*, os Administradores, *João Tomar* e *Carlos Ramos.*

REGULAMENTO DOS REQUISITOS DE SEGURANÇA FÍSICA PARA AS INSTALAÇÕES DA UNIDADE DE REGISTO

Artigo 1.º

Objeto

O presente regulamento estabelece as regras aplicáveis aos requisitos de segurança física aplicáveis às unidades de registo.

Artigo 2.º

Âmbito

A presente norma aplica-se às unidades de registo que prestam serviços nos termos do Decreto-Lei n.º 27/2023, de 20 de outubro.

A2025/S2/BO53/13505
Deliberação n.º 24/CA/2025

Artigo 3.º

Objetivos

1. As unidades de registo devem implementar e manter controlos de segurança física, com os seguintes objetivos:

a) Limitar o acesso físico às instalações e equipamentos da unidade de registo a pessoas autorizadas, assegurando a proteção através de perímetros de segurança e sob o controlo de, pelo menos, duas pessoas (dupla custódia);

b) Proteger as instalações e equipamentos da unidade de registo contra riscos ambientais;

c) Prevenir perdas, danos ou comprometimento de ativos, bem como a interrupção das atividades comerciais.

2. Nos termos da alínea a) do número anterior, no mínimo, duas autorizações distintas são necessárias para permitir o acesso a informações, áreas ou a realização de ações críticas, assegurando uma camada adicional de proteção.

Artigo 4.º

Siglas e definições

1. No presente regulamento são utilizadas as seguintes siglas:

a) ARME: Agência Reguladora Multissetorial da Economia

b) EC: Entidade Certificadora

c) ETSI: European Telecommunications Standards Institute

d) HVAC: Heating, Ventilation and Air Conditioning

e) ISO/IEC: International Organization for Standardization / International Electrotechnical

f) Commission

g) UPS: Uninterruptible Power Supply

h) UR: Unidade de Registo

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

a) "Unidade de Registo", a entidade responsável pelo registo e gestão de informações relacionadas com os serviços de confiança.

A2025/S2/BO53/13505
Deliberação n.º 24/CA/2025

Artigo 5.º

Controlos de segurança física para instalações da unidade de registo

1. A entrada no edifício ou no local onde são realizadas as operações da unidade de registo deve ser efetuada exclusivamente através de pontos de acesso limitados e devidamente controlados.

2. Deve existir uma receção controlada por pessoal ou outro meio de controlo de acesso físico, de modo a restringir o acesso ao edifício ou ao local onde são realizadas as operações da unidade de registo, permitindo-o apenas aos colaboradores autorizados.

3. Devem ser instaladas portas corta-fogo nos perímetros de segurança das instalações operacionais da unidade de registo, bem como sistemas de alarme, em conformidade com a legislação e regulamentação aplicáveis.

4. Devem ser implementados sistemas de deteção de intrusões em todas as portas externas das instalações operacionais da unidade de registo, os quais devem ser testados regularmente.

5. As instalações operacionais da unidade de registo devem permanecer fisicamente trancadas e protegidas com sistemas de alarme quando se encontrem desocupadas.

6. Devem existir barreiras físicas robustas, constituídas por paredes sólidas que se estendam desde o piso real até ao teto real.

7. Os documentos físicos (registos em papel) devem ser armazenados em locais seguros, como salas de arquivo com acesso restrito e barreiras físicas robustas, com o objetivo de prevenir roubos, danos acidentais ou acesso não autorizado à informação, garantindo a confidencialidade, integridade e disponibilidade da mesma.

8. Deve ser instalado um sistema que assegure a deteção e extinção automática de incêndios, o controlo da humidade e da temperatura, bem como a deteção de inundações, aplicável, em particular, às salas de arquivo.

9. Todos os colaboradores devem utilizar uma identificação visível.

10. O acesso às instalações operacionais da unidade de registo deve ser restrito a pessoas autorizadas e protegido através da utilização de controlos de autenticação multifator.

11. Todas as entradas e saídas das instalações operacionais da unidade de registo devem ser registadas, devendo:

a) O registo ser auditável;

b) Ser utilizado um sistema de controlo de acesso que permita a identificação do colaborador, o

A2025/S2/BO53/13505
Deliberação n.º 24/CA/2025

qual é considerado suficiente para o pessoal com acesso permanente.

12. As entradas e saídas das instalações da unidade de registo devem ser monitorizadas através de um sistema de videovigilância com câmaras.

13. Os visitantes devem ser acompanhados durante o acesso ao edifício ou às instalações da unidade de registo, devendo ser efetuado o registo da data e hora da entrada e saída.

14. Os fornecedores devem ter acesso às instalações operacionais da unidade de registo apenas quando estritamente necessário.

15. O acesso deve ser previamente autorizado e acompanhado.

16. Os direitos de acesso às instalações da unidade de registo devem ser revistos e atualizados com uma periodicidade mínima anual.

Artigo 6.º

Controlos para segurança de equipamentos

1. Os equipamentos devem estar localizados de forma a minimizar os riscos associados a ameaças ambientais e a acessos não autorizados.

2. Os equipamentos devem estar protegidos contra falhas de energia e outras anomalias elétricas, designadamente através da utilização de sistemas de alimentação ininterrupta (UPS) e geradores.

3. A cablagem de energia elétrica e de telecomunicações que suporta o funcionamento das instalações operacionais da autoridade de registo deve estar protegida contra interceção e danos.

4. Todos os equipamentos devem ser mantidos e sujeitos a processos de manutenção, de acordo com as instruções do fabricante.

5. Todos os equipamentos que armazenam informação devem ser cuidadosamente verificados antes de serem eliminados ou reutilizados, com o objetivo de prevenir o acesso a informação sensível por parte de pessoas não autorizadas. O método utilizado para a destruição da informação deve garantir a sua irrecuperabilidade, mesmo face a técnicas avançadas de recuperação.

Artigo 7.º

Controlos gerais

1. As informações comerciais, sensíveis ou críticas devem ser guardadas sob chave quando não estiverem a ser utilizadas e sempre que as instalações da autoridade de registo se encontrem

A2025/S2/BO53/13505
Deliberação n.º 24/CA/2025

desocupadas, devendo ser implementada uma política de secretária limpa.

2. Os postos de trabalho devem ser desligados, bloqueados com palavra-passe ou protegidos através de fechadura com chave, ou outros controlos equivalentes, quando não estiverem a ser utilizados, devendo ser implementada uma política de ecrã limpo.

3. Qualquer movimentação de materiais e equipamentos de ou para as instalações da autoridade de registo carece de autorização prévia.

Artigo 8.º

Entrada em vigor

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

Feita na Cidade da Praia, aos 26 de fevereiro de 2025. — O Conselho de Administração, A Presidente, *Leonilde Santos*, os Administradores, *João Tomar* e *Carlos Ramos*.

A2025/S2/BO53/13505
Deliberação n.º 24/CA/2025

MUNICÍPIO DA BOA VISTA
Assembleia Municipal

Deliberação n.º 01/AMBV/2025

Sumário: Apreciando e aprovando a proposta que fixa a gratificação da Presidente da Assembleia Municipal.

De 10 de fevereiro de 2025

A Assembleia Municipal da Boa Vista, reunida na sua 1ª Sessão Ordinária, no dia 10 de fevereiro de 2025, convocada nos termos do artigo 77º da Lei n.º 134/IV/95, de 03 de julho (Estatuto dos Municípios) e nos termos do artigo 28º do Regimento da Assembleia Municipal da Boa Vista, delibera, nos termos dos artigos 13º e 16º da Lei n.º 28/V/97, de 23 de junho e do artigo 10º da Lei n.º 14/91, de 30 de dezembro apreciar e aprovar a seguinte proposta da Assembleia Municipal da Boa Vista:

1. Apreciação e Aprovação da proposta que fixa a gratificação de funções da Presidente da Assembleia Municipal em 20% do vencimento mensal do Presidente da República e os restante direitos conferidos pela lei, com efeito a partir de 23 de dezembro de 2024, data que se iniciou o mandato dos órgãos Municipais, decorrente das eleições Autárquicas de 01 de dezembro de 2024.

Efetuada a apreciação da proposta, a Sra. Presidente da Assembleia Municipal colocou à votação, tendo a mesma sido aprovada, por unanimidade com 17 (dezassete) votos a favor, sendo 12 (doze) votos da bancada do Partido Africano de Independência de Cabo Verde – PAICV e 5 (cinco) votos da bancada do Movimento Para Democracia – MPD e 0 (zero) abstenções.

Cidade de Sal-Rei, aos 10 de fevereiro de 2025. — A Presidente, *Marízia Rosângela Brito Lima Oliveira.*

A2025/S2/BO53/13505
Deliberação n.º 01/AMBV/2025

MUNICÍPIO DA BOA VISTA
Assembleia Municipal

Deliberação n.º 02/AMBV/2025

Sumário: Apreciando e aprovando a proposta do exercício de funções da Secretaria da Mesa da Assembleia Municipal a meio tempo e a respectiva remuneração.

De 10 de fevereiro de 2025

A Assembleia Municipal da Boa Vista, reunida na sua 1 ª Sessão Ordinária, no dia 10 de fevereiro de 2025, convocada nos termos do artigo 77º da Lei n.º 134/IV/95, de 03 de julho (Estatuto dos Municípios) e nos termos do artigo 28º do Regimento da Assembleia Municipal da Boa Vista, delibera, nos termos do artigo 71º da Lei n.º 134/IV/95, de 03 de julho, apreciar e aprovar a seguinte proposta da mesa da Assembleia Municipal:

1. Apreciação e Aprovação da proposta do exercício das funções da secretária da Mesa da Assembleia Municipal a meio tempo, e fixar a sua remuneração em 50% do vencimento da Secretária Municipal da Câmara Municipal da Boa Vista, com efeito a partir de 23 de dezembro de 2024, data que se iniciou o mandato dos Órgãos Municipais, decorrente das eleições Autárquicas de 01 de dezembro de 2024.

Efetuada a apreciação da proposta, a senhora Presidente da Assembleia Municipal colocou à votação, tendo a mesma sido aprovada com 12 (doze) votos a favor: sendo 12 (doze) votos a favor da bancada do Partido Africano da Independência de Cabo Verde-PAICV, 0 (zero) votos contra e 5 (cinco) Abstenções da bancada do Movimento Para Democracia - MPD.

Cidade de Sal-Rei, aos 10 de fevereiro de 2025. — A Presidente, *Marízia Rosângela Brito Lima Oliveira.*

A2025/S2/BO53/13505
Deliberação n.º 02/AMBV/2025

MUNICÍPIO DA BOA VISTA
Assembleia Municipal

Deliberação n.º 03/AMBV/2025

Sumário: Apreciando e aprovando a proposta de profissionalização de 6 (seis) Vereadores a tempo inteiro.

De 10 de fevereiro de 2025

A Assembleia Municipal da Boa Vista, reunida na sua 1ª Sessão Ordinária, no dia 10 de fevereiro de 2025, convocada nos termos do artigo 77º da Lei n.º 134/IV/95, de 03 de julho (Estatuto dos Municípios) e nos termos do artigo 28º do Regimento da Assembleia Municipal da Boa Vista, delibera, nos termos do disposto do artigo 88º da Lei n.º 134/IV/95 de 03 de julho, conjugado com o n.º 2 do artigo n.º 12º da Lei n.º 28/V/97, de 23 de junho, apreciar e aprovar a seguinte proposta da Câmara Municipal da Boa Vista:

1. Aprovação da Proposta de Profissionalização de 6 (seis) Vereadores a Tempo Inteiro e as respetivas Remunerações.

a) Nádia Sofia Lima Santos

b) Abel José Silva Ramos

c) Fabienne Louise Oliveira Pires

d) João Manuel Silva Mosso Mendes

e) Clara Maria Correia Barros

f) João Henrique Barros Correia

Efetuada a apreciação da proposta, a Sra. Presidente da Assembleia Municipal colocou à votação, tendo a mesma sido Aprovada, com 12 (Doze) votos a favor da bancada do Partido Africano da Independência de Cabo Verde-PAICV, 5 (cinco) votos Contra da bancada do Movimento para Democracia-MPD e 0 (zero) Abstenções.

Cidade de Sal-Rei, aos 10 de fevereiro de 2025. — A Presidente, *Marízia Rosângela Brito Lima Oliveira.*

A2025/S2/BO53/13505
Deliberação n.º 03/AMBV/2025

II Série
BOLETIM OFICIAL
Registo legal, nº2/2001
de 21 de Dezembro de 2001

I.N.C.V., S.A. informa que a transmissão de actos sujeitos a publicação na I e II Série do Boletim Oficial devem obedecer às normas constantes no artigo 28º e 29º do Decreto-lei nº8/2011, de 31 de Janeiro de 2011.