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