## ANEXO II

# REGULAMENTO DE AVALIAÇÃO DE CONFORMIDADE DE PRESTADORES QUALIFICADOS DE SEVIÇOS DE CONFIANÇA

## PREÂMBULO

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

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

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

Para a prossecução destas atribuições, no âmbito da sua competência como Entidade Reguladora do Sector das Comunicações Eletrónicas, incluindo, principalmente, as funções como autoridade credenciadora, a ARME deve emitir e publicar no seu sítio da *Internet* e no *Boletim Oficial* as regras de 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 os serviços eletrónicos de 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.

Os serviços de confiança para que possam ser prestados continuamente por prestadores qualificados de serviços de confiança dentro da Infraestrutura de Chaves Públicas de Cabo Verde, é necessário que a implementação de um sistema de avaliação de conformidade para garantir que esses serviços cumprem os requisitos normativos nacionais e internacionais que lhe são aplicáveis.

O regulamento de avaliação de conformidade de prestadores qualificados de serviços de confiança tem como objeto, a uniformização dos 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 .

CAPÍTULO I

**Disposições Gerais**

Artigo 1.º

**Objeto**

Este regulamento tem como objetivo, uniformizar 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 2.º

**Âmbito**

Este regulamento aplica-se a todos os organismos de certificação credenciados pela autoridade credenciadora, para realizar avaliação de conformidade de prestadores de serviços de confiança com o objetivo de atribuição e manutenção do estatuto de prestadores de serviço qualificado.

Artigo 3.º

**Siglas e definições**

1. No presente regulamento são utilizadas as seguintes siglas:

   *a)* ETSI: European Telecommunications Standards Institute;

   *b)* ICP: Infraestrutura de Chaves Pública;

   *c)* NT: Norma Técnica;

   *d)* PSC: Prestador de Serviços de Confiança;

   *e)* RFA: Relatório Final de Auditoria;

   *f)* RPI: Relatório de Primeiras Impressões;

   *g)* TI: Tecnologias de Informação.

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

   *a)* Acreditação: a atividade de acreditação consiste na avaliação e reconhecimento da competência técnica de entidades para efetuar atividades específicas de avaliação da conformidade, nomeadamente ensaios, calibrações, certificações e inspeções;

   *b)* Avaliação de conformidade: a avaliação da conformidade consiste, designadamente, na realização de ensaios, calibrações, inspeções, certificações, verificações, realizados com o objetivo de demonstrar que um dado bem, produto, processo ou serviço cumpre com os requisitos que lhe são aplicáveis. Nalguns

casos, a avaliação da conformidade é legalmente exigida, quando relacionada com a segurança desse produto ou serviço.

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

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

## CAPÍTULO II

## Avaliação de Conformidade

### Artigo 4.º

### Auditorias pré-operacionais e periódicas

1. A avaliação de conformidade do prestador qualificado de serviço de confiança é realizada sob a forma de auditoria pré-operacional, para efeitos de atribuição do respetivo estatuto, bem como a auditorias anuais ou periódicas, a contar da data de início da auditoria inicial, nos seguintes termos:

   *a)* Auditorias completas, pelo menos, a cada vinte e quatro meses;

   *b)* Auditorias de acompanhamento, nos anos em que não se realizem as auditorias completas.

2. A auditoria de prestadores qualificados de serviço de fornecimento de certificados publicamente confiáveis deve ser feita anualmente, de forma completa, conforme os documentos *ETSI EN 319 403-2* e *WEBTRUST SSL*.

3. As avaliações de conformidade são efetuadas às custas do prestador qualificado de serviços, por organismo de certificação credenciado pela autoridade credenciadora, nos termos do Regulamento de Credenciação de Organismos de Certificação.

4. A autoridade credenciadora publica no seu *website* a lista de organismos de certificação credenciados, que devem realizar as avaliações de conformidade observando os requisitos do presente regulamento.

5. A partir da receção do relatório de auditoria, a autoridade credenciadora decide pela 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, observados os procedimentos previstos nos padrões referidos na Tabela, disposta no anexo, parte integrante deste regulamento.

Artigo 6.º

**Plano da auditoria**

1. O prestador de serviço de confiança que desenvolve a sua atividade, na totalidade ou em parte, em vários locais, deve garantir que operam sob o mesmo sistema de gestão e são alvo de auditorias internas, de acordo com os procedimentos internos do prestador de serviço de confiança.
2. Nos casos referidos no número 1, a avaliação deve ser efetuada com base em amostragem, a definir pelo organismo de certificação, tendo como orientação as seguintes informações:
   *a)* Os resultados das auditorias internas anteriores;
   *b)* As vulnerabilidades, ameaças e riscos a que cada local está sujeito;
   *c)* Os resultados das revisões feitas pelo órgão/grupo de gestão;
   *d)* As diferenças e variações na dimensão e na atividade dos locais;
   *e)* A complexidade do sistema de gestão do PSC;
   *f)* A complexidade dos sistemas de informação de cada um dos locais;
   *g)* A interação com sistemas de informação críticos do PSC;
   *h)* As diferenças nos requisitos legais em vigor.
3. As informações referidas no n.º 2 devem ser levadas em consideração para definição do tamanho e composição da equipa de auditoria e do tempo de execução da auditoria.

Artigo 7.º

**Tipos e fases da auditoria**

1. As auditorias para efeitos de avaliação de conformidade do prestador qualificado de serviço de confiança são as seguintes:
   *a)* Auditorias pré-operacionais, também conhecidas como auditorias de concessão;
   *b)* Auditorias operacionais, também conhecidas como auditorias de acompanhamento ou renovação.
2. As fases, para efeitos das auditorias referidas no número anterior, são as seguintes:
   *a)* Fase 1: pré-avaliação;
   *b)* Fase 2: auditoria no local;
   *c)* Fase 3: 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) reunião preliminar com o representante da entidade a auditar, com o objetivo de estabelecer o plano para a fase 2 da auditoria e obter um conhecimento da estrutura e da extensão do(s) serviço(s) auditado(s) do prestador qualificado de serviços de confiança.

2. Devem ser verificados, de acordo com a especificidade de cada entidade a auditar, os seguintes documentos e 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 PSC (autoavaliação):

   *d)* Declaração de Práticas;

   *e)* Políticas Aplicáveis aos Serviços;

   *f)* Plano de Segurança;

   *g)* Política de Segurança;

   *h)* Plano de Contingência/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)* Quando no serviço avaliado é incorporado um componente certificado anteriormente, os documentos que comprovam essa certificação.

3. Os seguintes documentos podem ser incluídos na fase 1 da auditoria, caso sejam relevantes:

   *a)* A verificação de registos referentes à entidade legal;

   *b)* Os acordos para cobrir responsabilidades;

   *c)* As relações contratuais entre o PSC e possíveis contratados que operam ou fornecem serviços de subcomponentes,

   *d)* Auditorias ou certificações internas/externas,

   *e)* Revisão do gerenciamento de segurança e outras investigações com relação à auditoria preliminar das conformidades parciais ou não conformidades autodeclaradas.

4. Os auditores devem entrar em acordo com o prestador de serviços de confiança quando e onde a fase 1 da auditoria será realizada, se no local ou remotamente ou uma combinação de ambas.

5. A avaliação documental deve estar concluída antes do início da fase 2, independentemente do local onde é realizada.

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

7. O Calendário e Plano de Auditoria deverá ser enviado previamente à Entidade auditada, devendo conter no mínimo, para cada dia de auditoria, os seguintes elementos:

   *a)* Os itens que irão ser alvo de apreciação;

   *b)* O local onde a auditoria se realizará; e

   *c)* As pessoas com funções de confiança que devem 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 avaliação no local**

1. Na fase 2, ou 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 as seguintes:

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

   *b)* Confirmar que os serviços de confiança implementados pelo prestador de serviço 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 relacionados com os serviços de confiança do prestador de serviços de confiança:

   *a)* Implementação de requisitos de serviços de confiança;

   *b)* Processos e procedimentos de organização relacionados aos serviços de confiança;

   *c)* Processos e procedimentos técnicos relacionados com os serviços de confiança;

   *d)* Interface dos componentes dos serviços de confiança;

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

   *f)* Produtos relacionados a serviços de confiança (sistemas confiáveis), como módulos criptográficos; e

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

4. Se o serviço usar componentes auditadas separadamente, deve ser garantido o cumprimento dos requisitos desses componentes, em particular no que toca à segurança de informação.

5. O organismo de certificação apresenta o Relatório de Primeiras Impressões-RPI, e comunica de forma verbal, as não-conformidades encontradas durante o processo de auditoria na fase 1 e na fase 2.

6. O RPI pode ser transcrito em documento, classificado de forma apropriada, e remetido 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 conter as seguintes informações:

   *a)* Um relato da auditoria, incluindo um resumo da análise do documento e da(s) norma(s), especificações publicamente disponíveis e/ou requisitos regulatórios com base nos quais a auditoria foi realizada;

   *b)* Um relato da auditoria da análise de risco de segurança da informação do PSC;

   *c)* Tempo total de auditoria utilizado e especificação detalhada do tempo gasto na revisão de documentos, avaliação da análise de risco, auditoria no local e relatório de auditoria;

   *d)* As investigações de auditoria que foram seguidas, a justificativa para a sua seleção e a metodologia empregada, incluindo a metodologia de amostragem e os procedimentos de teste;

*e)* Áreas cobertas pela auditoria, incluindo os requisitos de certificação e os locais que foram auditados, os registos analisados e as metodologias de auditoria utilizadas;

*f)* Observações feitas, tanto positivas quanto negativas;

*g)* Detalhes de quaisquer não-conformidades identificadas, apoiados por evidências objetivas (se aplicável) e uma referência exclusiva ao requisito que não foi cumprido; e

*h)* Comentários sobre a conformidade do PSC e dos serviços de confiança que ele presta com os critérios com base nos quais a auditoria foi realizada, juntamente com uma declaração clara de não conformidade e, quando aplicável, qualquer comparação útil com os resultados de auditorias anteriores do PSC e dos serviços de confiança em questão.

2. Também podem fazer parte do relatório de auditoria questionários preenchidos, listas de verificação, observações, registos ou anotações do auditor.

3. As informações sobre as amostras avaliadas durante a auditoria devem ser incluídas no relatório de auditoria ou em outra documentação de certificação.

4. O relatório deve considerar a adequação da organização e dos procedimentos internos adotados pela PSC para proporcionar confiança nos serviços de confiança.

5. A fim de fornecer uma base para a decisão de confirmar que o PSC e seus serviços fiduciários que estão sendo auditados atendem aos critérios de auditoria definidos, os auditores devem produzir relatórios claros que forneçam informações suficientes para tomar essa decisão.

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

7. O relatório deve ser distribuído, da seguinte forma, às seguintes entidades, em até 10 (dez) dias úteis após a conclusão da fase 2:

   *a)* Um (1) exemplar para a Entidade Auditada; e

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

8. Nas auditorias de PSC que fornecem certificados publicamente confiáveis, o organismo de certificação deve emitir, também, relatório no formato definido nos seguintes documentos, a depender do esquema de acreditação do organismo de certificação e do 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.

10. O RFA será analisado pela autoridade credenciadora, juntamente com os demais documentos referenciados no Regulamento dos Requisitos para Prestadores Qualificados de Serviços de Confiança, para a finalidade de atribuição/manutenção do estatuto de prestador qualificado de serviços de confiança da entidade auditada.

11. Os documentos utilizados como evidência da auditoria devem ser mantidos por 5 anos pelo organismo de avaliação de conformidade e serem apresentados à autoridade credenciadora, se solicitado.

Artigo 11.º

**Plano das ações de correção**

1. Havendo não conformidades apontadas no RFA, o PSC deve elaborar um Plano de Ações Corretivas, onde constem, para cada não conformidade, nos seguintes moldes:

   *a)* N.º 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 deve ser assinado por pelo menos um dos integrantes do Grupo de Gestão/Conselho

3. Executivo do PSC e deve ser enviado ao organismo de avaliação de conformidade e à ARME em até 10 dias úteis após o recebimento do RFA.

4. As Não Conformidades de Alto Impacto devem ser corrigidas em prazo acordado com o organismo de certificação, que avalia as ações corretivas e seus prazos e fornece informações ao PSC sobre as tarefas de avaliação adicionais necessárias para verificar se as não conformidades foram corrigidas.

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

   *a)* no prazo de 3 meses após a notificação ao PSC das não conformidades do relatório de auditoria; ou

   *b)* no prazo de 6 meses após a notificação ao PSC das não conformidades do relatório de auditoria, quando se demonstre que a complexidade da ação corretiva requer um longo período.

6. O PSC deve fornecer ao organismo de certificação os documentos necessários para avaliar a complexidade da ação corretiva referida no número 5.

CAPÍTULO III

**Disposições Finais**

Artigo 12.º

**Entrada em vigor**

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

**ANEXO**

**A Tabela estabelece a relação entre os serviços de confiança com os padrões a serem utilizadas pelos organismos de certificação para realizar a avaliação de conformidade.**

| Serviço de confiança definido no | Padrões para avaliação de |
|---|---|

| Decreto-Lei 23/2023 | conformidade |
|---|---|
| Fornecimento de certificados qualificados de assinaturas eletrónicas (Art.º 53º) | ISO/IEC 17021-1<br>ISO/IEC 17065<br>ETSI EN 319 403-1<br>ETSI EN 319 403-3<br>OU<br>WebTrust for CA<br>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<br>ISO/IEC 17065<br>ETSI EN 319 403-1<br>ETSI EN 319 403-2<br>ETSI EN 319 403-3<br>OU<br>WebTrust for CA<br>WebTrust Network Security<br>WebTrust SSL<br>WebTrust SSL EV |
| Fornecimento de selos temporais qualificados (Art.º 69º) | ISO/IEC 17021-1<br>ISO/IEC 17065<br>ETSI EN 319 403-1<br>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) | |