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