ANEXO III

REGULAMENTO DOS REQUISITOS MÍNIMOS DE SEGURANÇA FÍSICA DE INSTALAÇÕES DE PRESTADORES QUALIFICADOS DE SERVIÇOS 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 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 as regras de técnicas e de segurança aplicáveis ao exercício da atividade de prestação de serviço de confiança, e do artigo 99.º, do Decreto-Lei n.º 27/2023, de 20 de outubro.

A Autoridade Credenciadora, ao abrigo do artigo 83.º, do Decreto-lei n.º 27/2023, de 20 de outubro tem a competência de credenciar os prestadores qualificados de serviços de confiança; controlar os prestadores de serviços de confiança; supervisionar os prestadores qualificados de serviços de confiança estabelecidos no território nacional por forma a

garantir, por meio de atividades de supervisão a priori e a posteriori, que os prestadores e os serviços de confiança qualificados por eles prestados cumprem os requisitos estabelecidos naquele diploma legal; e atribuir e retirar o estatuto de qualificado aos prestadores de serviços de confiança e aos serviços por eles prestados.

Assim, no âmbito do quadro regulatório de referência previsto no Decreto-lei n.º 27/2023, de 20 de outubro, cabe à Autoridade Credenciadora definir quais os requisitos a serem cumpridos pelos prestadores qualificados de serviços de confiança, especialmente as entidades certificadoras, bem como estabelecer o procedimento da sua credenciação.

De entre os requisitos a serem atendidos pelas unidades de registo que executam operações para os prestadores qualificados de serviços de confiança, encontram-se os de segurança física de ambiente.

Portanto, o Regulamento de Segurança Física de Instalações de prestadores de serviços de confiança tem como objeto a definição dos requisitos de segurança física aplicáveis aos prestadores qualificados de serviços de confiança da Infraestrutura de Chaves Públicas de Cabo Verde; e a apresentação dos requisitos e controlos essenciais para garantir a segurança física de uma entidade certificadora, visando a proteção contra potenciais riscos e ameaças que podem comprometer a sua integridade e operações, de acordo com o Decreto-lei n.º 27/2023, de 20 de outubro, e das seguintes normas de referência internacional no respeitante à atividade de certificação digital, WEBTRUST FOR CA; ETSI EN 319 401; ETSI EN 319 411-1; ETSI EN 319 411-2; ISO/IEC 27001; ISO/IEC 27002.

CAPÍTULO I

Disposições Gerais

Artigo 1.º

Objeto

O presente regulamento:

a) define os requisitos de segurança física aplicáveis aos prestadores qualificados de serviços de confiança da ICP-CV;

b) apresenta os requisitos e controlos essenciais para garantir a segurança física de uma entidade certificadora, visando a proteção contra potenciais riscos e ameaças que podem comprometer a sua integridade e operações.

Artigo 2.º

Âmbito

O presente regulamento aplica-se a prestadores de serviços de confiança para obtenção e renovação do estatuto de prestador qualificado dos serviços definidos 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 tem 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, às áreas ou à realização de ações críticas, garantindo uma camada extra de proteção, de forma a garantir que uma pessoa com acesso autorizado só consiga aceder se outra pessoa também o aprovar.

Artigo 4.º

Siglas e definições

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.

Artigo 5.º

Requisitos das Instalações relacionadas com a criação e gestão de certificados

1. A entrada no edifício apenas deve ser realizada através de pontos de acesso limitados e controlados.
2. Devem ser criados perímetros de segurança ao redor das instalações relacionadas com a criação e gestão de certificados.
3. As instalações relacionadas com a criação e gestão de certificados devem estar numa instalação fisicamente segura, com pelo menos 4 níveis de segurança para aceder os ativos, sistemas e informação sensíveis, conforme o anexo, parte integrante deste regulamento.
4. Os sistemas devem estar separados fisicamente de outros sistemas, mesmo que sejam da mesma organização, a fim de garantir que apenas o pessoal autorizado tem o devido acesso.
5. O processo deve ser realizado em um ambiente capaz de proteger fisicamente os sistemas e dados envolvidos de riscos associados a acessos não autorizados.
6. No caso de instalações partilhadas com outras organizações, as mesmas devem estar fora do perímetro relacionado com a criação e gestão de certificados.
7. As funções relacionadas com as operações podem ser suportadas dentro da mesma área, desde que o acesso seja limitado ao pessoal autorizado para o efeito.

8. As chaves de acesso devem ser mantidas separadas fisicamente, de forma que apenas o pessoal de confiança e com acesso autorizado obtenha o respetivo acesso.

9. Todos os colaboradores devem usar uma identificação visível.

Artigo 6.º

Controlos de segurança para visitantes

1. Todas as entradas físicas devem ser alvo de controlo e supervisão, para restringir apenas ao pessoal autorizado o acesso ao edifício ou instalações operacionais da entidade certificadora.

2. Todos os visitantes devem ser acompanhados por pessoal autorizado para o efeito, enquanto estiverem no edifício e nas instalações operacionais da entidade certificadora e ter a sua data de entrada e de saída registados.

3. Os fornecedores, uma vez autorizados, devem ter acesso às instalações operacionais da entidade certificadora, apenas quando 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 desde o chão real até o teto real;

   b) Porta corta-fogo nos perímetros de segurança;

   c) O acesso às instalações operacionais da entidade certificadora deve ser restrito a pessoas autorizadas e protegido através da utilização de controlos de autenticação multi-fator;

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

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

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

   a) Sistema de deteção de inundação;

   b) Sistema de proteção contra descargas atmosféricas;

   c) Sistema de proteção contra emissão de radiação eletromagnética;

   d) Sistema de climatização HVAC, suportado por gerador e capaz de fazer o controlo da temperatura, humidade e com capacidade para alarmística;

   e) Sistema que realize a deteção e extinção automática de incêndios.

3. Proteção contra falhas de serviços públicos de apoio:

   a) Energia: através de implementação de sistemas de UPS;

   b) Implementação de uma fonte de energia alternativa (gerador) que permita o abastecimento contínuo de energia as instalações e sistemas críticos em situações de falha de energia;

   c) Telecomunicações: através de serviço de acesso à Internet com redundância ao nível de equipamentos e 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 alarme quando desocupadas;

   c) Sistema de alarmística na porta, e janela quando aplicável, para monitorização, caso a mesma seja deixada aberta;

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

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

Artigo 8.º

Controlos para segurança de equipamentos

1. Devem ser implementados controlos para proteger os equipamentos e informações relacionados com o serviço, caso os mesmos sejam levados para fora 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 reduzir os riscos associados a ameaças ambientais e de acesso não autorizado.

4. Os equipamentos devem estar protegidos contra falhas de energia e outras anomalias elétricas, como por UPS 's e geradores.

5. A cablagem de energia elétrica e 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 passar por 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 informação sensível por parte de pessoas não autorizadas.

Artigo 9.º

Controlos gerais

1. As informações comerciais, sensíveis ou críticas devem ser guardadas à chave quando não estiverem a ser utilizadas e quando as instalações da prestadora de serviços de confiança estiverem 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 (p.e: política de ecrã limpo);

3. Qualquer movimentação de materiais e equipamentos de e 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

ANEXO

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

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.
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.
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.