ANEXO V

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

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.

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 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 pelos prestadores qualificados de serviços de confiança, encontram-se os de segurança física.

Portanto, o Regulamento de Segurança Física de Instalações de unidades de registo tem como objeto a definição define os requisitos de segurança física aplicáveis aos prestadores qualificados de serviços de confiança da Infraestrutura de Chaves Públicas de Cabo Verde; e apresenta os requisitos e controlos essenciais para garantir a segurança física de uma unidade de registo, 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.

Artigo 1.º

Objeto

O presente documento:

a) define os requisitos de segurança física aplicáveis aos prestadores qualificados de serviços de confiança da Infraestrutura de Chaves Públicas de Cabo Verde; e

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

Artigo 2.º

Âmbito

A presente norma aplica-se aos prestadores de serviços de confiança que desejam obter ou renovar o estatuto de prestador qualificado de um ou mais serviços definidos no Decreto-lei n.º 27/2023, de 20 de outubro, especialmente às unidades de registo.

Artigo 3.º

Objetivos

1. A segurança física é a primeira linha de defesa contra ameaças externas e internas, e representa uma camada de proteção importante para a salvaguarda de ativos, como equipamentos, infraestrutura e dados.

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

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

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

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

3. O fator referido na alínea *a)*, do úmero anterior, requer, pelo menos, duas autorizações necessárias para permitir o acesso a informações, às áreas ou à realização de ações críticas, garantindo uma camada extra de proteção, de forma a assegurar que mesmo que uma pessoa com acesso autorizado tente atuar, o acesso não será concedido a menos que outra pessoa também o aprove.

Artigo 4.º

Siglas

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) PQSC: Prestador Qualificado de Serviços de Confiança

h) PSC: Prestador de Serviços de Confiança

i) UPS: Uninterruptible Power Supply

j) UR: Unidade de Registo

Artigo 5.º

Controlos de segurança física para instalações da unidade de registo

1. A entrada no edifício ou no sítio onde são realizadas as operações da unidade de registo apenas deve ser realizada através de pontos de acesso limitados e controlados.

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

3. Devem ser consideradas portas corta-fogo nos perímetros de segurança ao redor das instalações operacionais da unidade de registo, bem como a existência de alarmes considerando o cumprimento da conformidade com a legislação e regulamentação aplicável.

4. Sistemas de deteção de intrusões implementados em todas as portas externas das instalações operacionais da unidade de registo, que devem ser testadas regularmente.

5. As instalações operacionais da unidade de registo devem estar fisicamente trancadas e protegidas com alarme quando desocupadas.

6. Devem existir barreiras físicas robustas com paredes sólidas desde o chão real até o 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 evitar roubos, danos acidentais ou acesso não autorizado a informação (por forma a preservar a confidencialidade, integridade e disponibilidade da informação).

8. Deve ser instalado um sistema que realize a deteção e extinção automática de incêndios, controlo da humidade e temperatura, bem como um sistema de deteção de inundação, aplicável em particular às salas de arquivo.
9. Todos os colaboradores devem usar 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 multi-fator.
11. Todas as entradas e saídas das instalações operacionais da unidade de registo devem ser registadas:

    a) O registo deve ser auditável;

    b) Um sistema de controlo de acesso que permita a identificação do colaborador é suficiente para o pessoal com acesso permanente.
12. As entradas e saídas das instalações da unidade de registo devem ser monitorizadas através de sistema de videovigilância com câmaras.
13. Os visitantes devem ser acompanhados durante o acesso ao edifício ou 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 necessário.
15. O acesso deve ser 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 reduzir os riscos associados a ameaças ambientais e de acesso não autorizado.
2. Os equipamentos devem estar protegidos contra falhas de energia e outras anomalias elétricas (p.e: UPS e Gerador).
3. A cablagem de energia elétrica e 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 passar por um processo de manutenção de acordo com as instruções do fabricante.

5. 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. O método usado para destruir a 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 à chave quando não estiverem a ser utilizadas e quando as instalações da autoridade de registo estiverem desocupadas, através da implementação de 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, através da implementação de uma política de ecrã limpo;
3. Qualquer movimentação de materiais e equipamentos de e 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 à data da sua publicação