AGÊNCIA REGULADORA MULTISSETORIAL DA ECONOMIA - ARME
Conselho de Administração

Deliberação n.º 23/CA/2025

Sumário: Aprovando o regulamento que estabelece as condições de elegibilidade de prestadores de serviços de confiança, para obterem e manterem o estatuto de qualificados, no âmbito do Decreto-Lei n.º 27/2023, de 20 de outubro.

De 26 de fevereiro de 2025

Preâmbulo

A Agência Reguladora Multissetorial 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, constitui-se como uma autoridade administrativa independente, de base institucional, dotada de competências reguladoras, incluindo a regulamentação, supervisão e sancionamento de infrações. A sua finalidade principal consiste na regulação técnica e económica dos setores das comunicações eletrónicas, energia, água e transportes coletivos urbanos e interurbanos de passageiros, conforme estabelecido no n.º 1 do artigo 2.º do referido diploma legal.

No âmbito das suas atribuições, a ARME assume, entre outras, a competência de supervisionar as entidades de certificação, nos termos da alínea f) do artigo 15.º do Decreto-Lei n.º 50/2018, de 20 de setembro. Esta competência é particularmente relevante no contexto da regulação do setor das comunicações eletrónicas, onde a segurança e a confiança nas transações eletrónicas assumem um papel central.

O Decreto-Lei n.º 27/2023, de 20 de outubro, que estabelece as normas aplicáveis aos serviços de confiança, nomeadamente no que diz respeito às transações eletrónicas, veio instituir um quadro legal abrangente para a regulação de diversas modalidades de serviços de confiança, tais como assinaturas eletrónicas, selos eletrónicos, selos temporais, documentos eletrónicos, serviços de certificados para autenticação de sítios *web*, arquivo eletrónico, certificados eletrónicos de atributos, gestão de dispositivos de criação de assinaturas e selos eletrónicos à distância, e livros-razão eletrónicos. No artigo 82.º deste diploma, atribui-se à ARME, enquanto Entidade Reguladora do Setor das Comunicações Eletrónicas, as funções de autoridade credenciadora no âmbito dos serviços de confiança.

Para a prossecução destas atribuições, 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, nos termos do artigo 99.º do Decreto-Lei n.º 27/2023, de 20 de outubro. Estas regras visam assegurar que os prestadores de serviços de confiança cumpram os requisitos legais e técnicos necessários para a atribuição e manutenção do estatuto de prestador qualificado, garantindo assim a confiança e a segurança dos serviços prestados no âmbito da

A2025/S2/BO53/13505
Deliberação n.º 23/CA/2025

Infraestrutura de Chaves Públicas de Cabo Verde (ICP-CV).

O presente regulamento define as condições de elegibilidade para que os prestadores de serviços de confiança possam obter e manter o estatuto de prestador qualificado, em conformidade com o disposto no Decreto-Lei n.º 27/2023, de 20 de outubro. Para tal, estabelece-se um conjunto de requisitos técnicos, organizacionais e de segurança que os prestadores devem cumprir, alinhados com as normas internacionais de referência aplicáveis, nomeadamente as normas ETSI, ISO/IEC, IETF RFC, entre outras.

A atribuição do estatuto de prestador qualificado de serviços de confiança pressupõe a verificação do cumprimento dos requisitos legais previstos no artigo 26.º do Decreto-Lei n.º 27/2023, de 20 de outubro, e a realização de auditorias de conformidade por organismos credenciados. Este estatuto tem uma duração de três anos, podendo ser renovado por igual período, desde que se mantenham as condições que justificaram a sua atribuição inicial.

O presente regulamento visa, assim, estabelecer um quadro normativo claro e rigoroso para a credenciação e supervisão dos prestadores de serviços de confiança, garantindo a qualidade, a segurança e a confiança dos serviços prestados no âmbito da ICP-CV, em conformidade com as melhores práticas internacionais e com a legislação aplicável.

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, estabelece as condições de elegibilidade de prestadores de serviços de confiança, para obterem e manterem o estatuto de qualificados, no âmbito do Decreto-Lei n.º 27/2023 de 20 de outubro.

Artigo 1.º

Aprovação

É aprovado o regulamento que estabelece as condições de elegibilidade de prestadores de serviços de confiança, para obterem e manterem o estatuto de qualificados, no âmbito do Decreto-Lei n.º 27/2023 de 20 de outubro.

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, O Presidente, *Leonilde Santos*, os Administradores, *João Tomar* e *Carlos Ramos*.

A2025/S2/BO53/13505
Deliberação n.º 23/CA/2025

REGULAMENTO DOS REQUISITOS PARA PRESTADORES QUALIFICADOS DE SERVIÇOS DE CONFIANÇA

Artigo 1.º

Objeto

O presente regulamento estabelece as condições de elegibilidade aplicáveis aos prestadores de serviços de confiança, nos termos do disposto no Decreto-Lei n.º 27/2023, de 20 de outubro, para a obtenção e manutenção do estatuto de prestador de serviços de confiança qualificado.

Artigo 2.º

Âmbito

O presente regulamento aplica-se aos prestadores de serviços de confiança que pretendam obter ou renovar o estatuto de prestador qualificado para um ou mais serviços de confiança, nos termos definidos no Decreto-Lei n.º 27/2023, de 20 de outubro.

Artigo 3.º

Siglas

1. No presente regulamento são utilizadas as seguintes siglas:

a) ARME: Agência Reguladora Multissetorial da Economia;

b) ETSI: European Telecommunications Standards Institute;

c) FIPS PUB: Federal Information Processing Standard Publications;

d) HSM: Hardware Security Module;

e) ISO/IEC: International Organization for Standardization / International Electrotechnical Commission;

f) QSCD: Dispositivos Qualificados de Criação de Assinaturas/Selos Eletrônicos;

g) RFC: Request for Comments.

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

a) "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;

A2025/S2/BO53/13505
Deliberação n.º 23/CA/2025

b) "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;

c) "Serviço de confiança", um serviço eletrónico geralmente prestado mediante pagamento, nos termos do Decreto-Lei n.º 27/2023, de 20 de outubro;

Artigo 3.º

Requisitos para prestadores qualificados de serviços de confiança

1. Os prestadores de serviços de confiança que pretendam fornecer serviços qualificados devem proceder à sua credenciação junto da autoridade credenciadora.

2. Para efeitos de credenciação, os prestadores de serviços de confiança devem preencher o formulário de Pedido de Credenciação de Prestador Qualificado de Serviços de Confiança, disponível no sítio eletrónico da autoridade credenciadora, e apresentar a documentação e os comprovativos exigidos nos termos do Decreto-Lei n.º 27/2023, de 20 de outubro.

3. Para obter o estatuto de prestador de serviços de confiança qualificado, os prestadores devem assegurar que as suas instalações, procedimentos, competências do pessoal, equipamentos e sistemas cumprem as normas de segurança aplicáveis ao exercício da sua atividade, observando os seguintes requisitos:

a) Estabelecer ou adaptar a sua atividade operacional de acordo com os requisitos definidos no Decreto-Lei n.º 27/2023, de 20 de outubro, e nos documentos constantes da tabela que integra o anexo ao presente regulamento, do qual faz parte integrante;

b) Elaborar uma Declaração de Práticas para cada tipo de serviço prestado, com o objetivo de informar os utilizadores e terceiras partes sobre a organização e execução das atividades do prestador, bem como sobre as características dos serviços de confiança prestados;

c) No caso de prestadores de serviços de confiança que emitam certificados digitais qualificados, elaborar uma Declaração de Práticas de Certificação e uma Política de Certificação, em conformidade com as normas e requisitos aplicáveis:

i. A Declaração de Práticas de Certificação deve observar obrigatoriamente a estrutura definida na IETF RFC 3647, descrevendo os processos que o prestador de serviços utilizará na criação e manutenção dos certificados.

ii. A Política de Certificação deve indicar os tipos de certificados emitidos pelo prestador, em conformidade com a norma ETSI 319 411-2, e descrever cada tipo em termos de qualidade.

A2025/S2/BO53/13505
Deliberação n.º 23/CA/2025

iii. A Política de Certificação pode constituir um documento autónomo ou integrar a Declaração de Práticas de Certificação.

iv. Os documentos referidos substituem a Declaração de Práticas no que diz respeito ao fornecimento de certificados digitais.

v. Caso o prestador ofereça outros serviços além da emissão de certificados digitais, deve elaborar uma Declaração de Práticas para cada um dos demais serviços prestados.

d) Elaborar o Plano de Segurança, nos termos previstos no artigo 25.º do Decreto-Lei n.º 27/2023, de 20 de outubro, em conformidade com as disposições da norma ISO/IEC 27001 e com os requisitos estabelecidos no artigo 6.º do presente regulamento;

e) Efetuar uma Avaliação de Riscos, de acordo com as disposições do documento ETSI EN 319 401 e da norma ISO/IEC 27005, a qual deve ser submetida ao órgão executivo do prestador de serviços para conhecimento e aprovação;

f) Elaborar e manter um Inventário de todos os ativos de informação, atribuindo uma classificação que seja consistente com a avaliação de riscos realizada, em conformidade com as disposições da norma ISO/IEC 27002. O inventário deve ser atualizado sempre que ocorram alterações nos ativos e revisto, no mínimo, anualmente;

g) Elaborar um Plano de Contingência, que inclua, no mínimo, os requisitos estabelecidos no artigo 7.º do presente regulamento;

h) Elaborar uma Política de Pessoal, responsável pelas funções de gestão dos serviços de confiança, que contenha, no mínimo, os requisitos descritos no artigo 8.º;

i) Elaborar um Plano de Cessação de Atividades que contenha, no mínimo, os requisitos descritos no artigo 9.º.

j) Utilizar sistemas e dispositivos fiáveis, de acordo com o disposto no artigo 10.º.

k) Desenvolver a atividade em instalações físicas adequadas, em conformidade com os requisitos definidos no Regulamento de Segurança Física de Instalações de Prestadores Qualificados de Serviços de Confiança.

l) No caso de prestadores de serviços que emitam certificados digitais, as respetivas atividades de registo devem ser executadas em ambiente físico.

m) Contratar os serviços de um Organismo de Avaliação de Conformidade credenciado pela autoridade credenciadora, para realização de auditoria pré-operacional, para fins de obtenção do estatuto de Prestador Qualificado de Serviços de Confiança, e auditoria operacional anual, para

A2025/S2/BO53/13505
Deliberação n.º 23/CA/2025

fins de manutenção do estatuto de qualificado, conforme definido no Regulamento de Avaliação de Conformidade.

Artigo 4.º

Pedido de credenciação

1.O candidato a prestador qualificado de serviços de confiança, para iniciar o processo de credenciação inicial, deve submeter à Agência Reguladora Multissetorial da Economia (ARME) os seguintes documentos:

a) Pedido de Credenciação de Prestador Qualificado de Serviços de Confiança, devidamente preenchido;

b) Estatutos da pessoa coletiva e, no caso de sociedades, contrato de sociedade;

c) Relação de todos os sócios, com especificação das respetivas participações, bem como dos membros dos órgãos de administração e de fiscalização. No caso de sociedades anónimas, deve ser apresentada a relação de todos os acionistas com participações significativas, diretas ou indiretas;

d) Declarações subscritas por todas as pessoas singulares e coletivas envolvidas, atestando que não se encontram em nenhuma das situações indiciadoras de falta de idoneidade;

e) Prova do substrato patrimonial e dos meios financeiros disponíveis, designadamente a realização integral do capital social;

f) Descrição da organização interna e Plano de Segurança, em conformidade com os requisitos estabelecidos no presente regulamento;

g) Demonstração dos meios técnicos e humanos exigidos pela autoridade credenciadora, incluindo certificados de conformidade dos produtos de serviços de confiança emitidos por organismos de certificação;

h) Programa geral da atividade prevista para os primeiros três anos de operação;

i) Descrição geral das atividades exercidas nos últimos três anos ou, no caso de entidades constituídas há menos tempo, desde a sua constituição, acompanhada do balanço e contas dos exercícios correspondentes;

j) Comprovação de contrato de seguro válido, que cubra adequadamente a responsabilidade civil decorrente da atividade de certificação;

k) Documentos técnicos referidos no n.º 3 do artigo 3.º do presente regulamento;

A2025/S2/BO53/13505
Deliberação n.º 23/CA/2025

l) Relatório da auditoria pré-operacional, que contemple a avaliação de conformidade de todos os serviços para os quais seja solicitado o estatuto de qualificado.

2. Os documentos apresentados são analisados pela autoridade credenciadora, que decide sobre a aceitação ou recusa do pedido de atribuição do estatuto de prestador qualificado de serviços de confiança.

3. O estatuto de prestador qualificado de serviços de confiança é válido por um período de três anos, podendo ser renovado por períodos de igual duração.

Artigo 5.º

Renovação da credenciação

1. A estrutura para os prestadores qualificados de serviços de confiança, que deve ser encaminhar à autoridade credenciadora para os prestadores de prestadores para os prestadores qualificados de serviços de confiança:

a) Pedido de Renovação de Credenciação de Prestador Qualificado de Serviços de Confiança, devidamente preenchido, de acordo com o formulário disponível no sítio da Internet da autoridade credenciadora;

b) Atualização dos documentos referidos no n.º 1 do artigo 4.º do presente regulamento;

c) Atualização dos documentos técnicos definidos no n.º 3 do artigo 3.º do presente regulamento;

d) Relatório de auditoria operacional, que inclua a última avaliação de conformidade de todos os serviços para os quais seja solicitada a renovação do estatuto de qualificado.

2. Os documentos apresentados são analisados pelos órgãos competentes da autoridade credenciadora, podendo o pedido de renovação do estatuto de prestador qualificado de serviços de confiança ser aceite ou recusado.

Artigo 6.º

Plano de segurança

1. O prestador qualificado de serviços de confiança deve elaborar um Plano de Segurança que inclua, no mínimo, as seguintes informações:

a) Descrição da estrutura organizacional e funcional, bem como da atividade de serviços de confiança prestada;

b) Especificação dos processos de avaliação e garantia da idoneidade e capacidade técnica do

A2025/S2/BO53/13505
Deliberação n.º 23/CA/2025

pessoal em funções;

c) Especificação dos requisitos de segurança física, lógica e operacional;

d) Requisitos de disponibilidade da informação, incluindo redundância de sistemas e planos de contingência;

e) Requisitos de proteção da informação, com distinção dos níveis de segurança e dos perfis de acesso implementados;

f) Definição das funções que conferem acesso aos atos e instrumentos dos serviços de confiança, respetivos requisitos de segurança e perfis de acesso;

g) Descrição dos produtos de assinatura eletrónica utilizados, com identificação das respetivas certificações de conformidade, quando aplicável;

h) Descrição e avaliação de outros riscos de segurança;

i) Indicação dos responsáveis pela implementação do Plano de Segurança;

j) Indicação do processo de revisão periódica estabelecido.

3. A equipa que atua diretamente nos serviços de confiança deve ser formalmente informada sobre a existência e o conteúdo do Plano de Segurança.

Artigo 7.º

Plano de contingência

1. O prestador qualificado de serviços de confiança deve dispor de procedimentos que permitam assegurar a continuidade dos serviços em sistemas de recuperação alternativos, de modo a fazer face à eventual ocorrência de desastres ou incidentes que possam comprometer o funcionamento normal dos serviços prestados. Estes procedimentos devem garantir que a migração dos sistemas primários para os sistemas de recuperação não coloque em risco a segurança dos sistemas.

2. No caso do prestador de serviços de emissão de certificados e selos digitais, deve ser garantida a disponibilidade permanente dos serviços de distribuição, revogação e consulta do estado de revogação de certificados, mesmo em situações de incidentes.

3. O prestador qualificado de serviços de confiança deve implementar um Plano de contingência que inclua, no mínimo:

a) A possibilidade de adulteração ou acesso não autorizado às chaves privadas, próprias ou de terceiros sob sua custódia, quando aplicável;

A2025/S2/BO53/13505
Deliberação n.º 23/CA/2025

b) A invasão dos seus sistemas e da rede interna;

c) Incidentes de segurança física e lógica;

d) A indisponibilidade da infraestrutura;

e) Fraudes ocorridas no registo do utilizador, na emissão, expedição, distribuição, revogação e gestão de certificados, no caso de se tratar de um prestador qualificado de serviços de confiança que emita certificados digitais.

4. O Plano de contingência deve incluir os seguintes procedimentos:

a) Retoma das operações num prazo que minimize o impacto para os utilizadores;

b) Notificação aos requerentes, titulares, destinatários e demais entidades com as quais existam acordos, sobre qualquer ocorrência que comprometa a utilização segura dos serviços prestados;

c) Notificação às autoridades competentes, sempre que aplicável;

d) Revogação dos certificados afetados, sempre que necessário;

e) Procedimentos para a interrupção ou suspensão de serviços e para a investigação do incidente;

f) Análise e monitorização dos registos de auditoria;

g) Gestão do relacionamento com o público e com os meios de comunicação social, sempre que aplicável.

5. Todos os intervenientes no Plano de contingência devem receber formação específica para lidar com incidentes.

6. O plano deve ser atualizado e testado, no mínimo, uma vez por ano, bem como sempre que o prestador identifique alterações no seu ambiente ou sistema que possam gerar riscos para a segurança da informação.

Artigo 8.º

Política de pessoal

1. O prestador qualificado de serviços de confiança deve adotar as seguintes regras de seleção e contratação de funcionários, de modo a reforçar e respeitar as disposições de segurança exigidas para o exercício da sua atividade:

a) Para funções de gestão da infraestrutura que suporta os serviços de confiança, deve empregar pessoal especializado, com conhecimentos específicos em assinatura eletrónica, certificação

A2025/S2/BO53/13505
Deliberação n.º 23/CA/2025

digital e outras tecnologias relevantes para os serviços prestados, bem como em segurança da informação e proteção de dados pessoais;

b) Todo o pessoal que desempenha funções relacionadas com os processos que suportam os serviços de confiança deve estar livre de conflitos de interesse que possam comprometer a sua imparcialidade;

c) As funções relacionadas com os processos que suportam os serviços de confiança não podem ser desempenhadas por pessoas que se encontrem em situação indicadora de falta de idoneidade;

d) No âmbito da sua estrutura organizativa, deve contemplar, pelo menos, os seguintes cargos e funções necessários à operação dos sistemas que suportam os serviços de confiança:

i. Administrador de sistemas: responsável pela instalação, configuração e manutenção dos sistemas, com acesso controlado às configurações relacionadas com a segurança;

ii. Operador de sistemas: encarregado da operação diária dos sistemas, com autorização para realizar cópias de segurança e reposição de informação;

iii. Administrador de segurança: responsável pela gestão e implementação das regras e práticas de segurança;

iv. Auditor de sistemas: autorizado a monitorizar os registos de atividade dos sistemas;

v. Administrador de registo: responsável pela aprovação da emissão, suspensão e revogação de certificados, no caso de o prestador qualificado de serviços de confiança emitir certificados e selos digitais.

2. Os postos de trabalho ou funções, referidos nas subalíneas *i)*, *iii)* e *iv)* da alínea *d)* do número anterior não podem ser desempenhados pela mesma pessoa.

Artigo 9.º

Plano de cessação de atividades

1. O prestador qualificado de serviços de confiança deve dispor de um Plano de Cessação de Atividades atualizado, no qual conste que, antes de terminar os seus serviços, adotará as seguintes medidas:

a) Informará do término da sua atividade todos os assinantes e demais entidades com as quais mantém acordos ou outras formas de relações estabelecidas, incluindo as partes confiantes, outros prestadores de serviços de confiança e as autoridades competentes, designadamente os órgãos de supervisão;

A2025/S2/BO53/13505
Deliberação n.º 23/CA/2025

b) Revogará a autorização de todos os subcontratantes para atuar em nome do prestador na execução de quaisquer funções relacionadas com o processo de emissão de *tokens* de serviço de confiança;

c) Transferirá as obrigações para uma entidade confiável, de modo a garantir a manutenção de todas as informações necessárias para comprovar a operação do prestador por um período razoável, exceto se for demonstrado que o prestador não possui tais informações;

d) Destruirá ou retirará de uso as suas chaves privadas, incluindo cópias de *backup*, de forma a impossibilitar a sua recuperação;

e) Tomará as providências necessárias para transferir a prestação dos serviços de confiança aos seus clientes existentes para outro prestador qualificado.

2. O prestador qualificado de serviços de confiança deve celebrar um acordo que garanta a cobertura dos custos associados ao cumprimento dos requisitos mínimos previstos no número anterior, em caso de falência ou de impossibilidade de suportar esses custos por meios próprios, dentro dos limites estabelecidos pela legislação aplicável em matéria de insolvência.

3. O prestador qualificado de serviços de confiança deve declarar nas suas práticas as disposições adotadas para a cessação da sua atividade.

4. O prestador qualificado de serviços de confiança mantém ou transfere para uma entidade confiável as suas obrigações de disponibilizar a sua chave pública ou os seus *tokens* de serviço de confiança às partes interessadas, por um período razoável.

Artigo 10.º

Dispositivos e sistemas fiáveis

1. O prestador qualificado de serviços de confiança deve utilizar sistemas e dispositivos fiáveis para a realização das suas operações, com as seguintes características:

a) Os Dispositivos Seguros de Hardware (HSM) utilizados para operações que envolvem chaves criptográficas devem preencher os seguintes critérios:

i. Ter garantia de EAL 4 ou superior, de acordo com a norma ISO/IEC 15408, ou critérios de avaliação equivalentes reconhecidos a nível nacional ou internacional para a segurança das tecnologias de informação, desde que correspondam a um alvo de segurança ou perfil de proteção que cumpra os requisitos dos documentos aplicáveis ao serviço prestado, com base numa análise de risco e considerando medidas de segurança físicas e outras medidas de segurança não técnicas; ou

A2025/S2/BO53/13505
Deliberação n.º 23/CA/2025

ii. Cumprir os requisitos identificados na ISO/IEC 19790 ou FIPS PUB 140-2 nível 3 ou FIPS PUB 140-3 nível 3.

b) Os dispositivos criptográficos seguros devem ser operados na sua configuração, conforme descrito na documentação de orientação de certificação apropriada, ou numa configuração equivalente que atinja o mesmo objetivo de segurança.

c) Os Dispositivos Qualificados de Criação de Assinaturas/Selos Eletrónicos (QSCD), fornecidos pelo prestador aos titulares, no âmbito dos serviços de emissão de certificados digitais, quando aplicável.

d) Os algoritmos e parâmetros criptográficos utilizados nas diferentes operações e serviços executados pelo prestador qualificado de serviços de confiança devem refletir, com especial atenção, a durabilidade dos esquemas de assinatura relativamente à sua resistência a ataques, uma vez que isso afeta diretamente o período de validade que se pretende atribuir aos certificados e assinaturas criados.

e) Para tal, devem ser utilizadas as recomendações do Capítulo 8 do documento ETSI TS 119 312, considerando sempre a sua versão mais recente.

f) Os sistemas utilizados na execução dos processos críticos devem ser fiáveis e cumprir, no mínimo, os requisitos 7.4-04 a 7.4-10 do documento ETSI EN 319 401.

2. Os requisitos para os sistemas fiáveis podem ser garantidos através da utilização, por exemplo, de sistemas em conformidade com o CEN TS 419 261, o CEN EN 419 241-1 ou com um perfil de proteção adequado (ou perfis), definido de acordo com a norma ISO/IEC 15408.

Artigo 11.º

Entrada em vigor

O presente regulamento 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, O Presidente, *Leonilde Santos*, os Administradores, *João Tomar* e *Carlos Ramos*.

A2025/S2/BO53/13505
Deliberação n.º 23/CA/2025