arme
Agência
Reguladora
Multissectorial da Economia

CONSELHO DE ADMINISTRAÇÃO

DELIBERAÇÃO N.º 05/CA/2025

de 24 de janeiro

Aprovação da versão 2.0 da Declaração de Práticas de Certificação da Entidade de Certificação Raiz de Cabo Verde (ECR-CV)

O Decreto-Lei n.º 44/2009, de 9 de novembro, cria a Infraestrutura de Chaves Públicas de Cabo Verde - ICPCV, destinada a estabelecer uma estrutura de confiança eletrónica, de forma que as entidades de certificação que lhe estão subordinadas disponibilizem serviços que garantam a realização de transações eletrónicas seguras; a autenticação forte; e as assinaturas eletrónicas de transações ou informações e documentos eletrónicos, assegurando a sua autoria, integridade, não repúdio e confidencialidade.

Considerando o 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; e regula a validade, eficácia e valor probatório dos documentos eletrónicos, o reconhecimento e aceitação, na ordem jurídica cabo-verdiana, dos meios de identificação eletrónica de pessoas singulares e coletivas e prevê as normas aplicáveis ao Sistema de Certificação Eletrónica.

Tendo em conta a Consulta Pública dos Projetos de Regulamentos referentes às Regras Técnicas e de Segurança aplicáveis ao exercício da atividade de prestação de serviços de confiança, aprovada pela Deliberação n.º 42/CA/2024, de 18 de dezembro, mencionadas na Declaração de Práticas de Certificação da Entidade de Certificação Raiz de Cabo Verde - ECR-CV – DPC - e que, uma vez aprovadas, serão devidamente consideradas para aplicação e conformidade.

Considerando a necessidade de atualização da Declaração de Práticas de Certificação da Entidade de Certificação Raiz de Cabo Verde – ECR-CV - DPC (versão 1.0), aprovada através da Deliberação n.º 02/2013 de 07 de fevereiro, do Conselho Gestor, que descreve as práticas e os procedimentos da ECR-CV, na execução dos seus serviços como Entidade de Certificação Raiz da ICP-CV.

Considerando que a Declaração de Práticas de Certificação da Entidade de Certificação Raiz de Cabo Verde – ECR-CV - DPC (versão 1.0) é atualizada com base nas atualizações dos documentos *Baseline Requirements* e *Extended Validation SSL* e *CodeSign Guidelines* do *WebTrust Principles and Criteria* e publicações do CA/Browser Forum, disponíveis no sítio https://cabforum.org.

Tel.: (+238) 260 44 00 / 01 / 02 / 03
Fax: (+238) 261 30 69
Endereço: Chã d'Areia, Praia | Cabo Verde

CP: nº 892
E-mail: info@arme.cv
Site: www.arme.cv

Tendo em conta que, conforme os "Procedimentos para Aprovação", definidos no número 10.3 da Declaração de Práticas de Certificação da Entidade de Certificação Raiz de Cabo Verde – ECR-CV - DPC (versão 1.0), aprovada através da Deliberação n.º 02/2013 de 07 de fevereiro, correções (ou atualizações) deverão ser publicadas sob a forma de novas versões desta DPC, substituindo qualquer DPC anteriormente definida.

Considerando que nos termos do n.º 2, do artigo 41.º, do Decreto-Lei n.º 27/2023, de 20 de outubro, a Declaração de Práticas de Certificação da Entidade de Certificação Raiz de Cabo Verde – ECR-CV - DPC deve obedecer a padrões internacionalmente reconhecidos sem prejuízo da sua conformidade com as disposições do referido diploma.

O Conselho de Administração da Agência Reguladora Multissectorial da Economia - ARME, enquanto Autoridade Credenciadora da ICP-CV, conforme estatuído no n.º 82.º do Decreto-Lei n.º 27/2023 de 20 de outubro, na sua reunião ordinária de 24 janeiro de 2025 e ao abrigo n.º 3, do artigo 41.º, do Decreto-Lei n.º 27/2023 de 20 de outubro, delibera o seguinte:

Artigo 1.º

Aprovação

É aprovada a versão 2.0 da Declaração de Práticas de Certificação da Entidade de Certificação Raiz de Cabo Verde ECR-CV, parte integrante da presente Deliberação.

Artigo 2.º

Entrada em vigor

A presente Deliberação entra em vigor no dia seguinte ao da sua aprovação.

Feita na Cidade da Praia, aos 24 de janeiro de 2025.

O Conselho de Administração,

/ Leonilde Santos /
Presidente

/ João Tomar /
Administrador

/ Carlos Ramos /
Administrador

ECR-CV
ENTIDADE DE CERTIFICAÇÃO RAIZ DE CABO VERDE

DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DA ENTIDADE DE CERTIFICAÇÃO RAIZ DE CABO VERDE (DPC DA ECR-CV)

Políticas

Identificação do documento: DPC DA ECR-CV

Identificação da CA: ECR-CV

Nível de Acesso: Público

Versão: 2.0

Data:

Próxima revisão:

Aprovado:

Conteúdo

1. Introdução

1.1. Visão Geral

1.1.1. O Governo de Cabo Verde, através do Decreto-Lei n.º 44/2009, de 09 de novembro, criou a Infraestrutura de Chaves Públicas de Cabo Verde (ICP-CV), destinada a estabelecer uma estrutura de confiança eletrónica, de forma que as Entidades de Certificação (EC), que lhe são subordinadas disponibilizem serviços que garantam:

a) A realização de transações eletrónicas seguras;
b) A autenticação forte;
c) Assinaturas eletrónicas de transações ou informações e documentos eletrónicos, assegurando a sua autoria, integridade, não repúdio e confidencialidade.

1.1.2. A estrutura hierárquica da ICP-CV compreende uma Entidade de Certificação Raiz, denominada Entidade de Certificação Raiz de Cabo Verde (ECR-CV) e demais entidades a ela subordinadas e que se encontram credenciadas pela Autoridade Credenciadora, nomeadamente Entidades de Certificação (EC's), Unidades de Registo vinculadas a estas e Prestadores de Serviço de Suporte.

1.1.3. Os certificados da ECR-CV ocupam o topo da cadeia hierárquica da ICP-CV e contêm as chaves públicas utilizadas para assinar os seus próprios certificados e suas Listas de Certificados Revogados - LCR, os certificados das EC's de nível imediatamente subsequente ao seu.

1.1.4. O presente documento é denominado de Declaração de Práticas de Certificação – DPC, descreve as práticas e os procedimentos ECR-CV, na execução dos seus serviços como Entidade de certificação Raiz da ICP-CV.

1.1.5. Esta DPC é atualizada com base nas atualizações dos documentos Baseline Requirements e Extended Validation SSL e CodeSign Guidelines do WebTrust Principles and Criteria e publicações do CA/Browser Forum, disponíveis no sítio https://cabforum.org.

1.1.5. Esta DPC foi elaborada com base na estrutura do documento Request for Comments (RFC) 3647.

1.2. Nome e Identificação do documento

1.2.1. O Nome de referência a este documento é "DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DA ICP-CV".

1.2.2. A identificação desta DPC, de acordo com seu Object Identifier (OID), é 2.16.132.1.3.1.1.

1.2.3. Esta DPC refere-se exclusivamente à Entidade de Certificação Raiz da ICP-CV.

INFORMAÇÃO DO DOCUMENTO				
Versão	**Estado**	**OID**	**Data de emissão**	**Validade**
2.0	Aprovado	2.16.132.1.3.1.1		Não Aplicável

localização	

1.3. Participantes da ICP-CV

A alínea *a)* do n.º 1, do artigo 2.º, do Decreto-Lei n.º 44/2009, de 09 de novembro, dispõe sobre a estrutura da ICP-CV.

1.3.1. Entidades de Certificação

1.3.1.1. Entidade de Certificação Raiz de Cabo Verde (ECR-CV): a ECR-CV presta serviços de certificação de topo da cadeia de certificação da ICP-CV, executa e zela pela aplicação das políticas de certificados e diretrizes aprovadas pelo CG. Neste contexto, ECR-CV possui os certificados de níveis mais altos na ICP-CV, que contêm as chaves públicas correspondentes às chaves privadas da Entidade de Certificação Raiz, que são utilizadas para assinar os seus próprios certificados, os certificados das EC´s de nível imediatamente subsequente ao seu e as suas Listas de Certificados Revogados (LCR).

1.3.1.2. Entidades de Certificação subordinadas à ECR-CV: entidade ou pessoa coletiva que presta serviço de confiança, designadamente cria ou fornece meios para a criação, verificação e validação de assinaturas e se encontra devidamente credenciada pela Autoridade Credenciadora.

1.3.2. Unidades registo

Entidades internas ou externas associadas a uma EC, que são responsáveis pela identificação e autenticação de requerentes de certificados de utilizador final e que, em representação da EC, iniciam ou transmitem pedidos de revogação de certificados e aprovam os pedidos de renovação de certificados. A ECR-CV, devido à sua natureza e atuação, não possui Unidade de Registo associada à sua atividade. A identificação e registo das EC´s de nível imediatamente subsequente ao da ECR-CV é realizada durante o seu processo de credenciação.

1.3.3. Titulares do certificado

1.3.3.1. Titulares do certificado da ECR-CV: A ECR-CV tem a responsabilidade pela emissão do seu próprio certificado e dos certificados das EC´s de nível imediatamente subsequente ao seu.

1.3.3.2. Titulares de certificados de utilizadores finais: Os certificados de utilizadores finais são emitidos pela EC's subordinadas à ECR-CV.

1.3.4. Partes confiáveis

Considera-se terceira parte, a parte que confia no teor, validade e aplicação do certificado digital.

1.3.5. Outros participantes

1.3.5.1. Conselho Gestor da ICP-CV (CG): tem a competência de garantir que as declarações de práticas de certificação das EC's, bem como da Entidade de Certificação Raiz de Cabo Verde, estejam em conformidade com a política de certificação da ICP-CV;

1.3.5.2. Autoridade Credenciadora (AC): entidade competente para a credenciação, supervisão e fiscalização das EC´s.

1.3.5.3. O Núcleo Operacional para a Sociedade de Informação (NOSi) é prestador de serviço de suporte à ECR-CV, na medida em que disponibiliza sua infraestrutura física e lógica e de recursos humanos especializados. A Polícia Judiciária é prestadora de serviço de suporte à ECR-CV, enquanto entidade que disponibiliza sua infraestrutura física para efeitos de ambiente de contingência.

1.4. Uso do certificado

1.4.1. Uso apropriado do certificado

Os certificados emitidos pela ECR-CV têm como objeto exclusivo prover a sua própria identificação e a identificação das EC's de nível imediatamente subsequente ao seu. A ECR-CV tem a responsabilidade de divulgação de suas chaves públicas de forma segura.

1.4.2 Proibição de uso de certificado

Os certificados emitidos pela ECR-CV não podem identificar ou verificar qualquer entidade ou assinatura além dos propósitos descritos nesta DPC.

1.5. Gestão da DPC

1.5.1. Organização do documento

Nome: Agência Reguladora Multissectorial da Economia - ARME

1.5.2. Contatos:

Endereço: Av. Da China, 5º Piso, Chã de Areia, Praia, Cabo Verde

Telefone: (+238) 260 44 00/01/02/03

Página web: http://www.pki.ecrcv.cv

E-mail: pki.ecrcv@ecrcv.cv

1.5.3. Conformidade da DPC com a PC

Esta DPC confere conformidade à PC da ECR-CV.

1.5.4. Procedimentos de aprovação da DPC

1.5.4.1 A aprovação interna desta DPC e seguintes correcções (ou actualizações) deverão ser levadas a cabo pelo Grupo de Trabalho de Administração de Segurança. Correcções (ou actualizações) deverão ser publicadas sob a forma de novas versões desta DPC, substituindo qualquer DPC anteriormente definida. O Grupo de Trabalho de Administração de Segurança deverá ainda determinar quando é que as alterações na DPC levam a uma alteração nos identificadores dos objectos (OID) da DPC.

1.5.4.2 Após a aprovação interna pelo conselho executivo, a DPC e as respetivas alterações são submetidas à aprovação da autoridade credenciadora.

1.5.4.3 A autoridade credenciadora, então, submete esta DPC aos membros do CG da ICP-CV para aprovação final através de deliberação publicada no Boletim Oficial

1.6. Acrónimos

SIGLA	DESCRIÇÃO
ARME	Agência Reguladora Multissectorial da Economia
EC	Entidade de Certificação
ECR-CV	Entidade de Certificação Raiz da ICP-CV
ACT	Autoridade de Carimbo do Tempo
UR	Unidade de Registo
CG da ICP- CV	Conselho Gestor da Infraestrutura de Chaves Públicas de Cabo Verde
DN	*Distinguished Name*
B.O.	Boletim Oficial
DPC	Declaração de Práticas de Certificação
DPCT	Declaração de Práticas de Carimbo do Tempo

DPPSC	Declaração de Práticas de Prestador de Serviço de Confiança
EAT	Entidade de Auditoria do Tempo
ICP-CV	Infraestrutura de Chaves Públicas de Cabo Verde
IEC	*International Electrotechnical Commission*
ISO	*International Organization for Standardization*
ITU	*International Telecommunications Union*
LCR	Lista de Certificados Revogados
OID	*Object Identifier*
PC	Política de Certificado
PCT	Política de Carimbo do Tempo
PCN	Plano de Continuidade de Negócio
PS	Política de Segurança
PSC	Prestadores de Serviço de Confiança
PSS	Prestador de Serviço de Suporte
RFC	*Request For Comments*
UTC	*Coordinated Universal Time*

2. Responsabilidades Publicação e Repositório

2.1. Repositório

2.1.1. O repositório da ECR-CV encontra-se localizado no seu sítio web http://pki.ecrcv.cv.

2.1.2. O repositório da ECR-CV disponibiliza o seu próprio certificado e a sua LCR e a lista das Entidades de Certificação cujos certificados são assinados pela ECR-CV e que integram a ICP-CV.

2.2. Informações publicadas no repositório

2.2.1. Conforme as regras estabelecidas nesta DPC os certificados e as LCR's da ECR-CV, bem como os certificados das EC's de nível imediatamente subsequente ao da ECR-CV são publicados no repositório localizado na página *Web* http://pki.ecrcv.cv.

2.2.2. As alterações a esta DPC, além de serem publicadas no seu repositório, são publicadas no B.O e são comunicadas pela ECR-CV às entidade integrantes da ICP-CV, bem como às EC's com as quais possui acordos de certificação cruzada.

2.2.3. As informações publicadas pela ECR-CV no seu repositório, nomeadamente o seu certificado, a sua LCR, a sua DPC e demais informações têm disponibilidade para consulta de 80,0%, excluindo os tempos de paragem programadas para o fim de semana ou para o período noturno.

2.2.4. Os certificados emitidos pela ECR-CV incluem a identificação do seu sítio web.

2.3. Tempo ou frequência de publicação de informação

2.3.1. Os certificados da ECR-CV são publicados imediatamente após a sua emissão.

2.3.2. A frequência da emissão de LCR e sua publicação estão descritos nos itens 4.9.8, 4.9.9 e 4.12 desta DPC.

2.4. Consulta e controlo de acesso aos repositórios

2.5.1. As Consultas a esta DPC, aos certificados e LCR's da ECR-CV não têm quaisquer restrições.

2.5.2. Os controlos de acesso a esta DPC restringem a escrita, sem prejuízo de permitirem a leitura desta.

3. Identificação e Autenticação

Antes da emissão e inclusão dos atributos nos certificados digitais a ECR-CV confirma a autenticidade da identidade e/ou atributos das EC's às quais emite certificados e que se encontram devidamente credenciadas na ICP-CV. As EC's estão proibidas de usar nomes em seus certificados que violam os direitos de propriedade intelectual de terceiros. Caso seja detetada este tipo de violação, a ECR-CV reserva-se o direito de rejeitar a solicitação sem prejuízo das responsabilidades a que fica sujeito o solicitante.

3.1. Atribuição de nomes

3.1.1. Tipos de nomes

No âmbito da ICP-CV, os tipos de nomes atribuídos identificam inequivocamente as EC's subordinadas à ECR-CV. A correspondente identificação é realizada de acordo com o DN (Distinguished Names) – padrão da ITU-T X.501.

3.1.2. Identificação única para os nomes

Um identificador único é atribuído aos certificados emitidos pela ECR-CV, de forma a identificar, univocamente, a EC para a qual o certificado foi emitido, conforme o disposto em 7.1.4.

3.1.3. Anonimato ou pseudónimo dos titulares do certificado

No âmbito da ECR-CV, no processo de emissão de certificados para as EC's não é permitido o uso de pseudónimo.

3.1.4 Interpretação de vários tipos de nomes

Nomes distintos em certificados são interpretados usando os padrões ITU-T X.501 e a sintaxe ASN.1.

3.1.5. Nomes Distintos

Os Identificadores "Distinguished Name" - DN aplicados pela ECR-CV às EC's, devem ser distintos para cada uma delas. De forma a garantir que o campo DN é único para cada EC, entretanto, podem ser adicionados números ou letras, conforme o padrão ITU-T X.509. A extensão "Unique Identifiers" não é usada para distinguir as EC's com nome idêntico.

3.1.6. Decisão sobre a disputa de nomes.

A ECR-CV reserva o direito de decidir sobre as disputas de nomes das EC's de nível imediatamente subsequente ao seu. Durante o processo de autenticação, é responsabilidade da EC solicitante do certificado fazer prova de direito ao uso de um nome específico (DN) em seu certificado, de acordo com a legislação em vigor.

3.1.7. Reconhecimento, autenticação e papel de marcas registadas

3.1.7.1. As entidades não podem solicitar certificados com conteúdos que violam os direitos de propriedade intelectual de terceiros.

3.1.7.2. No procedimento de autenticação e identificação do titular do certificado, a entidade requisitante do certificado terá que apresentar os documentos legais que demonstram o direito à utilização do nome requisitado.

3.1.7.3. Não compete à ECR-CV verificar o direito da EC, que solicita um certificado, de usar uma marca registada.

3.1.7.4. A ECR-CV reserva-se o direito de revogar qualquer certificado envolvido em uma disputa.

3.2. Validação inicial de identidade

A ECR-CV realiza a identificação do solicitante ou de serviços, incluindo os serviços relacionados à EC, através dos meios legais de comunicação ou investigação, que são considerados necessários para identificar a pessoa coletiva ou singular.

3.2.1. Método para comprovar a posse de chave privada

A ECR-CV verifica se a EC, de nível subsequente ao seu, possui a chave privada correspondente à chave pública para a qual está a ser solicitado o certificado digital. Para essa finalidade a ECR-CV utiliza as referências constantes da RFC 4210 e da sua atualização RFC 6712.

3.2.2. Autenticação da identificação de pessoa coletiva

3.2.2.1. O processo de autenticação da identidade de uma pessoa coletiva, deve obrigatoriamente garantir que a pessoa coletiva para quem vai ser emitido o certificado é quem na realidade diz ser e que a criação da assinatura, através de dispositivo de criação de assinatura, exige a intervenção de pessoas singulares que, estatutariamente, representam essa pessoa coletiva.

3.2.2.2. A ECR-CV responsabiliza-se pela guarda de toda a documentação utilizada para verificação da identidade da pessoa coletiva que requisita um certificado, garantindo a verificação da identidade dos seus representantes legais, por meio legalmente reconhecido e, com garantias, no caso dos seus representantes legais não se encontrarem na cerimónia de emissão de certificado, os poderes bastantes do representante nomeado pela entidade para a referida emissão.

3.2.2.3. A ECR-CV mantém políticas e procedimentos internos que são revistos regularmente de modo a cumprir eventuais requisitos de organizações de que venha a integrar, bem como cumprir os Requisitos de Linha de Base (CA/B Fórum), as Diretrizes de EV e as Diretrizes de Assinatura de Código EV.

3.2.3. Autenticação da identidade de um indivíduo

Não aplicável.

3.2.4. Informações não verificadas do titular do certificado

Não aplicável.

3.2.5. Validação dos representantes legais

Na emissão de certificado de EC´s subordinadas à ECR-CV é verificado se a pessoa singular é o representante legal da pessoa coletiva responsável pela EC.

3.2.6. Critérios para interoperabilidade

3.2.6.1. No caso de solicitação por parte de uma EC de acordos de interoperabilidade, tendo como base a certificação cruzada com outras infraestruturas de chaves públicas, a ECR-CV deve exigir no mínimo a seguinte documentação:

a) A Declaração de Práticas de Certificação;
b) O último relatório de auditoria, demonstrando a total conformidade com o estabelecido na sua DPC;
c) Os parâmetros respeitantes a validação técnica da certificação cruzada.

3.2.6.2. Todos os pedidos de acordos de interoperabilidade devem ser devidamente aprovados pelo CG da ICP-CV.

3.2. Identificação e autenticação para solicitação de novo par de chaves

3.3.1. Identificação e autenticação chaves de rotina

3.3.1.1. O processo de emissão, pela ECR-CV, de um novo certificado para uma EC subordinada, pode ser feito de forma simplificada, antes da validade do certificado vigente da EC expirar. A solicitação referente à nova chave é assinada usando a chave válida atual.

3.3.1.2. Complementarmente, um representante legal da EC deve preencher e assinar, em papel ou digitalmente, o formulário destinado à correspondente solicitação, disponibilizado pela ECR-CV. Após a receção desse formulário e sua consequente validação a ECR-CV iniciará o processo de emissão do novo certificado.

3.3.2. Identificação e autenticação para novas chaves após a revogação

Após revogação de certificado, a geração de novo par de chaves e respetiva emissão de certificado segue os procedimentos para a autenticação e identificação inicial.

3.4. Identificação e autenticação para solicitação de revogação

3.4.1. A entidade que solicita a revogação do certificado de uma EC deverá ser identificada. Somente as entidades listadas no número 4.9.3 podem solicitar a revogação do certificado de uma EC subordinada.

3.4.2. O procedimento para solicitação de revogação de certificado pela ECR-CV está descrito no número 4.9.4. Solicitações de revogação de certificados devem ser registadas.

4. Requisitos operacionais do ciclo de vida do certificado

4.1. Solicitação de Certificado

As ECs que pretendem integrar a ICP-CV, antes do envio da sua solicitação à ECR-CV para emissão do seu certificado devem passar pelo processo de credenciação e de registo de EC's, de acordo com a legislação e normas em vigor.

4.1.1. Permissão para solicitação de certificado

4.1.1.1. A ARME é a entidade responsável para encaminhar a solicitação para emissão dos certificados auto assinados da ECR-CV ao CG.

4.1.1.2. A Permissão para emissão do certificado auto assinado da ECR-CV é concedida pelo CG da ICP-CV que, se assim entender, pode solicitar auditoria de conformidade a esta entidade antes da respetiva aprovação.

4.1.1.3. A solicitação de um certificado de uma EC subordinada à ECR-CV deve ser feita pelos seus representantes legais e, somente, após a conclusão do processo de credenciação.

4.1.2 Responsabilidades e Processo de registo

São responsabilidades da ECR-CV:

a) A criação e a administração do seu par de chaves criptográficas;

b) A emissão e distribuição do seu certificado digital;

c) A emissão e a distribuição de certificados das EC's diretamente subordinadas a ela;

d) A publicação de certificados por ela emitidos;

e) A revogação de certificados por ela emitidos;

f) A emissão, administração e a publicação de sua LCR;

h) A implementação de acordos de certificação cruzada, conforme as diretrizes estabelecidas pelo CG da ICP-CV;

i) A aplicação de medidas de segurança e controlo, previstas nesta DPC e na POLÍTICA DE SEGURANÇA DA ICP-CV, quando envolve os seus processos, procedimentos e atividades;

j) A manutenção dos processos, procedimentos e atividades em conformidade com a legislação vigente e com as normas, práticas e regras estabelecidas pelo CG da ICP-CV;

k) A manutenção e a garantia da integridade, do sigilo e da segurança da informação por ela tratada; e

l) A implementação e o teste regular do seu Plano de Continuidade de Negócio - PCN.

4.2. Processamento de Solicitação de certificado à ECR-CV

Somente as EC's credenciadas no âmbito da ICP-CV podem solicitar à ECR-CV a emissão do seu certificado correspondente.

4.2.1. Funções de Identificação e autenticação

A ECR-CV realiza as funções de identificação e autenticação conforme o número 3.2 desta DPC.

4.2.2. Aprovação ou rejeição de pedidos de certificado

Os procedimentos para aprovação ou rejeição de solicitações de certificados dirigidos à ECR-CV são os descritos no item 3.2 desta DPC.

4.2.3. Tempo para processar a solicitação de certificado

A cerimónia de emissão de um certificado para uma EC subordinada à ECR-CV, deve ser realizada, no máximo, 30 (trinta) dias úteis após a receção da solicitação e observada a sua aprovação.

4.3. Processo de Emissão de certificado

4.3.1. Emissão de Certificados pela ECR-CV

4.3.1.1. Para efeitos de emissão do seu certificado, a EC solicitante deve encaminhar à ECR-CV uma solicitação por meio dos seus representantes legais e de acordo com o padrão PKCS#10[1].

4.3.1.2. A emissão do certificado de uma EC subordinada à ECR-CV é efetuada por meio de uma cerimónia que decorre na zona de alta segurança da ECR-CV e, em que se encontram presentes:

a) No mínimo por três (3) membros do Grupo de Trabalho, obedecendo à regra de segregação de funções;

b) Quaisquer observadores, aceites pelos membros do Grupo de Trabalho;

c) Dois (2) representantes da ARME.

4.3.1.3. A cerimónia de emissão de certificado da ECR-CV é constituída pelos seguintes passos:

[1] cf. RFC 2986. 2000, PKCS #10: Certification Request Syntax Specification, version 1.7.

a) Identificação e autenticação de todas as pessoas presentes na cerimónia, com as garantias de que os membros do Grupo de Trabalho têm os artefactos, ferramentas e os poderes e permissões necessários para executar os comandos para emissão do certificado;

b) Os membros do Grupo de Trabalho da ECR-CV efetuam o procedimento de arranque de processamento da ECR-CV e emitem o certificado;

c) Os membros do Grupo de Trabalho da ECR-CV arquivam o certificado num suporte tecnológico (não regravável);

d) A cerimónia de emissão fica terminada com a execução do procedimento de finalização de processamento da ECR-CV, pelos membros do Grupo de Trabalho da ECR-CV;

4.3.1.4. A validade do certificado emitido tem início logo após a sua emissão.

4.3.1.5. A ECR-CV não emite certificados a titulares ou usuários finais, pelo que não se aplica, para a ECR-CV, o cenário de restrições ou autorizações ao processamento de registos de DNS para autorização da autoridade de certificação.

4.3.2. Notificações para o titular do certificado

Após a emissão do certificado, a ECR-CV envia uma mensagem eletrónica com as informações pertinentes a confirmar a emissão bem-sucedida.

4.4. Aceitação do certificado

4.4.1. Conduta sobre a aceitação do certificado

4.4.1.1. A ECR-CV, no processo de emissão de um certificado para uma EC subordinada, garante que as informações contidas nesse certificado foram verificadas de acordo com esta DPC.

4.4.1.2. No momento da entrega do certificado, durante a cerimónia de sua emissão pela ECR-CV, o representante legal da EC confirma a receção do certificado através da assinatura do Termo de Cerimónia de Entrega de Chave Pública.

4.4.1.3. Considera-se o certificado aceite quando os dados constantes do mesmo são confirmados pela EC através de envio de mensagem eletrónica ou na primeira utilização da chave privada correspondente.

4.4.1.4. A confirmação dos dados do certificado deve ser realizada pela EC titular do certificado no prazo de 2 (dois) dias úteis, contados a partir da sua receção, após o qual o certificado será considerado aceite.

4.4.1.5. Ao aceitar o certificado, a EC titular do certificado:

a) Concorda com as responsabilidades, obrigações e deveres a ela impostas por esta DPC;

b) Garante que não teve conhecimento de que pessoas não autorizadas tiveram acesso à chave privada associada ao certificado; e

c) Confirma que todas as informações de certificado fornecidas durante o processo de credenciamento são verdadeiras e estão reproduzidas no certificado de forma correta e completa.

4.4.1.6. A comunicação sobre a não aceitação de um certificado no prazo previsto, acompanhada da correspondente justificativa, implica na realização de uma nova cerimónia, onde é feita a revogação do certificado não aceite e a emissão de um novo certificado.

4.4.2. Publicação do certificado pela ECR-CV

O certificado da ECR-CV e os certificados das EC's subordinadas são publicados de acordo com o ponto 2.2 desta DPC.

4.4.3. Notificação de emissão para outras entidades

A notificação para outras entidades, sem prejuízo de outras formas de comunicação, é fornecida nas condições e meios descritos no ponto 2.2 desta DPC.

4.5. Uso do par de chaves e do certificado

As operações da EC titular de certificado emitido pela ECR-CV devem ser realizadas de acordo com a sua Declaração de Práticas de Certificação - DPC e com as Políticas de Certificado - PC, que por sua vez devem obedecer aos normativos da ICP-CV, no que tange às redações das DPC's e das PC's das EC's credenciadas e subordinadas à ECR-CV.

4.5.1. Uso da chave privada e do certificado da EC titular

Os mecanismos de controlo e de proteção da chave privada da EC subordinada a ECR-CV devem ser descritos na sua DPC e esta deve usar a sua chave privada de acordo com os requisitos e procedimentos definidos na referida DPC.

4.5.2 Uso da chave pública e do certificado por terceiras partes confiáveis

4.5.2.1. Terceiras partes confiáveis devem estar em concordância com os termos estabelecidos nesta DPC, relativamente às práticas relacionadas à autenticação do titular, à política operacional e aos procedimentos para controlo de segurança que são implementados pela EC emissora do certificado.

4.5.2.2 Os procedimentos para conferir confiança à terceira parte confiável encontram-se descritos no item 9.6.4 desta DPC.

4.6. Renovação de certificados

Não se aplica.

4.6.1. Circunstâncias para renovação de certificados

Não se aplica.

4.6.2. Quem pode solicitar a renovação

Não se aplica.

4.6.3. Processamento de solicitação para renovação de certificados

Não se aplica.

4.6.4. Notificação para nova emissão de certificado para o titular

Não se aplica.

4.6.5. Procedimento para aceitação de uma renovação de um certificado

Não se aplica.

4.6.6. Publicação de uma renovação de um certificado pela ECR-CV

Não se aplica.

4.6.7. Notificação de emissão de certificado pela ECR-CV para outras entidades

Não se aplica.

4.7. Nova chave de certificado

4.7.1. Circunstâncias para nova chave de certificado

Não se aplica

4.7.2 Quem pode requisitar a certificação de uma nova chave pública

Não se aplica

4.7.3 Processamento de requisição de novas chaves de certificado

Não se aplica

4.7.4 Notificação de emissão de novo certificado para o titular

Não se aplica

4.7.5 Conduta constituindo a aceitação de uma nova chave certificada

Não se aplica

4.7.6 Publicação de uma nova chave certificada pela ECR-CV.

Não se aplica

4.7.7 Notificação de uma emissão de certificado pela ECR-CV para outras entidades

Não se aplica

4.8. Modificação de certificado

Não se aplica

4.8.1. Circunstâncias para modificação de certificado

Não se aplica

4.8.2. Quem pode requisitar a modificação de certificado

Não se aplica

4.8.3. Processamento de requisição de modificação de certificado

Não se aplica

4.8.4. Notificação de emissão de novo certificado para o titular

Não se aplica

4.8.5. Conduta constituindo a aceitação de uma modificação de certificado

Não se aplica

4.8.6. Publicação de uma modificação de certificado pela ECR-CV

Não se aplica

4.8.7. Notificação de uma emissão de certificado pela ECR-CV para outras entidades

Não se aplica

4.9. Suspensão e revogação de certificado

4.9.1. Âmbito

4.9.1.1. A revogação de certificados é uma ação através da qual o certificado deixa de estar válido antes do fim do seu período de validade, perdendo a sua operacionalidade.

4.9.1.2. Os certificados depois de revogados não podem voltar a ser válidos.

4.9.2. Circunstâncias para revogação

4.9.2.1 Um certificado uma de EC subordinada à ECR-CV pode ser revogado a qualquer instante, por solicitação da própria EC titular do certificado ou por decisão motivada da ECR-CV, resguardados os princípios do contraditório e da ampla defesa.

4.9.2.2. Um certificado pode ser revogado por uma das seguintes razões:

a) Comprometimento ou suspeita de comprometimento da chave privada;

b) Perda da chave privada;

c) Incorreções graves nos dados fornecidos;

d) Equipamento tecnológico deixar de ser utilizado no âmbito da ICP-CV;

e) Comprometimento ou suspeita de comprometimento da senha de acesso à chave privada

f) Comprometimento ou suspeita de comprometimento da chave privada da ECR-CV;

g) Perda, destruição ou deterioração do dispositivo de suporte da chave privada (por exemplo, suporte/token criptográfico);

h) Revogação do certificado da ECR-CV;

i) Incumprimento por parte da ECR-CV ou EC titular das responsabilidades previstas na presente DPC;

j) Sempre que haja razões credíveis que induzam que os serviços de certificação possam ter sido comprometidos, de tal forma que coloquem em causa a fiabilidade dos certificados;

k) Por resolução judicial.

4.9.3. Quem pode submeter o pedido de revogação

4.9.3.1. Estão legitimados a submeter o pedido de revogação, sempre que se verifiquem alguma das condições descritas no ponto 4.9.2., as seguintes entidades:

a) O CG da ICP-CV;

b) A ECR-CV;

c) A Autoridade Credenciadora;

d) As EC's integrantes da ICP-CV, mediante justificativa fundamentada;

e) Uma parte confiante, sempre que demonstre que o certificado foi utilizado com fins diferentes dos previstos.

4.9.3.2. A ECR-CV guarda toda a documentação utilizada para verificação da identidade e autenticidade da entidade que efetua o pedido de revogação, garantindo a verificação da identidade dos seus representantes legais, por meio legalmente reconhecido, não aceitando poderes de representação para o pedido de revogação do certificado de EC.

4.9.4. Procedimento para o pedido de revogação

4.9.4.1. Todos os pedidos de revogação devem ser endereçados para a ECR-CV por escrito ou por mensagem eletrónica assinada digitalmente, em formulário de pedido de revogação[2], observando o seguinte:

a) Identificação e autenticação da entidade que efetua o pedido de revogação;

b) Registo e arquivo do formulário de pedido de revogação;

c) Devido a segurança e urgência no processo, O Conselho Executivo decide sobre a aprovação ou recusa do pedido de revogação do certificado;

d) A decisão da alínea c) deve, a seu tempo, ser comunicada ao CG.

4.9.4.2. Sempre que se decidir e se proceder com a revogação de um certificado, o processo é concluído com a publicação de uma nova LCR e de seguida a ECR-CV deve comunicar à EC titular do certificado revogado a informação sobre a conclusão do processo.

4.9.4.3. Em qualquer dos casos listados no número 4.9.3.1, é arquivada a descrição pormenorizada de todo o processo de decisão, ficando documentado:

a) Data do pedido de revogação;
b) Nome do titular do certificado (assinante);
c) Exposição pormenorizada dos motivos para o pedido de revogação;
d) Nome e funções da pessoa que solicita a revogação;
e) Informação de contacto da pessoa que solicita a revogação;

[2] 13 PJ.ECRCV_53.2.2_0001_pt.doc, Formulário para pedido de revogação de certificado de EC subordinada à ECR-CV

f) Assinatura da pessoa que solicita a revogação.

4.9.4.4 O prazo para a revogação de certificado de uma EC subordinada á ECR-CV é de no máximo 24 (vinte e quatro) horas. O prazo contar-se-á a partir da receção pela ECR-CV da solicitação de revogação da EC titular do certificado ou da determinação de revogação emitida pela própria ECR-CV, mediante solicitação das entidades listadas no número 4.9.3.1.

4.9.5. Prazo para solicitar uma revogação

A solicitação de revogação deve ser imediata quando configuradas as circunstâncias definidas no item 4.9.2 desta DPC.

4.9.6. Prazo para processar o pedido de revogação

A ECR-CV deve processar uma revogação no prazo estabelecido no número 4.9.4.4.

4.9.7. Requisitos de verificação de revogação para as partes confiáveis

O status dos certificados estará disponível na LCR da ECR-CV, nas condições descritas no número 2.1.

4.9.8. Frequência de emissão de LCR

4.9.8.1. A LCR da ECR-CV é atualizada, no máximo, a cada 90 (noventa) dias. Em caso de revogação de certificado de EC subordinada, a nova LCR é emitida no prazo previsto no item 4.9.3 e a ECR-CV notifica todas as EC's subordinadas a ela.

4.9.8.2. Se o certificado da ECR-CV for revogado, a ECR-CV emite uma nova LCR com período de validade igual ao do seu certificado e encerra a emissão de futuras LCR.

4.9.9. Tempo máximo para a publicação da LCR

A LCR é divulgada no repositório dentro de um dia útil após sua geração.

4.9.10. Receção de pedidos de revogação e verificação de status on-line

Não são aceites pedidos de revogação on-line direcionados ao sistema de certificação da ECR-CV. A única forma de consulta on-line de status de certificado é a realizada por meio da LCR.

4.9.11. Requisitos para verificação de revogação on-line

Não se aplica

4.9.12. Outras formas disponíveis para divulgação de revogação

As Informações sobre a revogação de certificado de uma EC diretamente subordinada a ECR-CV e os certificados auto assinados desta, também, podem ser divulgadas por meio de publicações no B.O e na página web da ECR-CV.

4.9.13. Requisitos especiais para o caso de comprometimento de chave

4.9.13.1. As EC's que tiverem suas chaves comprometidas devem informar tal facto à ECR-CV.

4.9.12.2. As DPC's das EC's devem definir os meios que serão utilizados para se notificar um comprometimento ou suspeita de comprometimento de suas chaves.

4.9.14. Circunstâncias para suspensão

A suspensão de certificados de EC's subordinadas à ECR-CV, não é permitida, salvo em casos específicos e determinados pelo CG da ICP-CV.

4.9.15. Quem pode solicitar suspensão

A ECR-CV ou a EC titular do certificado, após aprovação do CG da ICP-CV.

4.9.16. Procedimento para solicitação de suspensão

Os procedimentos de solicitação de suspensão devem ser especificados na DPC e PC's da EC titular do certificado.

4.9.17. Prazo limite de suspensão

O prazo limite da suspensão deve ser especificados na DPC e PC's da EC titular do certificado.

4.10. Serviços de status de certificado

4.10.1. Características operacionais

Os Certificados da ECR-CV contêm as informações para aceder ao ponto de distribuição de LCR.

4.10.2. Disponibilidade dos serviços

Conforme número 2.2. desta DPC.

4.10.3. Funcionalidades operacionais

Conforme número 4.9. desta DPC.

4.11. Encerramento de atividades

A DPC da EC titular deve descrever os requisitos e os procedimentos que deverão ser adotados nos casos de extinção dos serviços da EC, conforme as disposições constantes do normativo "REQUISITOS PARA PRESTADORES QUALIFICADOS DE SERVIÇOS DE CONFIANÇA".

4.12. Custódia e recuperação de chave

Não é permitida a custódia (escrow) das chaves privadas da ECR-CV.

4.12.1. Política e práticas de custódia e recuperação de chave

Não se aplica à ECR-CV.

4.12.2. Política e práticas de encapsulamento e recuperação de chave de sessão

Não se aplica à ECR-CV.

5. Controlos da instalação, de gestão e de operações

A ECR-CV implementou várias regras e políticas que incidem sobre os controlos físicos, procedimentais e humanos, que suportam os requisitos de segurança constantes nesta DPC.

Estas regras e políticas seguem as boas práticas recomendadas pelos principais standards internacionais relativos à segurança de informação, designadamente a norma ISO 27001.

5.1. Controlos Físicos

5.1.1. Construção e localização das instalações

5.1.1.1.As instalações da ECR-CV são desenhadas de forma a proporcionar um ambiente capaz de controlar e auditar o acesso aos sistemas de certificação, estando fisicamente protegidas do acesso não autorizado, dano ou interferência. A arquitetura de segurança da ECR-CV utiliza o conceito de defesa em profundidade, ou seja, ela é constituída por níveis de segurança, que garantem que o acesso a um nível de segurança mais elevado só é possível quando previamente se tenha alcançado o nível imediatamente anterior, nunca sendo possível, em qualquer local das instalações, aceder ao nível de segurança (n) a partir de outro que não seja o nível (n-1).

5.1.1.2.As operações da ECR-CV são realizadas numa sala de alta segurança, inserida noutra zona também de alta segurança e, dentro de um edifício que reúne diversas condições de segurança, nomeadamente o controlo total de acessos que previne, deteta e impede acessos não autorizados, baseado em múltiplos níveis de segurança física.

5.1.2. Acesso físico

5.1.2.1.Os sistemas da ECR-CV estão protegidos por 8 níveis de segurança física hierárquicos, garantindo-se que o acesso a um nível de segurança mais elevado só é possível quando previamente se tenha alcançado os privilégios necessários ao nível imediatamente anterior.

5.1.2.2.As atividades operacionais sensíveis da ECR-CV, nomeadamente a criação e armazenamento de material criptográfico, e as atividades desenvolvidas no âmbito do ciclo de vida do processo de certificação como a autenticação, a verificação e a emissão de certificados ocorrem dentro da zona restrita de mais alta segurança. Os acessos físicos são automaticamente registados e armazenados para efeitos de auditorias

5.1.3. Energia e ar-condicionado

O ambiente seguro da ECR-CV possui equipamentos de energia e ar condicionado redundantes que garantem condições de funcionamento 24 horas por dia / 7 dias por semana.

5.1.4. Exposição à água

5.1.4.1.As instalações onde se localizam o ambiente físico do ECR-CV estão localizadas a cerca de 69 metros do nivel do mar.

5.1.4.2.O interior da zona de alta segurança tem instalado os mecanismos devidos (detetores de inundação) para minimizar o impacto de uma eventual inundação nos ambientes do mesmo.

5.1.5. Prevenção e proteção contra incendio

O ambiente seguro da ECR-CV tem instalado os mecanismos necessários (um sistema de detecção e extinção automática de incêndio) para detectar e apagar fogos ou outros incidentes derivados de chamas ou fumos. Estes mecanismos estão em conformidade com os regulamentos existentes:

a) Sistemas de deteção e alarme de incêndio estão instalados nos vários níveis físicos de segurança;
b) Equipamento fixo e móvel de extinção de incêndios estão disponíveis, colocados em sítios estratégicos e de fácil acesso de modo a poderem ser rapidamente usados no início de um incêndio e extingui-lo com sucesso;
c) Procedimentos de emergência bem definidos, em caso de incêndio.

5.1.6. Guarda de suportes de armazenamento

5.1.6.1.Todos os suportes de informação sensível são guardados em cofres dentro da zona de alta segurança, assim como num ambiente distinto externo ao edifício com controlos de acessos físicos e lógicos apropriados para restringir o acesso apenas a elementos autorizados dos Grupos de Trabalho. Para além das restrições de acessos, também tem implementado mecanismos de proteção contra acidentes.

5.1.6.2.Quando, para efeito de arquivo de cópias de segurança, informação sensível é transportada da zona de alta segurança para o ambiente externo, o processo é executado sob supervisão de pelo menos 2 (dois) elementos do Grupo de Trabalho que têm por obrigação garantir o transporte seguro da informação até ao local de destino. A informação (ou o token de transporte da informação) deverá estar sempre sob controlo visual dos membros do Grupo de Trabalho.

5.1.6.3.Em situações que implicam a deslocação física de hardware de armazenamento de dados (i.e., discos rígidos, HSM etc.) para fora da zona de alta segurança, por motivos que não o

arquivo de cópias de segurança, cada elemento de hardware deverá ser verificado para garantir que não contém dados sensíveis. Nestas situações, a informação tem de ser eliminada usando todos os meios necessários para o efeito (formatar o disco rígido, reset do hardware criptográfico ou mesmo destruição física do equipamento de armazenamento).

5.1.7. Eliminação de resíduos

5.1.7.1.Documentos e materiais em papel que contenham informação sensível são triturados antes da sua eliminação.

5.1.7.2.É garantido que não é possível recuperar nenhuma informação dos suportes de informação utilizados para armazenar ou transmitir informação sensível (através de formatação "segura" de baixo nível ou destruição física), antes dos mesmos serem eliminados.

5.1.7.3.Os equipamentos criptográficos ou chaves físicas de acesso lógico são fisicamente destruídos ou seguem as recomendações de destruição do respetivo fabricante, antes da sua eliminação. Outros equipamentos de armazenamento (discos rígidos, tapes, etc) deverão ser devidamente limpos de modo a não ser possível recuperar nenhuma informação (através de formatações seguras, ou destruição física dos equipamentos).

5.1.8. Instalações de segurança (backup) externas (off-site) para a ECR-CV

Todas as cópias de segurança são guardadas em ambiente seguro em instalações distintas das instalações primárias, alojadas em cofres e armários seguros situados em zonas com controlos de acesso físicos e lógicos, de modo a restringir o acesso a apenas ao pessoal autorizado, garantindo também a proteção contra danos acidentais.

5.2. Controlos de Procedimentos

5.2.1. Perfis qualificados

5.2.1.1.Definem-se como pessoas qualificadas todos os colaboradores, fornecedores e consultores que tenham acesso ou que controlem operações criptográficas ou de autenticação.

5.2.1.2.No âmbito da ECR-CV os papéis de confiança são agrupados em seis categorias diferentes (que correspondem a seis Grupos de Trabalho distintos) de modo a garantir que as operações sensíveis sejam efetuadas por diferentes pessoas qualificadas, pertencentes a diferentes Grupos de Trabalho, assegurando que, no mínimo, cada grupo de trabalho tenha dois membros.

5.2.1.3.Só estão autorizadas entradas na "Zona de Alta Segurança" perante a presença mínima de dois elementos, pertencente a Grupos de Trabalho distintos, nomeadamente os integrantes dos grupos de trabalho de Segurança e de Auditoria.

5.2.1.4.Como medida adicional de segurança, a ECR-CV considera relevante e obrigatória, a presença em todas as intervenções de um elemento de Auditoria.

5.2.2. Conselho Executivo

5.2.2.1.É responsável pela nomeação dos membros dos restantes grupos e pela tomada de decisões de nível crítico para a EC. Este grupo deve ser constituído por um mínimo de 3(três) membros sendo estes pertencentes ao conselho de administração da ARME.

5.2.2.2.As responsabilidades deste grupo são:

a) Rever e aprovar as políticas propostos pelo grupo de trabalho de Administração de Segurança;
b) Designar os membros dos restantes grupos de trabalho;
c) Disponibilizar a identificação de todos os indivíduos que pertencem aos vários grupos de trabalho, num ou mais locais de fácil acesso pelos indivíduos autorizados;
d) Gerir o Ambiente de Gestão;
e) Divulgar novas políticas aos restantes membros dos Grupos;
f) Tomar decisões críticas sobre o funcionamento da ECR-CV;
g) Substituição de um conjunto de cartões de administrador. Esta operação só é necessária ser realizada se deseja ampliar ou reduzir o número de cartões de administrador;
h) Substituição de um conjunto de cartões de operador. Esta operação só é necessária se deseja ampliar ou reduzir o número de cartões de operador ou substituir algum cartão deteriorado;
i) Dado que se opera em modo FIPS140-2 Nível 3, tem autorização para a geração de conjuntos de cartões de operador e chaves. Esta operação só se requer durante a cerimónia de geração de chaves da própria ECR-CV ou para uma EC subordinada;
j) Pedir a aprovação de políticas ao Conselho Gestor.

5.2.3. Grupo de Auditoria

5.2.3.1.É responsável por efetuar a auditoria interna de todas as ações relevantes e necessárias para assegurar a operacionalidade da ECR-CV. Este grupo deve ter um mínimo de 2 (dois) elementos.

5.2.3.2.As responsabilidades deste grupo são:

a) Auditar a execução e confirmar a exatidão dos processos e cerimónias da ECR-CV;
b) Registar todas as operações sensíveis;
c) Investigar suspeitas de fraudes procedimentais;
d) Verificar periodicamente a funcionalidade dos controlos de segurança (dispositivos de alarme, de controlo de acessos, sensores de fogo, etc) existentes nos vários ambientes;

e) Registar os resultados de todas as ações por si realizadas;
f) Assumir o papel de Auditor de Sistema;
g) Validar que todos os recursos utilizados são seguros;
h) Verificar periodicamente a integridade dos Ambientes de Custódia, assegurando que lá se encontram os artefactos respetivos e que estão devidamente identificados;
i) Verificar periodicamente os registos/logs da ECR-CV.

5.2.4. Grupo de Segurança

5.2.4.1.É responsável por propor todas as políticas da ECR-CV, assegurando que se encontram atualizadas.

5.2.4.2.É ainda responsável pela custódia de alguns artefatos sensíveis (tokens de autenticação, etc), que podem ser levantados pelos membros dos outros grupos mediante a satisfação de determinadas condições. Este grupo deve fazer uso dos vários ambientes seguros disponibilizados para a guarda dos artefatos de segurança. Este grupo deve ter um mínimo de 2 (dois) membros.

5.2.4.3.As responsabilidades deste grupo são:

a) Gerir o Ambiente de Administração de Segurança;
b) Definir e gerir todas as políticas da EC e garantir que se encontram atualizadas e adaptadas à realidade desta;
c) Garantir implementação das políticas definidas;
d) Assegurar que as medidas operacionais são executadas de acordo com esta DPC.
e) Assegurar que todos os documentos relevantes e relacionados, direta ou indiretamente, com o funcionamento da ECR-CV e existentes em formato papel se encontram armazenados no Ambiente de Informação;
f) Explicar todos os mecanismos de segurança aos funcionários que devam conhece-los e de sensibiliza-los para as questões de segurança levando-os a fazer cumprir as normas e políticas de segurança estabelecidas.
g) Permitir e averiguar os acessos à aplicação da ECR-CV (grupos, regras, logs);
h) Verificar perfis de certificados e end entities na aplicação da ECR-CV;
i) Verificar os certificados;
j) Assegurar que cada vez que se inicia o Sistema operativo da ECR-CV, é necessário a inserção dos cartões de operador associados às chaves;
k) Autorizar a criação de chaves da aplicação, durante a cerimónia de geração de chaves para a ECR-CV;
l) Gerir o Ambiente de Custódia;
m) Manter a custódia de artefatos sensíveis (tokens de autenticação, etc.) utilizando os meios adequados que respondam às necessidades de segurança respetivas;

n) Disponibilizar com segurança os artefatos à sua guarda, a membros dos outros grupos e explicitamente autorizados a aceder aos mesmos, após o cumprimento dos procedimentos de identificação e segurança apropriados.

5.2.5. Grupo de Administração de Sistemas

5.2.5.1.É responsável pela instalação e configuração de base (hardware e software) da ECR-CV até à sua inicialização.

5.2.5.2.As responsabilidades deste grupo são:

a) Instalar, interligar e configurar o hardware da EC;
b) Instalar e configurar o software de base da EC;
c) Manter um Inventário atualizado com todos os produtos relacionados com a EC;
d) Gerir e atualizar os produtos instalados;
e) Gestão dos CAs;
f) Configurar as palavras-passe iniciais necessárias, que irão ser alteradas posteriormente pelos responsáveis;
g) Preparar comunicados sobre:
    i. As palavras-passe iniciais;
    ii. Hash do(s) CD(s) de instalação utilizados;
    iii. A lista de todos os artefactos (univocamente identificados) indispensáveis à inicialização e operação da ECR-CV.

5.2.6. Grupo de Operação de Sistemas

5.2.6.1.É responsável por executar as tarefas de rotina essenciais ao bom funcionamento e operacionalidade da ECR-CV.

5.2.6.2.As responsabilidades deste grupo são:

a) Gerir o Ambiente de Produção e o Ambiente de Operação;
b) Realizar as tarefas de rotina da ECR-CV, incluindo operações de cópias de segurança dos seus sistemas;
c) Execução de tarefas de monitorização dos sistemas ECR-CV;
d) Monitorizar, reportar e quantificar todos os incidentes e avarias de software e hardware, despoletando os processos apropriados à correção das mesmas;
e) Pedir a aprovação dos formulários resultantes das cerimónias ao Conselho executivo para armazenamento no ambiente de informação;
f) Assumir o papel de Operador de Sistema.

5.2.7. Administração de Registo

5.2.7.1.É responsável por assegurar a emissão, renovação, suspensão e revogação de certificados.

5.2.7.2.As responsabilidades deste grupo são:

a) Validar a documentação a ser entregue pelo titular para emissão/revogação de certificados;
b) Emitir Certificados caso este processo não esteja automatizado;
c) Revogar/Suspender certificados caso este processo não esteja automatizado.

5.2.8. Número de pessoas necessário por tarefa

5.2.8.1.Existem rigorosos procedimentos de controlo que obrigam à divisão de responsabilidades baseada nas especificidades de cada Grupo de Trabalho, e de modo a garantir que tarefas sensíveis apenas podem ser executadas por um conjunto múltiplo de pessoas autenticadas.

5.2.8.2.Os procedimentos de controlo interno foram elaborados de modo a garantir um mínimo de 2 indivíduos autenticados para se ter acesso físico ou lógico aos equipamentos de segurança.

5.2.9. Funções que requerem separação de Responsabilidades

A matriz seguinte define as incompatibilidades (assinaladas por X) entre a pertença ao grupo/subgrupo identificado na coluna esquerda e a pertença ao grupo/subgrupo identificado na primeira linha, no contexto desta EC:

Grupo de Trabalho	Administração		Operação	Administração	Auditoria	Conselho Executivo
	Segurança	Sistemas	Sistemas	Registo	Sistemas	
Administração de Segurança		x			x	x
Administração de Sistemas	x				x	x
Operação de Sistemas					x	x
Administração de Registo					x	x
Auditoria de Sistemas	x	x	x	x		x
Conselho executivo	x	x	x	x	x	

5.3. Medidas de Segurança de Pessoal

5.3.1. Antecedentes, qualificação, experiência e requisitos de idoneidade

Todo o pessoal que desempenhe funções de confiança no ECR-CV deve cumprir os seguintes requisitos:

a) Apresentar provas de antecedentes, qualificações e experiência necessárias para a realização das tarefas inerentes à sua função;
b) Ter sido nomeado formalmente para a função a desempenhar;
c) Ter recebido formação e treino adequado para o desempenho da respetiva função;
d) Garantir confidencialidade, relativamente a informação sensível sobre a ECR-CV ou dados de identificação dos titulares de certificados;
e) Garantir o conhecimento dos termos e condições para o desempenho da respetiva função; e
f) Garantir que não desempenha funções que possam causar conflito com as suas responsabilidades nas atividades da ECR-CV.

5.3.2. Procedimentos de verificação de antecedentes

A verificação de antecedentes é realizada durante o processo de credenciação das pessoas nomeadas para exercer cargos em qualquer uma das funções de confiança. A verificação de antecedentes inclui:

a) Confirmação de identificação, usando documentação emitida por fontes fiáveis,
b) Investigação de registos criminais.

5.3.3. Requisitos de Formação e treino

5.3.3.1.Os membros dos Grupos de Trabalho devem participar de ações de formação e treinamento de forma a permitir que as tarefas que desempenham sejam realizadas de forma satisfatória e competente.

5.3.3.2.Os elementos dos Grupos de Trabalho, estão adicionalmente sujeitos a um plano de formação e treino, englobando os seguintes tópicos:

a) Certificação digital e Infraestruturas de Chave Pública;
b) Conceitos gerais sobre segurança da informação;
c) Formação específica para o seu papel dentro do Grupo de Trabalho;
d) Funcionamento operacional da ECR-CV;
e) Política de Certificados e Declaração de Práticas de Certificação;
f) Recuperação face a desastres;
g) Procedimentos para a continuidade da atividade e,
h) Aspetos legais básicos relativos à prestação de serviços de certificação.

5.3.4. Frequência e requisitos para reciclagem técnica

Sempre que necessário será ministrado treino e formação complementar aos membros dos Grupos de Trabalho, de modo a garantir o nível pretendido de profissionalismo para a execução competente e satisfatória das suas responsabilidades. Em particular:

a) Sempre que exista qualquer alteração tecnológica, introdução de novas ferramentas ou modificação de procedimentos, é levada a cabo a adequada formação para todo o pessoal afeto à ECR-CV;
b) Sempre que são introduzidas alterações nas Políticas de Certificação ou Declaração de Práticas de Certificação são realizadas sessões de reciclagem aos elementos da ECR-CV.

5.3.5. Frequência e sequência de rotação de funções

Não aplicável.

5.3.6. Sanções para ações não autorizadas

5.3.6.1.Consideram-se ações não autorizadas todas as ações que desrespeitem a Declaração de Práticas de Certificação, quer sejam realizadas de forma deliberada ou sejam ocasionadas por negligência.

5.3.6.2.São aplicadas sanções de acordo com as regras do ECR-CV e das leis de segurança nacional, a todos os indivíduos que realizem ações não autorizadas ou que façam uso não autorizado dos sistemas.

5.3.7. Requisitos acesso a consultores e prestadores de serviço externos

O acesso dos Consultores e dos prestadores de serviços externos à Zona de Alta Segurança (ZAS) é efetuado sob a supervisão e na presença de integrantes do grupo de trabalho da ECR-CV, após o respetivo registo de acesso em livro de presença.

5.3.8. Documentação fornecida ao pessoal

É disponibilizado aos membros dos Grupos de Trabalho toda a informação adequada para que estes possam realizar as suas tarefas de modo competente e satisfatório.

5.4. Procedimentos de Log de Auditoria.

5.4.1. Tipos de eventos registados

Eventos significativos geram registos auditáveis. Estes incluem, pelo menos os seguintes:

a) Tentativas de acesso (com e sem sucesso) para solicitar, gerar, assinar, emitir ou revogar chaves de certificados;
b) Tentativas de acesso (com e sem sucesso) para criar, modificar ou apagar informação dos titulares dos certificados;

c) Tentativas de acesso (com e sem sucesso) e alterações dos parâmetros de segurança do sistema operativo;
d) Emissão e publicação de LCR's's;
e) Arranque e paragem de aplicações;
f) Tentativas de acesso (com e sem sucesso) de início e fim de sessão;
g) Tentativas de acesso (com e sem sucesso) de criar, modificar, apagar contas do sistema;
h) Cópias de segurança, recuperação ou arquivo dos dados;
i) Alterações ou atualizações de software e hardware;
j) Manutenção dos sistemas;
k) Operações realizadas por membros dos Grupos de Trabalho;
l) Alteração de Recursos Humanos;
m) Tentativas de acesso (com e sem sucesso) às instalações por parte de pessoal autorizado ou não;
n) A cerimónia de geração de chaves e sistemas envolvidos na mesma, tais como servidores aplicacionais, base de dados e sistema operativo.

5.4.2. Frequência de auditoria de registos

Os registos são analisados e revistos na base diária e de forma automatizada, produzindo o envio de alertas para o grupo de trabalho de Auditoria, e sempre que haja suspeitas ou atividades anormais ou ameaças de algum tipo. Ações tomadas, baseadas na informação dos registos são também documentadas.

5.4.3. Período de retenção para registos de auditoria

Os registos das informações, inclusive arquivos de auditoria, devem ser retidas nos sistemas por, no mínimo, 3 (três) meses, e depois de arquivadas devem ser conservadas por um período mínimo de 20 (vinte) anos.

5.4.4. Proteção de registos de auditoria

Os registos são analisados exclusivamente por membros do Grupo de Trabalho de Auditoria e reportados ao Conselho Executivo.

Os registos são protegidos por mecanismos eletrónicos auditáveis, de modo a detectar e impedir a ocorrência de tentativas de modificação, remoção ou outros esquemas de manipulação não autorizada dos dados.

As cópias de segurança dos registos do ECR-CV são armazenadas em local seguro e em cofres.

A destruição de um arquivo de auditoria só poderá ser efetuada após autorização expressa do Conselho Executivo e executada na presença de, no mínimo dois elementos, um elemento de segurança e um de auditoria, sendo que este ato deverá ficar registado em registos de Auditoria.

5.4.5. Procedimentos para cópia de segurança (Backup) de registos de auditoria

São criadas cópias de segurança regulares dos registos em sistemas de armazenamento de alta capacidade.

5.4.6. Sistema de coleta de dados de auditoria (interno ou externo)

O processo de tratamento e recolha de registos de auditoria é constituído por uma combinação de processos automáticos e manuais, executados pelos sistemas operativos, pelas aplicações da ECR-CV e pelo pessoal que as opera. Todos os registos de auditoria são armazenados nos sistemas internos da ECR-CV.

5.4.7. Notificação de agentes causadores de eventos

Eventos auditáveis, são registados no sistema de auditoria e guardados de modo seguro, sem haver notificação ao sujeito causador da ocorrência do evento.

5.4.8. Avaliações de vulnerabilidade

Os registos auditáveis são regularmente analisados de modo a minimizar e eliminar potenciais tentativas de quebrar a segurança do sistema. São realizados quatro testes de intrusão por ano, de forma a verificar e avaliar vulnerabilidades. O resultado da análise é reportado ao Conselho executivo da ECR-CV para rever e aprovar um plano de implementação e correção das vulnerabilidades detetadas.

5.5. Arquivo de Registos

5.5.1. Tipos de registos arquivados

Todos os dados auditáveis são arquivados, conforme registo de eventos detalhado no numero 5.4.1, assim como informação de pedidos de certificados e documentação de suporte ao ciclo de vida das várias operações.

As informações e eventos que são registados e arquivados são:

a) Os registos de auditoria especificados no ponto 5.4.1 desta DPC;
b) As cópias de segurança dos sistemas que compõem a infraestrutura fisica do Data Center do Estado;
c) Toda a documentação relativa ao ciclo de vida dos certificados, designadamente:
    i. Procedimentos de emissão e revogação de certificados de serviço;
    ii. Formulários de emissão e receção dos certificados de serviço;
d) Acordos de confidencialidade;
e) Protocolos estabelecidos com as Entidades Subscritoras;
f) Contratos estabelecidos entre o ECR-CV e outras entidades - apenas disponibilizados a quem solicitar a sua visualização, após avaliação e aprovação prévia do pedido;
g) Autorizações de acesso aos sistemas de informação;

h) Acessos aos artefactos existentes nas custódias.

5.5.2. Período de retenção para arquivo

Para cada registo arquivado os períodos de retenção são os seguintes:

a) a) As LCR's e os certificados de assinatura digital devem ser retidos por um período não inferior a 40 (quarenta) anos a contar da data de expiração ou revogação, e podem, para fins de consulta histórica, ser conservados permanentemente;
b) As cópias dos documentos para identificação apresentadas no momento da solicitação e da revogação de certificados e os termos de titularidade e responsabilidade devem ser retidos, no mínimo, por 20 (vinte) anos; e
c) As demais informações, inclusive arquivos de auditoria, devem ser retidas nos sistemas por, no mínimo, 3 (três) meses, e depois de arquivadas devem ser conservadas por um período mínimo de 20 (vinte) anos.

5.5.3. Proteção de arquivo

O arquivo:

a) É protegido para que apenas membros autorizados dos Grupos de Trabalho possam consultar e ter acesso ao seu conteúdo,
b) É protegido contra qualquer modificação ou tentativa de remoção,
c) É protegido contra a deterioração do media onde é guardado, através de migração periódica para media novo,
d) É protegido contra a obsolescência do hardware, sistemas operativos e outros software, pela conservação do hardware, sistemas operativos e outros software que passam a fazer parte do próprio arquivo, de modo a permitir o acesso e uso dos registos guardados, de modo intemporal; e
e) É guardado de modo seguro em ambientes externos.

5.5.4. Procedimentos de cópia de arquivo

Cópias de segurança dos arquivos são efetuados, de modo incremental ou total e guardadas em dispositivos apropriados.

O grupo de trabalho da ECR-CV verifica a integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

5.5.5. Requisitos para datação de registos

Algumas das entradas dos arquivos contêm informação de data e hora, que é prestado por um serviço preciso de referência temporal.

5.5.6. Sistema de coleta de dados de arquivo (interno e externo)

Os sistemas de recolha de dados de arquivo são internos.

5.5.7. Procedimentos para obter e verificar informação de arquivo

5.5.7.1.Apenas membros autorizados dos Grupos de Trabalho têm acesso aos arquivos para verificação da sua integridade.

5.5.7.2.São realizadas de forma automática verificações de integridade dos arquivos eletrónicos (cópias de segurança) na altura da sua criação, em caso de erros ou comportamentos imprevistos, deve-se realizar novo arquivo

5.6. Renovação de Chaves

5.6.1.A renovação de chaves é feita apenas em caso de desastre ou comprometimento, conforme a secção 5.7.

5.6.2.Apenas as entidades de certificação com certificados válidos podem requerer a renovação do respetivo par de chaves, desde que a geração de novo par de chaves esteja conforme a secção 5.7.

5.7. Recuperação em caso de Desastre ou Comprometimento

5.7.1. Procedimentos em caso de Incidente ou Comprometimento

5.7.1.1.As cópias de segurança das chaves privadas da ECRCV (geradas e mantidas de acordo com o numero 5.1.8) e dos registos arquivados (número 5.5.1) são guardados em ambientes seguros externos e disponíveis em caso de desastre ou comprometimento.

5.7.1.2.No caso de comprometimento da chave privada da ECR-CV, esta deverá tomar as seguintes ações:

a) Proceder à sua revogação imediata;
b) Revogar todos os certificados dela, dependentes;
c) Informar todos os titulares dos seus certificados e terceiras partes conhecidas;
d) Informar todas as Entidades que compõem ICP-CV.

5.7.2. Corrupção dos Recursos Informáticos, do Software e/ou dos Dados

5.7.2.1.No caso dos recursos informáticos, software e/ou dados estarem corrompidos ou existir suspeita de corrupção, as cópias de segurança da chave privada da EC e os registos arquivados podem ser obtidos para verificação da integridade dos dados originais.

5.7.2.2.Se for confirmado que os recursos informáticos, software e/ou dados estão corrompidos, devem ser tomadas medidas apropriadas de resposta ao incidente. A resposta ao incidente pode incluir o restabelecimento do equipamento/dados corrompidos, utilizando equipamento similar e/ou recuperando cópias de segurança e registos arquivados. Até que sejam repostas as

condições seguras, a ECR-CV suspenderá os seus serviços e notificará a Autoridade Credenciadora.

5.7.3. Procedimentos em caso de Comprometimento da Chave Privada da Entidade

No caso da chave privada da EC ser comprometida ou haver suspeita do seu comprometimento, devem ser tomadas medidas apropriadas de resposta ao incidente. As respostas a esse incidente podem incluir:

a) Informar a Autoridade Credenciadora e o Conselho Gestor da ICP-CV;
b) Revogação do certificado da ECR-CV e de todos os certificados emitidos na hierarquia de confiança da ECR-CV;
c) Notificação de todos titulares de certificados emitidos na hierarquia de confiança da ECR-CV;
d) Geração de novo par de chaves para a ECR-CV e inclusão nos vários sistemas/browsers;
e) Renovação de todos os certificados emitidos na hierarquia de confiança da ECR-CV.

5.7.4. Capacidade de continuidade da Atividade em caso de Desastre

A ECR-CV dispõe dos recursos de computação, software, cópias de segurança e registos arquivados nas suas instalações secundárias de segurança, necessários para restabelecer ou recuperar operações essenciais (emissão e revogação de certificados, com a publicação de informação de revogação) com base em procedimentos definidos no Plano de Contingência, após um desastre natural ou outro.

5.8. Procedimentos em caso de extinção de ECR-CV

Em caso de cessação de atividade como prestador de serviços de Certificação, a ECR-CV executa os procedimentos previstos no Plano de Cessação de Atividades, conforme artigo 36º do Decrto-lei nº 27/2023, de 20 de outubro.

Em caso de alterações do organismo/estrutura responsável de gestão da atividade da EC, esta deve informar de tal facto à Autoridade Credenciadora Nacional e ao Conselho Gestor da ICP-CV.

6. Controles Técnicos de Segurança

6.1. Criação e Instalação do Par de Chaves

6.1.1. Criação do par de chaves

6.1.1.1. A criação do par de chaves criptográficos da ECR-CV é processada em hardware específico com certificação validada do tipo "FIPS 140-2 Level 3" e os algoritmos correspondentes à sua criação obedecem aos requisitos definidos nesta DPC.

6.1.1.2. As EC's subordinadas à ECR-CV são responsáveis pela criação dos seus pares de chaves, após o deferimento do seu pedido de credenciamento e a consequente aprovação da sua integração na estrutura hierárquica da ICP-CV.

6.1.2. Entrega da chave privada à entidade

Não se aplica.

6.1.3. Entrega da chave pública para emissor de certificado

6.1.3.1. A EC subordinada à ECR-CV entrega a cópia de sua chave pública, em formato definido nesta DPC e conforme a documentação e formulários da ECR-CV.

6.1.3.2. O representante legal da EC é o responsável pela entrega da chave pública correspondente à chave privada da EC, em cerimónia específica, em data e hora previamente estabelecidas pela ECR-CV. Todos os eventos ocorridos nessa cerimónia são registados para fins de auditoria.

6.1.4. Entrega de chave pública da ECR-CV a terceiras partes

6.1.4.1. A Chave pública da ECR-CV é disponibilizada às EC's subordinadas e considera-se realizada com a publicação do respetivo certificado no endereço eletrónico identificado no número 2.1, sem prejuízo de uma comunicação por mensagem eletrónica dirigida aos representantes das EC´s subordinadas contendo as informações sobre a referida publicação.

6.1.4.2. A disponibilização do certificado da ECR-CV para o utilizador final e outros integrantes da ICP-CV é realizada através da publicação do certificado correspondente à chave privada no endereço eletrónico identificado no número 2.1 e posterior publicação sobre a informação nos meios de comunicação com o objetivo de informar sobre a publicação no seu repositório.

6.1.5. Dimensão das chaves

De forma a prevenir possíveis ataques de criptanálise que descubram a chave privada correspondente ao par de chaves no seu período de utilização, a dimensão das chaves é a seguinte:

a) Mínimo de 4096 bits RSA para a chave da ECR-CV;

b) Mínimo de 4096 bits RSA para a chave das EC subordinadas.

6.1.6. Implementação dos parâmetros de chaves assimétricas e verificação da qualidade dos parâmetros

6.1.6.1. A implementação dos parâmetros da chave pública e verificação da qualidade deverá ter sempre por base a norma que define o algoritmo.

6.1.6.2. As chaves da EC são criadas com base na utilização de processos aleatórios/pseudoaleatórios descritos no ANSI X9.17 (Anexo C), de acordo com o estipulado nas normas ISO 9564-1 e 11568-5 respetivamente.

6.1.7. Propósitos de uso de chave (conforme o campo "key usage" na X.509 v3)

A chave privada da ECR-CV é utilizada apenas para a assinatura de seu próprio certificado, dos certificados das EC's subordinadas a ela e de sua LCR.

6.2. Proteção da Chave Privada e controle de engenharia do módulo criptográfico

A chave privada da ECR-CV é armazenada de forma cifrada no mesmo componente seguro de hardware utilizado para sua criação. O acesso a esse componente é controlado por meio de chave criptográfica de ativação.

6.2.1. Padrões e controle para módulo criptográfico

Para a geração dos pares de chaves da ECR-CV assim como para o armazenamento das chaves privadas, a ECR-CV utiliza um módulo criptográfico em hardware que cumpre as seguintes normas:

a) Common Criteria EAL 4+; e/ou

b) FIPS 140-2, nível 3;

6.2.2. Controle "n de m" para chave privada

6.2.2.1. O controlo multi-pessoal apenas é utilizado para as chaves de EC, pois a chave privada dos certificados está sob controlo exclusivo do seu titular.

6.2.2.2. A ECR-CV implementa um conjunto de mecanismos e técnicas que obrigam à participação de vários membros do Grupo de Trabalho para efetuar operações criptográficas sensíveis na sua EC.

6.2.3. Controle de Chave privada da Cadeia V1

6.2.3.1.A ativação da chave privada da Cadeia de Certificação V1 da ECR-CV é efetuada através da autenticação no módulo criptográfico pelas pessoas indicadas pelo Conselho Gestor da ICP-CV, sendo obrigatória a utilização de autenticação de dois factores (consola de

autenticação portátil e chaves de ativação com código PIN associado). As pessoas indicadas possuem partes dos dados de ativação, e devem autenticar-se para que seja possível efectuar a ativação da chave.

6.2.3.2.Para a ativação das chaves privadas da ECR-CV é necessária, no mínimo, a intervenção de 3 pessoas dos Grupos de Trabalho. Após ativar a chave privada, esta permanecerá ativada até que o processo de desativação seja executado.

6.2.3.3. Os dados de ativação necessários para a utilização da chave privada da ECR-CV são divididos em várias partes, acessíveis e à responsabilidade das pessoas indicadas. Um determinado número destas partes (m=2) do número total de partes (n=6) é necessário para ativar a chave privada da ECR-CV guardada no módulo criptográfico em hardware. São necessárias duas (m) partes para a ativação da chave privada da ECR-CV.

6.2.4. Controle de Chave privada da Cadeia V2 e da Cadeia SSL

6.2.4.1. Os dados de ativação necessários para a utilização da chave privada da ECR-CV são armazenados em cartões com PINs de ativação, acessíveis e à responsabilidade de diferentes pessoas nomeados pelo Conselho Gestor da ICP-CV. Um determinado número desses cartões (m=1) do número total de cartões (n=5) é necessário para ativar a chave privada da ECR-CV.

6.2.4.2. Cada cartão referido no número 6.2.4.1 será atribuído a uma pessoa nomeada pelo CG da ICP-CV e o seu PIN correspondente que serve como elemento de segurança do cartão é atribuído a uma segunda pessoa também nomeada pelo CG da ICP-CV. Configurando-se assim, um controlo multipessoal, "*multi-person control*", no processo de ativação da Chave Privada.

6.2.4.3. Os cartões e os PINs ficarão, cada um deles, guardados num cofre, em gavetas diferentes e individualizadas, localizado em um ambiente seguro com controlo de acesso restrito e monitoramento.

6.2.5. Custódia (escrow) de chave privada

Não é permitida a custódia (escrow) das chaves privadas da ECR-CV.

6.2.6. Cópia de segurança de chave privada

6.2.4.1. A ECR-CV mantém cópia de segurança da sua própria chave privada. A cópia é armazenada cifrada e protegida com um nível de segurança não inferior àquele definido para a versão original da chave, e mantida pelo prazo de validade do certificado correspondente.

6.2.4.2. ECR-CV não mantém cópia de segurança das chaves privadas das EC's subordinadas.

6.2.7. Arquivamento de chave privada

Não se aplica.

6.2.8. Inserção de chave privada em módulo criptográfico

A chave privada da ECR-CV é inserida no módulo criptográfico de acordo com o estabelecido no número 6.1.1.

6.2.9. Armazenamento de chave privada em módulo criptográfico

As chaves privadas da ECR-CV são armazenadas de forma cifrada nos módulos do hardware criptográfico.

6.2.10. Método de ativação de chave privada

6.2.8.1. Através de senha e de dispositivo de controlo de acesso ao hardware (token) os operadores que detêm autorização para ativação da chave privada fazem suas respetivas autenticações, que lhes permite proceder com a ativação da chave privada da ECR-CV no modulo criptográfico. Para se executar o processo de ativação da chave privada é necessária a autenticação de dois operadores com permissões para sua ativação. Após a ativação da chave privada, esta permanecerá assim até que o processo de desativação seja executado.

6.2.11. Método de desativação de chave privada

6.2.9.1. A chave privada da ECR-CV é desativada quando a partição respetiva é colocada offline e o servidor ou APPLIANCE for desligado. Uma vez desativada, esta permanecerá inativa até que o processo de ativação seja executado.

6.2.9.2. Quando a chave privada da ECR-CV for desativada, em decorrência da revogação ou expiração do seu certificado, esta deve ser eliminada da memória do módulo criptográfico. Qualquer espaço em disco onde a chave eventualmente estivesse armazenada deve ser sobrescrito.

6.2.12. Método de destruição de chave privada

6.2.10.1. As chaves privadas da ECR-CV (incluindo as cópias de segurança) são apagadas/destruídas num procedimento devidamente identificado e auditado assim que terminada a sua data de validade ou se revogadas antes deste período.

6.2.10.2. A ECR-CV, garante que do processo de destruição das chaves privadas não restarão resíduos destas que possam permitir a sua reconstrução. Para tal, utiliza a função de formatação (inicialização a zeros) disponibilizada pelo hardware criptográfico ou outros meios apropriados, de forma a garantir a total destruição das chaves privadas da sua EC.

6.3. Outros Aspetos do Gestão do Par de Chaves

6.3.1. Arquivo de chave pública

É efetuada uma cópia de segurança de todas as chaves públicas da ECR-CV pelos membros do Grupo de Trabalho permanecendo armazenadas após a expiração dos certificados correspondentes, para verificação de assinaturas geradas durante seu prazo de validade.

6.3.2. Períodos de operação do certificado e períodos de uso para as chaves pública e privada

6.3.2.1. O período de utilização das chaves é determinado pelo período de validade do certificado, pelo que, após este expirar, as chaves deixam de poder ser utilizadas, dando origem à cessação permanente da sua operacionalidade e da utilização que lhes foi destinada.

6.3.2.2. A validade dos diversos tipos de certificados e período em que os mesmos devem ser renovados, é o seguinte:

a) O certificado da ECR-CV tem uma validade de 24 anos, com renovação a cada 12 anos;

b) Os certificados das EC's subordinadas têm validade de 12 anos, com renovação a cada 6 anos (tempo máximo permitido).

6.4. Dados de Ativação

6.4.1. Geração e instalação dos dados de ativação

Os dados de ativação necessários para a utilização da chave privada da ECR-CV são divididos em várias partes, ficando sob a responsabilidade de diferentes membros do Grupo de Trabalho. As diferentes partes são geradas de acordo com o definido no processo/cerimónia de geração de chaves e obedecem aos requisitos definidos pela norma FIPS140-2 nível 3.

6.4.2. Proteção dos dados de ativação

Os dados de ativação da chave privada da ECR-CV (em partes separadas e/ou palavra-passe) são memorizados e/ou guardados em tokens que evidenciem tentativas de violação e/ou guardados em envelopes que são guardados em cofres seguros.

6.4.3. Outros aspetos dos dados de ativação

Não se aplica.

6.5. Controles de Segurança Computacional

6.5.1. Requisitos técnicos específicos de segurança computacional

6.5.1.1. A cerimónia para a criação dos pares de chaves da ECR-CV e emissão dos certificados das EC's subordinadas são realizadas num ambiente off-line, para impedir o acesso remoto não autorizado. As informações utilizadas nesses procedimentos devem ser mantidas num ambiente off-line, com acesso restrito.

6.5.1.2. Cada computador servidor da ECR-CV que é utilizado nos processos de emissão, expedição, distribuição, revogação e administração dos certificados possui as seguintes características:

a) Controlo de acesso aos serviços e perfis da ECR-CV;

b) Clara separação das tarefas e atribuições relacionadas a cada perfil da ECR-CV;

c) Uso de criptografia para segurança de base de dados;

d) Criação e guarda de registos de auditoria da ECR-CV;

e) Procedimentos internos de segurança para garantir a integridade dos dados e dos processos críticos; e

f) Procedimentos para cópias de segurança (backup).

6.5.2. Classificação da segurança computacional

Não se aplica.

6.6. Controlos Técnicos do Ciclo de Vida

6.6.1 Controlos de desenvolvimento de sistema

A ECR-CV utiliza um sistema projetado e desenvolvido por terceiros de acordo com regras de desenvolvimento de sistemas e de gestão de mudanças.

6.6.2 Controlos de gestão de segurança

6.6.2.1. Uma metodologia formal de gestão de configuração é usada para instalação e manutenção contínua do sistema de certificação da ECR-CV. Novas versões do sistema somente são instaladas após comunicação do fabricante e testes em ambiente de homologação da ECR-CV.

6.6.2.2. É fornecida metodologia com registos de auditoria que permite verificar que o sistema da ECR-CV não foi alterado antes da sua primeira utilização. As configurações e alterações do sistema são executadas e auditadas por membros do Grupo de Trabalho.

6.6.3 Controlos de segurança de ciclo de vida

Não se aplica.

6.7. Controlos de Segurança de Rede

O computador servidor da ECR-CV que hospeda o sistema de certificação opera off-line e encontra-se fisicamente desconectado de qualquer rede.

6.8. Carimbo de Tempo

Não se aplica.

7. Perfis de certificado, LCR e OCSP

7.1. Perfis dos certificados da ECR-CV

O formato dos certificados emitidos pela ECR-CV está em conformidade com:

a) O padrão ITU.T X.509;

b) A RFC 5280;

c) Esta DPC.

7.1.1. Número de versão

7.1.1.1. O certificado da ECR-CV tem como base a versão 3 do padrão ITU X.509.

7.1.1.2. Os certificados das EC´s subordinadas são emitidos com base na versão 3 do padrão ITU-T X.509.

7.1.2. Extensões de certificado

7.1.2.1 O certificado da ECR-CV é criado com as seguintes extensões previstas na versão 3 do padrão ITU-T X.509:

a) basicConstraints: contém o campo cA=True. O campo pathLenConstraint não é utilizado.

b) keyUsage: contém apenas os bits keyCertSign(5) e cRLSign(6) ligados. Os demais bits estão desligados.

c) cRLDistributionPoints: contém o endereço na Web onde se obtém a LCR correspondente ao certificado:

i. LCR da cadeia V1: http://pki.ecrcv.cv/pub/crl/ec_raiz_crl001.crl
ii. LCR da cadeia V2: http://pki.ecrcv.cv/pub/crl/ec_raiz_crl002.crl
iii. LCR da cadeia SSL: http://pki.ecrcv.cv/pub/crl/ec_raiz_SSL_crl001.crl

d) Certificate Policies: policyIdentifier: contem o Object Identifier (OID) da DPC da ECR-CV. O PolicyQualifiers contém: o atributo id- qt-cps com o endereço Web desta DPC (http://pki.ecrcv.cv/legislacao/dpcdaecrcv.pdf).

e) SubjectKeyIdentifier: contém o hash da chave pública da ECR-CV.

7.1.2.2 As EC´s subordinadas podem implementar quaisquer das extensões previstas na versão 3 do padrão ITU-T X.509.

7.1.2.2.1 As seguintes extensões são obrigatórias:

a) "Authority Key Identifier", não crítica: o campo keyIdentifier contém o hash, obtido com algoritmo da família SHA, da chave pública da EC que emite o certificado;

b) "Subject Key Identifier", não crítica: Contém o hash, obtido com algoritmo da família SHA, da chave pública da EC titular do certificado;

c) "Key Usage", crítica: os bits keyCertSign e cRLSign devem estar ativados, podendo ser ativados outros bits para casos específicos;

d) "Certificate Policies", não crítica. O campo policyIdentifier deve conter:

i. Se a EC emite certificados para outras EC's, o campo policyIdentifier deve conter o OID da DPC da EC titular do certificado; ou
ii. Se a EC emite certificados para usuários finais, campo policyIdentifier deve conter os OID das PC's implementadas, contendo o campo policyQualifiers com o atributo id-qt-cps e o endereço Web da DPC da AC.

e) "Basic Constraints", crítica: deve conter o campo cA=True; e

f) "CRL Distribution Points", não crítica: deve conter endereço na Web onde se obtém a LCR correspondente ao certificado, conforme item 7.1.2.1.c.

7.1.2.2.2. Para as EC's que emitem certificado SSL também é obrigatória a extensão:

a) "Extended Key Usage", não crítica: deve conter o propósito server authentication OID = 1.3.6.1.5.5.7.3.1. Pode conter o propósito client authentication OID = 1.3.6.1.5.5.7.3.2;

7.1.2.2.3. Para as EC's que emitem certificado SSL é opcional a seguinte extensão:

a)"Authority Information Access", não crítica: a primeira entrada deve conter o método de acesso id-ad-caIssuer, utilizando um dos seguintes protocolos de acesso, HTTP, HTTPS ou LDAP, para a recuperação da cadeia de certificação.

7.1.3 Identificadores de algoritmo

7.1.3.1 O campo identificador de algoritmo dos certificados da ECR-CV deve conter o OID da rsaEncryption.

7.1.3.2 Os certificados das EC's subordinadas devem conter o OID da rsaEncryption correspondente.

7.1.4 Formatos de nome

7.1.4.1 Para os certificados da ECR-CV os nomes do titular e do emissor do certificado, que constam do campo "Distinguished Name" (DN), coincidem e seguem o padrão ITU-T X.501/ISO/IEC 9594-2, como abaixo descrito:

a) Para o certificado da cadeia V1:

```
C = "CV"
O = "ICP-CV"
OU = "ANAC-Agencia Nacional das Comunicacoes"
CN = "Entidade de Certificacao Raiz de Cabo Verde 001"
```

b) Para o certificado da cadeia V2:

```
C = "CV"
O = "ICP-CV"
OU = "Agencia Reguladora Multissectorial da Economia -ARME"
CN = "Entidade de Certificacao Raiz de Cabo Verde 002"
```

c) Para o certificado da Cadeia SSL:

```
C = "CV"
O = "ICP-CV"
OU = "Agencia Reguladora Multissectorial da Economia -ARME"
CN = "Entidade de Certificacao Raiz de Cabo Verde SSL 001"
```

7.1.4.2 Os nomes do titular e do emissor do certificado de AC de nível imediatamente subsequente ao da ECR-CV, constantes do campo "*Distinguished Name*" (DN), seguem o padrão ITU-T X.501/ISO/IEC 9594-2, da seguinte forma:

a) DN do titular:

```
C = "CV"
O = "ICP-CV"
OU = <CN da cadeia>
CN = <nome da EC subordinada>
```

b) DN do emissor:

```
C = "CV"
O = "ICP-CV"
OU = "Agencia Reguladora Multissectorial da Economia -ARME"
CN = <CN da cadeia>
```

7.1.5. Restrições de nome

7.1.5.1. Não são admitidos caracteres especiais ou de acentuação nos campos do DN.

7.1.5.2. O nome da EC titular do certificado é definido durante o processo de credenciamento.

7.1.6 OID (Object Identifier) da DPC

O OID desta DPC é 2.16.132.1.3.1.1.

7.1.7 Uso da extensão "Policy Constraints"

Não se aplica no contexto da ECR-CV. Se a EC subordinada emite certificados para usuários finais a extensão "Policy Constraints", opcionalmente, pode ser utilizada na forma definida pela RFC 5280.

7.1.8 Sintaxe e semântica dos qualificadores de política

Os certificados emitidos pela ECR-CV implementam qualificadores de políticas para a extensão "Certificate Policies", de acordo com o número 7.1.2 desta DPC.

7.1.9 Semântica de processamento para as extensões críticas de PC

Não se aplica.

7.2. Perfil de LCR

Os certificados das EC's subordinadas devem ter as suas validades verificadas pela LCR da ECR-CV antes de serem utilizados. Também deve ser verificada a autenticidade da LCR da ECR-CV por meio da verificação da sua assinatura e do período de validade da LCR.

7.2.1 Número(s) da versão

A LCR da ECR-CV é definida de acordo com a versão 2 do padrão ITU X.509.

7.2.2 Extensões de LCR e de suas entradas

A LCR emitida pela ECR-CV implementa as seguintes extensões previstas na RFC 5280:

a) ***AuthorityKeyIdentifier***: contém o mesmo valor do campo "*Subject Key Identifier*";

b) ***cRLNumber***: contém um número sequencial para cada LCR emitida.

7.3. Perfil de OCSP

Não se aplica

7.3.1. Número(s) de versão

Não se aplica

7.3.2. Extensões de OCSP

Não se aplica

8. Auditoria de conformidade e outras avaliações

Por determinação do CG da ICP-CV, entidades externas podem realizar inspeções regulares para verificação de conformidade da DPC e o processo operacional da ECR-CV com a legislação nacional. O Grupo de Trabalho de Auditoria de Sistemas da ECR-CV, tem a

responsabilidade de, periodicamente, verificar aplicação das regras, procedimentos, cerimónias e aplicação processos durante as operações da ECR-CV.

8.1. Frequência e motivação das auditorias

As entidades integrantes da ICP-CV, durante o processo de credenciamento passam por uma auditoria pré-operacional, e são obrigadas a realizar auditorias anuais, para fins de manutenção de credenciamento.

8.2. Identificação/Qualificação do avaliador

As fiscalizações das entidades integrantes da ICP-CV são realizadas por entidades acreditadas de acordo com os Requisitos para a Credenciação de Organismos de Certificação

8.3. Relação do avaliador com a entidade avaliada

As Auditorias à ECR-CV são realizadas por entidades indicadas pelo CG da ICP-CV. As auditorias das restantes entidades integrantes da ICP-CV, podem ser realizadas pela Autoridade Credenciadora ou por entidade acreditada de acordo com os Requisitos para a Credenciação de Organismos de Certificação.

8.4. Tópicos cobertos pela avaliação

Os tópicos cobertos pela avaliação devem estar em conformidade com a legislação, o documento Requisitos para Prestadores Qualificados de Serviços de Confiança e de acordo com outros normativos da ICP-CV, bem como as regulamentações aplicáveis para Auditoria WebTrust.

8.5. Ações e medidas resultantes de uma não conformidade

Se numa auditoria forem detetadas não conformidades, a autoridade credenciadora estipula os prazos para correção das mesmas e determina a marcação de uma nova ação de fiscalização.

8.6. Comunicação dos resultados

A comunicação dos resultados deve ser conforme o estipulado no documento "Requisitos para Prestadores Qualificados de Serviços de Confiança". .

9. OUTROS NEGÓCIOS E ASSUNTOS JURÍDICOS

9.1. Tarifas

9.1.1. Tarifas de emissão e renovação de certificados

As tarifas de emissão e de renovação de certificado pela ECR-CV, são fixadas pela ARME nos termos da legislação em vigor.

9.1.2. Tarifas de acesso ao certificado

Não se aplica.

9.1.3. Tarifas de revogação ou de acesso à informação de status

Não se aplica.

9.1.4. Tarifas para outros serviços

As tarifas para outros serviços da ECR-CV são definidas em documento próprio elaborado pela ARME, de acordo com a legislação em vigor.

9.1.5. Política de reembolso

Não se aplica.

9.2. Responsabilidade Financeira

A responsabilidade da ECR-CV é verificada conforme previsão constante da legislação.

9.2.1. Cobertura do seguro

Não se aplica.

9.2.2. Outros ativos

Não se aplica.

9.2.3. Cobertura de seguros ou garantia para entidades finais

Não se aplica.

9.3. Confidencialidade da informação do negócio

9.3.1. Âmbito de informações confidenciais

9.3.1.1. Como princípio geral, todo documento, informação ou registo que contenha dados pessoais fornecidos à ECR-CV é considerado confidencial, salvo quando expressamente autorizado pelo respetivo titular.

9.3.1.2. As informações no âmbito da ECR-CV não são copiadas, reproduzidas, armazenadas, traduzidas ou transmitidas a terceiras partes por quaisquer meios sem antes haver o consentimento escrito do Conselho Executivo da ECR-CV.

9.3.2. Informações fora do âmbito de informações confidenciais

9.3.2.1 Os Certificados, as LCR's e as informações corporativas ou pessoais que necessariamente façam parte deles ou de diretórios públicos são consideradas informações não confidenciais.

9.3.2.3 A ECR-CV pode divulgar informações por tipo e quantidade de certificados ou carimbos de tempo emitidos no âmbito da ICP-CV.

9.3.3. Proteção de informações confidenciais

No âmbito da ECR-CV o acesso a informações confidenciais deve ser efetuado por meios que asseguram a sua proteção e a confidencialidade, evitando o seu uso ou divulgação a terceiros, sob pena de responsabilização, na forma da lei.

9.4. Privacidade da informação pessoal

9.4.1. Mecanismos de proteção de privacidade

A ECR-CV assegura que são implementados mecanismos de proteção de dados pessoais, conforme legislação em vigor.

9.4.2. Tratamento de Dados Pessoais

Como princípio geral, todo documento, informação ou registo que contenha dados pessoais fornecido à ECR-CV será considerado confidencial, salvo quando houver norma que permita a divulgação de informação ou quando expressamente autorizado pelo respetivo titular.

9.4.3. Informações não consideradas dados pessoais

Informações sobre revogação de certificados de EC's subordinadas são fornecidas na LCR da ECR-CV.

9.4.4. Responsabilidade pela proteção de informação.

A ECR-CV é responsável em caso de pela divulgação indevida de informações confidenciais, nos termos da legislação aplicável.

9.4.5. Aviso e consentimento para utilização de dados pessoais.

9.4.5.1. Os dados pessoais obtidas pela ECR-CV podem ser utilizadas ou divulgadas a terceiros mediante autorização expressa do respetivo titular, conforme legislação em vigor.

9.4.5.2. O titular de certificado e seu representante legal terão amplo acesso a quaisquer dos seus dados pessoais e identificações, e poderão autorizar a divulgação de seus registos a outras pessoas.

9.4.5.3. Autorizações formais podem ser apresentadas de duas formas:

a) por meio eletrônico, contendo assinatura válida garantida por certificado reconhecido pela ICP-CV; ou

b) por meio de pedido escrito assinado e com carimbo institucional.

9.4.6. Divulgação em processo judicial ou administrativo

9.4.6.1. Como regra geral, nenhum documento, informação ou registo sob a guarda da ECR-CV será fornecido a terceiros, salvo ao seu titular ou o seu representante legal, devidamente constituído e com poderes específicos, sendo que é vedada a transferência de poderes de representação.

9.4.6.2. As informações privadas ou confidenciais sob a guarda da ECR-CV podem ser utilizadas para a instrução de processo administrativo ou judicial, ou por ordem judicial ou da autoridade administrativa competente, observada a legislação aplicável quanto ao sigilo e proteção dos dados perante terceiros.

9.4.7. Outras circunstâncias de divulgação de informação

Não se aplica.

9.5. Direitos de Propriedade Intelectual

De acordo com a legislação vigente.

9.6. Declarações e Garantias

9.6.1. Declarações e Garantias da ECR-CV

A ECR-CV declara e garante que:

9.6.1.1. Autorização para certificado

A ECR-CV e EC's subordinadas no âmbito da ICP-CV, implementam procedimentos para verificar a autorização para a emissão de um certificado, de acordo com os números 3 e 4 desta DPC.

A autoridade credenciadora, no âmbito da autorização concedida pelo CG da ICP-CV, analisa, audita e fiscaliza os processos de emissão de certificados pelas EC's subordinadas, com base nas suas DPCs, PC's e normas complementares.

9.6.1.2. Precisão da informação

A ECR-CV e EC's subordinadas implementam procedimentos para verificar a precisão da informação publicada nos seus certificados, conforme as normas aprovadas no âmbito da ICP-CV.

9.6.1.3. Identificação do requerente

A ECR-CV e EC's subordinadas implementam procedimentos para verificar identificação dos requerentes contida nos certificados, conforme os números 3 e 4 desta DPC.

9.6.1.4. Consentimento dos titulares

A ECR-CV e EC's subordinadas implementam termos de consentimento de acesso a informação e de titularidade, nos termos da legislação em vigor.

9.6.1.5. Serviço

O acesso ao repositório da ECR-CV, que contém informação sobre os seus certificados e LCR's, encontra-se disponível 24x7.

9.6.1.6. Revogação

A revogação de certificado no âmbito da ICP-CV é realizada pela ECR-CV pelas razões especificadas na legislação em vigor e nos documentos Baseline Requirements, EV Guidelines e/ou EV Code Signing Guidelines.

9.6.1.7. Existência Legal

Esta DPC está em conformidade legal com a legislação aplicável.

9.6.2. Declarações e Garantias da UR

Não se aplica.

9.6.3. Declarações e garantias do titular

9.6.3.1. Toda a informação necessária para a identificação de uma EC titular de um certificado deve ser fornecida de forma completa e precisa. Ao aceitar o certificado emitido pela ECR-CV, a EC subordinada é responsável pelas informações que constam do certificado e por ela fornecidas.

9.6.3.2. A EC titular deve informar à ECR-CV qualquer comprometimento de sua chave privada e solicitar a imediata revogação do seu certificado.

9.6.4. Declarações e garantias das terceiras partes

9.6.4.1. As terceiras partes devem:

a) recusar a utilização do certificado para fins diversos dos previstos nesta DPC; e

b) verificar, a qualquer tempo, a validade do certificado.

9.6.4.2. O certificado da ECR-CV ou um certificado de uma EC subordinada é considerado válido quando:

a) O seu emissor for a ECR-CV;

b) Não constar da última LCR da ECR-CV;

c) Não estiver expirado; e

d) Puder ser verificado com o uso do certificado válido da ECR-CV.

9.6.4.3. A utilização ou aceitação de certificados para outros fins que não se encontram descritos na DPC e PC é por conta e risco da terceira parte que usar ou aceitar a utilização do respetivo certificado.

9.6.5. Representações e garantias de outros participantes

Não se aplica.

9.7. Isenção de garantias

Não se aplica.

9.8. Limitações de responsabilidades

A ECR-CV não responde pelos danos que não lhe sejam imputáveis ou a que não tenha dado causa, na forma da legislação em vigor.

9.9. Indemnizações

A ECR-CV responde pelos danos que der causa, e lhe sejam imputáveis, nos termos da legislação em vigor.

9.10. Prazo e Rescisão

Esta DPC entra em vigor a partir da sua aprovação pelo CG da ICP-CV e consequente publicação no B.O.

9.10.1. Término

Esta DPC vigora pelo período de um ano, pode ser corrigida, alterada e publicada como uma nova versão.

9.10.2. Efeitos da rescisão e sobrevivência

9.10.2.1. Os atos praticados com base nesta DPC são válidos e eficazes para todos os fins, produzindo efeitos mesmo após a sua revogação, extinção ou substituição.

9.10.2.2. No caso de descredenciamento de uma EC subordinada, os procedimentos adotados são os constantes do documento "Requisitos para Prestadores Qualificados de Serviços de Confiança" da ICP-CV.

9.10.2.3. No caso de descredenciamento da ECR-CV, o CG da ICP-CV, delibera, comunica às partes interessadas e publica sua decisão, fundamentada no B.O.

9.11. Avisos individuais e comunicações com os participantes

As notificações, intimações, solicitações ou qualquer outra comunicação necessária sujeita às práticas descritas nesta DPC serão feitas, preferencialmente, por e-mail assinado digitalmente, ou, na sua impossibilidade, por nota oficial da ECR-CV, assinada pelo seu Conselho Exeutivo ou através de publicação no B.O.

9.12. Alterações

9.12.1. Procedimento para emendas

Qualquer alteração nesta DPC deve ser submetida à aprovação do CG da ICP- CV.

9.12.2. Mecanismo de notificação e períodos

Mudança nesta DPC será publicado no B.O e no site da ECR-CV.

9.12.3. Circunstâncias na qual o OID deve ser alterado.

Não se aplica.

9.13. Solução de conflitos

Os litígios decorrentes desta DPC serão solucionados de acordo com a legislação vigor.

9.14. Legislação aplicável

Esta DPC cumpre as disposições constante no Decreto-lei n.º 27/2023, de 20 de outubro, e do Decreto-lei n.º 44/2009, de 09 de novembro, bem como está conforme a legislação aplicada em outras matérias em Cabo Verde.

9.15. Conformidade com a Lei aplicável

As operações executadas no âmbito da ECR-CV estão em conformidade com o Decreto-lei n.º 44/2009, de 09 de novembro

9.16. Disposições Diversas

9.16.1. Acordo completo

Esta DPC representa as obrigações e deveres aplicáveis à ECR-CV. Em caso de divergências entre esta DPC e outras resoluções do CG da ICP-CV, prevalecerá sempre versão mais recente aprovada e publicada.

9.16.2. Cessão

Não se aplica.

9.16.3. Autonomia das cláusulas

9.16.3.1. No caso em que uma ou mais cláusulas deste documento sejam inválidas ou nulas, em termos jurídicos, deverão ser consideradas como não efectivas.

9.16.3.2. A situação anterior é válida, apenas e só nos casos em que tais estipulações não sejam consideradas essenciais. É responsabilidade do CG a avaliação da essencialidade das mesmas.

9.16.4. Execução (honorários dos advogados e renúncia de direitos)

De acordo com a legislação vigente.

9.17 Outras provisões

Não se aplica.