Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação

Políticas

PJ.CNICV_24.1.1_0002_pt_eID

Versão: 4.0

Data: 08/06/2021

Classificação: Público

Identificador do documento: PJ.CNICV_24.1.1_0002_pt_eID

Título: Declaração de Práticas de Certificação da EC do Cartão Nacional de Identificação

Língua original: Português

Nível de acesso: Público

Data: 08/06/2021

Versão atual: 4.0

Histórico de Versões

ID Documento	Data	Detalhes	Autor(es)
1.0	01/07/2010	Versão inicial	MULTICERT
1.1	23/05/2017	Revisão 2017	MULTICERT
1.2	03/10/2017	Atualização de URLs na seção 3.3 Publicação e Repositório e atualização do URL do serviço OCSP	MULTICERT
2.0	02/12/2017	Versão Final	MULTICERT
3.0	10/2019	Revisão anual (sem alterações registadas)	INCM
4.0	06/2021	Revisão anual INCM (corrções textuais, não foram vetificadas alterações tecnicas)	MULTICERT/INCM

Documentos Relacionados

ID Documento	Detalhes	Autor(es)
PJ.CNICV_24.1.2_0009_pt_eID.pdf	Política de Certificados de Assinatura Digital Qualificada	MULTICERT S.A.
PJ.CNICV_24.1.2_0011_pt_eID.pdf	Política de Certificados de Autenticação	MULTICERT S.A.
PJ.CNICV_24.1.2_0010_pt_eID.pdf	Política de Certificados de Validação *on-line* OCSP	MULTICERT S.A.

Apêndices

ID Documento	Detalhes	Autor(es)
PJ.CNICV_53.2.1_0003_pt_eID.doc	Formulário de emissão de certificado de equipamento tecnológico pela EC de Identificação Civil Eletrónica	MULTICERT S.A.
PJ.CNICV_53.2.4_0003_pt_eID.doc	Formulário de receção de certificado de equipamento tecnológico emitido pela EC de Identificação Civil Eletrónica	MULTICERT S.A.
PJ.CNICV_53.2.2_0002_pt_eID.doc	Formulário de revogação de certificado emitido pela EC de Identificação Civil Eletrónica	MULTICERT S.A.

Resumo Executivo

Decorrente da implementação de vários programas públicos para a promoção das tecnologias de informação e comunicação, e a introdução de novos processos de relacionamento em sociedade, entre cidadãos, empresas, organizações não-governamentais e o Estado, com vista ao fortalecimento da sociedade de informação e do governo eletrónico (*eGovernment*), o Cartão Nacional de Identificação (CNI) fornece os mecanismos necessários para a autenticação digital forte da identidade do Cidadão perante os serviços da Administração Pública, assim como as assinaturas eletrónicas indispensáveis aos processos de desmaterialização que estão a ser disponibilizados pelo Estado.

A infraestrutura da Entidade de Certificação de Identificação e Autenticação Civil da República de Cabo Verde (ICP-CNICV) fornece uma hierarquia de confiança, promovendo a segurança eletrónica do Cidadão no seu relacionamento com o Estado. A Entidade de Certificação de Identificação e Autenticação Civil da República de Cabo Verde (EC IAC) estabelece uma estrutura de confiança eletrónica que proporciona a realização de transações eletrónicas seguras, a autenticação forte, um meio de assinar eletronicamente transações ou informações e documentos eletrónicos, assegurando a sua autoria, integridade e não repúdio, e assegurando a confidencialidade das transações ou informação.

A hierarquia de confiança da Entidade de Certificação de Identificação e Autenticação Civil de Cabo Verde encontra-se englobada na hierarquia da Infraestrutura de Chaves Pública da República de Cabo Verde (ICP-CV).

Este documento define os procedimentos e práticas utilizadas pela Entidade Certificadora do Cartão Nacional de Identificação de Cabo Verde no suporte à sua atividade de certificação digital, sendo referenciado como o documento de Declaração de Práticas de Certificação da Entidade Certificadora do Cartão Nacional de Identificação de Cabo Verde.

Conteúdo

1. DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO DA ENTIDADE DE CERTIFICAÇÃO DO CARTÃO NACIONAL DE IDENTIFICAÇÃO (EC EID)

1.1. Objetivo e Âmbito

O objetivo deste documento é definir os procedimentos e práticas utilizadas pela Entidade Certificadora do Cartão Nacional de Identificação de Cabo Verde no suporte à sua atividade de certificação digital.

1.1. Público-Alvo

Este documento deve ser lido por:

- Recursos humanos atribuídos aos grupos de trabalho da Entidade de Certificação de Identificação e Autenticação Civil,
- Terceiras partes encarregues de auditar a Entidade de Certificação de Identificação e Autenticação Civil,
- Todo o público, em geral.

1.2. Estrutura do Documento

Este documento segue a estrutura definida e proposta pelo grupo de trabalho PKIX do IETF[1], no documento RFC 3647[2], de acordo também com a estrutura recomendada pelo ICP-CV.

2. DEFINIÇÕES E ACRÓNIMOS

2.1. Acrónimos

ACRÓNIMO	DESCRIÇÃO
ANAC	Agencia Nacional das Comunicações
ANSI	*American National Standards Institute*
CA	*Certification Authority* (o mesmo que EC)
CN	*Common Name*

1 The Internet Engineering Task Force
[2] *cf.* RFC 3647. 2003, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

ACRÓNIMO	DESCRIÇÃO
CRL	Ver LCR
DL	Decreto-Lei
DN	*Distinguished Name*
DPC	Declaração de Práticas de Certificação
DPVC	Declaração de Práticas de Validação Cronológica
EC	Entidade de Certificação
EC Raiz	Entidade Certificadora Raiz da IPC-CV
eID	*Electronic identification*
GMT	Tempo Médio de Greenwich (*Greenwich Mean Time*)
IAC	Identificação e Autenticação Civil
ICP-CV	Infraestrutura de Chaves Públicas da República de Cabo Verde
LCR	Lista de Revogação de Certificados
MAC	*Message Authentication Codes*
OCSP	*Online Certificate Status Protocol*
OID	Identificador de Objeto
OU	*Organization Unit*
PC	Política de Certificado
PKCS	*Public-Key Cryptography Standards*
PKI	*Public Key Infrastructure* (Infraestrutura de Chave Pública)
SICV-CNI	Sistema de Informação do Ciclo de Vida do Cartão Nacional de identificação

ACRÓNIMO	DESCRIÇÃO
SHA	*Secure Hash Algorithm*
SSCD	*Secure Signature-Creation Device*
TSA	*Time-Stamping Authority* (o mesmo que EVC)

2.2. Definições

DEFINIÇÃO	DESCRIÇÃO
Assinatura digital	Modalidade de assinatura eletrónica avançada baseada em sistema criptográfico assimétrico composto de um algoritmo ou série de algoritmos, mediante o qual é gerado um par de chaves assimétricas exclusivas e interdependentes, uma das quais privada e outra pública, e que permite ao titular usar a chave privada para declarar a autoria do documento eletrónico ao qual a assinatura é aposta e concordância com o seu conteúdo e ao destinatário usar a chave pública para verificar se a assinatura foi criada mediante o uso da correspondente chave privada e se o documento eletrónico foi alterado depois de aposta a assinatura.
Assinatura eletrónica	Resultado de um processamento eletrónico de dados suscetíveis de constituir objeto de direito individual e exclusivo e de ser utilizado para dar a conhecer a autoria de um documento eletrónico.
Assinatura eletrónica avançada	Assinatura eletrónica que preenche os seguintes requisitos: i) Identifica de forma unívoca o titular como autor do documento; ii) A sua aposição ao documento depende apenas da vontade do titular; iii) É criada com meios que o titular pode manter sob seu controlo exclusivo; iv) A sua conexão com o documento permite detetar toda e qualquer alteração superveniente do conteúdo deste.
Assinatura eletrónica qualificada	Assinatura digital ou outra modalidade de assinatura eletrónica avançada que satisfaça exigências de segurança idênticas às da

DEFINIÇÃO	DESCRIÇÃO
	assinatura digital baseadas num certificado qualificado e criadas através de um dispositivo seguro de criação de assinatura.
Autoridade Credenciadora	Entidade competente para a credenciação e fiscalização das entidades certificadoras.
Certificado	Documento eletrónico que liga os dados de verificação de assinatura ao seu titular e confirma a identidade desse titular.
Certificado qualificado	Certificado que é emitido por entidade certificadora que reúne os requisitos referidos no Decreto-Lei nº44/2009.
Chave privada	Elemento do par de chaves assimétricas destinado a ser conhecido apenas pelo seu titular, mediante o qual se apõe a assinatura digital no documento eletrónico, ou se decifra um documento eletrónico previamente cifrado com a correspondente chave pública.
Chave pública	Elemento do par de chaves assimétricas destinado a ser divulgado, com o qual se verifica a assinatura digital aposta no documento eletrónico pelo titular do par de chaves assimétricas, ou se cifra um documento eletrónico a transmitir ao titular do mesmo par de chaves.
Credenciação	Ato pelo qual é reconhecido a uma entidade que o solicite e que exerça a atividade de entidade certificadora o preenchimento dos requisitos definidos no presente diploma para os efeitos nele previsto.
Dados de criação de assinatura	Conjunto único de dados, como chaves privadas, utilizado pelo titular para a criação de uma assinatura eletrónica.
Dados de verificação de assinatura	Conjunto de dados, como chaves públicas, utilizado para verificar uma assinatura eletrónica.
Dispositivo de criação de assinatura	Suporte lógico ou dispositivo de equipamento utilizado para possibilitar o tratamento dos dados de criação de assinatura.

DEFINIÇÃO	DESCRIÇÃO
Dispositivo seguro de criação de assinatura	Dispositivo de criação de assinatura que assegure, através de meios técnicos e processuais adequados que, i) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura só possam ocorrer uma única vez e que a confidencialidade desses dados se encontre assegurada; ii) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura não possam, com um grau razoável de segurança, ser deduzidos de outros dados e que a assinatura esteja protegida contra falsificações realizadas através das tecnologias disponíveis; iii) Os dados necessários à criação de uma assinatura utilizados na geração de uma assinatura possam ser eficazmente protegidos pelo titular contra a utilização ilegítima por terceiros; iv) Os dados que careçam de assinatura não sejam modificados e possam ser apresentados ao titular antes do processo de assinatura.
Documento eletrónico	Documento elaborado mediante processamento eletrónico de dados.
Endereço eletrónico	Identificação de um equipamento informático adequado para receber e arquivar documentos eletrónicos.
Estampilha temporal	Estrutura de dados que liga a representação eletrónica de um *datum* com uma data/hora particular, estabelecendo evidência de que o *datum* existia nessa data/hora.
Parte confiante	Receptor de uma estampilha temporal que confia na mesma.
Sistema TSA (*TSA system*)	Composição de produtos IT e componentes, organizados de modo a suportar o fornecimento de serviços de validação cronológica.
UTC (*Coordinated Universal Time*)	Escala de tempo baseada no segundo, como definido na *ITU-R Recommendation TF.460-5* [10].
UTC(k)	Escala de tempo fornecida pelo laboratório "k" que garante ±100 ns em relação ao UTC (conforme *ITU-R Recommendation TF.536-1*)

DEFINIÇÃO	DESCRIÇÃO
Validação cronológica	Declaração de uma EVC que atesta a data e hora da criação, expedição ou receção de um documento eletrónico.

3. CONTEXTO GERAL

O presente documento é uma Declaração de Práticas de Certificação, ou DPC, cujo objetivo se prende com a definição de um conjunto de práticas para a emissão e validação de Certificados e para a garantia de fiabilidade desses mesmos certificados. Não se pretende nomear regras legais ou obrigações, mas antes informar, pretendendo-se que este documento seja simples, direto e entendido por um público alargado, incluindo pessoas sem conhecimentos técnicos ou legais.

Este documento descreve as práticas gerais de emissão e gestão de Certificados seguidas pela Entidade Certificadora do Cartão Nacional de Identificação de Cabo Verde (EC eID) e, explica o que um certificado fornece e significa, assim como os procedimentos que deverão ser seguidos por Partes Confiantes e por qualquer outra pessoa interessada para confiarem nos certificados emitidos pela EC eID. Este documento pode sofrer atualizações regulares e está sujeito a revisões anuais.

Os Certificados emitidos pela EC eID contêm uma referência à DPC de modo a permitir que Partes confiantes e outras pessoas interessadas possam encontrar informação sobre o certificado e sobre a entidade que o emitiu.

4. ENQUADRAMENTO

As práticas de criação, assinatura e de emissão de Certificados, assim como de revogação de certificados inválidos levadas a cabo por uma Entidade de Certificação (EC) são fundamentais para garantir a fiabilidade e confiança de uma infraestrutura de Chaves Públicas (“PKI”).

Esta DPC aplica-se especificamente à EC eID (de acordo com a estrutura recomendada pela ICP-CV) e respeita e implementa os seguintes *standards*:

- *RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework,*
- *RFC 5280 - Internet X.509 PKI - Certificate and CRL Profile*.

Esta DPC satisfaz os requisitos impostos pela Declaração de Práticas de Certificação da ECR CV e específica como implementar os seus procedimentos e controlos, e ainda como a EC eID atinge os requisitos especificados.

4.1. Identificação do Documento

Este documento é a Declaração de Práticas de Certificação da EC eID. A DPC é representada num certificado através de um número único designado de "identificador de objeto" (OID), sendo o valor do OID associado a este documento apresentado na tabela a abaixo. O OID da Política de Certificado é utilizado de acordo com o explicitado na secção 6.1.2.

Este documento é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 4
Estado do Documento	Versão Final
OID	2.16.132.1.3.2.1.1.1
Data de Emissão	Junho 2021
Validade	1 ano
Localização	http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf

4.2. Participantes na Infraestrutura de Chave Pública

4.2.1. Entidades Certificadoras

A EC eID insere-se na hierarquia de confiança da ICP-CV (Infraestrutura de Chaves Públicas da República de Cabo Verde), constituindo-se numa entidade subordinada do Estado, sendo o seu certificado assinado pela Entidade de Certificação de Identificação e Autenticação Civil (EC IAC). Deste modo, a EC eID encontra-se dois níveis abaixo da EC Raiz de Cabo Verde. A sua função principal providenciar a gestão de serviços de certificação: emissão, operação, suspensão, revogação para os seus subscritores.

A EC eID emite certificados de,

- Assinatura Digital Qualificada do Cidadão e do Residente;

- Autenticação para o Cidadão e do Residente;
- Serviços do Cartão Nacional de Identificação, i.e., certificados para serviços necessários no âmbito do Cartão Nacional de identificação:
    - Validação *on-line* OCSP.

4.2.2. Unidades de Registo

As Unidades de Registos (UR) são entidades que, por via do estabelecimento de um acordo com uma EC, estas delegam a prestação de serviços de identificação e registo de utilizadores, bem como a gestão de pedidos de revogação de certificados.

As ERs desenvolvem a sua atividade de acordo com o estabelecido na DPC da respetiva EC, devem estar obrigatoriamente vinculadas a uma EC e também passam pelo processo de credenciamento junto da ANAC.

O Sistema de Informação Ciclo de Vida do Cartão Nacional de Identificação (denominado em diante de SICV-CNI) permite o controlo de todo o processo, desde o pedido, até à sua entrega final, passando pela emissão, renovação e cancelamento do Cartão.

O SICV-CNI é uma das componentes intervenientes na estrutura global de suporte à operação do Cartão Nacional de Identificação, sendo responsável pela execução, gestão e controlo dos principais processos administrativos relacionados com o Cartão.

4.2.3. Titulares de certificados

No contexto deste documento o termo subscritor/titular aplica-se a todos os utilizadores finais a quem tenham sido atribuídos certificados por uma EC do Estado ou EC subordinada do Estado.

De acordo com as regras da ANAC[3], são considerados titulares de certificados emitidos pela EC eID, aqueles cujo nome está inscrito no campo *Subject* do certificado e utilizam o certificado e respetiva chave privada de acordo com o estabelecido nas diversas políticas de certificado descritas neste documento, sendo emitidos certificados para as seguintes categorias titulares:

[3] *cf.* ICP-CV Manual Política de Certificados da ICP- secção 1.3.3.1.3.

- Pessoa singular (i.e., Cidadão de Cabo Verde e Residente) – certificados de assinatura digital qualificada e autenticação;
- Equipamentos tecnológicos – certificados de validação *on-line* OCSP.

4.2.3.1. Patrocinador

A emissão de certificados para equipamentos tecnológicos (p.e.: computadores, *firewall*, *routers*, servidores, etc.) é efetuada sempre sob responsabilidade humana, sendo esta entidade designada por patrocinador.

O patrocinador aceita o certificado e é responsável pela sua correta utilização, bem como pela proteção e salvaguarda da sua chave privada.

4.2.4. Partes Confiantes

As partes confiantes ou destinatários são pessoas singulares, entidades ou equipamentos que confiam na validade dos mecanismos e procedimentos utilizados no processo de associação do nome do titular com a sua chave pública, ou seja confiam que o certificado corresponde na realidade a quem diz pertencer.

Nesta DPC, considera-se uma parte confiante, aquela que confia no teor, validade e aplicabilidade do certificado emitido no "ramo" da EC eID da hierarquia de confiança da ICP-CV, podendo ser titular de certificados da comunidade ICP-CV ou não.

4.2.5. Outros participantes

4.2.5.1. Entidade Credenciadora

A Entidade Credenciadora assume o papel de entidade que disponibiliza serviços de auditoria/inspeção de conformidade, no sentido de aferir se os processos utilizados pelas EC nas suas atividades de certificação, estão conformes, de acordo com os requisitos mínimos estabelecidos e legislação vigente.

Como Entidade Credenciadora, compete-lhe a:

a) Condução de auditorias,
b) Gestão do controlo de qualidade de todo o processo de certificação,
c) Fixação de procedimentos e documentação relativa às auditorias,
d) Gestão dos relatórios de auditoria, nomeadamente, na elaboração e receção (quando efetuados por pessoal externo);

e) Fixação de planos de medidas corretivas aplicáveis às entidades certificadoras da ICP-CV,
f) Fixação e acompanhamento de metas para indicadores de qualidade que deverá propor para aprovação da Entidade Credenciadora no contexto de objetivos estratégicos previamente fixados pela própria,
g) Gestão da bolsa de auditores;
h) Apresentação à Entidade Credenciadora de proposta de registo e de rescisão de registo de entidades certificadoras na ICP-CV;
i) Promoção da competência técnica dos auditores.

4.2.5.2. Conselho Gestor do ICP-CV

O Conselho Gestor da ICP-CV é a entidade responsável pela gestão global e administração de toda a infraestrutura de Chaves Públicas da República de Cabo Verde, pela aprovação da integração das Entidades Certificadoras do Estado, e a quem cabe pronunciar-se sobre as políticas e práticas de certificação das entidades certificadoras que integram a ICP-CV.

Compete ao Conselho Gestor da ICP-CV:

a) Definir e aprovar, de acordo com as normas ou especificações internacionalmente reconhecidas, as políticas e as práticas de certificação a observar pelas Entidades Certificadoras que integram a ICP-CV;
b) Garantir que as declarações de práticas de certificação das várias Entidades Certificadoras do Estado, incluindo a Entidade Certificadora Raiz, estão em conformidade com as Políticas de Certificado da ICP-CV;
c) Definir e publicar os critérios para aprovação das entidades certificadoras que pretendam integrar a ICP-CV;
d) Aprovar a integração na ICP-CV das Entidades Certificadoras do Estado que obedeçam aos requisitos estabelecidos no presente diploma e que se enquadrem nos critérios previamente estabelecidos e referidos na alínea anterior;
e) Obter da Autoridade Credenciadora um parecer de auditoria e conformidade sobre as Entidades Certificadoras que se pretendam constituir como Entidades Certificadoras do Estado;
f) Aferir da conformidade dos procedimentos seguidos pelas Entidades Certificadoras do Estado com as políticas e diretivas aprovadas, sem prejuízo das competências legalmente cometidas à Autoridade Credenciadora;

g) Decidir pela exclusão da ICP-CV das Entidades Certificadoras do Estado em caso de não conformidade com as políticas e práticas aprovadas, comunicando tal facto à Autoridade Credenciadora;
h) Pronunciar-se sobre as melhores práticas internacionais no exercício das atividades de certificação eletrónica e propor a sua aplicação.

4.3. Utilização do Certificado

Os certificados emitidos no domínio da EC eID são utilizados, pelos diversos sistemas, aplicações, mecanismos e protocolos, com o objetivo de garantir os seguintes serviços de segurança:

a) Confidencialidade;
b) Integridade;
c) Autenticação e,
d) Não-repúdio.

Estes serviços são obtidos com recurso à utilização de criptografia de chave pública, através da sua utilização na estrutura de confiança que a EC eID e ICP-CV proporcionam. Assim, os serviços de identificação e autenticação, integridade e não-repúdio são obtidos mediante a utilização de assinaturas digitais. A confidencialidade é garantida através dos recursos a algoritmos de cifra, quando conjugados com mecanismos de estabelecimento e distribuição de chaves.

4.3.1. Utilização adequada

Os requisitos e regras definidos neste documento, aplicam-se a todos os certificados emitidos pela EC eID.
Os certificados emitidos para equipamentos tecnológicos, têm como objetivo a sua utilização em serviços de autenticação e no estabelecimento de canais cifrados.

Os certificados emitidos pela EC eID são também utilizados pelas Partes Confiantes para verificação da cadeia de confiança de um certificado emitido sob a EC eID, assim como para garantir a autenticidade e identidade do emissor de uma assinatura digital gerada pela chave privada correspondente à chave pública contida num certificado emitido sob a EC eID.

4.3.2. Utilização não autorizada

Os certificados poderão ser utilizados noutros contextos apenas na extensão do que é permitido pelas regras da ICP-CV e pela legislação aplicável.

Os certificados emitidos pela EC eID não poderão ser utilizados para qualquer função fora do âmbito das utilizações descritas anteriormente.

Os serviços de certificação oferecidos pela EC eID, não foram desenhados nem estão autorizados a ser utilizados em atividades de alto risco ou que requeiram um atividade isenta de falhas, como as relacionadas com o funcionamento de instalações hospitalares, nucleares, controlo de tráfego aéreo, controlo de tráfego ferroviário, ou qualquer outra atividade onde uma falha possa levar à morte, lesões pessoais ou danos graves para o meio ambiente.

4.4. Gestão das Políticas

4.4.1. Entidade responsável pela gestão do documento

A gestão desta política de certificados é da responsabilidade do RNI.

4.4.2. Contacto

Nome	***RNI - Direcção Geral dos Registos, Notariado e Identificação***
Morada	*Avenida da China - Encosta da Achada Santo António* *CP 286 A – Praia*
Correio eletrónico	geral.sniac@sniac.goc.cv / Rita.Ramos@rni.gov.cv
Telefone	**+238 – 333 7214/ 515 9197**

5. DISPOSIÇÕES LEGAIS

5.1. Obrigações e Direitos

5.1.1. Obrigações da EC

A Entidade Certificadora de Identificação Civil Eletrónica está obrigada a:

a) Realizar as suas operações de acordo com esta Política,

b) Declarar de forma clara todas as suas Práticas de Certificação no documento apropriado,

c) Proteger as suas chaves privadas,

d) Emitir certificados de acordo com o *standard* X.509,

e) Emitir certificados que estejam conformes com a informação conhecida no momento de sua emissão e livres de erros de entrada de dados,

f) Garantir a confidencialidade no processo da geração dos dados da criação da assinatura e a sua entrega por um procedimento seguro ao titular,

g) Utilizar sistemas e produtos fiáveis que estejam protegidos contra toda a alteração e que garantam a segurança técnica e criptográfica dos processos de certificação,

h) Utilizar sistemas fiáveis para armazenar certificados reconhecidos que permitam comprovar a sua autenticidade e impedir que pessoas não autorizadas alterem os dados,

i) Arquivar sem alteração os certificados emitidos,

j) Garantir que podem determinar com precisão da data e hora em que emitiu, revogou ou suspendeu um certificado,

k) Empregar pessoal com qualificações, conhecimentos e experiência necessárias para a prestação de serviços de certificação,

l) Revogar os certificados nos termos da secção 7.9 Suspensão e Revogação de Certificados deste documento e publicar os certificados revogados na CRL do repositório da respetiva EC, com a frequência estipulada na secção 7.9.11,

m) Publicar a sua DPC e as Políticas de Certificado aplicáveis no seu repositório garantindo o acesso às versões atuais assim como as versões anteriores,

n) Notificar com a rapidez necessária, os titulares dos certificados em caso da EC proceder à revogação ou suspensão dos mesmos, indicando o motivo que originou esta ação,

o) Colaborar com as auditorias dirigidas pela Autoridade Credenciadora, para validar a renovação das suas próprias chaves,

p) Operar de acordo com a legislação aplicável,

q) Proteger, em caso de existirem, as chaves que estejam sobre sua custódia,

r) Garantir a disponibilidade da CRL de acordo com as disposições da secção 7.10.1.1,

s) Em caso de cessar a sua atividade, deverá comunicar o facto com uma antecedência mínima de três meses a todos os titulares dos certificados emitidos assim como à Autoridade Credenciadora,

t) Cumprir com as especificações contidas na norma sobre Proteção de Dados Pessoais.,

u) Conservar toda a informação e documentação relativa a um certificado reconhecido e as Declarações de Práticas de Certificação vigentes em cada momento e durante vinte anos desde o momento da emissão e,

v) Disponibilizar os certificados da EC eID e da ECR-CV.

5.1.2. Obrigações das Unidades de Registo

As Unidades de Registos (ER) ficam obrigadas a:

a) Garantir a identidade do requerente no ato de pedido de Cartão Nacional de Identificação;

b) Garantir que todos os dados do titular são verdadeiros, verificados através de documentos emitidos por entidades credíveis;

c) Garantir o armazenamento da documentação inerente a cada pedido, em local seguro e por 20 anos;

d) Garantir a entrega do Cartão Nacional de Identificação ao seu titular;

e) Garantir que a alteração de estado de um certificado é comunicado ao seu titular

f) Gerir os pedidos de Revogação;

g) Manter informada a EC, de todo o processo de pedido de Cartão Nacional de Identificação;

h) Manter informada a EC, de todos recursos Humanos que dela faz parte;

i) Executar os procedimentos com base nas regras emitidas pela EC.

5.1.3. Obrigações dos Titulares de Certificados

Os titulares de Certificados emitidos pela EC eID, ficam obrigados a:

a) Limitar e adequar a utilização dos certificados de acordo com as utilizações previstas nas Políticas de Certificado,

b) Tomar todos os cuidados e medidas necessárias para garantir a posse exclusiva da sua chave privada,

c) Solicitar de imediato a revogação de um certificado em caso de ter conhecimento ou suspeita de compromisso da chave privada correspondente à chave pública contida no certificado, de acordo com a secção 7.9.3,

d) Não utilizar um certificado digital que tenha perdido a sua eficácia, quer por ter sido revogado, suspendido ou por ter expirado (excedido o seu período de validade),

e) Submeter às Entidade de Certificação (ou de Registo) a informação que considerem exata e completa com relação aos dados que estas solicitem para realizar o processo de registo. Deve informar a EC de qualquer modificação desta informação e,

f) Não monitorizar, manipular ou efetuar ações de "engenharia inversa" sobre a implantação técnica (*hardware* e *software*) dos serviços de certificação, sem a devida autorização prévia, por escrito, da EC eID.

5.1.4. Obrigações das partes confiantes

É obrigação das partes que confiam nos certificados emitidos pela EC eID:

a) Limitar a fiabilidade dos certificados às utilizações permitidas para os mesmos em conformidade com o expresso na Política de Certificado correspondente,

b) Verificar a validade dos certificados no momento de realizar qualquer operação baseada nos mesmos,

c) Assumir a responsabilidade na correta verificação das assinaturas digitais,

d) Assumir a responsabilidade na comprovação da validade, revogação ou suspensão dos certificados em que confia,

e) Ter pleno conhecimento das garantias e responsabilidades aplicáveis na aceitação e uso de certificados em que confia, aceitar sujeitar-se às mesmas,

f) Notificar qualquer acontecimento ou situação anómala relativa ao certificado, que possa ser considerado como causa de revogação do mesmo, utilizando os meios que a EC eID publique no seu sítio *Web*.

5.1.5. Obrigações do Repositório

O MJT é responsável pelas funções de repositório da EC eID, publicando, entre outras, informação relativa às práticas adotadas e ao estado dos certificados emitidos (LCR).

A plataforma tecnológica do repositório está configurada de acordo com os seguintes indicadores e métricas:

- Disponibilidade de serviços da plataforma de 99,5%, em período 24hx7d, excluindo manutenções necessárias efetuadas em horário de menor utilização, garantindo-se durante o tempo da disponibilidade:
  - Mínimo de 99,990% de respostas a pedidos de obtenção da LCR;
  - Mínimo de 99,990% de respostas a pedidos do documento da DPC;
- Número máximo de pedidos de LCR: 50 pedidos/minuto;
- Número máximo de pedidos da DPC: 50 pedidos/minuto;
- Número médio de pedidos de LCR: 20 pedidos/minuto;
- Número médio de pedidos da DPC: 20 pedidos/minuto.

O acesso à informação disponibilizada pelo repositório é efetuado através do protocolo HTTPS e HTTP, estando implementado os seguintes mecanismos de segurança:

- LCR e DPC só podem ser alterados através de processos e procedimentos bem definidos,
- Plataforma tecnológica do repositório encontra-se devidamente protegida pelas técnicas mais atuais de segurança física e lógica,
- Os recursos humanos que gerem a plataforma têm formação e treino adequado para o serviço em questão.

5.2. Responsabilidades

5.2.1. Responsabilidades da EC

a) A EC eID responde pelos danos e prejuízos que cause a qualquer pessoa em exercício da sua atividade de acordo com o art. 62 do DL 33/2007;

b) A EC eID responde pelos prejuízos que cause aos titulares ou a terceiros pela falta ou atraso na inclusão no serviço de consulta sobre a vigência dos certificados, da revogação ou suspensão dum certificado, uma vez que tenha conhecimento dele;

c) A EC eID assume toda a responsabilidade mediante terceiros pela atuação dos titulares das funções necessárias à prestação de serviços de certificação;

d) A responsabilidade da administração / gestão da EC eID assenta sobre bases objetivas e cobre todo o risco que os particulares sofram sempre que seja consequência do funcionamento normal ou anormal dos seus serviços;

e) A EC eID só responde pelos danos e prejuízos causados pelo uso indevido do certificado reconhecido, quando não tenha consignado no certificado, de forma clara reconhecida por terceiros o limite quanto à possível utilização;

f) A EC eID não responde quando o titular superar os limites que figuram no certificado quanto as suas possíveis utilizações, de acordo com as condições estabelecidas e comunicadas ao titular;

g) A EC eID não responde se o destinatário dos documentos assinados eletronicamente não os comprovar e tiver em conta as restrições que figuram no certificado quanto às suas possíveis utilizações e,

h) A EC eID não assume qualquer responsabilidade no caso de perca ou prejuízo:

   a. Dos serviços que prestam, em caso de guerra, desastres naturais ou qualquer outro caso de força maior,

   b. Ocasionados pelo uso dos certificados quando excedam os limites estabelecidos pelos mesmo na Política de Certificados e correspondente DPC,

   c. Ocasionado pelo uso indevido ou fraudulento dos certificados ou CRL emitidos pela EC eID.

5.2.2. Responsabilidades da Unidade de Registo

Nada a assinalar.

5.3. Publicação e Repositório

O MJT mantém um repositório em ambiente *Web*, permitindo que as Partes Confiantes efetuem pesquisas *on-line* relativas à revogação e outra informação referente ao estado dos Certificados.

É disponibilizada, *online*, 24hx7d a seguinte informação pública:

- Cópia eletrónica do documento de políticas da ICP-CV, assinado eletronicamente, por indivíduo devidamente autorizado e com certificado digital atribuído para o efeito:
    - URI: https://ecrcv.cv

- Cópia eletrónica deste DPC e Políticas de Certificados (PC) mais atuais da EC eID, assinada eletronicamente, por individuo devidamente autorizado e com certificado digital atribuído para o efeito:
    - DPC da EC eID disponibilizada no URI:
        - http://pki.cni.gov.cv/pub/pol/dpc_eceid.html.pdf
    - PC de certificado de Assinatura Digital Qualificada disponibilizada no URI:
        - http://pki.cni.gov.cv/pub/pol/pc_ass.html.pdf
        - http://pki.cni.gov.cv/pub/pol/pc_ass_residente.html.pdf
    - PC de certificado de Autenticação disponibilizada no URI:
        - http://pki.cni.gov.cv/pub/pol/pc_aut.html.pdf
        - http://pki.cni.gov.cv/pub/pol/pc_aut_residente.html.pdf
- LCR da EC eID – URI:
    - http://pki.cni.gov.cv/pub/lrc/eceid<ID_CA>.crl
    - http://pki.cni.gov.cv/pub/lrc/eceid<ID_CA>_delta.crl
- Certificado da EC eID – URI:
    - http://pki.cni.gov.cv/pub/cert/eceid/
- Serviço on-line de verificação de estado de certificado (Online Certificate Status Protocol - OCSP)
    - http://ocsp.eciad.cni.gov.cv/publico/ocsp
- Outra informação relevante – URI:
    - http://pki.cni.gov.cv/

Adicionalmente, serão conservadas todas as versões anteriores das PCs e da DPC da EC eID, disponibilizando-as a quem as solicite (desde que justificado), ficando, no entanto fora do repositório público de acesso livre.

5.3.1. Frequência de Publicação

É garantida a disponibilização da seguinte informação pública *online*, utilizando os mesmos protocolos e garantindo a mesma disponibilidade do repositório da EC eID:

- Cópia eletrónica da última versão da DPC e PC de cada EC subordinada, assinada eletronicamente, por individuo devidamente autorizado e com certificado digital atribuído para o efeito – URI a ser identificado pela EC subordinada;
- LCR de cada EC subordinada – URI a ser identificado pela EC subordinada;
- Certificados da EC subordinada e certificados emitidos por cada EC subordinada, de acordo com a política definida pela EC subordinada na sua DPC.

5.3.2. Controlo de acesso

A informação publicada estará disponível na Internet, sendo sujeita a mecanismos de controlo de acesso (acesso somente para leitura). Estão implementadas medidas de segurança lógica e física para impedir que pessoas não autorizadas possam adicionar, apagar ou modificar registos do repositório.

5.4. Auditoria de Conformidade

Uma inspeção regular de conformidade a esta DPC e a outras regras, procedimentos, cerimónias e processos será levada a cabo pelos membros do Grupo de Trabalho de Auditoria de Sistemas da EC eID.

Para além de auditorias de conformidade, serão efectuadas outras fiscalizações e investigações para assegurar a conformidade da EC eID com a legislação nacional. A execução destas auditorias, fiscalizações e investigações poderá ser delegada a uma entidade externa de auditoria.

5.4.1. Frequência ou motivo da auditoria

As auditorias de conformidade são realizadas anualmente de acordo com a legislação sendo que o Relatório de Auditoria de Segurança é entregue até 31 de Março[4]. A EC precisa de provar, com a auditoria e relatório de segurança anuais (produzidos pelo auditor de segurança acreditado), que a avaliação dos riscos foi assegurada, tendo sido identificado e implementado todas as medidas necessárias para a segurança de informação.

5.4.2. Identidade e qualificações do auditor

O auditor é uma pessoa ou organização, de reconhecida idoneidade, com experiência e qualificações comprovadas na área da segurança da informação e dos sistemas de informação, infraestruturas de chaves pública, familiarizado com as aplicações e programas de certificação digital e na execução de auditorias de segurança.

A Autoridade Credenciadora é responsável pela nomeação do pessoal que realiza a auditoria.

O auditor deverá ser selecionado no momento da realização de cada auditoria, devendo em termos gerais cumprir os seguintes requisitos:

a) Experiência em PKI, segurança e processos de auditoria em sistema de informação,
b) Independência a nível orgânico da Entidade Certificadora (para os casos de auditorias externas),
c) Credenciado pela Entidade Credenciadora.

5.4.3. Relação entre o auditor e a Entidade Certificadora

O auditor e membros da sua equipa são independentes, não atuando de forma parcial ou discriminatória em relação à entidade que é submetida à auditoria.

O auditor de segurança necessita de garantir que nenhum membro da equipa executa funções parciais ou discriminatórias ligadas à Entidade Certificadora nem que trabalhou para a mesma nos últimos três anos.

Na Relação entre o auditor e a entidade submetida a auditoria, deve estar garantido inexistência de qualquer vínculo contratual.

[4] cf. Decreto Regulamentar n.º 18/2007, de 24 de Dezembro.

Entre o Auditor e a parte auditada (Entidade Certificadora) não deve existir nenhuma relação, atual ou prevista, financeira, legal ou de qualquer outro género que possa originar um conflito de interesses.

Deve ser tido em conta por parte do auditor, o cumprimento do estabelecido na legislação em vigor sobre a proteção de dados pessoais, na medida em que o auditor poderá aceder a dados pessoais dos ficheiros dos titulares das EC. O auditor tem de ser independente da entidade de certificação; ter competência reconhecida; experiência e qualificações sólidas na área da segurança de informação, no desempenho de auditorias de segurança e no uso do *standard* ISO 27002 (antiga ISO/IEC 17799).

5.4.4. Âmbito da auditoria

O âmbito das auditorias e outras avaliações inclui a conformidade com a legislação nacional, Políticas emitidas pela ICP-CV, com esta DPC e outras regras, procedimentos e processos (especialmente os relacionados com operações de gestão de chaves, recursos, controlos de gestão e operação e, gestão de ciclo de vida de certificados).

5.4.5. Procedimentos após uma auditoria com resultado deficiente

Se numa auditoria resultarem irregularidades:

- A Entidade Auditada deve estipular prazos para cumprir as irregularidades/não-conformidades detetadas;
- Irregularidades e não-conformidades devem ser dadas a conhecer à Entidade Credenciadora para servirem de referência a futuras fiscalizações;

5.5. Sigilo

5.5.1. Chaves Privadas

As chaves privadas e as chaves públicas são propriedade do titular, independentemente do meio físico utilizado para o seu armazenamento.

O Titular conserva sempre o direito sobre as marcas, produtos ou nome comercial contido no certificado.

5.5.2. Divulgação de Informação de Revogação e de Suspensão de Certificado

A utilização de um certificado deve ser antecedida pela verificação do estado do mesmo, pelas partes confiantes, através das LCR.

O titular é sempre informado sobre a alteração de estado do seu certificado, e, em caso de suspensão ou revogação, qual o seu motivo.

5.5.3. Quebra de sigilo por motivos legais

Documentos, informações ou registos da EC eID apenas serão disponibilizados mediante ordem judicial ou por determinação legal.

5.5.4. Informações a terceiros

Nenhum documento, informação ou registo que esteja sob a guarda do MJT ou qualquer outra entidade, inerente à EC eID, deve ser fornecido a terceiros exceto se estiver devidamente identificado e autorizado a fazê-lo.

5.5.5. Divulgação por solicitação do titular

Não aplicável.

5.5.6. Direitos de propriedade intelectual

Todos os direitos de propriedade intelectual, incluindo os que se referem a certificados e LCR emitidos, OID, DPC e PC, bem como qualquer outro documento, propriedade da EC eID pertencem ao MJT.

6. IDENTIFICAÇÃO E AUTENTICAÇÃO

6.1. Registo Inicial

6.1.1. Disposições Legais

A atribuição de nomes segue a convenção determinada pelo ICP-CV sendo atribuído aos certificados de equipamentos tecnológicos o nome qualificado do domínio e/ou o âmbito da sua utilização (“Serviços do Cartão Nacional de Identificação de Cabo Verde”).

A operação dos certificados emitidos pela EC eID está sempre na dependência do MJT. O patrocinador dos certificados de equipamentos tecnológicos será um colaborador devidamente identificado de um organismo na dependência do MJT.

6.1.2. Tipos de nomes

O certificado da EC eID, assim com os certificados emitidos pela EC eID, é identificado por um nome único (DN – *Distinguished Name*) de acordo com *standard* X.500.

O nome único destes certificados está identificado nas respetivas Políticas de Certificados:

Tipo de Certificado	OID da Política de Certificados
Assinatura Digital Qualificada - Cidadão	**2.16.132.1.2.100. 1.1.1.1**[5]
Assinatura Digital Qualificada – Residente	**2.16.132.1.2.100. 1.1.2.1**[6]
Autenticação – Cidadão	**2.16.132.1.2.101.1.1.1.1**[7]
Autenticação – Residente	**2.16.132.1.2.101.1.1.2.1**[8]
Validação *ON-LINE* (OCSP)	**2.16.132.1.2.2.1.1.1.1**[9]

6.1.3. Necessidade de nomes significativos

A EC eID irá assegurar, dentro do seu "ramo" da hierarquia de confiança do ICP-CV:

- a não existência de certificados que, tendo o mesmo nome único, identifiquem entidades (equipamento) distintas,
- a relação entre o titular e a organização a que pertence é a mesma que consta no certificado e é facilmente percetível e identificável pelos Humanos.

[5] cf. PJ.CNICV_24.1.2_0009_pt_eID - Política de Certificado de Assinatura Digital Qualificada do Cidadão.
[6] cf. PJ.CNICV_24.1.2_0013_pt_eID - Política de Certificados de Assinatura Digital Qualificada do Residente
[7] cf. PJ.CNICV_24.1.2_0011_pt_eID - Política de Certificado de Autenticação.
[8] cf. PJ.CNICV_24.1.2_0012_pt_eID - Política de Certificados de Autenticação do Residente
[9] cf. PJ.CNICV_24.1.2_0010_pt_eID - Política de Certificados de Validação On-line.

6.1.4. Interpretação de formato de nomes

As regras utilizadas pela EC eID para interpretar o formato dos nomes seguem o estabelecido no RFC 5280[10] para certificados emitidos a partir de 31 de Dezembro de 2003, assegurando que todos os atributos *DirectoryString* dos campos *issuer* e *subject* do certificado são codificados numa *UTF8String*, com exceção dos atributos *country* e *serialnumber* que são codificados numa *PrintableString*.

6.1.5. Unicidade de nomes

Os identificadores do tipo DN são únicos para cada titular de certificado emitido dentro da EC eID e de cada uma das suas Entidades de Certificação subordinadas, não induzindo em ambiguidades.

De acordo com os seus processos de emissão, a EC eID rejeita a emissão de certificados com o mesmo DN para titulares distintos. Quando ocorrer tal situação, é permitido a adição de caracteres numéricos ao nome original de cada entidade, de forma a assegurar a unicidade do campo, desde que tal não induza uma parte confiante em ambiguidade.

6.1.6. Procedimento para resolver disputa de nomes

O MJ reserva o direito de tomar todas as decisões no caso da existência de disputa de nomes resultante da igualdade dos mesmos, entre diferentes pedidos de certificado.

6.1.7. Reconhecimento, autenticação, e função das marcas registadas

As entidades requisitantes de certificados, devem demonstrar que têm direito à utilização do nome requisitado, não podendo as designações, usadas nos certificados emitidos pela EC eID, infringir os direitos de propriedade intelectual de outros indivíduos ou entidades.

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

[10] cf. RFC 5280. 2002, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

6.1.8. Método de comprovação da posse de chave privada

No caso das pessoas singulares, o par de chaves e certificado é fornecido em cartão com chip criptográfico, personalizado fisicamente para o titular. A posse da chave privada é garantida pelo processo de emissão e personalização do cartão chip, pelo Sistema de Ciclo de Vida, que garante:

- O par de chaves é gerado em HSM criptográfico e importado para o chip criptográfico do cartão no ato da personalização do cartão para o seu titular.
- A Chave pública é enviada à EC para emissão do certificado digital correspondente, sendo este também personalizado no cartão,
- Cartão é entregue ao titular por método "cara-a-cara" (cf. Secção 7.2.2.1).

No caso do equipamento tecnológico, a comprovação da posse da chave privada será garantida através da presença física do patrocinador (ver secção 4.2.3.1), que apresentará o pedido de certificado no formato PKCS#10, cf. secção 6.1.10.1.

6.1.9. Autenticação da identidade de uma pessoa singular

O processo de autenticação da identidade de uma pessoa singular, garante que a pessoa singular para quem vai ser emitido o certificado é quem na realidade diz ser – este processo é efetuado pelo SICV-CNI. No âmbito dos processos "Pedido Inicial e Renovação", o SICV-CNI suporta as atividades relacionadas com a recolha e validação de dados biográficos e biométricos do cidadão, de modo a registar o pedido para emissão do Cartão Nacional de Identificação (e respetivos certificados digitais). Prevê também as funcionalidades de suporte à ocorrência de erros nas diversas ações de validação, de modo a suportar os procedimentos a realizar em cada situação, quer pelo funcionário, quer pelo Cidadão.

O procedimento de autenticação da pessoa singular, que solicita o Cartão Nacional de Identificação, está descrito na Política de Certificado correspondente (secção 5.3), sendo elas:

- Política de Certificado de Autenticação do Cidadão,
- Política de Certificado de Autenticação do Residente,
- Política de Certificado de Assinatura Eletrónica Qualificada do Cidadão,
- Política de Certificado de Assinatura Eletróncia Qualificada do Residente.

6.1.10. Autenticação da identidade de uma pessoa coletiva

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 de assinatura exige a intervenção de pessoas singulares que, estatutariamente, representam essa pessoa coletiva.

6.1.10.1. Certificado de equipamento tecnológico

O procedimento de autenticação da pessoa coletiva, que solicita o certificado para os serviços complementares do Cartão Nacional de Identificação, está descrito na Política de Certificado correspondente.

6.1.11. Informação de subscritor/titular não verificada

Toda a informação descrita no ponto 6.1.10.1 é verificada.

6.1.12. Validação de Autoridade

Nada a assinalar.

6.2. Critérios para interoperabilidade

De acordo com DPC da ECR-CV.

6.3. Identificação e Autenticação para pedidos de renovação de chaves

A identificação e autenticação para a renovação de certificados são realizadas utilizando os procedimentos para a autenticação e identificação inicial.

6.3.1. Identificação e autenticação para renovação de chaves, de rotina

Não existe renovação de chaves, de rotina. A renovação de certificados utiliza os procedimentos para a autenticação e identificação inicial, onde são gerados novos pares de chaves.

6.3.2. Identificação e autenticação para renovação de chaves, após 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.

6.4. Identificação e autenticação para pedido de revogação

Qualquer entidade integrada no domínio da ICP-CV, pode solicitar a revogação de um determinado certificado, havendo conhecimento ou suspeita de compromisso da chave privada do titular ou qualquer outro ato que recomende esta ação[11].

A EC eID guarda toda a documentação utilizada para verificação da identidade e autenticidade da entidade que efetua o pedido de revogação, que podem ser, entre outros:

- Titular do certificado, no caso de certificados de pessoa singular;
- Patrocinador nomeado pela entidade, no caso de certificado de equipamento tecnológico;
- Representante legal do MJ, com poderes de representação para o pedido de revogação de certificados;
- Parte confiante, sempre que demonstre que o certificado foi utilizado com fins diferente dos previstos.

Um formulário próprio[11] serve de base ao pedido de revogação de certificado e contém, entre outros, os seguintes elementos de identificação da entidade que inicia o pedido de revogação:

a) Denominação legal;

b) Número de pessoa coletiva, sede, objeto social, nome dos titulares dos corpos sociais e de outras pessoas com poderes para a obrigarem e número de matrícula na conservatória do registo comercial;

c) Nome completo, número de um documento de identificação que permita a identificação inequívoca da entidade (ou seu representante) que inicia o pedido de revogação;

d) Endereço e outras formas de contacto;

e) Indicação de pedido de revogação, indicando o nome único (DN) atribuído ao certificado, assim como a sua validade;

f) Indicação do motivo para revogação do certificado.

[11] cf. PJ.CNICV_53.2.2_0001_pt_IAC.doc. 2017, Formulário de revogação de certificado emitido pela EC Identificação e Autenticação Civil.

7. REQUISITOS OPERACIONAIS DO CICLO DE VIDA DO CERTIFICADO

7.1. Pedido de Certificado

7.1.1. Requisitos

Devem ser cumpridos os seguintes requisitos quando é feito um pedido de certificado:

- Conformidade com as políticas definidas pela EC eID;
- Pedido de certificado mediante apresentação de um pedido de certificado PKCS#10 válido;

7.1.2. Quem pode subscrever um pedido de certificado

O Sistema de Ciclo de Vida é a única entidade que pode subscrever pedidos de certificados de pessoa singular.

O patrocinador é a única entidade que pode subscrever pedidos de certificados para equipamento tecnológico, que seja utilizado no âmbito do Cartão Nacional de Identificação.

7.1.3. Processo de registo e responsabilidades

O processo de registo de certificado de pessoa singular é da única e total responsabilidade do Sistema de Ciclo de Vida.

O processo de registo de certificado de equipamento tecnológico é constituído pelos seguintes passos, a serem efetuados pela entidade de certificação subordinada requerente:

- Geração do par de chaves (chave pública e privada) pelo patrocinador,
- Geração do PKCS#10 correspondente pelo patrocinador;
- Geração do *hash* (SHA-256[12]) do PKCS#10, em formato PEM, pelo patrocinador;
- Arquivo do PKCS#10 e *hash* em suporte tecnológico não regravável, pelo patrocinador;
- Preenchimento pelo patrocinador do documento de validação da identidade da entidade, de acordo com secção 6.1.10.1;

[12] *cf.* NIST FIPS PUB 180-1. 1995, *The Secure Hash Algorithm (SHA-256). National Institute of Standards and Technology, "Secure Hash Standard", U.S. Department of Commerce*.

- Envio do CD/DVD e do documento corretamente preenchido ao contacto da EC eID

7.2. Processamento do pedido de certificado

7.2.1. Requisitos

Os pedidos de certificado, depois de recebidos pela EC eID, são considerados válidos se os seguintes requisitos forem cumpridos:

a) Receção e verificação de toda a documentação e autorizações exigidas;
b) Verificação da identidade do requisitante;
c) Verificação da exatidão e integridade do pedido de certificado;
d) Criação e assinatura do certificado;
e) Disponibilização do certificado ao titular.

Esta secção juntamente com a 7.3 descrevem detalhadamente todo o processo

7.2.2. Processos para a identificação e funções de autenticação

7.2.2.1. Certificado de pessoa singular

O SICV-CNI é responsável por todos os processos para a identificação e funções de autenticação.

7.2.2.2. Certificado de equipamento tecnológico

A Administração de Segurança da EC eID executa a identificação e a autenticação de toda a informação necessária nos termos da secção 6.1.10.1.

A Administração de Segurança da EC eID aprova a candidatura para um certificado de equipamento tecnológico quando os seguintes critérios são preenchidos:

- Identificação e autenticação, bem sucedida, de toda a informação necessária nos termos da secção 6.1.11 – é guardada toda a documentação utilizada para verificação da identidade e de poderes de representação;
- Formulário de pedido de emissão corretamente preenchido;
- PKCS#10 válido.

Em qualquer outra situação, será rejeitada a candidatura para emissão de certificado.

Após a emissão do certificado, os Administradores de Segurança da EC eID são responsáveis por entregar o certificado e restantes dados necessários pelo método "cara-a-cara" – tal ato é registado através do preenchimento e assinatura de formulário[13].

7.2.3. Aprovação ou recusa de pedidos de certificado

A aprovação de certificado passa pelo cumprimento dos requisitos exigidos nos pontos 7.2.1 e 7.2.2. Quando tal não se verifique, é recusada a emissão do certificado.

7.2.4. Prazo para processar o pedido de certificado

Após a aprovação do pedido de certificado, o certificado deverá ser emitido em não mais do que:

- 10 horas, no caso de certificado de pessoa singular,
- Cinco (5) dias úteis, no caso de certificado de equipamento tecnológico.

7.3. Emissão de Certificado

7.3.1. Procedimentos para a emissão de certificado

7.3.1.1. Certificado de pessoa singular

A emissão do certificado é efetuada como resposta ao pedido do Sistema de Ciclo de Vida.

A emissão dos certificados por parte da EC eID, indica que todos os procedimentos de processamento do pedido foram concluídos com sucesso.

Os procedimentos estabelecidos neste ponto são também aplicados aos casos de renovação de certificados, uma vez que implica a emissão de novos certificados.

A EC eID utiliza um procedimento de geração de certificados, que vincula de forma segura o certificado com a informação de registo, incluindo a chave pública, e protege a confidencialidade e integridade dos dados de registo.

[13] PJ.CNICV_53.2.4_0003_pt_eID.doc, Formulário de receção de certificado de equipamento tecnológico emitido pela EC de Identificação Civil Electrónica

Na infraestrura da PKI são gerados os pares de chaves e emitidos novos certificados pela EC eID associando assim cada chave pública ao cidadão/residente. Os certificados são enviados ao sistema de personalização cumprindo a norma PKCS#10, onde é personalizado um novo Cartão.
Quando a EC eID emite um certificado, efetuará as notificações que se estabelecem no ponto 7.3.2.

O período de vigência dos certificados está sujeito a uma possível extinção antecipada, provisória (suspenso) ou definitiva (revogação), quando se expliquem as causas que a motivem.

Todos os procedimentos relacionados com a emissão e com o estado de certificados são registados e arquivados.

7.3.1.2. Certificado de equipamento tecnológico

A emissão do certificado é efetuada por meio de uma cerimónia que decorre na zona de alta segurança da EC eID e, em que se encontram presentes:

- Dois (2) membros dos Grupo de Trabalho (mínimo)– a segregação de funções não possibilita a presença de um número inferior de elementos,
- Quaisquer observadores, aceites simultaneamente pelos membros dos Grupos de Trabalho e pelos representantes da entidade subordinada requerente (ou patrocinador no caso de certificado de equipamento tecnológico).

A cerimónia de emissão de certificado é constituída pelos seguintes passos:

- Identificação e autenticação de todas as pessoas presentes na cerimónia, garantindo que o(s) membro(s) dos Grupo de Trabalho têm os poderes necessários para os atos a praticar;
- Representante(s) da entidade subordinada requerente (ou patrocinador no caso de certificado de equipamento tecnológico) entregam, em mão, num suporte de armazenamento digital, o certificado e o formulário de emissão do certificado aos membros do Grupo de Trabalho da EC eID. O formulário é datado e assinado pelos membros do Grupo de Trabalho que o devolvem ao(s) representantes da entidade subordinada requerente (ou patrocinador no caso de certificado de equipamento tecnológico);
- Os membros do Grupo de Trabalho da EC eID efetuam o procedimento de arranque de processamento da EC eID e emitem o certificado (correspondente ao PKCS#10 fornecido num suporte tecnológico não regravável (CD/DVD)) em formato PEM;

- Os membros do Grupo de Trabalho da EC eID arquivam o certificado em formato PEM num dispositivo de armazenamento digital e preenchem o formulário de receção e aceitação de certificado[14], em duplicado;
- Após a assinatura de ambas as cópias do formulário de receção e aceitação de certificado pelo(s) representante(s) da entidade subordinada (ou patrocinador no caso de certificado de equipamento tecnológico) e pelos membros do Grupo de Trabalho, os membros do Grupo de Trabalho entregam o CD/DVD com o certificado em formato PEM ao(s) representante(s) da entidade subordinada (ou patrocinador no caso de certificado de equipamento tecnológico).
- A cerimónia de emissão fica terminada com a submissão do novo certificado nos sistemas de suporte e disponibilização no site da PKI;

O certificado emitido inicia a sua vigência no momento da sua emissão.

7.3.2. Notificação da emissão do certificado ao titular

O SICV-CNI é responsável por notificar o titular do certificado de pessoa singular.

A emissão do certificado é efetuada de forma presencial, no caso de certificado de equipamento tecnológico, de acordo com a secção anterior.

7.4. Aceitação do Certificado

7.4.1. Procedimentos para a aceitação de certificado

7.4.1.1. Certificado de pessoa singular

No âmbito do processo de "Entrega", o SICV-CNI suporta as seguintes atividades associadas à identificação do Cartão Nacional de Identificação:

- Entrega;
- Leitura;
- Ativação do cartão;
- Ativação dos certificados digitais;

[14] cf. PJ.CNICV_53.2.4_0001_pt_IAC.doc. 2017, Formulário de receção de certificado de EC subordinada da EC de Identificação e Autenticação Civil.

- Registo da entrega em perfeitas condições ao Cidadão.

Prevê também as funcionalidades de suporte à ocorrência de erros nas diversas atividades associadas à entrega, de modo a suportar os procedimentos a realizar em cada situação, quer pelo funcionário, quer pelo Cidadão, comunicando com outros sistemas como a EC que emitiu o certificado.

7.4.1.2. Certificado de equipamento tecnológico

O certificado considera-se aceite após a assinatura do formulário de emissão e aceitação de certificado pelo(s) representante(s) da entidade subordinada (ou patrocinador no caso de certificado de equipamento tecnológico), de acordo com a cerimónia de emissão.

Note-se que antes de ser disponibilizado o certificado aos representantes (ou patrocinador), e consequentemente lhe serem disponibilizadas todas as funcionalidades na utilização da chave privada e certificado, é garantido que,

a) O titular toma conhecimento dos seus direitos e responsabilidades;

b) O titular toma conhecimento das funcionalidades e conteúdo do certificado;

c) O titular aceita formalmente o certificado e as suas condições de utilização assinando para o efeito o Termo de Responsabilidade do Titular.

No termo de responsabilidade do titular constam os procedimentos necessários em caso de expiração, revogação e renovação do certificado, bem como os termos, condições e âmbito de utilização do mesmo.

7.4.2. Publicação do certificado

A EC eID não publica os certificados emitidos, disponibilizando-o integralmente ao titular (ou patrocinador), com os constrangimentos definidos no ponto 7.4.1.

7.4.3. Notificação da emissão de certificado a outras entidades

Nada a assinalar.

7.5. Uso do certificado e par de chaves

7.5.1. Uso do certificado e da chave privada pelo titular

Os titulares de certificados utilizarão a sua chave privada apenas e só para o fim a que estas se destinam (conforme estabelecido no campo do certificado "*keyUsage*") e sempre com propósitos legais.

A sua utilização apenas é permitida:

a) A quem estiver designado no campo "*Subject*" do certificado;

b) De acordo com as condições definidas nos pontos 4.3.1 e 4.3.2;

c) Desde que no âmbito do Projeto Cartão Nacional de Identificação de Cabo Verde e,

d) Enquanto o certificado se mantiver válido e não estiver na LCR da EC eID.

Adicionalmente,

- O certificado de assinatura digital qualificada atribuído a pessoa singular tem como objetivo a sua utilização em qualquer aplicação para efeitos de assinatura digital qualificada,
- O certificado de autenticação atribuído a pessoa singular, tem como objetivo a sua autenticação nos serviços disponibilizados pelo estado de Cabo Verde,
- O certificado de Validação *online* OCSP tem como objetivo a sua utilização em servidores OCSP[15].

7.5.2. Uso do certificado e da chave pública pelas partes confiantes

Na utilização do certificado e da chave pública, as partes confiantes apenas podem confiar nos certificados, tendo em conta apenas o que é estabelecido nesta DPC e na respetiva Política de Certificação. Para isso devem, entre outras, garantir o cumprimento das seguintes condições:

a) Ter conhecimento e perceber a utilização e funcionalidades proporcionadas pela criptografia de chave pública e certificados.

b) Ser responsável pela sua correta utilização;

c) Ler e entender os termos e condições descritas nas Políticas e Práticas de Certificação;

[15] *cf.* RFC 2560. 1999, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP

d) Verificar os certificados (validação de cadeias de confiança) e LCR, tendo especial atenção às suas extensões marcadas como críticas e propósito das chaves;

e) Confiar nos certificados, utilizando-os sempre que estes estejam válidos.

7.6. Renovação de Certificados Sem Geração de Novo Par de Chaves

A renovação de um certificado é o processo em que a emissão de um novo certificado utiliza os dados do anterior, não havendo alteração das chaves ou qualquer outra informação, com exceção do período de validade do certificado.

Esta prática não é suportada na ICP-CV.

7.7. Renovação de certificado com geração de novo par de chaves

A renovação de chaves do certificado (*certificate re-key*) é o processo em que um titular (ou patrocinador) gera um novo par de chaves e submete o pedido para emissão de novo certificado que certifica a nova chave pública. Este processo, no âmbito da ICP-CV, é designado por renovação de certificado com geração de novo par de chaves.

7.7.1. Motivo para a renovação de certificado com geração de novo par de chaves

É motivo válido para a renovação de certificado com geração de novo par de chaves, sempre e quando se verifique que,

a) O certificado está a expirar;
b) O suporte do certificado está danificado;
c) A informação do certificado sofre alterações.

7.7.2. Quem pode submeter o pedido de certificação de uma nova chave pública

Tal como na secção 7.1.2

7.7.3. Processamento do pedido de renovação de certificado com geração de novo par de chaves

Tal como na secção 7.2.

7.7.4. Notificação da emissão de novo certificado ao titular

Tal como na secção 7.3.2.

7.7.5. Procedimentos para aceitação de um certificado renovado com geração de novo par de chaves

Tal como na secção 7.4.1.

7.7.6. Publicação de certificado renovado com geração de novo par de chaves

Tal como na secção 7.4.2.

7.7.7. Notificação da emissão de certificado renovado a outras entidades

Tal como na secção 7.4.3.

7.8. Modificação de certificados

A alteração de certificados é o processo em que é emitido um certificado para um titular (ou patrocinador), mantendo as respetivas chaves, havendo apenas alterações na informação do certificado.

Esta prática não é suportada no âmbito da ICP-CV.

7.9. Suspensão e revogação de certificado

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

Os certificados depois de revogados não podem voltar a ser válidos, enquanto os certificados suspensos podem recuperar a sua validade.

7.9.1. Circunstâncias para revogação

Um certificado pode ser revogado por uma das seguintes razões:

- Comprometimento ou suspeita de comprometimento da chave privada;
- Perda da chave privada;
- Inexatidões graves nos dados fornecidos;
- Equipamento tecnológico deixa de ser utilizado no âmbito do Cartão Nacional de Identificação;

- Comprometimento ou suspeita de comprometimento da senha e acesso à chave privada (exemplo: PIN);
- Comprometimento ou suspeita de comprometimento da chave privada da EC eID ou de outra EC na cadeia de certificação até à ECR-CV;
- Perda, destruição ou deterioração do dispositivo de suporte da chave privada (por exemplo, suporte/*token* criptográfico);
- Revogação do certificado da EC eID ou de outra EC na cadeia de certificação até à ECR-CV;
- Incumprimento das responsabilidades previstas na presente DPC por parte da EC eID ou do titular;
- Sempre que haja razões credíveis que induzam que o serviços de certificação possam ter sido comprometidos, de tal forma que coloquem em causa a fiabilidade dos certificados;
- Por resolução judicial ou administrativa.

7.9.2. Quem pode submeter o pedido de revogação

Está legitimado para submeter o pedido de revogação, sempre que se verifiquem alguma das condições descritas no ponto 7.9.1, os seguintes:

a) O Titular (ou patrocinador, no caso de certificado de equipamento tecnológico) do certificado;

b) A EC eID;

c) A EC IAC;

d) A Entidade Credenciadora;

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

A EC eID guarda toda a documentação utilizada para verificação da identidade e autenticidade da entidade que efetua o pedido de revogação.

7.9.3. Procedimento para o pedido de revogação

7.9.3.1. Certificado de pessoa singular

No âmbito do processo “Cancelamentos” do Cartão Nacional de Identificação, o SICV-CNI suportará as atividades relacionadas com o registo dos pedidos de cancelamento, devido a motivos relacionados com roubo, extravio, morte, entre outros, comunicando essa informação à EC eID.

Associado ao cancelamento do Cartão Nacional de Identificação, está a atividade de revogação de todos os certificados emitidos para o titular do mesmo (Certificado de Assinatura e Certificado de Autenticação) e armazenados no referido cartão.

7.9.3.2. Certificado de equipamento tecnológico

Os procedimentos seguidos no pedido de revogação de certificado são os seguintes:

- Todos os pedidos de revogação devem ser endereçados para a EC eID por escrito ou por mensagem eletrónica assinada digitalmente, em formulário de pedido de revogação[11];
- Identificação e autenticação da entidade que efetua o pedido de revogação, conforme secção 6.1
- Registo e arquivo do formulário de pedido de revogação;
- Análise do pedido de revogação pelo Conselho Executivo da EC eID, que propõe ao responsável do organismo que tutela a EC eID a aprovação ou recusa do pedido de revogação;
- Mediante o parecer do Conselho Executivo da EC eID, o responsável do organismo que tutela a EC eID, decide a aprovação ou recusa do pedido de revogação do certificado;
- Sempre que se decidir revogar um certificado, a revogação é publicada na respetiva LCR.

Em qualquer dos casos, é arquivada a descrição pormenorizada de todo o processo de decisão, ficando documentado:

- Data do pedido de revogação,
- Nome do titular do certificado,
- Exposição pormenorizada dos motivos para o pedido de revogação,
- Nome e funções da pessoa que solicita a revogação,
- Informação de contacto da pessoa que solicita a revogação,
- Assinatura da pessoa que solicita a revogação.

7.9.4. Produção de efeitos da revogação

A revogação será feita de forma imediata. Após terem sido efetuados todos os procedimentos e seja verificado que o pedido é válido, o pedido não pode ser anulado.

7.9.5. Prazo para processar o pedido de revogação

O pedido de revogação deve ser tratado de forma imediata, pelo que em caso algum poderá ser superior a 24 horas.

7.9.6. Requisitos de verificação da revogação pelas partes confiantes

Antes de utilizarem um certificado, as partes confiantes têm como responsabilidade, verificar o estado de todo os certificados, através das LCR ou num servidor de verificação do estado *on-line* (via OCSP).

7.9.7. Motivos para suspensão

Os certificados emitidos pela EC eID, para pessoa singular, são emitidos em estado suspenso, sendo estes serão ativados, ou não, mediante decisão do seu titular, no ato da entrega do Cartão Nacional de Identificação.

Após ativação de um certificado, este só poderá ser suspenso a pedido do SICV-CNI. Este é responsável pelo registo do motivo da suspensão.

7.9.8. Quem pode submeter o pedido de suspensão

O pedido de suspensão só é aceite quando submetido pelo SICV-CNI.

7.9.9. Procedimentos para pedido de suspensão

São utilizadas mensagens eletrónicas entre o SICV-CNI e a EC.

7.9.10. Limite do período de suspensão

Nada a assinalar.

7.9.11. Periodicidade da emissão da lista de revogação de Certificados (LCR)

A EC eID disponibiliza nova LCR todos as semanas, e uma delta LCR diariamente

7.9.12. Período máximo entre a emissão e a publicação da LCR

O período máximo entre a emissão e publicação da LCR não deve ultrapassar as 3 horas.

7.9.13. Disponibilidade de verificação on-line do estado / revogação de certificado

A EC eID dispõe de serviços de validação OCSP do estado dos certificados de forma *on-line*. Esse serviço poderá ser acedido em http://ocsp.eciad.cni.gov.cv/publico/ocsp.

O período máximo entre a revogação e a disponibilização através do serviço de validação OCSP não deverá ultrapassar os 30 minutos.

7.9.14. Requisitos de verificação on-line de revogação

As partes confiantes deverão dispor de *software* capaz de operar o protocolo OCSP, de forma a obter a informação sobre o estado do certificado.

7.9.15. Outras formas disponíveis para divulgação de revogação

Nada a assinalar.

7.9.16. Requisitos especiais em caso de comprometimento de chave privada

Apenas quando se trate do comprometimento da chave privada de uma EC. Neste caso deverão ser adotados os procedimentos descritos na secção 7.16.2

7.10. Serviços sobre o estado do certificado

7.10.1. Características operacionais

O estado dos certificados emitidos está disponível publicamente através das LCR e através do serviço on-line de validação de estado de certificados (OCSP).

7.10.1.1. Disponibilidade do serviço

O Serviço sobre o estado do certificado está disponível 24 horas por dia, 7 dias por semana.

7.10.1.2. Características opcionais

Nada a assinalar.

7.11. Fim de subscrição

O fim da operacionalidade de um certificado acontece quando se verificarem uma das seguintes situações:

a) Revogação do certificado;

b) Por ter caducado o prazo de validade do certificado.

7.12. Procedimentos de auditoria de segurança

7.12.1. Tipo de eventos registados

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

- Pedido, emissão, renovação, reemissão e revogação de certificados;
- Publicação de LCR;
- Eventos relacionados com segurança, incluindo:
    - Tentativas de acesso (com e sem sucesso) a recursos sensíveis da EC;
    - Operações realizadas por membros dos Grupos de Trabalho,
    - Dispositivos físicos de segurança de entrada/saída dos vários níveis de segurança.

As entradas nos registos incluem a informação seguinte:

- Data e hora do evento;
- Identidade do sujeito que causou o evento;
- Descrição do evento.

7.12.2. Frequência da auditoria de registos

Os registos são analisados e revistos pelo menos uma vez por ano, e adicionalmente sempre que haja suspeitas ou atividades anormais ou ameaças de algum tipo. Ações tomadas baseadas na informação dos registos são também documentadas.

7.12.3. Período de retenção dos registos de auditoria

Os registos são mantidos por um mínimo de 2 (dois) meses e posteriormente arquivados por 20 (vinte) anos, em ambiente controlado, existente para o efeito.

7.12.4. Proteção dos registos de auditoria

Os registos são apenas analisados por membros autorizados dos Grupos de Trabalho.

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

7.12.5. Procedimentos para a cópia de segurança dos registos

São criadas cópias de segurança regulares dos registos em sistemas de armazenamento de alta capacidade com periodicidade não superior a uma semana.

7.12.6. Sistema de recolha de registos (Interno / Externo)

Os registos são recolhidos em simultâneo interna e externamente ao sistema da EC.

7.12.7. 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.

7.12.8. Avaliação de vulnerabilidades

Os registos auditáveis são regularmente analisados de modo a minimizar e eliminar potenciais tentativas de quebra de segurança do sistema.

7.13. Arquivo de registos

7.13.1. Tipo de dados arquivados

Todos os dados auditáveis são arquivados, assim como informação de pedidos de certificados e documentação de suporte ao ciclo de vida das várias operações.

7.13.2. Período de retenção em arquivo

Os dados sujeitos a arquivo são retidos no sistema pelo período mínimo de três meses, e depois de arquivados devem ser conservados por um período de 20 (vinte) anos.

7.13.3. Proteção dos arquivos

O arquivo é protegido de modo a que:

- Apenas membros autorizados dos Grupos de Trabalho possam consultar e ter acesso ao arquivo,
- O arquivo é protegido contra qualquer modificação ou tentativa de o remover,
- O arquivo é protegido contra a deterioração do media onde é guardado, através de migração periódica para media novo,
- O arquivo 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,
- Os arquivos são guardados de modo seguro em ambientes externos seguros.

7.13.4. Procedimentos para as cópias de segurança do arquivo

Cópias de segurança dos arquivos são efetuadas de modo incremental ou total e guardados em dispositivos WORM (*Write Once Read Many*).

7.13.5. Requisitos para validação cronológica dos registos

Algumas das entradas dos arquivos contêm informação de data e hora. Tais informações de data e hora não têm por base uma fonte de tempo segura.

7.13.6. Sistema de recolha de dados de arquivo (Interno / Externo)

Os sistemas de recolha de dados de arquivo são internos.

7.13.7. Procedimentos de recuperação e verificação de informação arquivada

Apenas membros autorizados dos Grupos de Trabalho têm acesso aos arquivos. A integridade do arquivo deve ser verificada através do seu restauro.

7.14. Renovação de chaves

A renovação de chaves, no âmbito da EC eID pressupõe a geração de novo par de chaves, ou seja uma nova emissão.

7.15. Recuperação em caso de desastre ou comprometimento

Esta secção descreve os requisitos relacionados com os procedimentos de notificação e de recuperação no caso de desastre ou de comprometimento.

7.16. Procedimentos em caso de incidente ou comprometimento

Cópias de segurança das chaves privadas da EC (geradas e mantidas de acordo com a secção 10.3) e dos registos arquivados (secção 7.12.1) são guardados em ambientes seguros externos e disponíveis em caso de desastre ou de comprometimento.

7.16.1. Corrupção dos recursos informáticos, do software e/ou dos dados

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.

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, o MJT suspenderá os serviços da EC eID e notificará a ANAC.

7.16.2. Procedimentos em caso de comprometimento da chave privada da entidade

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

- Revogação do certificado da EC eID e de todos os certificados emitidos no "ramo" da hierarquia de confiança da EC eID,
- Notificação à ANAC e todos os titulares de certificados emitidos no "ramo" da hierarquia de confiança da EC eID,
- Geração de novo par de chaves para a EC eID, e pedido de novo certificado à ECR-CV,
- Renovação de todos os certificados emitidos no "ramo" da hierarquia de confiança da EC eID.

7.16.3. Capacidade de continuidade da atividade em caso de desastre

O MJT 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) após um desastre natural ou outro.

7.17. Procedimentos em caso de extinção de EC ou UR

Em caso de cessação de atividade como prestador de serviços de Certificação, a EC eID deve, atempadamente, com uma antecedência mínima de três meses, proceder às seguintes ações:

a) Informar a ANAC;

b) Informar a ECR-CV;

c) Informar todos os titulares de certificados;

d) Revogar todos os certificados emitidos;

e) Efetuar uma notificação final aos titulares 3 (três) dias antes da cessação formal da atividade;

f) Garantir a transferência (para retenção por outra organização) de toda a informação relativa à atividade da EC, nomeadamente, chave da EC, certificados, documentação em arquivos (interno ou externo), repositórios e arquivos de registo de eventos.

Em caso de alterações do organismo/estrutura responsável de gestão da atividade da EC, esta deve informar de tal facto às entidades listadas nas alíneas anteriores.

7.18. Retenção e recuperação de chaves (Key escrow)

A EC eID só efetua a retenção da sua chave privada.

7.18.1. Políticas e práticas de recuperação de chaves

A chave privada da EC eID é armazenada num *token hardware* de segurança, sendo efetuada uma cópia de segurança utilizando uma ligação direta hardware a *hardware* entre dois *tokens* de segurança. A geração da cópia de segurança é o último passo da emissão de um novo par de chaves da EC eID.

A cerimónia de cópia de segurança utiliza um HSM com autenticação de dois fatores (consola de autenticação portátil e chaves de ativação, em que várias pessoas, cada uma delas possuindo uma chave, são obrigadas a autenticar-se antes que seja possível efetuar a cópia de segurança.

O *token hardware* de segurança com a cópia de segurança da chave privada da EC eID é colocado num cofre seguro em instalações seguras secundárias, e acessível apenas aos membros autorizados dos Grupos de Trabalho. O controlo de acesso físico a essas instalações impede a outras pessoas de obterem acesso não autorizado às chaves privadas.

A cópia de segurança da chave privada da EC eID pode ser recuperada no caso de mau funcionamento da chave original. A cerimónia de recuperação da chave utiliza os mesmos mecanismos de autenticação de dois fatores e com múltiplas pessoas, que foram utilizados na cerimónia de cópia de segurança.

7.18.2. Políticas e práticas de encapsulamento e recuperação de chaves de sessão

Nada a assinalar.

8. MEDIDAS DE SEGURANÇA FÍSICA, DE GESTÃO E OPERACIONAIS

Estão implementadas várias regras e políticas incidindo sobre controlos físicos, procedimentais e humanos, que suportam os requisitos de segurança constantes desta DPC. Esta secção descreve sucintamente os aspetos não técnicos de segurança que possibilitam, de modo seguro, realizar as funções de geração de chaves, autenticação dos titulares, emissão de certificados, revogação de certificados, auditorias e arquivo. Todos estes controlos não técnicos de segurança são críticos para garantir a confiança nos certificados, pois qualquer falta de segurança pode comprometer as operações da EC.

8.1. Medidas de segurança física

8.1.1. Construção e Localização Física das Instalações da EC

As instalações da EC eID 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 utiliza o conceito de defesa em profundidade, ou seja, por níveis de segurança, garantindo-se 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).

As operações da EC eID são realizadas numa sala numa zona 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.

As duas zonas de alta segurança são áreas que obedecem às seguintes características:

a) Paredes em alvenaria, betão ou tijolo;

b) Teto e pavimento com construção similar à das paredes;

c) Inexistência de janelas;

d) Porta de segurança, com chapa em aço, com as dobradiças fixas e ombreira igualmente em aço, com fechadura de segurança acionável eletronicamente, características corta – fogo e funcionalidade antipânico.

Adicionalmente, as seguintes condições de segurança são garantidas no ambiente da EC eID:

- Perímetros de segurança claramente definidos;
- Paredes, chão e teto em alvenaria, sem janelas, que impedem acessos não autorizados;
- Trancas e fechaduras anti roubo de alta segurança nas portas de acesso ao ambiente de segurança.
- O perímetro do edifício é estanque na medida em que não existem portas, janelas ou outras brechas não controladas, que possibilitem acessos não autorizados;
- Acesso ao ambiente passa obrigatoriamente por áreas de controlo humano, e por outros meios de controlo que restringem o acesso físico apenas a pessoal devidamente autorizado.

8.1.2. Acesso físico ao local

Os sistemas da EC eID estão protegidos por um mínimo de 4 níveis de segurança física hierárquicos (edifício em si, bloco de alta segurança, área de alta segurança, sala de alta segurança), 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.

Atividades operacionais sensíveis da EC, criação e armazenamento de material criptográfico, quaisquer atividades no âmbito do ciclo de vida do processo de certificação como autenticação, verificação e emissão ocorrem dentro da zona mais restrita de alta segurança. O acesso a cada nível de segurança requer o uso de um cartão magnético de autenticação. Acessos físicos são automaticamente registados e gravados em circuito fechado de TV para efeitos de auditorias.

O acesso ao cartão de identificação vermelho obriga a um duplo controlo de autenticação de acesso individual. A todo o pessoal não acompanhado, incluindo colaboradores ou visitantes não autenticados não é permitida a sua entrada e permanência em áreas de segurança. A não ser que todo o pessoal que circule dentro destas áreas de segurança seja garantidamente reconhecido por todos, é obrigatório o uso do respetivo cartão de acesso de modo visível, assim como garantir que não circulam indivíduos não reconhecidos sem o respetivo cartão de acesso visível.

O acesso à zona mais restrita de alta segurança requer controlo duplo, cada um deles utilizando dois fatores de autenticação, incluindo obrigatoriamente autenticação biométrica. O *hardware* criptográfico e *tokens* físicos seguros dispõem de proteção adicional, sendo guardados em cofres e armários seguros. O acesso à zona mais restrita de alta segurança, assim como ao *hardware* criptográfico e aos *tokens*

físicos seguros é restrito, de acordo com as necessidades de segregação de responsabilidades dos vários Grupos de Trabalho.

8.1.3. Energia e ar condicionado

O ambiente seguro possui equipamento redundante, que garante condições de funcionamento 24 horas por dia / 7 dias por semana, de,

- Alimentação de energia garantindo alimentação contínua ininterrupta com a potência suficiente para manter autonomamente a rede elétrica durante períodos de falta de corrente e para proteger os equipamentos face a flutuações elétricas que os possam danificar (o equipamento redundante consiste em baterias de alimentação ininterrupta de energia, e geradores de eletricidade a diesel), e
- Refrigeração/ventilação/ar condicionado que controlam os níveis de temperatura e humidade, garantindo condições adequadas para o correto funcionamento de todos os equipamentos eletrónicos e mecânicos presentes dentro do ambiente. Um sensor de temperatura, ativa um alerta GSM sempre que a temperatura atinge valores anormais. Este alerta GSM consiste em telefonemas com uma mensagem previamente gravada, para os elementos da equipa de manutenção.

8.1.4. Exposição à água

As zonas de alta segurança têm instalado os mecanismos devidos (detetores de inundação) para minimizar o impacto de inundações nos sistemas da EC eID.

8.1.5. Prevenção e proteção contra incêndio

O ambiente seguro tem instalado os mecanismos necessários para evitar e apagar fogos ou outros incidentes derivados de chamas ou fumos. Estes mecanismos estão em conformidade com os regulamentos existentes:

- Sistemas de deteção e alarme de incêndio estão instalados nos vários níveis físicos de segurança,
- 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,

- Procedimentos de emergência bem definidos, em caso de incêndio.

8.1.6. Salvaguarda de suportes de armazenamento

Todos os suportes de informação sensível contendo *software* e dados de produção, informação para auditoria, arquivo ou cópias de segurança são guardados em cofres e armários de segurança 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 (e.g., causados por água ou fogo).

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.

Em situações que impliquem a deslocação física de *hardware* de armazenamento de dados para fora da zona de alta segurança, por motivos que não o arquivo de cópias de segurança, cada elemento do *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).

8.1.7. Eliminação de resíduos

Documentos e materiais em papel que contenham informação sensível deverão ser triturados antes da sua eliminação.

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. 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*, ...) são devidamente inutilizados de modo a não ser possível recuperar nenhuma informação (através de formatações seguras, ou destruição física dos equipamentos).

8.1.8. Instalações externas (alternativa) para recuperação de segurança

Todas as cópias de segurança são guardadas em ambiente seguro em instalações externas, ficando alojadas em cofres e armários seguros situados em zonas com controlos de acesso físicos e lógicos, de modo a restringir o acesso apenas a pessoal autorizado, garantindo também a proteção contra danos acidentais (e.g., causados por água ou fogo).

8.2. Medida de segurança dos processos

A atividade de uma Entidade Certificadora (daqui em diante denominada por EC) depende da intervenção coordenada e complementar de um extenso elenco de recursos humanos, nomeadamente porque:

- Dados os requisitos de segurança inerentes ao funcionamento de uma EC é vital garantir uma adequada segregação de responsabilidades, que minimize a importância individual de cada um dos intervenientes,
- É necessário garantir que a EC apenas poderá ser sujeita a ataques do tipo *denial-of-service* mediante o conluio de um número significativo de intervenientes,

Pelo exposto, nesta secção, descrevem-se os requisitos necessários para reconhecer os papéis de confiança e responsabilidades associadas a cada um desses papéis. Esta secção inclui também a separação de deveres, em termos dos papéis que não podem ser executados pelos mesmos indivíduos.

8.2.1. Funções de Confiança

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

Os papéis de confiança estão agrupados em sete categorias diferentes (que correspondem a sete Grupos de Trabalho distintos) de modo a garantir que as operações sensíveis sejam efetuadas por diferentes pessoas autenticadas, eventualmente pertencentes a diferentes Grupos de Trabalho.

8.2.1.1. Grupo de Trabalho de Administração de Segurança

O Grupo de Trabalho de Administração de Segurança é responsável por propor, gerir e implementar todas as políticas da EC, assegurando que se encontram atualizadas, e garantir que toda a informação

indispensável ao funcionamento e auditoria da EC se encontra disponível[16], ao longo do tempo. O Grupo de Trabalho de Administração de Segurança assume também a função de Administração de HSM.

As responsabilidades deste grupo incluem:

- Gerir o Ambiente de Administração de Segurança, ambiente onde são armazenados artefactos sensíveis da EC;
- Definir e gerir todas as políticas da EC e garantir que se encontram atualizadas e adaptadas à realidade desta;
- Garantir implementação das políticas definidas;
- Assegurar que as PC's da EC são suportadas pela sua DPC.
- Assegurar que todos os documentos relevantes e relacionados, direta ou indiretamente, com o funcionamento da EC e existentes em formato papel[17] se encontram armazenados num ambiente controlado;
- Gerir e controlar os sistemas de segurança física, incluindo acessos, do ambiente de produção;
- Explicar todos os mecanismos de segurança aos funcionários que devam conhecê-los e de consciencializá-los para as questões de segurança levando-os a fazer cumprir as normas e políticas de segurança estabelecidas.
- Calendarizar cerimónias para testes, formações e auditoria dos sistemas de informação;
- Configurar os acessos à aplicação da EC (grupos, regras, logs);
- Configurar perfis de certificados na aplicação da EC;
- Ativação da interface de operação da EC;
- Ativação de chaves para sua utilização. Isto significa que cada vez que se inicie a EC, é necessário a inserção *tokens* criptográficos de ativação, para dar acesso às chaves criptográficas da EC.
- Autorização para a geração de chaves da aplicação. Esta operação é requerida durante a cerimónia de geração de chaves para a EC.

[16] Para elementos devidamente autorizados

[17] Os procedimentos a adoptar em relação aos documentos em formato electrónico serão definidos após a concretização do *Business Continuity Plan*

- Arranque do interface de configuração da EC e das restantes entidades que formam a ICP-CNICV.

8.2.1.2. Grupo de Trabalho de Administração de Registo

O Grupo de Trabalho de Administração de Registo é responsável por reportar as tarefas de rotina essenciais ao bom funcionamento e operacionalidade da EC assim como todos os incidentes sucedidos. Também é missão deste grupo operar a EC no que diz respeito à emissão, suspensão e revogação de certificados. Assume também a função Administrador de Sistemas e Operador de Sistemas.

As responsabilidades deste grupo são:

- Monitorizar, reportar e quantificar todos os incidentes e avarias de *software* e *hardware*, despoletando os processos apropriados à correção das mesmas;
- Emitir, suspender e revogar certificados de serviços em cerimónias periódicas

8.2.1.3. Grupo de Trabalho de Administração de Sistemas

O Grupo de Trabalho de Administração de Sistemas é responsável por instalar, configurar e fazer a manutenção (*hardware* e *software*) da EC, sem afetar a segurança da aplicação. Assume a também a função Administrador de Registo e Operador de Sistemas.

As responsabilidades deste grupo são:

- Manter um inventário atualizado de todos os produtos relacionados com a EC.
- Instalar, interligar e configurar o *hardware* da EC;
- Instalar e configurar o *software* de base da EC;
- Gerir e atualizar os produtos instalados;
- Preparar comunicados sobre:
    - As palavras-chave iniciais;
    - *Hash* do(s) CD(s) de instalação utilizados.

8.2.1.4. Grupo de Trabalho de Operação de Sistemas

O Grupo de Trabalho de Operação de Sistemas é responsável por operar diariamente os sistemas, realizando cópias de segurança e reposição de informação, caso necessário. Assume a também a função Administrador de Sistemas.

As responsabilidades deste grupo são:

- Realizar as tarefas de rotina da EC, incluindo operações de cópias de segurança dos seus sistemas;
- Gerir o Ambiente de Operação.

8.2.1.5. Grupo de Trabalho de Auditoria de Sistemas

O Grupo de Trabalho de Auditoria de Sistemas é responsável por efetuar a auditoria interna a todas as ações relevantes e necessárias para assegurar a operacionalidade da EC.

As responsabilidades deste grupo são:

- Auditar a execução e confirmar a exatidão dos processos e cerimónias da EC;
- Registar todas as operações sensíveis;
- Investigar suspeitas de fraudes procedimentais;
- Verificar periodicamente a funcionalidade dos controlos de segurança (dispositivos de alarme, de controlo de acessos, sensores de fogo, etc.) existentes nos vários ambientes;
- Registar todos os procedimentos passíveis de auditoria;
- Registar os resultados de todas as ações por si realizadas;
- Validar que todos os recursos usados são seguros;
- Verificação periódica da integridade dos Ambientes de Custódia, assegurando que lá se encontram os artefactos respetivos[18] e que estão devidamente identificados;
- Inspecionar a configuração estabelecida pelas tarefas de administração e os eventos registados.

8.2.1.6. Conselho Executivo

É responsável pela nomeação dos membros dos restantes grupos[19] e pela tomada de decisões de nível crítico para a EC. Este grupo deve ser constituído por um mínimo de três (três) membros.

As responsabilidades deste grupo são:

- Rever e aprovar as políticas propostas pelo Grupo de Trabalho de Administração de Segurança;

[18] Caso algum deles se encontre requisitado, o Grupo de Trabalho de Auditoria deverá verificar se existe registo do seu levantamento e contactar os elementos envolvidos no sentido de confirmar que o têm em seu poder
[19] Com exceção do Grupo de Trabalho de Instalação e do Grupo de Trabalho de Custódia

- Pedir a aprovação de Políticas à Entidade Credenciadora;
- Designar os membros dos restantes grupos de trabalho (à exceção do Grupo de Trabalho de Instalação e do Grupo de Trabalho de Custódia);
- Disponibilizar a identificação de todos os indivíduos que pertencem aos vários Grupos de Trabalho, num ou mais pontos, facilmente acessíveis pelos indivíduos autorizados.

8.2.1.7. Grupo de Trabalho de Custódia

É responsável pela custódia de alguns artefactos sensíveis (*tokens* de autenticação, etc.), que podem ser levantados pelos membros dos outros grupos mediante a satisfação de determinadas condições[20]. Note-se que, no sentido de melhorar os níveis de segurança, operacionalidade e continuidade de negócio da EC, poderão existir várias instâncias deste grupo, cada qual encarregue da custódia de um conjunto distinto de artefactos. Este grupo deve fazer uso dos vários ambientes seguros disponibilizados para a guarda deste tipo de itens.

As responsabilidades deste grupo são:

- Gestão do "Ambiente de Custódia" respetivo,
- Custódia de artefactos sensíveis (*tokens* de autenticação, etc.) usando os meios adequados que respondam às necessidades de segurança respetivas e,
- Disponibilização segura destes itens a membros de grupos autorizados e explicitamente indicados com permissões de acesso a esses itens, após o cumprimento dos procedimentos apropriados de segurança.

8.2.2. Número de pessoas exigidas por tarefa

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.

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. O acesso ao *hardware* criptográfico da EC segue procedimentos estritos envolvendo múltiplos indivíduos autorizados a aceder-

[20] Definidas para cada um dos artefactos à sua guarda

lhe durante o seu ciclo de vida, desde a receção e inspeção até à destruição física e/ou lógica do *hardware*. Após a ativação de um módulo com chaves operacionais, controlos adicionais de acesso são utilizados de modo a garantir que os acessos físicos e lógicos ao *hardware* só são possíveis com 2 ou mais indivíduos autenticados. Indivíduos com acesso físico aos módulos, não detêm as chaves de ativação e vice-versa.

8.2.3. Identificação e Autenticação para cada função

Cada membro de cada grupo autentica-se em conta própria para acesso à máquina sendo que o acesso a aplicação da EC eID é feito com recurso à utilização de um certificado digital próprio emitido para o efeito.

8.2.4. Funções que requerem separação de responsabilidades

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

Se pertence ao Grupo/Subgrupo...	Pode pertencer ao Grupo/Subgrupo... ?	Administração de Segurança	Administração de Registo	Administração de Sistemas	Operação de Sistemas	Auditoria de Sistemas	Conselho Executivo
Administração de Segurança				✖		✖	✖
Administração de Registo						✖	✖
Administração de Sistemas		✖				✖	✖
Operação de Sistemas						✖	✖
Auditoria de Sistemas		✖	✖	✖	✖		✖
Conselho Executivo		✖	✖	✖	✖	✖	

8.3. Medidas de Segurança de Pessoal

A admissão de pessoal com funções de confiança nos Grupos de Trabalho é apenas possível se,:

- Forem nomeados formalmente para a função,
- São pessoas idóneas;
- Apresentarem provas de antecedentes, qualificações e experiência necessárias para a realização das tarefas dos Grupos de Trabalho,
- Tiverem recebido formação e treino adequado para o desempenho da respetiva função,
- Garantir que o funcionário não revela informação sensível sobre a EC ou dados de identificação dos titulares,
- Garantir que o funcionário conhece os termos e condições para o desempenho da respetiva função e,
- Garantir que o funcionário não desempenha funções que possam causar conflito com as suas responsabilidades nas atividades da EC.

8.3.1. Requisitos relativos às qualificações, experiência, antecedentes e credenciação

A admissão de novos membros nos Grupos de Trabalho é apenas possível se apresentarem provas de conhecimento, qualificações e experiência necessárias para a realização das tarefas dos Grupos de Trabalho.

8.3.2. Procedimento de verificação de antecedentes

A verificação de antecedentes decorre do processo de credenciação dos indivíduos nomeados para exercer cargos em qualquer uma das funções de confiança. A verificação de antecedentes inclui:

- Confirmação de identificação, usando documentação emitida por fontes fiáveis e,
- Investigação de registos criminais.

8.3.3. Requisitos de formação e treino

É ministrado aos membros dos Grupos de Trabalho formação e treino adequado de modo a realizarem as suas tarefas satisfatória e competentemente.

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 do *software* e/ou *hardware* usado pela EC;

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.

8.3.4. Frequência e requisitos para ações de reciclagem

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,

- Sempre que existe qualquer alteração tecnológica, introdução de novas ferramentas ou modificação de procedimentos, é levada a cabo a adequada formação para todo o pessoal afeto às EC,
- Sempre que são introduzidas alterações nas Políticas de Certificação ou Declaração de Práticas de Certificação são realizadas sessões de reciclagem aos elementos das EC.

8.3.5. Frequência e sequência da rotação de funções

Nada a assinalar.

8.3.6. Sanções para ações não autorizadas

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

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

8.3.7. Requisitos para prestadores de serviços

Consultores ou prestadores de serviços independentes tem permissão de acesso à zona de alta segurança desde de que estejam sempre acompanhados e diretamente supervisionados pelos membros do Grupo de Trabalho.

Os procedimentos de verificação de antecedentes a aplicar nestas situações são os mesmos que são indicados na secção 8.3.2.

8.3.8. 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.

9. MEDIDAS DE SEGURANÇA TÉCNICAS

Esta secção define as medidas de segurança implementadas para a EC eID de forma a proteger chaves criptográficas geradas por esta, e respetivos dados de ativação. O nível de segurança atribuído à manutenção das chaves deve ser máximo para que chaves privadas e chaves seguras assim como dados de ativação estejam sempre protegidos e sejam apenas acedidos por pessoas devidamente autorizadas.

9.1. Geração e instalação do par de chaves

A geração dos pares de chaves da EC eID é processada de acordo com os requisitos e algoritmos definidos nesta política.

9.1.1. Geração do par de chaves

A geração de chaves criptográficas da EC eID é feito por um Grupo de Trabalho, composto por elementos autorizados para tal, numa cerimónia planeada e auditada de acordo com procedimentos escritos das operações a realizar. Todas as cerimónias de geração de chaves ficam registadas, datadas e assinadas pelos elementos envolvidos no Grupo de Trabalho

O *hardware* criptográfico, usado para a geração de chaves da EC eID, cumpre os requisitos FIPS 140-1 nível 3 e, efetua a manutenção de chaves, armazenamento e todas as operações que envolvem chaves criptográficas utilizando exclusivamente o *hardware*. O acesso a chaves críticas é protegido por políticas de segurança, divisão de papéis entre os Grupos de Trabalho, assim como através de regras de acesso limitado de utilizadores. As cópias de segurança de chaves criptográficas são efetuadas apenas usando *hardware*, permitindo que estas cópias sejam devidamente auditadas e que na eventualidade de uma perca de dados, possa haver uma recuperação total e segura das chaves.

9.1.2. Entrega da chave privada ao titular

A entrega da chave privada, associada aos certificados emitidos para o cidadão é efetuada em dispositivo criptográfico SSCD (Secure Signature-Creation Device).

9.1.3. Entrega da chave pública ao emissor do certificado

A chave pública é entregue à EC eID, de acordo com os procedimentos indicados na secção 7.3.1

9.1.4. Entrega da chave pública da EC às partes confiantes

A chave pública da EC eID será disponibilizada através do certificado da EC eID, assinado pela EC de Identificação e Autenticação Civil, conforme secção 4.2.1

9.1.5. Dimensão das chaves

O comprimento dos pares de chaves deve ter o tamanho suficiente, 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:

- 4096 bits RSA para a chave da EC eID,
- 2048 bits RSA para as chaves associadas aos certificados de equipamento tecnológico.

9.1.6. Parâmetros da chave pública e verificação da qualidade

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

As chaves da EC são geradas com base na utilização de processos aleatórios/pseudo aleatórios descritos no ANSI X9.17 (Anexo C), de acordo com o estipulado no PKCS#1.

9.1.7. Utilização das Chaves (campo "key usage" X.509 v3)

O campo "keyUsage" dos certificados, utilizado de acordo com o recomendado no RFC 5280 inclui a seguinte utilização.

a) Non-repudiation

9.2. Proteção da chave privada e características do módulo criptográfico

Nesta secção são considerados os requisitos para proteção da chave privada e para os módulos criptográficos da EC eID. Está implementada uma combinação de controlos físicos, lógicos e procedimentos, devidamente documentados, de forma a assegurar confidencialidade e integridade das chaves privadas da EC eID.

9.2.1. Normas e medidas de segurança do módulo criptográfico

Para a geração dos pares de chaves da EC eID assim como para o armazenamento das chaves privadas, o MJ utiliza módulo criptográfico em *hardware* que cumpre as seguintes normas:

- Segurança Física
  - *Common Criteria* EAL 4+ e/ou
  - FIPS 140-1, nível 3
- Certificações Regulamentares
  - U/L 1950 & CSA C22.2 *safety compliant*
  - FCC Part 15 – Class B
  - Certificação ISO – 9002
- Papéis
  - Autenticação de dois fatores

9.2.2. Controlo multi-pessoal (m de n) para a chave privada

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

Estão implementados um conjunto de mecanismos e técnicas que obrigam à participação de vários membros do Grupo de Trabalho para efetuar operações criptográficas sensíveis na EC.

Os dados de ativação necessários para a utilização da chave privada da EC eID são divididos em várias partes, acessíveis e à responsabilidade de diferentes membros do Grupo de Trabalho. Um determinado número destas partes (m) do total número de partes (n) é necessário para ativar a chave privada da EC eID guardada no módulo criptográfico em *hardware*. São necessárias duas (m) partes para a ativação da chave privada da EC eID.

9.2.3. Retenção da chave privada (key escrow)

A retenção da chave privada da EC eID é explicada em detalhe na secção 7.18.

9.2.4. Cópia de segurança da chave privada

A chave privada da EC eID tem pelo menos uma cópia de segurança, com o mesmo nível de segurança que a chave original, conforme secção 7.18

10. Não é permitida a retenção de chaves privadas.

10.1.1. Arquivo da chave privada

As chaves privadas da EC eID, alvo de cópias de segurança, são arquivadas conforme identificado na secção 7.18**Erro! A origem da referência não foi encontrada.**.

As chaves provadas dos titulares não são alvo de cópias.

10.1.2. Transferência da chave privada para/do módulo criptográfico

As chaves privadas da EC eID não são exportáveis a partir do *token* criptográfico FIPS 140-1 nível 3.

Mesmo se for efetuada uma cópia de segurança das chaves privadas da EC eID para um outro *token* criptográfico, essa cópia é feita diretamente, *hardware* para *hardware*, de uma forma que garante o transporte das chaves entre módulos numa transmissão cifrada.

10.1.3. Armazenamento da chave privada no módulo criptográfico

As chaves privadas da EC eID são armazenadas de forma cifrada nos módulos do *hardware* criptográfico.

10.1.4. Processo para ativação da chave privada

A chave privada da EC eID é ativada quando o sistema da EC é ligado. Esta ativação é efetivada através da autenticação no módulo criptográfico por, pelo menos, três membros dos grupos de trabalho que detêm em seu poder os artefactos necessários para a realização desta operação, sendo obrigatória a utilização de autenticação de dois fatores (consola de autenticação portátil e chaves de ativação com código PIN associado).

Uma vez a chave ativada, esta permanecerá assim até que o processo de desativação seja executado.

10.1.5. Processo para desativação da chave privada

A chave privada da EC eID é desativada quando o sistema da EC é desligado.

Para a desativação das chaves privadas da EC eID é necessária, no mínimo, a intervenção de dois elementos, membros dos grupos de trabalho. Uma vez desativada, esta permanecerá inativa até que o processo de ativação seja executado.

10.1.6. Processo para destruição da chave privada

As chaves privadas da EC eID (incluindo as cópias de segurança) são apagadas/destruídas, assim que de acordo com as instruções do fabricante do HSM, num procedimento devidamente identificado e auditado assim que terminada a sua data de validade (ou se revogadas antes deste período).

O MJ procede à destruição das chaves privadas garantindo que 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 EC.

10.1.7. Avaliação/nível do módulo criptográfico

Descrito na secção 9.2.1.

10.2. Outros aspetos da gestão do par de chaves

10.2.1. Arquivo da chave pública

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

10.2.2. Períodos de validade do certificado e das chaves

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

Neste sentido a validade dos diversos tipos de certificados e período em que os mesmos devem ser renovados, é o seguinte:

- o certificado de pessoa singular tem uma validade de cinco anos;
- os certificados de equipamento tecnológico têm uma validade de 3 anos e dois meses, sendo que são renovados mensalmente.

10.3. Dados de ativação

10.3.1. Geração e instalação dos dados de ativação

Os dados de ativação necessários para a utilização da chave privada da EC eID são divididos em várias partes (guardadas em chaves de ativação), ficando à 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 FIPS 140-1 nível 3.

10.3.1.1. Proteção dos dados de ativação

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

As chaves privadas da EC eID são guardadas, de forma cifrada, em *token* criptográfico.

10.3.1.2. Outros aspetos dos dados de ativação

Se for preciso transmitir os dados de ativação das chaves privadas, esta transmissão será protegida contra perdas de informação, roubo, alteração de dados e divulgação não autorizada.

Os dados de ativação são destruídos (por formatação e/ou destruição física) quando a chave privada associada é destruída.

10.4. Medidas de segurança informáticas

10.4.1. Requisitos técnicos específicos

O acesso aos servidores da EC eID é restrito aos membros dos Grupos de Trabalho com uma razão válida para esse acesso. O pedido de emissão de certificados é efetuado a partir da consola de operação.

A EC eID dispõe de dispositivos de proteção de fronteira, nomeadamente sistema *firewall*, assim como cumprem os requisitos necessários para identificação, autenticação, controlo de acessos, administração, auditorias, reutilização, responsabilidade e recuperação de serviços e troca de informação.

10.4.2. Avaliação/nível de segurança

Os vários sistemas e produtos empregues pela EC eID são fiáveis e protegidos contra modificações.

O módulo criptográfico em *Hardware* da EC eID satisfaz a norma FIPS 140-1 nível 3.

10.5. Ciclo de vida das medidas técnicas de segurança

10.5.1. Medidas de desenvolvimento do sistema

As aplicações são desenvolvidas e implementadas por terceiros de acordo com as suas regras de desenvolvimento de sistemas e de gestão de mudanças.

É fornecido metodologia auditável que permite verificar que o *software* da EC eID não foi alterado antes da sua primeira utilização. Toda a configuração e alterações do *software* são executadas e auditadas por membros do Grupo de Trabalho.

10.5.2. Medidas para a gestão da segurança

Estão implementados mecanismos e/ou Grupos de Trabalho, para controlar e monitorizar a configuração dos sistemas da EC. O sistema do EC eID, quando utilizado pela primeira vez, será verificado para garantir que o *software* utilizado é fidedigno e legal e que não foi alterado depois da sua instalação.

10.5.3. Ciclo de vida das medidas de segurança

As operações de atualização e manutenção dos produtos e sistemas da EC eID, seguem o mesmo controlo que o equipamento original e é instalado pelos membros do Grupo de Trabalho com adequada formação e seguindo os procedimentos definidos para o efeito.

10.6. Medidas de Segurança da rede

A EC eID dispõe de dispositivos de proteção de fronteira, nomeadamente sistema *firewall*, assim como cumpre os requisitos necessários para identificação, autenticação, controlo de acessos, administração, auditorias, reutilização, responsabilidade e recuperação de serviços e troca de informação.

10.7. Validação cronológica (*Time-stamping*)

Certificados, LCRs e outras entradas na base de dados contêm sempre informação sobre a data e hora dessa entrada. Tal informação não é baseada em mecanismos criptográficos.

11. PERFIS DE CERTIFICADO, CRL, E OCSP

11.1. Perfil de Certificado

Os utilizadores de uma chave pública têm que ter confiança que a chave privada associada é detida pelo titular remoto correto (pessoa ou sistema) com o qual irão utilizar mecanismos de cifra ou assinatura digital. A confiança é obtida através do uso de certificados digitais X.509 v3, que são estrutura de dados que fazem a ligação entre a chave pública e o seu titular. Esta ligação é afirmada através da assinatura digital de cada certificado por uma EC de confiança. A EC pode basear esta afirmação em meios técnicos (por exemplo, prova de posse da chave privada através de um protocolo desafio-resposta), na apresentação da chave privada, ou no registo efetuado pelo titular.

Um certificado tem um período limitado de validade, indicado no seu conteúdo e assinado pela EC. Como a assinatura do certificado e a sua validade podem ser verificadas independentemente por

qualquer *software* que utilize certificados, os certificados podem ser distribuídos através de linhas de comunicação e sistemas públicos, assim como podem ser guardados em qualquer tipo de unidades de armazenamento.[10]

O utilizador de um serviço de segurança que requeira o conhecimento da chave pública do utilizador necessita, normalmente, de obter e validar o certificado que contém essa chave. Se o serviço não dispuser de uma cópia fidedigna da chave pública da EC que assinou o certificado, assim como do nome da EC e informação relacionada (tal como o período de validade), então poderá necessitar um certificado adicional para obter a chave pública da EC e validar a chave pública do utilizador. Em geral, para validar a chave pública de um utilizador, pode ser necessária uma cadeia de múltiplos certificados, incluindo o certificado da chave pública do utilizador assinado por uma EC e, outros certificados adicionais de ECs assinados por outras ECs. [10]

O perfil dos certificados emitidos pela EC eID está de acordo com:

- Recomendação ITU.T X.509[21],
- RFC 5280[10] e,
- Política de Certificados da ICP-CV[22].

Os perfis dos certificados podem ser consultados nos documentos de Políticas de Certificados associadas a esta DPC, de acordo com a tabela da secção 5.3.

11.2. Perfil da lista de revogação de certificados

Quando um certificado é emitido, espera-se que seja utilizado durante todo o seu período de validade. Contudo, várias circunstâncias podem causar que um certificado se torne inválido antes da expiração do seu período de validade. Tais circunstâncias incluem a mudança de nome, mudança de associação entre o titular e os dados do certificado (por exemplo, um trabalhador que termina o emprego) e, o compromisso ou suspeita de compromisso da chave privada correspondente. Sob tais circunstâncias, a EC tem que revogar o certificado.

[21] cf. ITU-T Recommandation X.509. 1997, (1997 E): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework.

O protocolo X.509 define um método de revogação do certificado, que envolve a emissão periódica, pela EC, de uma estrutura de dados assinada, a que se dá o nome de Lista de Revogação de Certificados (LCR). A LCR é uma lista com identificação temporal dos certificados revogados, assinada pela EC e disponibilizada livremente num repositório público. Cada certificado revogado é identificado na LCR pelo seu número de série. Quando uma aplicação utiliza um certificado (por exemplo, para verificar a assinatura digital de um utilizador remoto), a aplicação verifica a assinatura e validade do certificado, assim como obtém a LCR mais recente e verifica se o número de série do certificado não faz parte da mesma. Note-se que uma EC emite uma nova LCR numa base regular periódica.

O perfil da LCR está de acordo com:

- Recomendação ITU.T X.509[21],
- RFC 5280[10] e,
- Política de Certificados da ICP-CV[23].

Os perfis das LCR podem ser consultados nos documentos de Políticas de Certificados associadas a esta DPC, relativamente à EC eID de acordo com a secção 5.3.

11.3. Perfil OCSP

O perfil dos certificados OCSP está de acordo com:

- Recomendação ITU.T X.509[21],
- RFC 5280[10] e,
- Política de Certificados da ICP-CV[23].

Os perfis dos certificados OCSP podem ser consultados no documento de Política de Certificados de Validação *on-line* OCSP associadas a esta DPC, de acordo com a secção 5.3.

12. ADMINISTRAÇÃO DE ESPECIFICAÇÃO

12.1. Procedimentos de mudança de especificação

A Administração de Segurança da EC eID determina a conformidade e aplicação interna desta DPC (e/ou respetivas PCs), submetendo-o de seguida à Entidade Autoridade Credenciadora – órgão

23 ANAC – Conteúdo Mínimo das Políticas de Certificado

competente para determinar a adequação das DPC (e/ou respetivas PCs) das diversas entidades, com a Política de Certificados definida pela ICP-CV – para aprovação.

A Administração de Segurança da EC eID é responsável pela constante atualização desta DPC garantindo que a mesma é revista pelo menos anualmente. Sempre que for registada necessidade de alterações as mesmas devem ser feitas pela Administração de Segurança, e revistas e aprovadas pelo Conselho Executivo e enviadas de seguida à Entidade Credenciadora para Aprovação.

12.1.1. Políticas de publicação e notificação

As atualizações a esta DPC e respetivas PCs serão publicadas imediatamente após a sua aprovação pela Entidade Credenciadora, de acordo com a secção 12.1.2.

12.1.2. Procedimentos para Aprovação

A aprovação interna desta DPC (e/ou respetivas PCs) e seguintes correções (ou atualizações) deverão ser levadas a cabo pelo Grupo de Trabalho de Administração de Segurança. Correções (ou atualizações) deverão ser publicadas sob a forma de novas versões desta DPC (e/ou respetivas PCs), substituindo qualquer DPC (e/ou respetivas PCs) anteriormente definida. O Grupo de Trabalho de Administração de Segurança deverá ainda determinar quando é que as alterações na DPC (e/ou respetivas PCs) levam a uma alteração nos identificadores dos objetos (OID) da DPC (e/ou respetivas PCs).
Após a aprovação interna, a DPC (e/ou respetivas PCs) é submetido à Entidade de Credenciadora, que é a entidade responsável pela aprovação e autorização de modificações neste tipo de documentos.

13. OUTRAS SITUAÇÕES E ASSUNTOS LEGAIS

Esta secção aborda aspetos de negócio e assuntos legais.

13.1. Taxas

13.1.1. Taxas por emissão ou renovação de certificados

Nada a assinalar.

13.1.2. Taxas para acesso a certificado

Nada a assinalar.

13.1.3. Taxas para acesso a informação do estado do certificado ou de revogação

O acesso a informação sobre o estado ou revogação dos certificados é livre e gratuita.

13.1.4. Taxas para outros serviços

Nada a assinalar.

13.1.5. Política de reembolso

Nada a assinalar.

13.2. Responsabilidade financeira

13.2.1. Seguro de cobertura

Nada a assinalar.

13.2.2. Outros recursos

Nada a assinalar.

13.2.3. Seguro ou garantia de cobertura para utilizadores

Nada a assinalar.

13.3. Confidencialidade da informação processada

13.3.1. Âmbito da confidencialidade da informação

Declara-se expressamente como informação confidencial, aquela que não poderá ser divulgada a terceiros:

a) As chaves privadas das EC eID;

b) As chaves privadas das entidades subordinadas da EC eID;

c) Toda a informação relativa aos parâmetros de segurança, controlo e procedimentos de auditoria;

d) Toda a informação de carácter pessoal proporcionada à EC eID durante o processo de registo dos subscritores de certificados, salvo se houver autorização explícita para a sua divulgação;

e) Planos de continuidade de negócio e recuperação;

f) Registos de transações, incluindo os registos completos e os registos de auditoria das transações;

g) Informação de todos os documentos relacionados com a EC eID (regras, políticas, cerimónias, formulários e processos), incluindo conceitos organizacionais, constitui informação financeira/comercial secreta, confidencial e/ou privilegiada, sendo propriedade do MJ. Estes documentos são confiados aos recursos humanos dos Grupos de Trabalho da EC eID com a condição de não serem usados ou divulgados para além do âmbito dos seus deveres nos termos estabelecidos, sem autorização prévia e explícita do MJ;

h) Todas as palavras-chave, PINs e outros elementos de segurança relacionados com a EC eID;

i) A identificação dos membros dos grupos de trabalho da EC eID;

j) A localização dos ambientes da EC eID e seus conteúdos.

13.3.2. Informação fora do âmbito da confidencialidade da informação

Considera-se informação de acesso público:

a) Política de Certificados,
b) Declaração de Práticas de Certificação,
c) LCR e,
d) Toda a informação classificada como "pública" (informação não expressamente considerada como "pública" será considerada confidencial).

A EC eID permite o acesso a informação não confidencial sem prejuízo de controlos de segurança necessários para proteger a autenticidade e integridade da mesma.

13.3.3. Responsabilidade de proteção da confidencialidade da informação

Os elementos dos Grupos de Trabalho ou outras entidades que recebam informação confidencial são responsáveis por assegurar que esta não é copiada, reproduzida, armazenada, traduzida ou transmitida a terceiras partes por quaisquer meios sem antes terem o consentimento escrito do MJ.

13.4. Privacidade dos dados pessoais

13.4.1. Medidas para garantia da privacidade

O Sistema de Ciclo de Vida é responsável pela implementação das medidas que garantem a privacidade dos dados pessoais, que estão de acordo com a Política de Certificação da ICP-CV.

13.4.2. Informação privada

Nada a assinalar.

13.4.3. Informação não protegida pela privacidade

Nada a assinalar.

13.4.4. Responsabilidade de proteção da informação privada

Nada a assinalar.

13.4.5. Notificação e consentimento para utilização de informação privada

Nada a assinalar.

13.4.6. Divulgação resultante de processo judicial ou administrativo

Nada a assinalar.

13.4.7. Outras circunstâncias para revelação de informação

Nada a assinalar.

13.5. Renúncia de garantias

A EC eID recusa todas as garantias de serviço que não se encontrem vinculadas nas obrigações estabelecidas neste DPC.

13.6. Indemnizações

De acordo com a legislação em vigor

13.7. Termo e cessação da atividade

13.7.1. Termo

Os documentos relacionados com a EC eID (incluindo esta DPC) tornam-se efetivos logo que sejam aprovados pela Entidade Credenciação e apenas são eliminados ou alterados por sua ordem.

Esta DPC entra em vigor desde o momento da sua publicação, no repositório da EC eID. Será válida, até que seja publicada uma nova versão.

13.7.2. Substituição e revogação da DPC

O Conselho Executivo ou a Entidade Credenciação podem decidir em favor da eliminação ou emenda de um documento relacionado com a EC eID (incluindo esta DPC) quando:

- Os seus conteúdos são considerados incompletos, imprecisos ou erróneos,
- Os seus conteúdos foram comprometidos.

Nesse caso, o documento eliminado será substituído por uma nova versão.

Esta DPC será substituída por uma nova versão com independência da transcendência das mudanças efetuadas na mesma, de modo que será sempre de aplicação na sua totalidade.

Quando a DPC for revogada será retirada do repositório público, garantindo-se contudo que será conservada durante 20 anos.

13.7.3. Consequências da cessação de atividade

Após o Conselho Executivo ou Entidade Credenciadora decidir em favor da eliminação de um documento relacionado com a EC, o Grupo de Trabalho de Administração de Segurança tem 30 dias úteis para submeter para aprovação ao Conselho Executivo e Entidade Credenciadora um documento substituto.

As obrigações e restrições que estabelece esta DPC, em referência a auditorias, informação confidencial, obrigações e responsabilidades da EC eID, nascidas sob sua vigência, subsistirão após sua substituição ou revogação por uma nova versão em tudo o que não se oponha a esta.

13.8. Notificação individual e comunicação aos participantes

Todos os participantes devem utilizar métodos razoáveis para comunicar uns com os outros. Esses métodos podem incluir correio eletrónico assinado digitalmente, fax, formulários assinados, ou outros, dependendo da criticidade e assunto da comunicação.

13.9. Alterações

13.9.1. Procedimento para alterações

No sentido de alterar este documento ou alguma das políticas de certificado, é necessário submeter um pedido formal ao Grupo de Trabalho de Administração de Segurança, indicando (pelo menos):

- A identificação da pessoa que submeteu o pedido de alteração,
- A razão do pedido,
- As alterações pedidas.

O Grupo de Trabalho de Administração de Segurança vai rever o pedido feito e, se verificar a sua pertinência, procede às atualizações necessárias ao documento, resultando numa nova versão de rascunho do documento. O novo rascunho do documento é depois disponibilizado a todos os membros do Grupo de Trabalho e às partes afetadas (se alguma) para permitir o seu escrutínio. Contando a partir da data de disponibilização, as várias partes têm 15 dias úteis para submeter os seus comentários. Quando esse período terminar, o Grupo de Trabalho de Administração de Segurança tem mais 15 dias úteis para analisar todos os comentários recebidos e, se relevante, incorporá-los no documento, após o que o documento é aprovado pelo Conselho Executivo e fornecido à Entidade de Credenciadora para aprovação. Depois da sua aprovação pelo Entidade Credenciadora, o documento é submetido para o Conselho Executivo para publicação, tornando-se as alterações finais e efetivas.

13.9.2. Prazo e mecanismo de notificação

No caso que a Entidade de Credenciação julgue que as alterações à especificação podem afetar a aceitabilidade dos certificados para propósitos específicos, comunicar-se-á aos utilizadores dos certificados correspondentes que se efetuou uma mudança e que devem consultar a nova DPC no repositório estabelecido.

13.9.3. Motivos para mudar de OID

O Grupo de Trabalho de Administração de Segurança deve determinar se as alterações à DPC obrigam a uma mudança no OID da política de Certificados ou no URL que aponta para a DPC.

No caso em que o Grupo de Trabalho de Administração de Segurança julgue que as alterações à especificação podem afetar à aceitabilidade dos certificados para propósitos específicos proceder-se-á ao aumento do número maior de versão do documento e colocado a zero o número menor da mesma. Também se modificarão os dois últimos números do Identificador de Objeto (OID) que o representa.

13.10. Disposições, para resolução de conflitos

Os conflitos, entre utilizadores e EC eID, deverão ser comunicadas, pela parte em disputa, à ANAC como Entidade Credenciadora, com o fim de tentar resolvê-lo entre as mesmas partes.

Para a resolução de qualquer conflito que possa surgir com relação a esta PC, as partes, com renúncia a qualquer outro foro que pudesse corresponder-lhes, submetem-se à Jurisdição de Contencioso Administrativo.

13.11. Legislação aplicável

É aplicável à atividade das entidades certificadoras a seguinte legislação específica:

a) Decreto-Lei nº 33/2007, de 24 de Setembro;

b) Decreto Regulamentar nº. 18/2007, de 24 de Dezembro;

c) Portaria nº 2/2008, de 28 de Janeiro;

d) Portaria nº 4/2008

e) Aviso nº 001/CA/2008

f) Decreto-Lei nº44/2009 de 9 de Novembro;

13.12. Conformidade com a legislação em vigor

Esta DPC é objeto de aplicação de leis nacionais e diretivas europeias usadas como referência, regras, regulamentos, ordenações, decretos e ordens incluindo, mas não limitadas a, restrições na exportação ou importação de *software*, *hardware* ou informação técnica.

É responsabilidade da Entidade Credenciadora zelar pelo cumprimento da legislação aplicável listada na secção 13.11.

13.13. Providências várias

13.13.1. Acordo completo

Todas as partes confiantes assumem na sua totalidade o conteúdo da última versão desta DPC.

13.13.2. Independência

No caso que uma ou mais estipulações deste documento, sejam ou tendam a ser inválidas, nulas ou irreclamáveis, em termos jurídicos, deverão ser consideradas como não efetivas.

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

13.13.3. Severidade

Nada a assinalar.

13.13.4. Execuções (taxas de advogados e desistência de direitos)

Nada a assinalar.

13.13.5. Força Maior

Nada a assinalar.

13.14. Outras providências

Nada a assinalar.

Referências Bibliográficas

ANAC, Estrutura da Declaração de Práticas de Certificação.

ANAC, Política de Certificados da ICP-CV e Requisitos mínimos de Segurança.

Portaria nº 2/2008, de 28 de Janeiro;

Decreto-Lei nº44/2009 de 9 de Novembro;

Decreto Regulamentar nº. 18/2007, de 24 de Dezembro;

Decreto-Lei nº 33/2007, de 24 de Setembro;

Portaria nº 4/2008

Aviso nº 001/CA/2008

FIPS 140-1. 1994, Security Requirements for Cryptographic Modules.

ISO/IEC 3166. 1997, Codes for the representation of names and countries and their subdivisions.

ITU-T Recommendation X.509. 1997, (1997 E): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework.

NIST FIPS PUB 180-4. 2015, The Secure Hash Algorithm (SHA-1). National Institute of Standards and Technology, "Secure Hash Standard", U.S. Department of Commerce.

RFC 1421. 1993, Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures.

RFC 1422. 1993, Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management.

RFC 1423. 1993, Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers.

RFC 1424. 1993, Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services.

RFC 2252. 1997, Lightweight Directory Access Protocol (v3).

RFC 2560. 1999, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.

RFC 2986. 2000, PKCS #10: Certification Request Syntax Specification, version 1.7.

RFC 3161. 2001, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).

RFC 3279. 2002, Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

RFC 3647. 2003, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

RFC 4210. 2005, Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP).

RFC 5280. 2008, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.