Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil

Políticas

PJ.CNICV_24.1.1_0001_pt_IAC.doc

Identificação do Projeto: Cartão Nacional de Identificação

Identificação da CA: IAC

Nível de Acesso: Público

Versão: 1.1

Data: 19/05/2017

Identificador do documento: PJ.CNICV_24.1.1_0001_pt_IAC.doc

Palavras-chave: CNI, Identificação, Autenticação

Tipologia documental: Políticas

Título: Declaração de Práticas de Certificação da EC de Identificação e Autenticação Civil

Língua original: Português

Língua de publicação: Português

Nível de acesso: Público

Data: 19/05/2017

Versão atual: 1.1

Identificação do Projeto: Cartão Nacional de Identificação

Identificação da CA: IAC

Cliente: MJ

Documentos Relacionados

ID Documento	Detalhes	Autor(es)
PJ.CNICV_24.1.2_0001_pt_IAC.doc	Política de Certificado da EC de Identificação e Autenticação Civil	MULTICERT S.A.
PJ.CNICV_24.1.2_0002_pt_IAC.doc	Política de Certificado da EC de Identificação Civil Eletrónica	MULTICERT S.A.
PJ.CNICV_24.1.2_0003_pt_IAC.doc	Política de Certificados da EC de Controlo de Acessos	MULTICERT S.A.
PJ.CNICV_24.1.2_0004_pt_IAC.doc	Política de Certificados da Entidade Certificadora de Documentos	MULTICERT S.A.
PJ.CNICV_24.1.2_0005_pt_IAC.doc	Política de Certificados de Validação Cronológica	MULTICERT S.A.

Apêndices

ID Documento	Detalhes	Autor(es)
PJ.CNICV_53.2.1_0001_pt_IAC.doc	Formulário de emissão de certificado de EC subordinada da EC de Identificação e Autenticação Civil	MULTICERT S.A.
PJ.CNICV_53.2.4_0001_pt_IAC.doc	Formulário de receção de certificado de EC subordinada da EC de Identificação e Autenticação Civil	MULTICERT S.A.
PJ.CNICV_53.2.1_0002_pt_IAC.doc	Formulário de emissão de certificado de equipamento tecnológico pela EC de Identificação e Autenticação Civil	MULTICERT S.A.
PJ.CNICV_53.2.4_0002_pt_IAC.doc	Formulário de receção de certificado de equipamento tecnológico emitido pela EC de Identificação e Autenticação Civil	MULTICERT S.A.
PJ.CNICV_53.2.2_0001_pt_IAC.doc	Formulário de revogação de certificado emitido pela EC de Identificação e Autenticação Civil	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 (EC IAC) 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 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 da República de Cabo Verde encontra-se englobada na hierarquia da Infraestrutura de Chaves Públicas da República de Cabo Verde (ICP-CV).

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

Sumário

Resumo Executivo 3

Sumário 4

1 Introdução 11

Definições e acrónimos 12

1.1 Acrónimos 12
1.2 Definições 13
2 Contexto Geral 16

2.1 Enquadramento 16
2.2 Identificação do Documento 16
2.3 Participantes na Infraestrutura de Chave Pública 17
2.3.1 Entidades Certificadoras 17
2.3.2 Entidades de Registo 17
2.3.3 Titulares de certificados 17
2.3.4 Partes Confiantes 17
2.3.5 Outros participantes 18
2.4 Utilização do Certificado 19
2.4.1 Utilização adequada 19
2.4.2 Utilização não autorizada 19
2.5 Gestão das Políticas 19
2.5.1 Entidade responsável pela gestão do documento 19
2.5.2 Contacto 19
3 Disposições Legais 21

3.1 Obrigações e Direitos 21
3.1.1 Obrigações da EC 21
3.1.2 Obrigações das Unidades de Registo 22
3.1.3 Obrigações dos Titulares de Certificados 22
3.1.4 Obrigações das partes confiantes 22
3.1.5 Obrigações do Repositório 22
3.2 Responsabilidades 23
3.2.1 Responsabilidades da EC 23
3.2.2 Responsabilidades da Unidade de Registo 23
3.3 Publicação e Repositório 24
3.3.1 Frequência de Publicação 24
3.3.2 Controlo de acesso 25
3.4 Auditoria de Conformidade 25
3.4.1 Frequência ou motivo da auditoria 25
3.4.2 Identidade e qualificações do auditor 25
3.4.3 Relação entre o auditor e a Entidade Certificadora 25

3.4.4 Âmbito da auditoria 26
3.4.5 Procedimentos após uma auditoria com resultado deficiente 26
3.5 Sigilo 26
3.5.1 Chaves Privadas 26
3.5.2 Divulgação de Informação de Revogação e de Suspensão de Certificado 26
3.5.3 Quebra de sigilo por motivos legais 26
3.5.4 Informações a terceiros 26
3.5.5 Divulgação por solicitação do titular 27
3.5.6 Direitos de propriedade intelectual 27
4 IDENTIFICAÇÃO E AUTENTICAÇÃO 28
4.1 Registo Inicial 28
4.1.1 Disposições Legais 28
4.1.2 Tipos de nomes 28
4.1.3 Necessidade de nomes significativos 28
4.1.4 Interpretação de formato de nomes 29
4.1.5 Unicidade de nomes 29
4.1.6 Procedimento para resolver disputa de nomes 29
4.1.7 Reconhecimento, autenticação, e função das marcas registadas 29
4.1.8 Método de comprovação da posse de chave privada 29
4.1.9 Autenticação da identidade de uma pessoa singular 29
4.1.10 Autenticação da identidade de uma pessoa colectiva 30
4.1.11 Informação de subscritor/titular não verificada 31
4.1.12 Validação de Autoridade 31
4.2 Critérios para interoperabilidade 31
4.3 Identificação e Autenticação para pedidos de renovação de chaves 31
4.3.1 Identificação e autenticação para renovação de chaves, de rotina 31
4.3.2 Identificação e autenticação para renovação de chaves, após revogação 31
4.4 Identificação e autenticação para pedido de revogação 32
5 Requisitos operacionais do ciclo de vida do certificado 33
5.1 Pedido de Certificado 33
5.1.1 Requisitos 33
5.1.2 Quem pode subscrever um pedido de certificado? 33
5.1.3 Processo de registo e responsabilidades 33
5.2 Processamento do pedido de certificado 34
5.2.1 Requisitos 34
5.2.2 Processos para a identificação e funções de autenticação 34
5.2.3 Aprovação ou recusa de pedidos de certificado 34
5.2.4 Prazo para processar o pedido de certificado 34
5.3 Emissão de Certificado 35
5.3.1 Procedimentos para a emissão de certificado 35
5.3.2 Notificação da emissão do certificado ao titular 35
5.4 Aceitação do Certificado 35
5.4.1 Procedimentos para a aceitação de certificado 35
5.4.2 Publicação do certificado 36

5.4.3 Notificação da emissão de certificado a outras entidades 36
5.5 Uso do certificado e par de chaves 36
5.5.1 Uso do certificado e da chave privada pelo titular 36
5.5.2 Uso do certificado e da chave pública pelas partes confiantes 37
5.6 Renovação de Certificados Sem Geração de Novo Par de Chaves 37
5.6.1 Motivos para renovação de certificado 37
5.6.2 Quem pode submeter o pedido de renovação de certificado 37
5.6.3 Processamento do pedido de renovação de certificado 37
5.6.4 Notificação de emissão de novo certificado ao titular 37
5.6.5 Procedimentos para aceitação de certificado 37
5.6.6 Publicação de certificado após renovação 37
5.6.7 Notificação da emissão do certificado a outras entidades 38
5.7 Renovação de certificado com geração de novo par de chaves 38
5.7.1 Motivo para a renovação de certificado com geração de novo par de chaves 38
5.7.2 Quem pode submeter o pedido de certificação de uma nova chave pública 38
5.7.3 Processamento do pedido de renovação de certificado com geração de novo par de chaves 38
5.7.4 Notificação da emissão de novo certificado ao titular 38
5.7.5 Procedimentos para aceitação de um certificado renovado com geração de novo par de chaves 38
5.7.6 Publicação de certificado renovado com geração de novo par de chaves 38
5.7.7 Notificação da emissão de certificado renovado a outras entidades 39
5.8 Modificação de certificados 39
5.8.1 Motivos para alteração do certificado 39
5.8.2 Quem pode submeter o pedido de alteração de certificado 39
5.8.3 Processamento do pedido de alteração de certificado 39
5.8.4 Notificação da emissão de certificado alterado ao titular 39
5.8.5 Procedimentos para aceitação de certificado alterado 39
5.8.6 Publicação do certificado alterado 39
5.8.7 Notificação da emissão de certificado alterado a outras entidades 39
5.9 Suspensão e revogação de certificado 39
5.9.1 Circunstâncias para revogação 40
5.9.2 Quem pode submeter o pedido de revogação 40
5.9.3 Procedimento para o pedido de revogação 40
5.9.4 Produção de efeitos da revogação 41
5.9.5 Prazo para processar o pedido de revogação 41
5.9.6 Requisitos de verificação da revogação pelas partes confiantes 41
5.9.7 Motivos para suspensão 41
5.9.8 Quem pode submeter o pedido de suspensão 41
5.9.9 Procedimentos para pedido de suspensão 41
5.9.10 Limite do período de suspensão 41
5.9.11 Periodicidade da emissão da lista de certificados revogados (LCR) 41
5.9.12 Período máximo entre a emissão e a publicação da LCR 42
5.9.13 Disponibilidade de verificação online do estado / revogação de certificado 42
5.9.14 Requisitos de verificação online de revogação 42

5.9.15 Outras formas disponíveis para divulgação de revogação 42
5.9.16 Requisitos especiais em caso de comprometimento de chave privada 42
5.10 Serviços sobre o estado do certificado 42
5.10.1 Características operacionais 42
5.10.2 Disponibilidade do serviço 42
5.10.3 Características opcionais 42
5.11 Fim de subscrição 42
5.12 Procedimentos de auditoria de segurança 43
5.12.1 Tipo de eventos registados 43
5.12.2 Frequência da auditoria de registos 43
5.12.3 Período de retenção dos registos de auditoria 43
5.12.4 Protecção dos registos de auditoria 43
5.12.5 Procedimentos para a cópia de segurança dos registos 43
5.12.6 Sistema de recolha de registos (Interno / Externo) 43
5.12.7 Notificação de agentes causadores de eventos 44
5.12.8 Avaliação de vulnerabilidades 44
5.13 Arquivo de registos 44
5.13.1 Tipo de dados arquivados 44
5.13.2 Período de retenção em arquivo 44
5.13.3 Protecção dos arquivos 44
5.13.4 Procedimentos para as cópias de segurança do arquivo 44
5.13.5 Requisitos para validação cronológica dos registos 44
5.13.6 Sistema de recolha de dados de arquivo (Interno / Externo) 44
5.13.7 Procedimentos de recuperação e verificação de informação arquivada 45
5.14 Renovação de chaves 45
5.15 Recuperação em caso de desastre ou comprometimento 45
5.15.1 Procedimentos em caso de incidente ou comprometimento 45
5.15.2 Corrupção dos recursos informáticos, do software e/ou dos dados 45
5.15.3 Procedimentos em caso de comprometimento da chave privada da entidade 45
5.15.4 Capacidade de continuidade da atividade em caso de desastre 46
5.16 Procedimentos em caso de extinção de EC ou ER 46
5.17 Retenção e recuperação de chaves (*Key escrow*) 46
5.17.1 Políticas e práticas de recuperação de chaves 46
5.17.2 Políticas e práticas de encapsulamento e recuperação de chaves de sessão 46
6 Medidas de segurança física, de gestão e operacionais 47
6.1 Medidas de segurança física 47
6.1.1 Construção e Localização Física das Instalações da EC 47
6.1.2 Acesso físico ao local 47
6.1.3 Energia e ar condicionado 48
6.1.4 Exposição à água 48
6.1.5 Prevenção e protecção contra incêndio 48
6.1.6 Salvaguarda de suportes de armazenamento 49
6.1.7 Eliminação de resíduos 49
6.1.8 Instalações externas (alternativa) para recuperação de segurança 49

6.2 Medida de segurança dos processos 49
6.2.1 Funções de Confiança 50
6.2.2 Número de pessoas exigidas por tarefa 52
6.2.3 Identificação e Autenticação para cada função 52
6.2.4 Funções que requerem separação de responsabilidades 53
6.3 Medidas de Segurança de Pessoal 53
6.3.1 Requisitos relativos às qualificações, experiência, antecedentes e credenciação 53
6.3.2 Procedimento de verificação de antecedentes 54
6.3.3 Requisitos de formação e treino 54
6.3.4 Frequência e requisitos para acções de reciclagem 54
6.3.5 Frequência e sequência da rotação de funções 54
6.3.6 Sanções para acções não autorizadas 54
6.3.7 Requisitos para prestadores de serviços 55
6.3.8 Documentação fornecida ao pessoal 55
7 MEDIDAS DE SEGURANÇA TÉCNICAS 56
7.1 Geração e instalação do par de chaves 56
7.1.1 Geração do par de chaves 56
7.1.2 Entrega da chave privada ao titular 56
7.1.3 Entrega da chave pública ao emissor do certificado 56
7.1.4 Entrega da chave pública da EC às partes confiantes 56
7.1.5 Dimensão das chaves 56
7.1.6 Parâmetros da chave pública e verificação da qualidade 57
7.1.7 Utilização das Chaves (campo "*key usage*" X.509 v3) 57
7.2 Protecção da chave privada e características do módulo criptográfico 57
7.2.1 Normas e medidas de segurança do módulo criptográfico 57
7.2.2 Controlo multi-pessoal (m de n) para a chave privada 57
7.2.3 Retenção da chave privada (*key escrow*) 58
7.2.4 Cópia de segurança da chave privada 58
7.2.5 Arquivo da chave privada 58
7.2.6 Transferência da chave privada para/do módulo criptográfico 58
7.2.7 Armazenamento da chave privada no módulo criptográfico 58
7.2.8 Processo para activação da chave privada 58
7.2.9 Processo para desactivação da chave privada 58
7.2.10 Processo para destruição da chave privada 58
7.2.11 Avaliação/nível do módulo criptográfico 59
7.3 Outros aspectos da gestão do par de chaves 59
7.3.1 Arquivo da chave pública 59
7.3.2 Períodos de validade do certificado e das chaves 59
7.4 Dados de activação 59
7.4.1 Geração e instalação dos dados de activação 59
7.4.2 Protecção dos dados de activação 59
7.4.3 Outros aspectos dos dados de activação 60
7.5 Medidas de segurança informáticas 60
7.5.1 Requisitos técnicos específicos 60

7.5.2 Avaliação/nível de segurança 60
7.6 Ciclo de vida das medidas técnicas de segurança 60
7.6.1 Medidas de desenvolvimento do sistema 60
7.6.2 Medidas para a gestão da segurança 60
7.6.3 Ciclo de vida das medidas de segurança 60
7.7 Medidas de Segurança da rede 61
7.8 Validação cronológica (*Time-stamping*) 61
8 PERFIS DE CERTIFICADO, CRL, E OCSP 62
8.1 Perfil de Certificado 62
8.2 Perfil da lista de revogação de certificados 62
8.3 Perfil OCSP 63
9 Administração de Especificação 64
9.1.1 Procedimentos de mudança de especificação 64
9.1.2 Políticas de publicação e notificação 64
9.1.3 Procedimentos para Aprovação 64
10 OUTRAS SITUAÇÕES E ASSUNTOS LEGAIS 65
10.1 Taxas 65
10.1.1 Taxas por emissão ou renovação de certificados 65
10.1.2 Taxas para acesso a certificado 65
10.1.3 Taxas para acesso a informação do estado do certificado ou de revogação 65
10.1.4 Taxas para outros serviços 65
10.1.5 Política de reembolso 65
10.2 Responsabilidade financeira 65
10.2.1 Seguro de cobertura 65
10.2.2 Outros recursos 65
10.2.3 Seguro ou garantia de cobertura para utilizadores 65
10.3 Confidencialidade da informação processada 66
10.3.1 Âmbito da confidencialidade da informação 66
10.3.2 Informação fora do âmbito da confidencialidade da informação 66
10.3.3 Responsabilidade de protecção da confidencialidade da informação 66
10.4 Privacidade dos dados pessoais 66
10.4.1 Medidas para garantia da privacidade 66
10.4.2 Informação privada 67
10.4.3 Informação não protegida pela privacidade 67
10.4.4 Responsabilidade de protecção da informação privada 67
10.4.5 Notificação e consentimento para utilização de informação privada 67
10.4.6 Divulgação resultante de processo judicial ou administrativo 67
10.4.7 Outras circunstâncias para revelação de informação 67
10.5 Renúncia de garantias 67
10.6 Indemnizações 67
10.7 Termo e cessação da atividade 67
10.7.1 Termo 67
10.7.2 Substituição e revogação da DPC 67
10.7.3 Consequências da cessação de atividade 68

10.8 Notificação individual e comunicação aos participantes 68
10.9 Alterações 68
10.9.1 Procedimento para alterações 68
10.9.2 Prazo e mecanismo de notificação 68
10.9.3 Motivos para mudança de OID 69
10.10 Disposições para resolução de conflitos 69
10.11 Legislação aplicável 69
10.12 Conformidade com a legislação em vigor 69
10.13 Providências várias 69
10.13.1 Acordo completo 69
10.13.2 Independência 69
10.13.3 Severidade 70
10.13.4 Execuções (taxas de advogados e desistência de direitos) 70
10.13.5 Força Maior 70
10.14 Outras providências 70
Referências Bibliográficas 71
Aprovação da Entidade Credenciadora 72

1 Introdução

Objetivos

O objetivo deste documento é definir os procedimentos e práticas utilizadas pela Entidade de Certificação de Identificação e Autenticação Civil de Cabo Verde no suporte à sua atividade de certificação digital.

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.

Estrutura do Documento

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

Os primeiros oito capítulos são dedicados a descrever os procedimentos e práticas mais importantes no âmbito da certificação digital da Entidade de Certificação de Identificação e Autenticação Civil de Cabo Verde. O capítulo nove descreve matérias legais.

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

Definições e acrónimos

1.1 Acrónimos

Acrónimo	
ANSI	*American National Standards Institute*
CA	*Certification Authority* (o mesmo que EC)
CRL	Ver LRC
DL	Decreto-Lei
DN	*Distinguished Name*
DPVC	Declaração de Práticas de Validação Cronológica
EC	Entidade de Certificação
GMT	Tempo Médio de Greenwich (*Greenwich Mean Time*)
IAC	Identificação e Autenticação Civil
ICP-CV	Infraestrutura de Chaves Públicas da República de Cabo Verde
LRC	Lista de Revogação de Certificados
MAC	*Message Authentication Codes*
OCSP	*Online Certificate Status Protocol*
OID	Identificador de Objeto
PC	Política de Validação Cronológica
PKCS	*Public-Key Cryptography Standards*
PKI	*Public Key Infrastructure* (Infraestrutura de Chave Pública)
SHA	*Secure Hash Algorithm*

SSCD	*Secure Signature-Creation Device*
TSA	*Time-Stamping Authority* (o mesmo que EVC)

1.2 Definições

Definição	
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 suscetível 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 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 previstos.
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.
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	Recetor 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*
UTC(k)	Escala de tempo fornecida pelo laboratório "k" que garante ±100 ns em relação ao UTC (conforme *ITU-R Recommendation TF.536-1*)
Validação cronológica	Declaração de uma EVC que atesta a data e hora da criação, expedição ou receção de um documento eletrónico.

2 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 pelo que se pretende 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 de Certificação de Identificação e Autenticação Civil de Cabo Verde (EC IAC) 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 IAC. Este documento pode sofrer atualizações regulares e está sujeito a revisões anuais.

Os Certificados emitidos pela EC IAC 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.

2.1 Enquadramento

As práticas de criação, assinatura e de emissão de Certificados, assim como de revogação de certificados 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 IAC (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*.

Satisfaz os requisitos impostos pela Declaração de Práticas de Certificação da ECR-CV e especifica como implementar os seus procedimentos e controlos, e ainda como a EC IAC atinge os requisitos especificados.

2.2 Identificação do Documento

Este documento é a Declaração de Práticas de Certificação da EC IAC. 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 o 2.16.132.1.3.3. O OID da Política de Certificado é utilizado de acordo com o explicitado na secção 4.1.2.

Este documento é identificado pelos dados constantes na seguinte tabela:

INFORMAÇÃO DO DOCUMENTO	
Versão do Documento	Versão 1.1
Estado do Documento	Aprovado
OID	2.16.132.1.3.3
Data de Emissão	Junho 2017
Validade	1 ano
Localização	https://pki.cni.gov/pub/pol/dpc_eciac.html

2.3 Participantes na Infraestrutura de Chave Pública

2.3.1 Entidades Certificadoras

A EC IAC insere-se na hierarquia de confiança da ICP-CV (Infraestrutura de Chaves Públicas da República de Cabo Verde), constituindo-se numa Entidade Certificadora do Estado, sendo o seu certificado assinado pela entidade certificadora de topo da cadeia de certificação da ICP-CV (i.e., pela Entidade Certificadora Raiz de Cabo verde. Deste modo, a EC IAC encontra-se no nível imediatamente abaixo da EC Raiz de Cabo Verde. A sua função principal providenciar a gestão de serviços de certificação: emissão, operação, suspensão, revogação dos certificados por si emitidos.

A EC IAC emite certificados de:

- Entidade de Certificação subordinada, i.e., certificados para entidades certificadoras subordinadas no âmbito do Cartão Nacional de Identificação,
- Serviços do Cartão Nacional de Identificação, i.e., certificados para serviços necessários no âmbito do Cartão Nacional de Identificação:
    - Entidade Certificadora de Documentos,
    - Validação cronológica.

2.3.2 Entidades de Registo

Nada a assinalar.

2.3.3 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 ICP-CV[2], são considerados titulares de certificados emitidos pela EC IAC, aqueles cujo nome está inscrito no campo *Subject* do certificado, que 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:

- Entidades de Certificação Subordinadas;
- Equipamentos tecnológicos – Entidade Certificadora de Documentos e Validação Cronológica

2.3.3.1 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.

2.3.4 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.

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

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

2.3.5 Outros participantes

2.3.5.1 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 ANAC, no contexto de objetivos estratégicos previamente fixados pela própria,
g) Gestão da bolsa de auditores;
h) Apresentação à ANAC de proposta de registo e de rescisão de registo de entidades certificadoras na ICP-CV;
i) Promoção da competência técnica dos auditores.

2.3.5.2 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.

2.4 Utilização do Certificado

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

a) Controlo de acessos;
b) Confidencialidade;
c) Integridade;
d) Autenticação e,
e) 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 IAC e ICP-CV proporcionam. Assim, os serviços de identificação, 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.

2.4.1 Utilização adequada

Os requisitos e regras definidos neste documento aplicam-se a todos os certificados emitidos pela EC IAC.
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 IAC são também utilizados pelas Partes Confiantes para verificação da cadeia de confiança de um certificado emitido sob a EC IAC, 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 IAC.

2.4.2 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 IAC não poderão ser utilizados para qualquer função fora do âmbito das utilizações descritas anteriormente.
Os serviços de certificação oferecidos pela EC IAC, não foram desenhados nem estão autorizados a ser utilizados em atividades de alto risco ou que requeiram uma 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.

2.5 Gestão das Políticas

2.5.1 Entidade responsável pela gestão do documento

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

2.5.2 Contacto

Nome:	*MJ - 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**

3 Disposições Legais

3.1 Obrigações e Direitos

3.1.1 Obrigações da EC

A Entidade Certificadora de Identificação e Autenticação Civil 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 da 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, a 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 5.9 deste documento e publicar os certificados revogados na CRL do repositório da respetiva EC, com a frequência estipulada na secção 5.9.11,

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, 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 ANAC (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 5.10.2,

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 IAC e da ECR-CV.

3.1.2 Obrigações das Unidades de Registo

Nada a assinalar.

3.1.3 Obrigações dos Titulares de Certificados

É obrigação dos titulares dos certificados emitidos:

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 5.9.3,

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 IAC.

3.1.4 Obrigações das partes confiantes

É obrigação das partes que confiem nos certificados emitidos pela EC IAC:

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 e 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 IAC publique no seu sítio *Web*.

3.1.5 Obrigações do Repositório

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

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 LRC;
    - Mínimo de 99,990% de respostas a pedidos do documento da DPC;

- Número máximo de pedidos de LRC: 50 pedidos/minuto;
- Número máximo de pedidos da DPC: 50 pedidos/minuto;
- Número médio de pedidos de LRC: 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:

- LRC 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.

3.2 Responsabilidades

3.2.1 Responsabilidades da EC

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

b) A EC IAC 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 IAC assume toda a responsabilidade mediante terceiros, pela atuação dos titulares e das funções necessárias à prestação de serviços de certificação;

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

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

g) A EC IAC 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 IAC não assume qualquer responsabilidade no caso de perda ou prejuízo:

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

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

   iv) Ocasionado pelo uso indevido ou fraudulento dos certificados, ou CRL emitidos pela EC IAC.

3.2.2 Responsabilidades da Unidade de Registo

Nada a assinalar.

3.3 Publicação e Repositório

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

O MJ disponibiliza sempre a seguinte informação pública online, 24hx7d:

- Cópia eletrónica do documento de políticas da ICP-CV, assinado eletronicamente, por indivíduo ou indivíduos, devidamente autorizados e com certificado digital atribuído para o efeito:
  - URI: http://pki.anac.cv/pub/pol/
- Cópia eletrónica deste documento e Políticas de Certificados (PC) mais atuais da EC IAC, assinada eletronicamente, por indivíduo ou indivíduos, devidamente autorizados e com certificado digital atribuído para o efeito:
  - DPC da EC IAC disponibilizada no URI:
    - http://pki.cni.gov.cv/pub/pol/dpc_eciac.html
  - PC de certificado da EC IAC disponibilizada no URI:
    - http://pki.cni.gov.cv/pub/pol/pc_eciac.html
  - PC de certificado da EC eID disponibilizada no URI:
    - http://pki.cni.gov.cv/pub/politicas/pc_eceid.html
  - DPC da EC eID disponibilizada no URI:
    - http://pki.cni.gov.cv/pub/pol/dpc_eceid.html
  - PC de certificado de Entidade Certificadora de Documentos disponibilizada no URI:
    - http://pki.cni.gov.cv/pub/pol/pc_ecd.html
  - PC de certificado de Validação Cronológica disponibilizada no URI:
    - http://pki.cni.gov.cv/pub/pol/pc_tsa.html
- LRC da EC IAC – URI:
  - http://pki.cni.gov.cv/pub/lrc/iac_crl<ID_CA>_crl.crl
- Certificado da EC IAC – URI:
  - http://pki.cni.gov.cv/pub/certificado/eciac.crt
- Outra informação relevante – URI:
  - http://pki.cni.gov.cv/pub/info/

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

3.3.1 Frequência de Publicação

O MJ garante que será disponibilizada sempre a seguinte informação pública online, utilizando os mesmos protocolos e garantindo a mesma disponibilidade do repositório da EC IAC:

- Cópia eletrónica do DPC e PC mais atuais de cada EC subordinada, assinada eletronicamente, por indivíduo devidamente autorizado e com certificado digital atribuído para o efeito – URI a ser identificado pela EC subordinada;
- LRC 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.

3.3.2 Controlo de acesso

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

3.4 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 IAC.

Para além de auditorias de conformidade, o MJ irá efetuar outras fiscalizações e investigações para assegurar a conformidade da EC IAC com a legislação nacional. A execução destas auditorias, fiscalizações e investigações poderá ser delegada a uma entidade externa de auditoria.

3.4.1 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[3]. 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 identificadas e implementadas todas as medidas necessárias para a segurança de informação.

3.4.2 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 chave 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 sistemas de informação,

b) Independência a nível orgânico da Entidade Certificadora (para os casos de auditorias externas),

c) Credenciado pela Entidade Credenciadora.

3.4.3 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 garantida a inexistência de qualquer vínculo contratual.

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

O cumprimento do estabelecido na legislação em vigor sobre a proteção de dados pessoais, deve ser tida em conta por parte do auditor, na medida em que o auditor poderá aceder a dados pessoais dos ficheiros dos titulares das EC.

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

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).

3.4.4 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).

3.4.5 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.

3.5 Sigilo

3.5.1 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.

3.5.2 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.

3.5.3 Quebra de sigilo por motivos legais

O MJ disponibiliza, mediante ordem judicial ou por determinação legal, documentos, informações ou registos da EC IAC que estejam à sua guarda.

3.5.4 Informações a terceiros

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

3.5.5 Divulgação por solicitação do titular

Não aplicável.

3.5.6 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 IAC pertencem ao MJ.

4 IDENTIFICAÇÃO E AUTENTICAÇÃO

4.1 Registo Inicial

4.1.1 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 IAC está sempre na dependência do MJ. O patrocinador dos certificados de equipamentos tecnológicos será um colaborador devidamente identificado, de um organismo na dependência do MJ.

4.1.2 Tipos de nomes

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

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

Tipo de Certificado	OID da Política de Certificados
EC IAC	2.16.132.1.2.1 [4]
EC eID	2.16.132.1.2.2 [5]
EC subordinada de Controlo de Acessos	2.16.132.1.2.3 [6]
Entidade Certificadora de Documentos	2.16.132.1.2.4 [7]
Validação cronológica	2.16.132.1.2.6 [8]

4.1.3 Necessidade de nomes significativos

A EC IAC 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.

[4] cf. PJ.CNICV_24.1.2_0001_pt_IAC.doc. 2017, Política de Certificados da EC de identificação e Autenticação Civil.
[5] cf. PJ.CNICV_24.1.2_0002_pt_ IAC.doc. 2017, Política de Certificados da EC do Cartão Nacional de Identificação.
[6] cf. PJ.CNICV_24.1.2_0003_pt_ IAC.doc. 2017, Política de Certificados da EC de Controlo de Acessos.
[7] cf. PJ.CNICV_24.1.2_0004_pt_ IAC.doc. 2017, Política de Certificados da Entidade Certificadora de Documentos.
[8] cf. PJ.CNICV_24.1.2_0005_pt_ IAC.doc. 2017, Política de Certificados de Validação Cronológica.

4.1.4 Interpretação de formato de nomes

As regras utilizadas pela EC IAC para interpretar o formato dos nomes seguem o estabelecido no RFC 5280[9] 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 em *UTF8String*, com exceção dos atributos *country* e *serialnumber* que são codificados em *PrintableString*.

4.1.5 Unicidade de nomes

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

De acordo com os seus processos de emissão, a EC IAC e as suas EC subordinadas rejeitam, dentro de cada EC, 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.

4.1.6 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.

4.1.7 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 IAC e pelas EC subordinadas 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.

4.1.8 Método de comprovação da posse de chave privada

Para as Entidades de certificação subordinadas da EC IAC, é considerado um mecanismo aceitável como método de comprovação da posse de chave privada a utilização do *Certificate Management Protocol* (CMP) definido no RFC 4210[10].

Na EC IAC a comprovação da posse da chave privada será garantida através da presença física de um representante autorizado da entidade subordinada, na cerimónia de emissão desse tipo de certificados. Nessa cerimónia, o representante da entidade subordinada apresentará o pedido de certificado no formato PKCS#10[11].

No caso do equipamento tecnológico, a comprovação da posse da chave privada será garantida através da presença física do patrocinador (ver secção 2.3.3.1), que apresentará o pedido de certificado no formato PKCS#10, cf. secção 4.1.10.2

4.1.9 Autenticação da identidade de uma pessoa singular

Nada a assinalar.

[9] cf. RFC 5280. 2002, *Internet* X.509 *Public Key Infrastructure Certificate and Certificate Revocation List* (CRL) *Profile*.
[10] cf. RFC 4210. 2005, *Internet* X.509 *Public Key Infrastructure Certificate Management Protocol* (CMP).
[11] cf. RFC 2986. 2000, PKCS #10: *Certification Request Syntax Specification*, version 1.7.

4.1.10 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.

4.1.10.1 Documentos para efeitos de identificação de EC subordinada

O MJ guarda toda a documentação utilizada para verificação da identidade da entidade subordinada, garantindo a verificação da identidade dos seus representantes legais, por meio legalmente reconhecido, e garantindo, no caso dos seus representantes legais não se encontrarem na cerimónia de emissão de certificado, os poderes bastantes do representante nomeado pela entidade para a referida emissão.

O documento[12] que serve de base ao registo da entidade subordinada contém, entre outros, os seguintes elementos:

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 do bilhete de identidade ou qualquer outro elemento que permita a identificação inequívoca das pessoas singulares que estatutária ou legalmente a representam;

d) Endereço e outras formas de contacto;

e) Indicação de que o certificado é emitido para a entidade, enquanto entidade de certificação subordinada da EC IAC, na hierarquia de confiança da ICP-CV, de acordo com a presente DPC;

f) Nome único (DN) a ser atribuído ao certificado de EC subordinada;

g) Informação, se necessário, relativa à identificação e aos poderes do(s) representante(s) nomeados pela entidade para estarem presentes na cerimónia de emissão do certificado de EC subordinada;

h) Outras informações relativas ao formato do pedido de certificado a serem apresentadas na cerimónia de emissão do certificado de EC subordinada.

4.1.10.2 Documentos para efeitos de identificação de Certificado de equipamento tecnológico

O MJ guarda toda a documentação utilizada para verificação da identidade do patrocinador, garantindo que o mesmo tem os poderes bastantes de representante nomeado pela entidade para a emissão do certificado digital. O documento[13] que serve de base ao registo do pedido do certificado de equipamento tecnológico contém, entre outros, os seguintes elementos:

a) Denominação legal da pessoal coletiva (i.e., organismo da dependência do MJ);

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 permita a identificação inequívoca das pessoas singulares que estatutária ou legalmente a representam;

d) Endereço e outras formas de contacto;

e) Indicação de que o certificado digital de equipamento tecnológico é emitido para a entidade, na hierarquia de confiança da ICP-CV, de acordo com a presente DPC;

f) Nome único (DN) a ser atribuído ao certificado;

[12] cf. PJ.CNICV_53.2.1_0001_pt_IAC.doc. 2017, Formulário de emissão de certificado de EC subordinada da EC de identificação e Autenticação Civil
[13] cf. PJ.CNI_53.2.1_0002_pt_IAC.doc. 2017, Formulário de emissão de certificado de equipamento tecnológico pela EC de Identificação e Autenticação Civil.

g) Informação relativa à identificação e aos poderes do(s) patrocinador(es) nomeados pela entidade para efetuarem presencialmente o pedido do certificado digital de equipamento tecnológico (apresentado mediante o preenchimento de formulário próprio[14] e do fornecimento do pedido de certificado no formato PKCS#10);

h) Outras informações relativas ao formato do pedido de certificado, assim como ao conteúdo do DN do certificado.

O certificado e restantes dados necessários serão entregues ao patrocinador pelo método "cara-a-cara", sendo tal ato registado através do preenchimento e assinatura de formulário[15] que é arquivado pela EC IAC.

4.1.11 Informação de subscritor/titular não verificada

Toda a informação descrita nas secções 4.1.10.1 e 4.1.10.2 é verificada.

4.1.12 Validação de Autoridade

Nada a assinalar.

4.2 Critérios para interoperabilidade

De acordo com DPC da ECR-CV.

4.3 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.

4.3.1 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.

4.3.2 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.

[14] cf. PJ.CNICV_53.2.4_0001_pt_IAC.doc. 2017, Formulário de pedido de certificado de equipamento tecnológico emitido pela EC de Identificação e Autenticação Civil.
[15] cf. PJ.CNICV_53.2.4_0002_pt_IAC.doc. 2017, Formulário de receção de certificado de equipamento tecnológico emitido pela EC de Identificação e Autenticação Civil.

4.4 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[16].

A EC IAC 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[16] 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;

g) Informação das atividades a efetuar pela EC subordinada para revogar todos os certificados emitidos pela mesma, no caso de revogação de certificado de EC subordinada.

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

5 Requisitos operacionais do ciclo de vida do certificado

5.1 Pedido de Certificado

5.1.1 Requisitos

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

- Conformidade com as políticas definidas pela IAC;
- Pedido de certificado mediante apresentação de um pedido de certificado PKCS#10 válido;
- No caso de entidade subordinadas, o processo de credenciação da EC em questão já deve ter ocorrido e a mesma já deve ter autorização de início de atividade.

5.1.2 Quem pode subscrever um pedido de certificado?

Todas as entidades e organismos que atuem na dependência do MJ podem subscrever um pedido de certificado de entidade de certificação subordinada da EC IAC, apenas no âmbito do Cartão Nacional de Identificação.

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.

5.1.3 Processo de registo e responsabilidades

O processo de registo de EC subordinada (ou 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) pela EC subordinada (patrocinador, no caso de certificado de equipamento tecnológico);
- Geração do PKCS#10 correspondente pela EC subordinada (patrocinador, no caso de certificado de equipamento tecnológico);
- Geração do *hash* (SHA-256[17]) do PKCS#10, em formato PEM, pela EC subordinada (patrocinador, no caso de certificado de equipamento tecnológico);
- Arquivo do PKCS#10 e *hash* em suporte tecnológico não regravável (CD/DVD), pela EC subordinada (patrocinador, no caso de certificado de equipamento tecnológico);
- Preenchimento pela EC subordinada (patrocinador, no caso de certificado de equipamento tecnológico) de documento de validação da identidade da entidade, de acordo com secção 4.1.10.1;
- Envio do CD/DVD e do documento corretamente preenchido ao contacto da EC IAC.

[17] 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.*

5.2 Processamento do pedido de certificado

5.2.1 Requisitos

Os pedidos de certificado, depois de recebidos pela EC IAC, 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.

A presente secção e a secção 5.3 descrevem detalhadamente todo o processo

5.2.2 Processos para a identificação e funções de autenticação

Os Administradores de Segurança da EC IAC executam a identificação e a autenticação de toda a informação necessária nos termos da secção 4.1.10.

Os Administradores de Segurança da EC IAC aprovam 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 4.1.10.2 – toda a documentação utilizada para verificação da identidade e de poderes de representação, é guardada;
- 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 IAC 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[18].

5.2.3 Aprovação ou recusa de pedidos de certificado

A aprovação de certificado passa pelo cumprimento dos requisitos exigidos nos pontos 5.2.1 e 5.2.2. Quando tal não se verifique, é recusada a emissão do certificado.

5.2.4 Prazo para processar o pedido de certificado

Após a aprovação do pedido de certificado, o certificado deverá ser emitido em, não mais do que, cinco (5) dias úteis.

[18] PJ.CNICV_53.2.4_0002_pt_IAC.doc, Formulário de receção de certificado de equipamento tecnológico emitido pela EC de Identificação e Autenticação Civil

5.3 Emissão de Certificado

5.3.1 Procedimentos para a emissão de certificado

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

- Três (3) membros do Grupo de Trabalho – a segregação de funções não possibilita a presença de um número inferior de elementos,
- Quaisquer observadores aceites simultaneamente pelos membros do Grupo 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) do 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, o CD/DVD e o formulário de emissão do certificado aos membros do Grupo de Trabalho da EC IAC. 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 IAC efetuam o procedimento de arranque de processamento da EC IAC e emitem o certificado (correspondente ao PKCS#10 fornecido no CD/DVD);
- Os membros do Grupo de Trabalho da EC IAC arquivam o certificado num suporte tecnológico não regravável) e preenchem o formulário de receção e aceitação de certificado[19], 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 certificado, num suporte tecnológico não regravável, ao(s) representante(s) da entidade subordinada (ou patrocinador no caso de certificado de equipamento tecnológico).
- A cerimónia de emissão fica terminada com a execução do procedimento de finalização de processamento da EC IAC, pelos membros do Grupo de Trabalho da EC IAC;

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

5.3.2 Notificação da emissão do certificado ao titular

A emissão do certificado é efetuada de forma presencial, de acordo com a secção anterior.

5.4 Aceitação do Certificado

5.4.1 Procedimentos para a aceitação de certificado

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 cerimónia de emissão (conforme secção 5.3.1).

[19] 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.

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 formulário correspondente[20].

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.

5.4.2 Publicação do certificado

A EC IAC não publica os certificados emitidos, disponibilizando-o integralmente ao titular (ou patrocinador), com os constrangimentos definidos no ponto 5.4.1.

5.4.3 Notificação da emissão de certificado a outras entidades

Nada a assinalar.

5.5 Uso do certificado e par de chaves

5.5.1 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 nas 2.4.1 e 2.4.2;

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 LRC da EC IAC.

Adicionalmente,

- O certificado de EC subordinada só pode ser utilizado para assinar certificados e respetiva LRC, assim como certificados necessários para a operação e serviços (equipamentos tecnológicos) da EC subordinada,
- O certificado de Entidade Certificadora de Documentos tem como objetivo a assinatura de dados a colocar no Cartão Nacional de Identificação, garantindo-lhe integridade e Autenticidade,
- O certificado de servidor Web SSL tem como objetivo a sua utilização na autenticação e estabelecimento de canais cifrados de acordo com o protocolo SSL/TLS, por equipamento cujo nome qualificado do domínio esteja designado no campo "*CommonName*" ou na extensão *Subject Alternative Name*,
- O certificado de validação cronológica tem como objetivo a sua utilização em servidores de validação cronológica[21].

[20] 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
[21] *cf.* RFC 3161. 2001, *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).*

5.5.2 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 descritos nas Políticas e práticas de certificação;

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

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

5.6 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 anteriores do certificado, 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.

5.6.1 Motivos para renovação de certificado

Nada a assinalar.

5.6.2 Quem pode submeter o pedido de renovação de certificado

Nada a assinalar.

5.6.3 Processamento do pedido de renovação de certificado

Nada a assinalar.

5.6.4 Notificação de emissão de novo certificado ao titular

Nada a assinalar.

5.6.5 Procedimentos para aceitação de certificado

Nada a assinalar.

5.6.6 Publicação de certificado após renovação

Nada a assinalar.

5.6.7 Notificação da emissão do certificado a outras entidades

Nada a assinalar.

5.7 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.

5.7.1 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 ou indicia deterioração que poderá comprometer a sua utilização a curto prazo;

c) A informação do certificado sofre alterações.

5.7.2 Quem pode submeter o pedido de certificação de uma nova chave pública

Tal como na secção 5.1.2

5.7.3 Processamento do pedido de renovação de certificado com geração de novo par de chaves

Tal como na secção 5.2

5.7.4 Notificação da emissão de novo certificado ao titular

Tal como na secção 5.3.2

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

Tal como na secção 5.4.1

5.7.6 Publicação de certificado renovado com geração de novo par de chaves

Tal como na secção 5.4.2

5.7.7 Notificação da emissão de certificado renovado a outras entidades

Tal como na secção 5.4.3

5.8 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.

5.8.1 Motivos para alteração do certificado

Nada a assinalar.

5.8.2 Quem pode submeter o pedido de alteração de certificado

Nada a assinalar.

5.8.3 Processamento do pedido de alteração de certificado

Nada a assinalar.

5.8.4 Notificação da emissão de certificado alterado ao titular

Nada a assinalar.

5.8.5 Procedimentos para aceitação de certificado alterado

Nada a assinalar.

5.8.6 Publicação do certificado alterado

Nada a assinalar.

5.8.7 Notificação da emissão de certificado alterado a outras entidades

Nada a assinalar.

5.9 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.

5.9.1 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 IAC 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 IAC ou da ECR-CV;
- Incumprimento das responsabilidades previstas na presente DPC por parte da EC IAC ou do titular;
- Sempre que haja razões credíveis que induzam que os serviços de certificação possam ter sido comprometidos, de tal forma que coloquem em causa a fiabilidade dos certificados;
- Por resolução judicial ou administrativa.

5.9.2 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 5.9.1, os seguintes:

a) A EC subordinada (ou patrocinador, no caso de certificado de equipamento tecnológico) titular do certificado;

b) A EC IAC;

c) A Entidade Credenciadora;

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

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

5.9.3 Procedimento para o pedido de revogação

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

- Todos os pedidos de revogação devem ser endereçados para a EC IAC por escrito ou por mensagem eletrónica assinada digitalmente, em formulário de pedido de revogação[16];
- Identificação e autenticação da entidade que efetua o pedido de revogação, conforme secção 5.9.2
- Registo e arquivo do formulário de pedido de revogação;
- Análise do pedido de revogação pelo Conselho Executivo da EC IAC, que propõe ao responsável do organismo que tutela a EC IAC a aprovação ou recusa do pedido de revogação;
- Mediante o parecer do Conselho Executivo da EC IAC, o responsável do organismo que tutela a EC IAC, 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.

5.9.4 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.

5.9.5 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.

5.9.6 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 online (via OCSP).

5.9.7 Motivos para suspensão

A EC IAC não suspende certificados.

5.9.8 Quem pode submeter o pedido de suspensão

Nada a assinalar.

5.9.9 Procedimentos para pedido de suspensão

Nada a assinalar.

5.9.10 Limite do período de suspensão

Nada a assinalar.

5.9.11 Periodicidade da emissão da lista de certificados revogados (LCR)

A EC IAC publica uma nova LCR no repositório, sempre que haja uma revogação. Quando não existam alterações ao estado de validade dos certificados, ou seja, se nenhuma revogação se tiver produzido a EC IAC disponibiliza nova LCR a cada 30 dias.

5.9.12 Período máximo entre a emissão e a publicação da LCR

O período máximo entre a emissão e publicação da LCR não deve ultrapassar os 30 minutos.

5.9.13 Disponibilidade de verificação *on-line* do estado / revogação de certificado

Não Aplicável.

5.9.14 Requisitos de verificação *on-line* de revogação

Não aplicável.

5.9.15 Outras formas disponíveis para divulgação de revogação

Nada a assinalar.

5.9.16 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 5.15.3.

5.10 Serviços sobre o estado do certificado

5.10.1 Características operacionais

O estado dos certificados emitidos está disponível publicamente através das LCR.

5.10.2 Disponibilidade do serviço

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

5.10.3 Características opcionais

Nada a assinalar.

5.11 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.

5.12 Procedimentos de auditoria de segurança

5.12.1 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 LRC;
- 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.

5.12.2 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.

5.12.3 Período de retenção dos registos de auditoria

Os registos são mantidos por um mínimo de 3 (três) meses e posteriormente arquivados por 20 (vinte) anos, em ambiente controlado, existente para o efeito.

5.12.4 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.

5.12.5 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 de um mês.

5.12.6 Sistema de recolha de registos (Interno/Externo)

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

5.12.7 Notificação de agentes causadores de eventos

Eventos auditáveis são registados e guardados de forma segura, sem haver notificação ao sujeito causador da ocorrência do evento.

5.12.8 Avaliação de vulnerabilidades

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

5.13 Arquivo de registos

5.13.1 Tipo de dados arquivados

Todos os dados auditáveis são arquivados (conforme indicado na secção 5.12), assim como informação de pedidos de certificados e documentação de suporte ao ciclo de vida das várias operações.

5.13.2 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.

5.13.3 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 outro *software*, pela conservação do *hardware*, sistemas operativos e outro *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.

5.13.4 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*).

5.13.5 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.

5.13.6 Sistema de recolha de dados de arquivo (Interno/Externo)

Os sistemas de recolha de dados de arquivo são internos.

5.13.7 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.

5.14 Renovação de chaves

Apenas as entidades de certificação subordinadas da EC IAC, com certificados válidos, podem requerer a renovação do respetivo par de chaves. Na EC IAC, o conceito de renovação, pressupõe a geração de novo par de chaves, ou seja uma nova emissão.

5.15 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.

5.15.1 Procedimentos em caso de incidente ou comprometimento

Cópias de segurança das chaves privadas da EC (geradas e mantidas de acordo com a secção 7.4) e dos registos arquivados (secção 5.12.1) são guardados em ambientes seguros externos e disponíveis em caso de desastre ou de comprometimento.

5.15.2 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 MJ suspenderá os serviços da EC IAC e notificará a ANAC.

5.15.3 Procedimentos em caso de comprometimento da chave privada da entidade

No caso da chave privada da EC IAC 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 IAC e de todos os certificados emitidos no "ramo" da hierarquia de confiança da EC IAC,
- Notificação das EC subordinadas, ANAC e todos os titulares de certificados emitidos no "ramo" da hierarquia de confiança da EC IAC,
- Geração de novo par de chaves para a EC IAC, e pedido de novo certificado à ECR-CV,
- Renovação de todos os certificados emitidos no "ramo" da hierarquia de confiança da EC IAC.

5.15.4 Capacidade de continuidade da atividade em caso de desastre

O MJ 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.

5.16 Procedimentos em caso de extinção de EC ou ER

Em caso de cessação de atividade, como prestador de serviços de Certificação, a EC IAC 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 2 (dois) 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.

5.17 Retenção e recuperação de chaves (*Key escrow*)

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

5.17.1 Políticas e práticas de recuperação de chaves

A chave privada da EC IAC 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 IAC.

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 IAC 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 IAC 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.

5.17.2 Políticas e práticas de encapsulamento e recuperação de chaves de sessão

6 Nada a assinalar.Medidas de segurança física, de gestão e operacionais

O MJ implementou várias regras e políticas incidindo sobre controlos físicos, procedimentais e humanos, que suportam os requisitos de segurança constantes nesta 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.

6.1 Medidas de segurança física

6.1.1 Construção e Localização Física das Instalações da EC

As instalações da EC IAC 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 IAC 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 IAC:

- 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.

6.1.2 Acesso físico ao local

Os sistemas da EC IAC 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.

A 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.

6.1.3 Energia e ar condicionado

O ambiente seguro do MJ 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.

6.1.4 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 IAC.

6.1.5 Prevenção e proteção contra incêndio

O ambiente seguro do MJ 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.

6.1.6 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, a informação sensível é transportada da zona de alta segurança para o ambiente externo ao original, 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.

Nas 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).

6.1.7 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).

6.1.8 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).

6.2 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.

6.2.1 Funções de Confiança

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

O MJ estabeleceu que os papéis de confiança fossem 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.

6.2.1.1 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[22], 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[23] 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 seguranças 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.
- Arranque do interface de configuração da EC e das restantes entidades que formam a ICP do Cartão Nacional de Identificação.

6.2.1.2 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.

[22] Para elementos devidamente autorizados
[23] Os procedimentos a adoptar em relação aos documentos em formato electrónico serão definidos após a concretização do *Business Continuity Plan*

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.

6.2.1.3 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.

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;

6.2.1.4 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.

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.

6.2.1.5 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[24] e que estão devidamente identificados;
- Inspecionar a configuração estabelecida pelas tarefas de administração e os eventos registados;

[24] 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

6.2.1.6 Comissão Executiva

É responsável pela nomeação dos membros dos restantes grupos[25] 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,
- Pedir a aprovação de Políticas à Entidade Credenciadora
- Designar os membros dos restantes grupos de trabalho (à exceção do Grupo de Trabalho de Instalação, do Grupo de Trabalho de Auditoria e do Grupo de Trabalho de Custódia),
- Disponibilizar a identificação de todos os indivíduos que pertencem aos vários Grupos de Trabalho, em um ou mais pontos de acesso facilmente acessíveis pelos indivíduos autorizados.

6.2.1.7 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[26]. 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.

6.2.2 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-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.

6.2.3 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 IAC é feito com recurso à utilização de um certificado digital próprio emitido para o efeito.

[25] Com exceção do Grupo de Trabalho de Instalação e do Grupo de Trabalho de Custódia
[26] Definidas para cada um dos artefactos à sua guarda

6.2.4 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		✘	✘	✘	✘	✘	

6.3 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.

6.3.1 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.

6.3.2 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,
- Verificação de situação de crédito,
- Verificação de histórico de empregos anteriores,
- Comprovativo de escolaridade e de residência.

6.3.3 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.

6.3.4 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.

6.3.5 Frequência e sequência da rotação de funções

Nada a assinalar.

6.3.6 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 do MJ e das leis de segurança nacional, a todos os indivíduos que realizem ações não autorizadas ou que façam uso não autorizado dos sistemas.

6.3.7 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.

6.3.8 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.

7 MEDIDAS DE SEGURANÇA TÉCNICAS

Esta secção define as medidas de segurança implementadas para a EC IAC 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.

7.1 Geração e instalação do par de chaves

Apenas são gerados pares de chaves para a EC IAC sendo a sua geração processada de acordo com os requisitos e algoritmos definidos nesta política.

7.1.1 Geração do par de chaves

A geração de chaves criptográficas da EC IAC 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 IAC, cumpre os requisitos FIPS 140-1 nível 3 e/ou *Common Criteria* EAL 4+ 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 perda de dados, possa haver uma recuperação total e segura das chaves.

7.1.2 Entrega da chave privada ao titular

A EC IAC não gera a chave privada associada aos certificados que emite.

7.1.3 Entrega da chave pública ao emissor do certificado

A chave pública é entregue à EC IAC, de acordo com os procedimentos indicados na secção 5.3.1

7.1.4 Entrega da chave pública da EC às partes confiantes

A chave pública da EC IAC será disponibilizada através do certificado da EC IAC, assinado pela EC do Estado, conforme secção 5.4.2.

7.1.5 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 (o comprimento mínimo da chaves é 2048 bits RSA), para a chave da EC IAC,
- 4096 bits RSA (o comprimento mínimo da chaves é 2048 bits RSA), para a chave da EC subordinada eID. No entanto, devido a imperativos técnicos dos certificados emitidos pela EC subordinada de Controlo de Acessos (certificados não X.509), o tamanho de chave dessa será 1024 bits RSA,

- 2048 bits RSA para as chaves associadas aos certificados de equipamento tecnológico.

7.1.6 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).

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

De acordo com secção 8.1.

7.2 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 IAC. O MJ implementou uma combinação de controlos físicos, lógicos e procedimentos, devidamente documentados, de forma a assegurar confidencialidade e integridade das chaves privadas da EC IAC.

7.2.1 Normas e medidas de segurança do módulo criptográfico

Para a geração dos pares de chaves da EC IAC 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

7.2.2 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.

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

7.2.3 Retenção da chave privada (*key escrow*)

A retenção da chave privada da EC IAC é explicada em detalhe na secção 5.17

7.2.4 Cópia de segurança da chave privada

A chave privada da EC IAC tem pelo menos uma cópia de segurança, com o mesmo nível de segurança que a chave original, conforme secção 5.17

7.2.5 Arquivo da chave privada

As chaves privadas da EC IAC, alvo de cópias de segurança, são arquivadas conforme identificado na secção 5.17

7.2.6 Transferência da chave privada para/do módulo criptográfico

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

Mesmo se for feito uma cópia de segurança das chaves privadas da EC IAC 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.

7.2.7 Armazenamento da chave privada no módulo criptográfico

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

7.2.8 Processo para ativação da chave privada

A chave privada da EC IAC é ativada quando o sistema da EC é ligado. Esta ativação é efetivada através da autenticação no módulo criptográfico por, pelo menos, três elementos, 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.

7.2.9 Processo para desativação da chave privada

A chave privada da EC IAC é desativada assim que não seja necessária a sua utilização. Para a desativação das chaves privadas da EC IAC 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.

7.2.10 Processo para destruição da chave privada

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

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.

7.2.11 Avaliação/nível do módulo criptográfico

Descrito na secção 7.2.1

7.3 Outros aspetos da gestão do par de chaves

7.3.1 Arquivo da chave pública

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

7.3.2 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 deste, 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 da EC IAC tem uma validade de 12 anos, sendo utilizado para assinar certificados durante os seus primeiros cinco anos de validade, sendo reemitido após os primeiros quatro anos e nove meses de validade;
- O certificado de EC subordinada tem uma validade de seis anos, sendo utilizado para assinar certificados durante o seu primeiro ano de validade, sendo reemitido após os primeiros onze meses de validade;
- Os certificados de equipamento tecnológico (à exceção do certificado de servidor *Web*) têm uma validade de 3 anos e dois meses, renovados mensalmente;
- O certificado de servidor *Web* tem uma validade de três anos, sendo reemitido um mês antes do final da sua validade.

7.4 Dados de ativação

7.4.1 Geração e instalação dos dados de ativação

Os dados de ativação necessários para a utilização da chave privada da EC IAC 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.

7.4.2 Proteção dos dados de ativação

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

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

7.4.3 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.

7.5 Medidas de segurança informáticas

7.5.1 Requisitos técnicos específicos

O acesso aos servidores da EC IAC 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 IAC 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.

7.5.2 Avaliação/nível de segurança

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

O módulo criptográfico em *Hardware* da EC IAC satisfaz a norma EAL 4+ *Common Criteria for Information Technology Security Evaluation* e/ou FIPS 140-1 nível 3.

7.6 Ciclo de vida das medidas técnicas de segurança

7.6.1 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 fornecida metodologia auditável que permite verificar que o *software* da EC IAC 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.

7.6.2 Medidas para a gestão da segurança

O MJ tem mecanismos e/ou Grupos de Trabalho para controlar e monitorizar a configuração dos sistemas da EC. O sistema da EC IAC, 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.

7.6.3 Ciclo de vida das medidas de segurança

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

7.7 Medidas de Segurança da rede

A EC IAC 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.

7.8 Validação cronológica (*Time-stamping*)

Certificados, LRCs 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.

8 PERFIS DE CERTIFICADO, CRL, E OCSP

8.1 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, uma estrutura de dados que faz 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[9].

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 de 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[9].

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

- Recomendação ITU.T X.509,
- RFC 5280 e,
- Política de Certificados da ICP-CV[27].

Os perfis dos certificados podem ser consultados nos documentos de Políticas de Certificados associadas a esta DPC, de acordo com a secção 3.3.

8.2 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.

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 (LRC). A LRC é uma lista com identificação temporal dos certificados revogados, assinada pela EC e disponibilizada livremente num repositório público. Cada certificado revogado é identificado na LRC 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 LRC mais recente e verifica se o número de série do certificado não faz parte da mesma. Note-se que uma EC emite uma nova LRC numa base regular periódica.

O perfil da LRC está de acordo com:

- Recomendação ITU.T X.509**Erro! Indicador não definido.**,

27 ANAC – Conteúdo Mínimo das Políticas de Certificado

- RFC 5280 e,
- Política de Certificados da ICP-CV**Erro! Indicador não definido.**.

Os perfis das LRC podem ser consultados nos documentos de Políticas de Certificados associadas a esta DPC, relativamente à EC IAC (de acordo com a secção 3.3.)

8.3 Perfil OCSP

Não Aplicável.

9 Administração de Especificação

9.1.1 Procedimentos de mudança de especificação

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

9.1.2 Políticas de publicação e notificação

As acualizações a esta DPC e respetivas PCs serão publicadas imediatamente após a sua aprovação pela Entidade Credenciadora, de acordo com a secção 10.9.1.

9.1.3 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 submetida à Entidade Credenciadora, que é a entidade responsável pela aprovação e autorização de modificações neste tipo de documentos.

10 OUTRAS SITUAÇÕES E ASSUNTOS LEGAIS

Esta secção aborda aspetos de negócio e assuntos legais.

10.1 Taxas

10.1.1 Taxas por emissão ou renovação de certificados

Nada a assinalar.

10.1.2 Taxas para acesso a certificado

Nada a assinalar.

10.1.3 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.

10.1.4 Taxas para outros serviços

Nada a assinalar.

10.1.5 Política de reembolso

Nada a assinalar.

10.2 Responsabilidade financeira

10.2.1 Seguro de cobertura

Nada a assinalar.

10.2.2 Outros recursos

Nada a assinalar.

10.2.3 Seguro ou garantia de cobertura para utilizadores

Nada a assinalar.

10.3 Confidencialidade da informação processada

10.3.1 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 IAC;

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

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

d) Toda a informação de carácter pessoal proporcionada à EC IAC 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 IAC (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 IAC 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 IAC;

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

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

10.3.2 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) LRC e,

d) Toda a informação classificada como "pública" (informação não expressamente considerada como "pública" será considerada confidencial).

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

10.3.3 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.

10.4 Privacidade dos dados pessoais

10.4.1 Medidas para garantia da privacidade

Nada a assinalar, dado que não são emitidos certificados pessoais sob a EC IAC.

10.4.2 Informação privada

Nada a assinalar.

10.4.3 Informação não protegida pela privacidade

Nada a assinalar.

10.4.4 Responsabilidade de proteção da informação privada

Nada a assinalar.

10.4.5 Notificação e consentimento para utilização de informação privada

Nada a assinalar.

10.4.6 Divulgação resultante de processo judicial ou administrativo

Nada a assinalar.

10.4.7 Outras circunstâncias para revelação de informação

Nada a assinalar.

10.5 Renúncia de garantias

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

10.6 Indemnizações

De acordo com a legislação em vigor

10.7 Termo e cessação da atividade

10.7.1 Termo

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

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

10.7.2 Substituição e revogação da DPC

O Conselho Executivo ou a Entidade Credenciadora podem decidir em favor da eliminação ou emenda de um documento relacionado com a EC IAC (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.

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

10.8 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.

10.9 Alterações

10.9.1 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 Credenciadora para aprovação. Depois da sua aprovação, o documento é submetido para o Conselho Executivo para publicação, tornando-se as alterações finais e efetivas.

10.9.2 Prazo e mecanismo de notificação

No caso em que a Entidade Credenciadora 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.

10.9.3 Motivos para mudança 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 a 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.

10.10 Disposições para resolução de conflitos

Todos os conflitos entre utilizadores e a EC IAC deverão ser comunicados 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 DPC, as partes, com renúncia a qualquer outro foro que pudesse corresponder-lhes, submetem-se à Jurisdição de Contencioso Administrativo.

10.11 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) Aviso nº 001/CA/2008

e) Portaria nº 4/2008

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

10.12 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 anterior.

10.13 Providências várias

10.13.1 Acordo completo

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

10.13.2 Independência

No caso em 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 Entidade Credenciadora a avaliação da essencialidade das mesmas.

10.13.3 Severidade

Nada a assinalar.

10.13.4 Execuções (taxas de advogados e desistência de direitos)

Nada a assinalar.

10.13.5 Força Maior

Nada a assinalar.

10.14 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 (v1.7).*

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 5280. 2008, *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).*

Aprovação da Comissão Executiva