NOSi, EPE – Núcleo Operacional da Sociedade de Informação

Declaração de Práticas de Certificação de Entidade Certificadora NOSI CA – G2

Versão	Data	Autor
1.0	27/07/2021	Direção de Segurança & Compliance

Controlo de Documentação

Cód.	Versão	Data da Versão	Criado por	Aprovado por	Classificação
	1.0	27/07/2021	Direção de Segurança & Compliance		Público

Histórico de Alterações

Versão	Data	Alterado por	Descrição
1.0	27/07/2021		Criação do Documento

Implementado	Revisto	Aprovado

Informações de Contacto

Nome	Endereço	Email
Direção de Segurança & Compliance	Praia-Santiago	dsc@nosi.cv

Índice

1. Introdução

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 sendo objetivo deste documento nomear regras legais ou obrigações, mas sim informar, pretende-se que este documento seja simples, direto e entendido por um público alargado, incluindo pessoas sem conhecimentos técnicos ou legais.

Este documento descreve as práticas gerais de emissão e gestão de certificados, seguidas pela Entidade de Certificação Subordinada NOSI CA – G2, doravante NOSI CA, e, explica o significado e função de um certificado, assim como os procedimentos que deverão ser seguidos por Partes Confiantes e por qualquer outra pessoa interessada, para confiarem nos certificados emitidos pelo NOSI CA. Este documento pode sofrer atualizações regulares.

Os certificados emitidos pelo NOSI CA 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.

1.1. Visão geral

As práticas de criação, assinatura e de emissão de certificados, assim como de revogação de certificados inválidos, levadas a cabo por uma Entidade de Certificação (EC) são fundamentais para garantir a fiabilidade e confiança de uma infraestrutura de Chaves Públicas ("*PKI – Public Key Infrastructure*").

Este documento aplica-se especificamente ao NOSI CA, respeita e implementa os *standards* identificados no capítulo "Referências Bibliográficas".
O objetivo deste documento é definir os procedimentos e práticas utilizadas pelo NOSI CA, no suporte à sua atividade de certificação digital.

1.1.1. Público alvo

Este documento é público e destina-se a todos quantos se relacionam com o NOSI CA.

1.2. Nome e Identificação do Documento

Este documento segue a estrutura definida e proposta pelo grupo de trabalho PKIX do IETF, no documento RFC 3647 [1], bem como os "REQUISITOS MÍNIMOS DE REDACÇÃO PARA DECLARAÇÃO DE PRÁTICAS DE CERTIFICAÇÃO (DPC) DA ICP-CV".

O ponto 1.6. apresenta um conjunto de acrónimos e definições úteis para a leitura do documento. Os oito seguintes, são dedicados aos procedimentos e práticas mais importantes no âmbito da certificação digital do NOSI CA. O Nono ponto é reservado a matérias legais.

Este documento é identificado pelos dados constantes na seguinte tabela:

Informação do documento	
Versão do Documento	Versão 1.0
Estado do Documento	
OID	
Data de Emissão	14/07/2021
Validade	1 ano
Localização	https://nosi.cv

1.3. Participantes PKI

1.3.1. Entidades Certificadoras

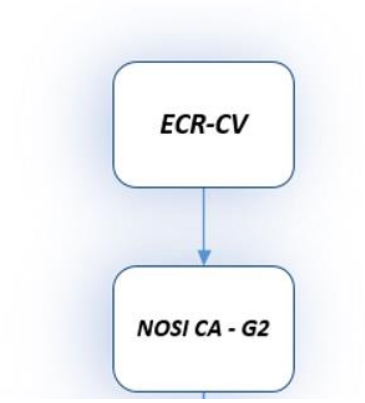
[1] cf. RFC 3647. 2003, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

O NOSI CA é uma entidade de certificação credenciada pela Autoridade Credenciadora, conforme previsto na legislação Cabo-verdiana, estando deste modo habilitada legalmente a emitir todo o tipo de certificados digitais, incluindo os certificados digitais qualificados. Insere-se em duas hierarquias de confiança:

- Entidade Certificadora de Raiz de Cabo Verde (ECR-CV);
- NOSI Certificate Authority (NOSI CA);

Deste modo, o NOSI CA é reconhecido na maioria dos sistemas operativos sendo a sua função principal providenciar a gestão de serviços de certificação: emissão, operação, suspensão, revogação para os seus subscritores.

Esquematicamente:



O NOSI CA emite certificados:

- Certificados Qualificados:
  - Assinatura Qualificada para pessoa singular:
    - Individual
      - ✓ Particular - Certificado emitido que inclui o nome do seu titular, que será utilizado para assinar documentos.

- ✓ Assinatura Qualificada de Qualidade (ordens Profissionais) Certificado com as mesmas características do Particular, no entanto acrescido de um atributo de qualidade, associado a uma entidade/organização (ex. Médico, Engenheiro, etc).

- ✓ Assinatura Qualificada para Representação de pessoa Coletiva Certificado com as mesmas características do Particular, no entanto acrescido de um atributo no qual é conferido os efeitos de representação de uma Organização ao seu titular. Estes poderes de representação são delegados ou conferidos pelos representantes legais da organização.

  - Assinatura Qualificada para pessoa coletiva:

    - ✓ Selo Eletrónico – Certificado emitido para a Organização, ou seja, o titular do certificado é uma pessoa coletiva. Este Certificado pode ser utilizado, a título de exemplo, para assinatura de faturas eletrónicas (emissão de grandes volumes com segurança acrescida), extratos de conta eletrónicos, declarações eletrónicas, certidões e outros tipos de documentos emitidos online por entidades públicas.

- Assinatura Eletrónica Avançada
  - ✓ Assinatura Avançada Singular - Certificados emitidos para particulares e profissionais, permitindo a assinatura eletrónica de documentos (sem valor probatório) e a identificação eletrónica segura e unívoca de uma pessoa.

1.3.2. Entidades Registo

Entidade de Registo (ER) é a entidade que aprova os nomes distintos (DN) dos titulares dos certificados e mediante avaliação do pedido, aceita ou rejeita a solicitação do mesmo.

Para além disso, a ER também tem autoridade para aprovar a revogação ou suspensão de certificados.
São ER's da PKI do NOSI:

- ER Interna - Operacionalizada pelos serviços internos do PKI do NOSI, detentora da EC.

As Entidades de Registo do PKI NOSI, cumprem os requisitos estabelecidos neste documento e estão sujeitas a Auditorias Externas, assim como Auditorias Internas.
As auditorias externas são efetuadas por auditores credenciados pela Autoridade Credenciadora Nacional.

1.3.2.1. ER Interna

No âmbito da Entidade de Certificação NOSI, a entidade de registo materializa-se pelos serviços internos da mesma que procedem ao registo e validação dos dados necessários, conforme explicitado na Política de Certificado de cada tipo de certificados emitidos.

1.3.3. Titulares dos Certificados

No contexto deste documento o termo subscritor/titular aplica-se a todos os utilizadores finais a quem tenham sido atribuídos certificados pela PKI do NOSI.
São considerados titulares de certificados emitidos pela PKI do NOSI, aquele cujo nome está inscrito no campo "Assunto" (*Subject)* do certificado e utilizam o certificado e respetiva chave privada de acordo com o estabelecido nas diversas políticas de certificado descritas neste documento, sendo emitidos certificados para as seguintes categorias titulares:

- Pessoa Singular;
- Pessoas Coletivas (Organizações).

Em alguns casos, os certificados são emitidos diretamente a pessoas singulares para uso pessoal, no entanto, existem situações em que quem solicita o certificado é diferente do titular do mesmo, por exemplo, uma organização pode solicitar certificados para os seus colaboradores para que estes representem a organização em transações/comércio

eletrónico. Nestas situações a entidade que solicita a emissão do certificado é diferente do titular do mesmo.

1.3.4. 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.

Neste documento, considera-se uma parte confiante, aquela que confia no teor, validade e aplicabilidade do certificado emitido pela PKI do NOSI.

1.3.5. Outros Participantes

1.3.5.1. Entidade Credenciadora

A Entidade Credenciadora é a entidade competente para a credenciação e fiscalização das entidades certificadoras.
De uma forma geral o papel da Entidade Credenciadora, exercida em Cabo Verde pela Entidade Certificadora Raiz Cabo Verde (ECRCV), está relacionado com a 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 na legislação Cabo-Verdiana, assim como com o estabelecido nesta DPC.

A Entidade Credenciadora é uma das “peças” que contribui para a confiabilidade dos Certificados Qualificados, pelas competências que exerce sobre as EC que os emitem. No âmbito das suas funções, exerce os seguintes papéis relativamente às EC:

a) Credenciação: procedimento de aprovação da EC para exercer a sua atividade, com base numa avaliação feita a parâmetros tão diversificados como a segurança física e lógica, procedimentos de acesso e de operação, e recursos humanos;

b) Registo: procedimento sem o qual a EC não poderá emitir os Certificados Digitais;

c) Fiscalização: procedimento assente em inspeções efetuadas às EC, com vista a regularmente verificar parâmetros de conformidade;

1.3.5.2. Entidade Registo

Descrito na secção 1.3.2

1.3.5.3. Entidades de Validação OCSP

As Entidades de Validação OCSP, têm como função comprovar o estado dos certificados emitidos, através da utilização do protocolo *Online Certificate Status Protocol* (OCSP), de forma a determinar o estado atual do certificado, a pedido de uma entidade, sem necessidade de recorrer à verificação do estado através da consulta das Listas de Certificados Revogados (CRL-Certificate Revogatiob List).
O serviço de Entidade de Validação OCSP é disponibilizado pela PKI da NOSI.

1.3.5.4. Auditor de Segurança

Figura independente do círculo de influência da Entidade de Certificação, devidamente acreditado pela Autoridade Credenciadora de Cabo Verde (ARME – Agência Regulamentação Multissectorial de Economia). A sua missão é auditar a infraestrutura da Entidade de Certificação, no que respeita a equipamentos, recursos humanos, processos, políticas e regras para avaliação de conformidade dos serviços de confiança ao abrigo do Decreto Lei nº 33/2007 de 24 de Setembro e do Decreto Regulamentar nº 18/2007 de 24 de Dezembro.

As Auditorias de conformidade deverão ocorrer, pelo menos, a cada 12 meses, com intuito de confirmar que o NOSI CA, como prestadora qualificada de serviços de confiança e os

serviços de confiança que disponibiliza, cumprem os requisitos estabelecidos pelo Decreto Lei nº 33/2007 de 24 de Setembro, e Decreto Regulamentar nº18/2007 de 24 de Dezembro.

1.4. Utilização do Certificado

Os certificados emitidos no domínio da PKI NOSI são utilizados, pelos diversos titulares, 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 PKI do NOSI proporciona. Assim, os serviços de identificação e autenticação, integridade e não-repúdio são obtidos mediante a utilização de assinaturas digitais. A confidencialidade é garantida através dos recursos a algoritmos de cifra, quando conjugados com mecanismos de estabelecimento e distribuição de chaves.

1.4.1. Utilização Adequada

Os requisitos e regras definidos neste documento aplicam-se a todos os certificados emitidos pela PKI do NOSI.

Os certificados emitidos pela PKI do NOSI são também utilizados pelas Partes Confiantes para verificação da cadeia de confiança de um certificado emitido sob o NOSI CA, 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 o NOSI CA.

1.4.1.1. Certificados Emitidos para Pessoas Física ou Jurídica

Os certificados emitidos para pessoas física ou jurídica, de acordo com o tipo de certificado adquirido, podem ser utilizados para:

- Assinar documentos
- Assinar correio eletrónico

1.4.1.2. Certificados emitidos para organizações

Os certificados para as organizações são emitidos para garantia de Identificação da Organização.

1.4.2. Utilização Não Autorizada

Os certificados poderão ser utilizados noutros contextos apenas na extensão do que é permitido pela legislação aplicável.

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

Os serviços de certificação oferecidos pela PKI do NOSI, 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.

1.5. Gestão das Políticas

1.5.1. Entidade Responsável pela gestão do documento

A gestão desta política de certificados é da responsabilidade do Grupo de Segurança da PKI do NOSI.

1.5.2. Contacto

Nome:	*PKI do NOSI*
Morada:	*Data Center Estado Cabo Verde, Av. António Mascarenhas – Achada Grande Frente – Santiago, Cabo Verde*
Correio Eletrónico:	*pki@nosi.cv*
Site:	https://nosi.cv/
Telefone:	(+238) 260 79 73

1.5.3. Entidade Responsável pela determinação da conformidade da DPC

O Grupo de Trabalho da PKI do NOSI determina a conformidade e aplicação interna desta DPC, submetendo-o de seguida ao Grupo de Gestão para aprovação.

1.5.4. Procedimentos para aprovação da DPC

A validação desta DPC e seguintes correções (ou atualizações) deverão ser levadas a cabo pelo Grupo de Trabalho da PKI do NOSI. As correções (ou atualizações) deverão ser publicadas sob a forma de novas versões desta DPC, substituindo qualquer DPC anteriormente definida. O Grupo de Trabalho da PKI do NOSI deverá ainda determinar quando é que as alterações na DPC levam a uma alteração nos identificadores dos objetos (OID) da DPC.

Após a fase de validação, a DPC é submetida ao Grupo de Gestão, que é a entidade responsável pela aprovação e autorização de modificações neste tipo de documentos.

1.6. Acrónimos e Definições

1.6.1. Acrónimos

Acrónimo	
ANSI	***American National Standards Institute***
CA	***Certification Authority (o mesmo que EC)***
DL	***Decreto-lei***
DN	***Distinguished Name***
DPC	***Declaração de Práticas de Certificação***
EC	***Entidade de Certificação***
ICP-CV	***Infraestrutura de chaves públicas de Cabo Verde***
CRL	***Certificate Revogation List***
MAC	***Message Authentication Codes***
OCSP	***Online Certificate Status Protocol***
OID	***Object Identifier (Identificador de Objecto)***
PKCS	***Public-Key Cryptography Standards***
PKI	***Public Key Infrastructure (Infra-estrutura de Chave Pública)***
SHA	***Secure Hash Algorithm***
SSCD	***Secure Signature-Creation Device***
URI	***Uniform Resource Identifier***

1.6.2. Definições

Assinatura digital, conforme disposto no Modalidade DL- nº33/2007, de 24 de setembro	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, conforme disposto no DL-nº33/2007, de 24 de setembro	Dados sob forma eletrónica anexos ou logicamente associados a uma mensagem de dados e que sirvam de método de autenticação.
Assinatura eletrónica avançada, conforme disposto no DL-nº33/2007, de 24 de setembro.	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, conforme disposto no DL-nº33/2007, de 24 de setembro.	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, conforme disposto no DL-nº33/2007, de 24 de setembro.	Entidade competente para a credenciação e fiscalização das Entidades de Certificação
Certificado, conforme disposto no DL- nº33/2007, de 24 de setembro	Documento eletrónico que liga os dados de verificação de assinatura ao seu titular e confirma a identidade desse titular.
Certificado qualificado, conforme disposto no DL-nº33/2007, de 24 de setembro	Certificado que contém os elementos referidos no artigo 67.º do DL 33/2007 [6] e é emitido por entidade de certificação que reúne os requisitos definidos no artigo 45.º do DL 33/2007.
Chave privada, conforme disposto no DL- nº33/2007, de 24 de setembro	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, conforme disposto no DL- nº33/2007, de 24 de setembro	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, conforme disposto no DL- nº33/2007, de 24 de setembro	Ato pelo qual é reconhecido a uma entidade, que o solicite e que exerça a atividade de entidade de certificação, o preenchimento dos requisitos definidos no DL-nº33/2007, de 24 de setembro para os efeitos nele, previstos.
Dados de criação de assinatura, conforme disposto no DL-nº33/2007, de 24 de setembro	Um conjunto único de dados, como códigos ou chaves criptográficas privadas, usado pelo signatário para a criação de uma assinatura eletrónica.
Dispositivo de criação de assinatura, conforme disposto no DL-nº33/2007, de 24 de setembro	Suporte lógico ou dispositivo de equipamento utilizado para possibilitar o tratamento dos dados de criação de assinatura.
Dispositivo seguro de criação de assinatura, conforme disposto no DL-nº33/2007, de 24 de setembro	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, conforme disposto no DL-nº33/2007, de 24 de setembro.	Documento elaborado mediante processamento eletrónico de dados.
Endereço eletrónico, conforme disposto no DL- nº33/2007, de 24 de Setembro.	Identificação de um equipamento informático adequado para receber e arquivar documentos eletrónicos.

2. Responsabilidade de publicação e repositório

2.1. Repositório

O NOSI CA é responsável pelas funções de repositório do NOSI CA, publicando, entre outras, informação relativa às práticas adotadas e o estado dos certificados emitidos (CRL).

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

- CRL 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.

2.2. Publicação de informação de certificação

O NOSI disponibiliza sempre a seguinte informação pública on-line no URL https://pki.nosi.cv:

a) Seu próprio certificado;
b) Uma cópia eletrónica atualizada da DPC do NOSI CA;
c) Uma cópia eletrónica atualizada das PC´s do NOSI CA;
d) Lista de Certificados Revogados do NOSI CA (CRL);
e) Uma relação das Entidades de Registos vinculadas e seus respetivos endereços de instalações técnicas em funcionamento;
f) Formulário para solicitação de emissão de certificado;
g) Formulário para solicitação de revogação/suspensão de certificado.

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

2.3. Periodicidade de publicação

O NOSI CA garante que as atualizações a esta DPC e respetivas políticas serão publicadas sempre que houver necessidade de se proceder a uma alteração.

Uma nova CRL do NOSI CA, será publicada, no mínimo, uma vez por dia.

2.4. Controlo de acesso aos repositórios

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

3. Identificação e autenticação

3.1. Atribuição de nomes

A atribuição de nomes segue a seguinte convenção:

- Aos certificados de pessoa singular é atribuído o nome real do titular (ou pseudónimo),
- Aos certificados de pessoa coletiva é atribuído o nome da entidade, sendo que no certificado consta o nome do representante legal;

3.1.1. Tipos de nomes

Os certificados emitidos pelo NOSI CA são identificados por nome único (DN – Distinguished Name) de acordo com a norma X.509.

O nome único destes certificados está identificado nas respetivas Políticas de Certificados (secção 3):

Tipo de Certificado	OID da Política de Certificados
Qualificado de Assinatura Digital e Selo Eletrónico	
Certificado Avançado	
Validação *On-line* OCSP	

3.1.2. Necessidade de nomes significativos

O NOSI CA irá assegurar, dentro da sua hierarquia de confiança:

- A não existência de certificados que, tendo o mesmo nome único, identifiquem entidades 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 (com exceção dos certificados com pseudónimos).

3.1.3. Anonimato ou pseudónimo de titulares

A NOSI CA emite certificados com pseudónimo de titulares, garantindo para o efeito que,

- O certificado contém o pseudónimo do titular, claramente identificado como tal, sendo conservados os elementos que comprovam a verdadeira identidade dos requerentes titulares de certificados com pseudónimo,
- Comunicará à autoridade judiciária, sempre que esta o ordenar nos termos legalmente previstos, os dados relativos à identidade dos titulares de certificados que sejam emitidos com pseudónimo seguindo-se, no aplicável, a legislação vigente.

3.1.4. Interpretação de formato de nomes

As regras utilizadas pela NOSI CA para interpretar o formato dos nomes seguem o estabelecido no RFC 5280, assegurando que todos os atributos DirectoryString dos campos issuer e subject do certificado são codificados numa UTF8String, com excepção dos atributos country e serial number que são codificados numa PrintableString.

3.1.5. Unicidade dos Nomes

De acordo com os seus processos de emissão, o NOSI CA rejeita a emissão de certificados com o mesmo DN para titulares distintos. Para cada tipo de certificado emitido, a respetiva Política de Certificados indica o conteúdo do serial number que deverá ser escolhido de modo a assegurar a unicidade do campo e a não induzir uma parte confiante em ambiguidade.

3.1.6. Reconhecimento, autenticação, e função das marcas registadas

Os nomes, emitidos pelo NOSI CA, respeitarão o máximo possível as marcas registadas. O NOSI CA não permitirá deliberadamente a utilização de nomes registados cuja propriedade não possa ser comprovada pelo requerente. Contudo poderá recusar a emissão de certificados com nomes de marcas registadas se entender que outra identificação é mais conveniente.

3.1.7. Método de comprovação da posse de Chave Privada

O par de chaves e certificado é fornecido em token criptográfico (SmartCard ou token USB) com chip criptográfico, personalizado fisicamente para o titular. A posse da chave privada é garantida pelo processo de emissão e personalização do token criptográfico, garantindo que:

- O par de chaves é gerado no HSM criptográfico e inserido no token criptográfico, por comunicação direta segura e sem ficar registado em qualquer dispositivo,
- O token criptográfico é personalizado para o titular do mesmo,

- A chave pública é enviada à NOSI CA para emissão do certificado digital correspondente, sendo este também inserido no token criptográfico.
- O token criptográfico, é entregue presencialmente.

No caso de emissão de certificados qualificado de Selo Eletrónico, existe ainda a opção da chave ser gerada pelo responsável indicado pela pessoa coletiva (Organização) num HSM próprio. Neste caso:

- O responsável e respetiva organização assume a responsabilidade pela chave gerada e pelo HSM utilizado para o efeito;
- Faz chegar á NOSI CA toda a documentação necessária acompanhada de um CSR SHA256;
- O certificado, após validação da documentação entregue, é devolvido ao responsável.

3.2. Validação de identidade no registo inicial

O NOSI CA é responsável por autenticar a identidade das entidades candidatas à obtenção de um certificado. Um certificado qualificado de assinatura digital é emitido para pessoa singular, sendo este o responsável pela sua utilização. Um Certificado Qualificado de Selo Eletrónico é emitido para uma Organização (pessoa legal), tendo associado, mas não representado no certificado, uma pessoa singular identificada como “responsável técnico”, que terá a responsabilidade de manusear e utilizar o certificado em nome da organização.

3.2.1. Certificado Qualificados

3.2.1.1. Autenticação de Identidade de uma Pessoa Singular

Descrito na secção 3.2.1.1 da Política de Certificação da Entidade Certificadora NOSICA – G2 disponível em https://pki.nosi.cv.

3.2.1.2. Autenticação de Identidade de uma Pessoa Coletivo (Selo Eletrónico)

Descrito na secção 3.2.1.2 da Política de Certificação da Entidade Certificadora NOSICA – G2 disponível em https://pki.nosi.cv.

3.2.2. Certificados Avançados

A validação inicial da identidade do requerente de um certificado avançado, emitido pelo NOSI CA, é efetuada através de documentação que é solicitada e enviada pelo requerente juntamente com o formulário de pedido de emissão de certificado avançado, através da qual valida os dados que constam no pedido, nomeadamente dados do titular, da Entidade Responsável que requer o certificado. As assinaturas constantes no formulário são verificadas de forma comparativa com as cópias dos documentos de identificação solicitadas.

3.2.3. Informação do Subscritor/Titular não verificada

Toda informação descritas nas secções 2.1 e 2.2.

3.2.4. Validação de Autoridade

Nada a assinalar.

3.2.5. Critérios para Interoperabilidade

Nada a assinalar

3.3. Identificação e autenticação para renovação de chaves

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

Não existe renovação de chaves, de rotina.

3.3.2. Renovação Após Revogação

Se um certificado é revogado, o indivíduo/organização será sujeito a todo o processo inicial de registo, de forma a obter um novo certificado.

3.4. Identificação e autenticação para pedido revogação

Qualquer entidade 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, designadamente:

- O titular do certificado
- Parte confiante, sempre que demonstre que o certificado foi utilizado com fins diferentes dos previstos.

Para o efeito deve-se proceder ao preenchimento do formulário próprio disponível no (https://pki.nosi.cv) do qual deve constar os seguintes elementos:

- Nome;
- Endereço e outras formas de contacto;
- Indicação do motivo para revogação do certificado.

A ER do NOSI CA guarda toda a documentação utilizada para verificação da identidade e autenticidade da entidade que efetua o pedido de revogação num periodo não inferior a 20 anos do certificado de assinatura digital qualificada.

4. Requisitos Operacionais do Ciclo de Vida do Certificado

4.1. Pedido de Certificado

O pedido de certificado deve ser formulado, mediante o preenchimento do Formulário próprio, disponível na loja on-line (www.store.nosi.cv) ou aos balcões da ER.

4.1.1. Quem pode subscrever um pedido certificado?

No âmbito geral da ER do NOSI CA, que emite certificados para público em geral.

Os Certificados Qualificados e Avançados de Assinatura Digital podem ser subscritos:

- Pelo Titular do certificado, quando o certificado é emitido para pessoa singular,

- Pelo Titular e Representantes legais da entidade, quando o certificado é emitido para pessoa singular associada a uma entidade (na qualidade ou em representação).

O Certificado Qualificado de Selo Eletrónico pode ser subscrito:

- Pelos representantes legais da pessoa coletiva com poderes para o ato, sendo designado por estes uma pessoa física, responsável pelo manuseamento e operação do certificado, denominada de "responsável técnico".

Para as Entidades de Registo, a emissão é restrita ao âmbito das mesmas, nomeadamente a ordem profissional, apenas são emitidos certificados qualificados de assinatura digital.

O pedido de certificado será subscrito pelo titular na qualidade ou função atestada pelos representantes legais da Entidade.

4.1.2. Processo de Registo e responsabilidades

O pedido de certificado é da responsabilidade dos intervenientes, identificados na secção anterior, assim como é da sua responsabilidade a veracidade dos dados fornecidos e disponibilização de toda a documentação necessária que a permita verificar.

O processo de registo é considerado efetivo após ser verificada e confirmada toda a informação constante no pedido, pelo NOSI CA ou ER designada.

O processo de registo inicia-se com o preenchimento do formulário disponível no repositório do NOSI CA ou aos balcões da ER designada.

4.2. Processamento do pedido de certificado

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

a) Pedido do Certificado;
b) Receção, verificação dos documentos e da identidade do requisitante;
c) Validação da exatidão e integridade do pedido de certificado;
d) Processo de emissão de certificado.

As secções 3.2, 4.2.1 e 4.3 descrevem detalhadamente todo o processo.

4.2.1. Processos para a identificação e funções de identificação

4.2.1.1. Certificado de pessoa singular

Conforme indicado na secção 3.2

4.2.1.2. Certificado de Pessoa Coletiva

Conforme indicado na secção 3.2

4.2.1.3. Aprovação ou recusa de pedidos de certificado

A aprovação de certificado passa pelo cumprimento dos requisitos exigidos no ponto 4.2 e 4.2.1.1.

Quando tal não se verifique, é recusada a emissão do certificado.

4.2.1.4. Prazo para processar o pedido do certificado

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

4.3. Emissão do certificado

Os certificados emitidos pelo NOSI CA, são emitidos através da plataforma disponibilizada pelo NOSI CA, de forma automática, após o registo e aprovação do pedido de Certificado. Após a aprovação, o request é enviado diretamente para a Entidade de Certificação a qual procede com a emissão do certificado.

Qualquer certificado emitido na PKI do NOSI CA é sujeito a uma aprovação. Esta aprovação depende do tipo de certificado e da Entidade de Certificação em causa. Para aprovação de certificado de utilizador final, o Grupo de Trabalho de Administração de Registo é responsável pela gestão e aprovação dos pedidos de certificados.

4.3.1. Emissão de Certificados Digitais Qualificados

No caso de Certificados Qualificados de Assinatura e de Selo Eletrónico, o certificado será armazenado em dispositivo de armazenamento seguro, que dependendo da opção escolhida, poderá ser um SmartCard (cartão com chip criptográfico) ou token USB, disponibilizado ao cliente.

4.3.2. Emissão de Certificados Avançados

Os Certificados avançados poderão ser disponibilizados em dispositivo de armazenamento seguro, tal como os certificados digitais qualificados, podendo, no entanto, também, ser disponibilizados através de Download,em dispositivo magnético (CD, Pen Drive, etc) ou via email.

4.3.3. Notificação da Emissão de Certificados

O titular do certificado é notificado da emissão do certificado através de chamada telefónica ou via email antes da receção do mesmo.

4.4. Aceitação do certificado

4.4.1. Procedimento para a Aceitação de Certificado

Para cada tipo de certificado, a respetiva Política de Certificado descreve o modo de aceitação do Certificado.

4.4.2. Publicação do Certificado

O NOSI CA não publica os certificados por ele emitidos, disponibilizando integralmente ao titular.

As condições para este efeito encontram-se definidas na secção 4.4.1. da PC.

4.4.3. Notificação da Emissão de Certificado a Outras Entidades

O NOSI CA não notifica outras entidades sobre a emissão de certificados excepto em acordo previamente estabelecidos.

4.5. Uso de certificado e par de Chaves

4.5.1. 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 na secção 4.5 da Política Certificação (PC);
c) Enquanto o certificado se mantiver válido e não estiver na CRL do NOSI CA.

4.5.2. Uso do certificado e par de chaves públicas 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 Política de Certificado e na respetiva DPC.

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 CRL, tendo especial atenção às suas extensões marcadas como críticas e propósito das chaves;
e) Confiar nos certificados, utilizando-os sempre que estes estejam válidos.

4.6. Renovação do certificado

Esta prática não é suportada pela PKI do NOSI CA.

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.

4.6.1. Motivos para renovação de certificado

Nada a assinalar.

4.6.2. Quem pode submeter o pedido de renovação de certificado

Nada a assinalar.

4.6.3. Processamento do pedido de renovação de certificado

Nada a assinalar.

4.6.4. Notificação de emissão de novo certificado ao titular

Nada a assinalar.

4.6.5. Procedimentos para aceitação de certificado

Nada a assinalar.

4.6.6. Publicação de Certificado após Renovação

Nada a assinalar.

4.6.7. Notificação da Emissão do Certificado a Outras Entidades

Nada a assinalar.

4.7. Renovação do Certificado com Geração de novo par de Chaves

O NOSI CA assume a renovação de certificado com geração de novo par de chaves, sendo considerada sempre uma nova emissão.

4.7.1. Motivo para Renovação do 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) Certificado está a expirar;
b) Suporte do certificado está a expirar;
c) A informação constante no certificado sofre alterações.

4.7.2. Quem pode submeter o pedido de certificado de uma nova chave pública

Tal como na secção 4.1.1.

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

Tal como na secção 4.1.2 e 4.2.

4.7.4. Notificação da emissão de novo certificado ao titular

Tal como na secção 4.3.2.

4.7.5. Procedimentos para aceitação de um certificado com geração de novo par de chave

Tal como secção 4.4.1.

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

Tal como secção 4.4.2.

4.7.7. Notificação da emissão de certificado renovado a outras entidades

Tal como secção 4.4.3.

4.8. Modificação de certificado

Esta prática não é suportada pela PKI do NOSI CA.

A alteração de certificados é o processo em que é emitido um certificado para um titular,

mantendo as respetivas chaves publicas, havendo apenas alterações na informação do certificado.

4.8.1. Motivos para alteração do certificado

Nada a assinalar.

4.8.2. Quem pode submeter o pedido de alteração de certificado

Nada a assinalar.

4.8.3. Processamento do pedido de alteração de certificado

Nada a assinalar.

4.8.4. Notificação da emissão de certificado alterado ao titular

Nada a assinalar.

4.8.5. Procedimentos para aceitação de certificado alterado

Nada a assinalar.

4.8.6. Publicação do certificado alterado

Nada a assinalar.

4.8.7. Notificação da emissão de certificado alterado a outras entidades

Nada a assinalar.

4.9. Suspensão e Revogação de Certificado

Na prática, a revogação e suspensão de certificados é uma ação através da qual o certificado deixa de estar válido antes do fim do seu período de validade, perdendo a sua operacionalidade. Os certificados depois de revogados não podem voltar a ser válidos, enquanto, os certificados suspensos podem recuperar a sua validade.

4.9.1. Motivos para a suspensão

O NOSICA, suspende os certificados nas circunstâncias seguintes:

a) A Pedido do próprio titular, devidamente identificado para o efeito
b) Suspeita de comprometimento da chave privada;

c) Suspeita de perda da chave privada;
d) Suspeita de perda, destruição ou deterioração do dispositivo de suporte da chave privada (por exemplo, suporte/token criptográfico);
e) Sempre que haja razões credíveis que induzam a suspeita que os serviços de certificação possam ter sido comprometidos, de tal forma que coloquem em causa a fiabilidade dos certificados;
f) Por ordem judicial ou, desde que devidamente fundamentada, pelas entidades integrantes da ICP-CV a saber:
    - Conselho Gestor da ICP-CV
    - Autoridade Credenciadora
    - ECR-CV

4.9.2. Quem pode submeter o pedido de suspensão

O pedido de suspensão só pode ser submetido pelo titular do certificado, devidamente identificado e sempre que se verifiquem alguma das condições descritas no ponto 4.9.1.

4.9.3. Procedimentos para pedido de suspensão

A suspensão poderá ser solicitada através de contacto direto com a NOSI CA (em dias úteis) a qual fornecerá todas as indicações necessárias para proceder a suspensão do certificado.

4.9.4. Limite do período de suspensão

O Certificado é suspenso pelo período de tempo definido no plano de segurança da NOSI CA, que em todo o caso não poderá ser superior a 3 (três) dias úteis.

4.9.5. Motivos para revogação

Um certificado pode ser revogado por uma das seguintes razões:

a) Comprometimento da chave privada
b) Perda ou roubo do cartão/token;
c) Atualização/alteração de dados;
d) Deterioração do cartão/token;
e) Utilização do certificado para atividades abusivas;
f) Falha na utilização do cartão/token;
g) Por ordem judicial ou, desde que devidamente fundamentada, pelas entidades integrantes da ICP-CV a saber:
    - Conselho Gestor da ICP-CV
    - Autoridade Credenciadora
    - ECR-CV
h) Cessação de funções do NOSI CA sem ter transmitido a sua documentação a outra entidade certificadora;
i) Se após pedido de suspensão pelo titular ultrapassar os 3 dias sem que este efectue o pedido de renovação;
j) Quando o NOSI CA tomar conhecimento do falecimento, interdição ou inabilitação do titular do certificado.

Após revogação de Certificado o NOSI CA não irá emitir certificado referente aos mesmos dados de criação de assinatura.

4.9.6. 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 4.9.5, as seguintes entidades:

- O próprio titular do certificado, devidamente identificado para o efeito;
- Uma parte confiante, sempre que demonstre que o certificado foi utilizado com fins diferente dos previstos.

O NOSI CA, guarda toda a documentação utilizada para verificação da identidade e autenticidade da pessoa que efetua o pedido de revogação por um periodo não inferior á 20 anos, garantindo a verificação da identidade do titular, por meio legalmente reconhecido, não aceitando poderes de representação para o pedido de revogação de certificados.

4.9.7. Procedimentos para solicitação de revogação

Todos os pedidos de revogação devem ser endereçados ao NOSI CA, ou ás Entidades de Registo por ela indicada, por escrito ou por mensagem eletrónica assinada digitalmente, em formulário próprio de pedido de revogação, observando o seguinte:

- Identificação e autenticação da entidade que efetua o pedido de revogação;
- Registo e arquivo do formulário de pedido de revogação;
- Análise do pedido de revogação pelo Grupo de Trabalho de Registos da PKI do NOSI CA, que aprova ou recusa o pedido;
- Sempre que se decidir revogar um certificado, a revogação é publicada na respetiva CRL.

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;
- 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.

4.9.8. 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.

4.9.9. 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. A revogação do certificado não tem efeitos retroativos.

4.9.10. Requisitos de verificação da revogação pelas partes confiantes

Antes de utilizarem um certificado, as partes confiantes têm como responsabilidade verificar o estado de todos os certificados, através das CRL ou num servidor de verificação do estado online (via OCSP).

4.9.11. Periodicidade da emissão da lista de certificados revogados (crl)

O NOSI CA disponibiliza uma nova CRL Base diariamente.

4.9.12. Período máximo entre a emissão e a publicação da crl

O período máximo entre a emissão e publicação da CRL não deverá ultrapassar 60 minutos.

4.9.13. Disponibilidade de verificação online do estado / revogação de certificado

O NOSI CA dispõe de serviços de validação OCSP do estado dos certificados online. Esse serviço poderá ser acedido em (https://ocsp.nosi.cv).

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

4.9.14. Requisitos de verificação online

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

4.9.15. Outras formas disponíveis de notificação da revogação

O titular do certificado é notificado via email, sempre que o certificado for revogado.

4.9.16. Requisitos especiais em caso de comprometimento de chave privada

No caso da chave privada do NOSI CA ser comprometida, devem ser tomadas medidas apropriadas de resposta ao incidente.

As respostas a esse incidente podem incluir:

- Revogação do certificado do NOSI CA e de todos os certificados emitidos no "ramo" da hierarquia de confiança do NOSI CA;
- Notificação da Autoridade Credenciadora e todos os titulares de certificados emitidos no "ramo" da hierarquia de confiança do NOSI CA;
- Geração de novo par de chaves para o NOSI CA;

Renovação de todos os certificados emitidos no "ramo" da hierarquia de confiança do NOSI CA.

4.10. Serviços sobre o estado do certificado

4.10.1. Características Operacionais

O estado dos certificados emitidos está disponível publicamente através das CRL (https://pki.nosi.cv), e o serviço OCSP (https://ocsp.nosi.cv).

4.10.2. Disponibilidade do Serviço

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

4.10.3. Características Opcionais

Nada a assinalar.

4.11. Fim 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.

4.12. Retenção e recuperação de chaves

A PKI do NOSI só efetua a retenção da sua chave privada.

5. Medidas de Segurança física de Gestão e Operacionais

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

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

5.1. Medidas de segurança física

5.1.1. Localização física e tipo de construção

As instalações da PKI do NOSI foram projectadas de forma a proporcionar um ambiente seguro por meio de uma Sala Cofre projectada para o efeito, e capaz de controlar e auditar o acesso aos sistemas de certificação, estando fisicamente protegidas de acessos não autorizados, danos ou interferências.

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.

5.1.2. Acesso físico ao local

Os sistemas da PKI do NOSI estão protegidos por um mínimo de 8 níveis de segurança física hierárquicos, garantindo-se que o acesso a um nível de segurança mais elevado só

é possível quando previamente se tenha alcançado os privilégios necessários ao nível imediatamente anterior.

Atividades operacionais sensíveis da PKI do NOSI, 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. Acessos físicos são automaticamente registados e armazenados para efeitos de auditorias.

5.1.3. Energia e ar condicionado

O ambiente seguro do PKI do NOSI possui equipamentos de energia e ar condicionado redundantes que garantem condições de funcionamento 24 horas por dia / 7 dias por semana, de:

a) **Alimentação de Energética** garantindo alimentação contínua ininterrupta com a potência suficiente para manter autonomamente a alimentação energética durante períodos de falhas de Rede Pública e para proteger os equipamentos face a flutuações elétricas que os possam danificar. Os equipamentos redundantes consistem em 2 NoBreaks com autonomia superior a 100 minutos, 2 Geradores a diesel , 2 Ramais de alimentação energética independentes.

b) **Refrigeração/Ventilação/Ar condicionado** que regulam e controlam os níveis de temperatura e humidade relativa, garantindo condições adequadas para o correto funcionamento de todos os equipamentos eletrónicos e mecânicos presentes dentro do ambiente. Os equipamentos redundantes consistem em 3 Chillers de produção de água fria, 22 InRows de AC, 2 Ramais de alimentação de liquido independentes.

5.1.4. Exposição à água

As instalações onde se localizam o ambiente PKI do NOSI estão localizadas a cerca de 69 metros do nivel do mar.
O interior da zona de alta segurança têm instalado os mecanismos devidos (detetores de inundação) para minimizar o impacto de uma eventual inundação nos ambientes do PKI do NOSI.

5.1.5. Prevenção e proteção contra incêndio

O ambiente seguro do PKI do NOSI tem instalado os mecanismos necessários (um sistema de detecção e extinsão automáticas de incêndio) para detetar e apagar fogos ou outros incidentes derivados de chamas ou fumos. Estes mecanismos estão em conformidade com os regulamentos existentes:

a) Sistemas de deteção e alarme de incêndio estão instalados nos vários níveis físicos de segurança;

b) Equipamento fixo e móvel de extinção de incêndios estão disponíveis, colocados em sítios estratégicos e de fácil acesso de modo a poderem ser rapidamente usados no início de um incêndio e extingui-lo com sucesso;

c) Procedimentos de emergência bem definidos, em caso de incêndio.

5.1.6. Salvaguarda de suportes de armazenamento

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

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

Em situações que implique a deslocação física de hardware de armazenamento de dados (i.e., discos rígidos, etc.) para fora da zona de alta segurança, por motivos que não o arquivo de cópias de segurança cada elemento de hardware deverá ser verificado para garantir que não contém dados sensíveis. Nestas situações, a informação tem de ser

eliminada usando todos os meios necessários para o efeito (formatar o disco rígido, reset do hardware criptográfico ou mesmo destruição física do equipamento de armazenamento).

5.1.7. Eliminação de resíduos

Documentos e materiais em papel que contenham informação sensível são 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, etc) deverão ser devidamente limpos de modo a não ser possível recuperar nenhuma informação (através de formatações seguras, ou destruição fisica dos equipamento).

5.1.8. 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).

5.2. Medida de segurança dos processos

A atividade de uma Entidade Certificadora 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 seção inclui também a separação de deveres, em termos dos papéis que não podem ser executados pelos mesmos indivíduos.

5.2.1. Grupos de Trabalho

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

A PKI do NOSI estabeleceu que os papéis de confiança fossem agrupados em seis categorias diferentes (que correspondem a seis Grupos de Trabalho distintos) de modo a garantir que as operações sensíveis sejam efetuadas por diferentes pessoas autenticados, eventualmente pertencentes a diferentes Grupos de Trabalho, assegurando que existem dois membros em cada grupo.

Só estão autorizadas entradas na “Zona de Alta Segurança” perante a presença mínima de dois elementos, pertencente a Grupos de Trabalho distintos, nomeadamente Segurança e Auditoria.

Como medida adicional de segurança, o NOSI CA considera relevante e obrigatória, a presença em todas as intervenções de um elemento de Auditoria.

5.2.1.1. Grupo de Gestão

É responsável pela nomeação dos membros dos restantes grupos e pela tomada de decisões de nível crítico para a EC. Este grupo deve ser constituído por um mínimo de 4 (quatro) membros sendo estes, nomeados pelo conselho de administração do NOSI EPE.

As responsabilidades deste grupo são:

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

5.2.1.2. Grupo de Auditoria

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

As responsabilidades deste grupo são:

a) Auditar a execução e confirmar a exatidão dos processos e cerimónias da EC;
b) Registar todas as operações sensíveis;
c) Investigar suspeitas de fraudes procedimentais;

d) Verificar periodicamente a funcionalidade dos controlos de segurança (dispositivos de alarme, de controlo de acessos, sensores de fogo, etc) existentes nos vários ambientes;
e) Registar os resultados de todas as ações por si realizadas;
f) Assumir o papel de Auditor de Sistema;
g) Validar que todos os recursos utilizados são seguros;
h) Verificar periodicamente a integridade dos Ambientes de Custódia, assegurando que lá se encontram os artefactos respetivos e que estão devidamente identificados;
i) Verificar periodicamente os registos/logs da EC.

5.2.1.3. Grupo de Segurança

É responsável por propor todas as políticas da EC, assegurando que se encontram atualizadas.

É ainda 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. 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. Este grupo deve ter um mínimo de 2 (dois) membros.

As responsabilidades deste grupo são:

a) Gerir o Ambiente de Administração de Segurança;
b) Definir e gerir todas as políticas da EC e garantir que se encontram atualizadas e adaptadas à realidade desta;
c) Garantir implementação das políticas definidas;
d) Assegurar que as PC's da EC são suportadas pela DPC da EC.
e) Assegurar que todos os documentos relevantes e relacionados, direta ou indiretamente, com o funcionamento da EC e existentes em formato papel se encontram armazenados no Ambiente de Informação;

f) Por explicar todos os mecanismos de segurança aos funcionários que devam conhece-los e de consciencializa-los para as questões de segurança levando-os a fazer cumprir as normas e políticas de segurança estabelecidas.
g) Permitir e averiguar os acessos à aplicação da EC (grupos, regras, logs);
h) Verificar perfis de certificados e end entities na aplicação da EC;
i) Verificar os certificados;
j) Ativação de chaves para sua utilização. Isto significa que cada vez que se inicie a EC, é necessário a inserção dos cartões de operador associados às chaves;
k) Autorização para a geração de chaves da aplicação. Esta operação é requerida durante a cerimónia de geração de chaves para a EC;
l) Gerir o Ambiente de Custódia;
m) Custódia de artefactos sensíveis (tokens de autenticação, etc.) utilizando os meios adequados que respondam às necessidades de segurança respetivas;
n) Disponibilização segura dos artefactos à sua guarda, a membros dos outros grupos e explicitamente autorizados a aceder aos mesmos, após o cumprimento dos procedimentos de identificação e segurança apropriados.

5.2.1.4. Grupo de Administração de Sistemas

É responsável pela instalação e configuração de base (hardware e software) da EC até à sua inicialização. Este grupo deve ter pelo menos 1 (um) membro.

As responsabilidades deste grupo são:

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

iii. A lista de todos os artefactos (univocamente identificados) indispensáveis à inicialização e operação da EC.

5.2.1.5. Grupo de Operação de Sistemas

É responsável por executar as tarefas de rotina essenciais ao bom funcionamento e operacionalidade da EC.

As responsabilidades deste grupo são:

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

5.2.1.6. Administração de Registo

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

As responsabilidades deste grupo são:

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

5.2.2. 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.

5.2.3. Funções que requerem separação de Responsabilidades

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

Grupo de Trabalho	Incompatível com:					
	(a)	(b)	(c)	(d)	(e)	(f)
Administração de Segurança (a)		x			x	
Administração de Sistemas (b)	x				x	
Operação de Sistemas (c)						
Administração de Registos (d)						
Auditoria (e)	x	x				
Gestão (f)					x	

5.3. Medidas de Segurança de Pessoal

5.3.1. Requisitos relativos às Qualificações, Experiência, Antecedentes e Credenciação

Todo o pessoal que desempenhe funções de confiança na PKI do NOSI deve cumprir os seguintes requisitos:

a) Ter sido nomeado formalmente para a função a desempenhar;

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

5.3.2. 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.

5.3.3. 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:

- Certificação digital e Infraestruturas de Chave Pública;
- Conceitos gerais sobre segurança da informação;
- Formação específica para o seu papel dentro do Grupo de Trabalho;
- Funcionamento operacional da PKI do NOSI;
- Política de Certificados e Declaração de Práticas de Certificação;
- Recuperação face a desastres;
- Procedimentos para a continuidade da atividade e,

- Aspetos legais básicos relativos à prestação de serviços de certificação.

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

5.3.5. Frequência e Sequência da Rotação de Funções

Nada a assinalar.

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

5.3.7. Requisitos para Prestadores de Serviços

Consultores ou prestadores de serviços independentes, tem permissão de acesso à zona de alta segurança desde que estejam sempre acompanhados e diretamente supervisionados pelos membros do Grupo de Trabalho e ficando o seu acesso registado no Livro de Presenças próprio.

5.3.8. Documentação Fornecida ao Pessoal

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

5.4. Procedimentos de Auditoria de Segurança

5.4.1. Tipo de Eventos Registados

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

a) Tentativas de acesso (com e sem sucesso) para solicitar, gerar, assinar, emitir ou revogar chaves de certificados;
b) Tentativas de acesso (com e sem sucesso) para criar, modificar ou apagar informação dos titulares dos certificados;
c) Tentativas de acesso (com e sem sucesso) e alterações dos parâmetros de segurança do sistema operativo;
d) Emissão e publicação de CRL's;
e) Arranque e paragem de aplicações;
f) Tentativas de acesso (com e sem sucesso) de início e fim de sessão;

g) Tentativas de acesso (com e sem sucesso) de criar, modificar, apagar contas do sistema;
h) Cópias de segurança, recuperação ou arquivo dos dados;
i) Alterações ou atualizações de software e hardware;
j) Manutenção dos sistemas;
k) Operações realizadas por membros dos Grupos de Trabalho;
l) Alteração de Recursos Humanos;
m) Tentativas de acesso (com e sem sucesso) às instalações por parte de pessoal autorizado ou não;
n) A cerimónia de geração de chaves e sistemas envolvidos na mesma, tais como servidores
o) aplicacionais, base de dados e sistema operativo.

5.4.2. Frequência da Auditoria de Registos

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

5.4.3. Período de Retenção dos Registos de Auditoria

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

5.4.4. Proteção dos Registos de Auditoria

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

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.

As cópias de segurança dos registos da PKI do NOSI são armazenadas em local seguro e em cofres.

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

5.4.5. Procedimentos para a cópia de Segurança dos Registos

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

5.4.6. Sistema de Recolha de Registos (Interno / Externo)

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

5.4.7. Notificação de agentes causadores de Eventos

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

5.4.8. Avaliação de Vulnerabilidades

Os registos auditáveis são regularmente analisados de modo a minimizar e eliminar potenciais tentativas de quebrar a segurança do sistema. São realizados quatro testes de intrusão por ano, de forma a verificar e avaliar vulnerabilidades. O resultado da análise é

reportado ao Grupo de Gestão da PKI do NOSI para rever e aprovar um plano de implementação e correção das vulnerabilidades detetadas.

5.5. Arquivo de Registos

5.5.1. Tipo de dados Arquivados

Todos os dados auditáveis são arquivados (conforme indicado na secção 5.4.1), assim como informação de pedidos de certificados e documentação de suporte ao ciclo de vida das várias operações.
As informações e eventos que são registados e arquivados são:

- Os registos de auditoria especificados no ponto 5.4.1 desta DPC;
- As cópias de segurança dos sistemas que compõem a infraestrutura da PKI do NOSI;
- Toda a documentação relativa ao ciclo de vida dos certificados, designadamente:
    - Procedimentos de emissão e revogação de certificados de serviço;
    - Formulários de emissão e receção dos certificados de serviço;
- Acordos de confidencialidade;
- Protocolos estabelecidos com as Entidades Subscritoras;
- Contratos estabelecidos entre a PKI do NOSI e outras entidades - apenas disponibilizados a quem solicitar a sua visualização, após avaliação e aprovação prévia do pedido;
- Autorizações de acesso aos sistemas de informação;
- Acessos aos artefactos existentes nas custódias.

5.5.2. Período de Retenção em Arquivo

Neste item, a DPC deve estabelecer os períodos de retenção para cada registo arquivado, observando que:

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

5.5.3. Proteção dos Arquivos

O arquivo:

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

5.5.4. Procedimentos para as cópias de Segurança do Arquivo

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

A EC deve verificar a integridade dessas cópias de segurança, no mínimo, a cada 6 (seis) meses.

5.5.5. Requisitos para Validação Cronológica dos Registos

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

5.5.6. Sistema de recolha de dados de Arquivo (Interno / Externo)

Os sistemas de recolha de dados de arquivo são internos.

5.5.7. Procedimentos de Recuperação e Verificação de Informação Arquivada

Apenas membros autorizados dos Grupos de Trabalho têm acesso aos arquivos para verificação da sua integridade.
São realizadas de forma automática verificações de integridade dos arquivos eletrónicos (cópias de segurança) na altura da sua criação, em caso de erros ou comportamentos imprevistos, deve-se realizar novo arquivo.

5.6. Renovação de Chaves

A renovação de chaves é feita apenas em caso de desastre ou comprometimento, conforme a secção 5.7.
Apenas as entidades de certificação da PKI do NOSI com certificados válidos podem requerer a renovação do respetivo par de chaves, desde que a geração de novo par de chaves esteja conforme a secção 5.7.

5.7. Recuperação em caso de Desastre ou Comprometimento

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

5.7.1. Procedimentos em caso de Incidente ou Comprometimento

As cópias de segurança das chaves privadas das EC's (geradas e mantidas de acordo com a secção 8.2.3.1) e dos registos arquivados (secção 5.5.1) são guardados em ambientes seguros externos e disponíveis em caso de desastre ou comprometimento.
No caso de comprometimento da chave privada do NOSI CA, esta deverá tomar as seguintes ações:

- Proceder à sua revogação imediata;
- Revogar todos os certificados dela, dependentes;
- Informar todos os titulares dos seus certificados e terceiras partes conhecidas;
- Informar todas as Entidades que compõem a PKI do NOSI.

5.7.2. 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, a NOSI CA suspenderá os seus serviços e notificará a Autoridade Credenciadora.

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

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

a) Informar a Autoridade Credenciadora Nacional e o Conselho Gestor da ICP-CV;
b) Revogação do certificado da EC e de todos os certificados emitidos no "ramo" da hierarquia de confiança da EC;

c) Notificação de todos titulares de certificados emitidos no “ramo” da hierarquia de confiança da EC;
d) Geração de novo par de chaves para a EC e inclusão nos vários sistemas/browsers;
e) Renovação de todos os certificados emitidos no “ramo” da hierarquia de confiança da EC.

5.7.4. Capacidade de continuidade da Atividade em caso de Desastre

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

5.8. Procedimentos em caso de extinção de EC ou ER

Em caso de cessação de atividade como prestador de serviços de Certificação, a EC executa os procedimentos previstos no Plano de Cessação de Atividades, conforme artigo 36º do DL nº33/2007.
Em caso de alterações do organismo/estrutura responsável de gestão da atividade da EC, esta deve informar de tal facto à Autoridade Credenciadora Nacional e ao Conselho Gestor da IPC-CV.

6. Medidas de Segurança Técnicas

Esta secção define as medidas de segurança implementadas pela PKI do NOSI para a EC, de forma a proteger chaves criptográficas geradas por estas, 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.

6.1. Geração e Instalação do Par de Chaves

A geração dos pares de chaves da NOSI CA são processados de acordo com os requisitos e algoritmos definidos nesta política.

6.1.1. Geração do Par de Chaves

A geração de chaves criptográficas do NOSI CA 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 do NOSI CA, cumpre os requisitos FIPS 140-2 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 perca de dados, possa haver uma recuperação total e segura das chaves.

A chave privada para os certificados digitais de pessoa singular e de pessoa coletiva, é gerada, diretamente em módulo criptográfico em hardware (p.e. smartcard), que cumpre os requisitos FIPS 140-2 nível 3 e/ou Common Criteria EAL 4+, sob controlo único do titular.

O funcionamento do NOSI CA é efetuado em modo on-line.

6.1.2. Entrega da Chave Privada ao Titular

A entrega da chave privada associada aos certificados de pessoa singular e de pessoa coletiva é efetuada em dispositivo criptográfico SSCD (Secure Signature-Creation Device).

6.1.3. Entrega da Chave Pública ao Emissor do Certificado

A chave pública é entregue aos requerentes, de acordo com os procedimentos indicados secção 4.4.

6.1.4. Entrega da chave pública da EC às partes Confiantes

A chave pública da EC será disponibilizada através do certificado do NOSI CA, conforme secção 2.2.

6.1.5. Dimensão das Chaves

O comprimento dos pares de chaves deve ter o tamanho suficiente, de forma a prevenir possíveis ataques de criptanálise que descubram a chave privada correspondente ao par de chaves no seu período de utilização.

A dimensão das chaves é a seguinte:

- 4096 bits RSA para a chave das EC's,

- 2048 bits RSA para as chaves associadas aos restantes certificados emitidos pelo NOSI CA com algoritmo de assinatura sha256RSA.

6.1.6. Geração dos 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 do NOSI CA são geradas com base na utilização de processos aleatórios/pseudo aleatórios descritos no ANSI X9.17, de acordo com o estipulado no PKCS#11.

6.1.7. Fins a que se destinam as Chaves (campo "key usage" X.509 v3)

Conforme descrito na secção 7.1.

6.2. Proteção da Chave Privada e Caraterísticas do módulo Criptográfico

Nesta secção são considerados os requisitos para proteção da chave privada e para os módulos criptográficos do NOSI CA. A PKI do NOSI implementou uma combinação de controlos físicos, lógicos e procedimentos, devidamente documentados, de forma a assegurar confidencialidade e integridade das chaves privadas do NOSI CA.

6.2.1. Normas e medidas de Segurança do módulo Criptográfico

Para a geração dos pares de chaves do NOSI CA assim como para o armazenamento das chaves privadas, a PKI do NOSI utiliza módulo criptográfico em hardware que cumpre as seguintes normas:

- Segurança Física
    - Common Criteria EAL 4+ e/ou
    - FIPS 140-2, nível 3
- Autenticação
    - Autenticação dois factores.

6.2.2. Controlo multi-pessoal (n de m) para a chave Privada

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

A PKI do NOSI implementou um conjunto de mecanismos e técnicas que obrigam à participação de vários membros do Grupo de Trabalho para efetuar operações criptográficas sensíveis no NOSI CA.

Todas as operações são efetuadas com um mínimo de dois elementos em funções qualificadas dentro da entidade e em tarefa distinta.

Os dados de ativação necessários para a utilização da chave privada da NOSI CA 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 NOSI CA guardada no módulo criptográfico em hardware. São necessárias duas (m) partes para a ativação da chave privada da NOSI CA.

6.2.3. Retenção da Chave Privada (key escrow)

O NOSI CA só efetua a retenção da sua chave privada

6.2.4. Cópia de Segurança da Chave Privada

A chave privada do NOSI CA tem pelo menos uma cópia de segurança, com o mesmo nível de segurança que a chave original.

6.2.5. Arquivo da Chave Privada

As chaves privadas do NOSI CA, alvo de cópias de segurança, são arquivadas conforme identificado na secção 6.2.3.

6.2.6. Transferência da Chave Privada para/do Módulo Criptográfico

As chaves privadas do NOSI CA não são extraíveis a partir do *token* criptográfico FIPS 140-2 nível 3.

6.2.7. Armazenamento da Chave Privada no Módulo Criptográfico

As chaves privadas do NOSI CA são armazenadas de forma cifrada nos módulos do hardware criptográfico.

6.2.8. Processo para Ativação da Chave Privada

O NOSI CA é uma Entidade Certificadora on-line, cuja chave privada é ativada quando o sistema da EC é ligado. Esta ativação é efetivada quando os administradores de sistema efetuam a ativação dos *slots* do módulo criptográfico, sendo obrigatório a autenticação utilizando dois fatores. Para a ativação da chave privada são necessários que pelo menos duas pessoas detentoras dos cartões de utilizadores. Uma vez a chave ativada, esta permanecerá assim até que o processo de desativação seja executado.

6.2.9. Processo para Desativação da Chave Privada

A chave privada do NOSI CA é desativada quando o sistema da EC é desligado. Uma vez desativada, esta permanecerá inativa até que o processo de ativação seja executado.

6.2.10. Processo para Destruição da Chave Privada

As chaves privadas do NOSI CA (incluindo as cópias de segurança) são apagadas/destruídas num procedimento devidamente identificado e auditado no mínimo 30 dias após terminada a sua data de validade (ou se revogadas antes deste período).

A PKI do NOSI 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.

6.2.11. Avaliação/nível do Módulo Criptográfico

Descrito na secção 6.2.1.

6.3. Outros aspetos da Gestão do par de Chaves

6.3.1. Arquivo da Chave Pública

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

6.3.2. Períodos de Validade do Certificado e das Chaves

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

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

- O certificado da EC, subordinada do NOSI CA tem uma validade de 12 anos, sendo utilizado para assinar certificados durante os seus primeiros 6 anos de validade, sendo reemitido após os 6 anos de validade;
- Os certificados de OCSP (Online Certificate Status Protocol) têm uma validade de 5 anos e 2 meses, sendo utilizados durante os seus primeiros quatro anos de validade, sendo reemitido após o quarto ano de validade;
- O certificado de pessoa singular tem uma validade de dois anos;
- O certificado de pessoa coletiva tem uma validade de dois anos;

6.4. Dados de Ativação

6.4.1. Geração e Instalação dos Dados de Ativação

Os dados de ativação necessários para a utilização da chave privada do NOSI CA são divididos em várias partes (guardadas em chaves PED – pequenos *tokens* de identificação digital, com o formato de *smartcard* – identificadoras de diferentes papéis no acesso à EJBCA *Appliance*(HSM embutido), 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 140-2 nível 3.

6.4.2. 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 do NOSI CA são guardadas, de forma cifrada, em *token* criptográfico.

6.4.3. 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.

6.5. Medidas de segurança informáticas

6.5.1. Requisitos Técnicos Específicos

O acesso aos servidores do NOSI CA é restrito aos membros dos Grupos de Trabalho com uma razão válida para esse acesso. O NOSI CA tem funcionamento online, sendo os pedidos de emissão de certificados efetuados a partir do módulo de operação do RA. O NOSI CA e o RA Management dispõem de dispositivos de proteção, designadamente firewall, e que cumpre os requisitos necessários para identificação, autenticação, controlo de acessos, administração, auditorias, reutilização, responsabilidade e recuperação de serviços e troca de informação.

6.5.2. Avaliação/nível de Segurança

Os vários sistemas e produtos empregues pelo NOSI CA são fiáveis e protegidos contra modificações. O módulo criptográfico em Hardware do NOSI CA satisfaz a norma EAL 4+ *Common Criteria for Information Technology Security Evaluation* e/ou FIPS 140-2 nível 3.

6.6. Ciclo de Vida das Medidas Técnicas de Segurança

6.6.1. Medidas de Desenvolvimento do Sistema

Nada a assinalar.

6.6.2. Medidas para a Gestão da Segurança

A PKI do NOSI tem mecanismos e/ou Grupos de Trabalho, para controlar e monitorizar a configuração dos sistemas do NOSI CA. O sistema do NOSI CA, 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.

6.6.3. Ciclo de Vida das Medidas de Segurança

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

6.7. Medidas de Segurança da Rede

O NOSI CA dispõe de dispositivos de proteção, 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. Perfil de certificado, CRL e OCSP

7.1. Perfil de certificado

Os utilizadores de uma chave pública têm que ter confiança que a chave privada associada é detida pelo titular remoto correto (pessoa ou sistema) com o qual irão utilizar mecanismos de cifra ou assinatura digital. A confiança é obtida através do uso de certificados digitais X.509 v3, que são estrutura de dados que fazem a ligação entre a chave pública e o seu titular.

Esta ligação é afirmada através da assinatura digital de cada certificado por uma EC de confiança. O NOSI CA 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 pelo NOSI CA. 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.

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 do NOSI CA que assinou o certificado, assim como do nome do NOSI CA e informação relacionada (tal como o período de validade), então poderá ter necessidade de um certificado adicional para obter a chave pública do NOSI CA 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 os certificados das EC´s que assinaram este e assim consecutivamente até chegar à EC Raiz.

O perfil dos certificados emitidos pelo NOSI CA está de acordo com:

- Recomendação ITU.T X.509;
- RFC 5280;
- Política de Certificado do NOSI CA;
- Legislação nacional aplicável.

Os perfis dos certificados, podem ser consultadas nos documentos de Políticas de Certificados associadas a esta DPC.

7.2. Perfil da lista de Revogação de Certificados (CRL- *Certificate Revogation List*)

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

O perfil da CRL está de acordo com:

- Recomendação ITU.T X.509;
- RFC 5280;
- Política de Certificado do NOSI CA; e
- Legislação nacional aplicável.

7.3. Perfil do Certificado OCSP

O perfil da OSCP está de acordo com:

- Recomendação ITU.T X.509;
- RFC 5280;
- Política de Certificado do NOSI CA; e
- Legislação nacional aplicável.

8. Auditoria e Avaliações 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 do NOSI CA.

Para além de auditorias de conformidade, o NOSI EPE irá efetuar outras fiscalizações e investigações para assegurar a conformidade do NOSI CA com a legislação nacional. A execução destas auditorias, fiscalizações e investigações poderá ser delegada a uma entidade externa de auditoria.

8.1. Frequência ou motivo da auditoria

As práticas de certificação do NOSI são alvo de auditorias periódicas, que terão como mínimo a periodicidade estipulada na lei, ou seja, uma periodicidade anual com a emissão de um relatório à data de 31 de Março do ano civil em causa. Esta auditoria será realizada por um Auditor credenciado pela Autoridade Credenciadora. Esta auditoria é realizada tomando como base as normas existentes para o efeito sendo os seus resultados comunicados à Autoridade Credenciadora que poderá tornar público o resultado de todo o processo.

No sentido de cumprir com estas obrigações, o NOSI CA mantém registo de todas as operações do ciclo de vida dos certificados e de todas as comunicações mantidas com as entidades de registo/certificação por si reconhecida. Da mesma forma, o NOSI CA obriga estas entidades a manter registo dos pedidos de subscrição recebidos e processado nos quais tenha estado envolvida.

Este registo deverá ser mantido num repositório de dados criado para o efeito e deverá poder ser confirmada através da análise dos registos das comunicações (em suporte eletrónico ou outro) com a entidade de certificação.

Para verificar o cumprimento destas disposições, o NOSI CA conduzirá auditorias periódicas sobre as entidades de registo/certificação como forma de determinar a adequação dos procedimentos operacionais e níveis de segurança tecnológicos às

Políticas de Certificados suportadas. O não cumprimento das condições contratuais pode conduzir à suspensão e/ou revogação do(s) certificado(s) emitido(s).

8.2. Identidade e qualificações do auditor

O auditor é uma figura independente do círculo de influência da Entidade de Certificação, de reconhecida idoneidade, com experiência e qualificações comprovadas na área da segurança da informação e dos sistemas de informação, infraestruturas de chaves pública, familiarizado com as aplicações e programas de certificação digital e na execução de auditorias de segurança. A sua missão é auditar a infraestrutura da Entidade de Certificação, no que respeita a equipamentos, recursos humanos, processos, políticas e regras.

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.

8.3. 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.

Na relação entre o auditor e a entidade submetida a auditoria, deve estar garantido 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.

8.4. Âmbito da auditoria

O âmbito das auditorias e outras avaliações inclui a conformidade com a legislação nacional e com este 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).

8.5. Procedimentos após uma auditoria com resultado deficiente

Se duma auditoria resultarem irregularidades, o auditor procede da seguinte forma:

a) Documenta todas as deficiências encontradas durante a auditoria;
b) No final da auditoria reúne com os responsáveis da entidade submetida a auditoria e apresenta de forma resumida um relatório de primeiras impressões (RPI);
c) Elabora o relatório final de auditoria. Este relatório deverá estar organizado de modo a que todas as deficiências sejam escalonadas por ordem decrescente de gravidade/severidade;
d) Submete o relatório final de auditoria à Autoridade Credenciadora e simultaneamente para os responsáveis da entidade auditada para apreciação;
e) Tendo em conta as irregularidades constantes no relatório, a entidade submetida à auditoria enviará um relatório de correção de irregularidades (RCI), para a Autoridade Credenciadora, no qual devem estar descritas as ações, metodologia e tempo necessário para corrigir as irregularidades;
f) A Autoridade Credenciadora depois de analisar este relatório toma uma das três seguintes opções, consoante o nível de gravidade/severidade das irregularidades:
    i. Aceita os termos, permitindo que a atividade seja desenvolvida até à próxima inspeção;
    ii. Permite que a entidade continue em atividade por um período máximo de 60 dias até à correção das irregularidades antes da revogação;

iii. Procede à revogação imediata da atividade.

8.6. Comunicação de resultados

Os resultados devem ser comunicados à Entidade Supervisora.

8.7. Self-Audits

Uma autoavaliação é realizada anualmente por auditores internos.

9. Outras situações e assuntos legais

Esta secção aborda aspetos de negócio e assuntos legais.

9.1. Taxas

9.1.1. Taxas por Emissão ou Renovação de Certificados

A serem identificadas em proposta formal a efetuar pela NOSI EPE.

9.1.2. Taxas para Acesso a Certificado

Nada a assinalar.

9.1.3. Taxas para Acesso a Informação do Estado do Certificado ou de Revogação

O acesso à informação sobre o estado ou revogação dos certificados (LRC), é livre e gratuita.

9.1.4. Taxas para Outros Serviços

As taxas para os serviços de validação cronológica e validação on-line OCSP são identificadas em proposta formal a efetuar pela NOSI EPE.

9.1.5. Política de Reembolso

Nada a assinalar.

9.2. Responsabilidade Financeira

9.2.1. Seguro de cobertura

O NOSI EPE dispõe do seguro obrigatório de responsabilidade civil, conforme artigo 45.º nº 1 alínea d), do Decreto-Lei n.º 33/2007, de 24 de Setembro.

9.2.2. Outros recursos

Nada a assinalar.

9.2.3. Seguro ou Garantia de Cobertura para Utilizadores

O NOSI EPE dispõe do seguro obrigatório de responsabilidade civil, conforme artigo 45.º nº 1 alínea d), do Decreto-Lei n.º 33/2007, de 24 de Setembro.

9.3. Confidencialidade da informação processada

9.3.1. Âmbito da confidencialidade da informação

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

a) As chaves privadas do NOSI CA;
b) Toda a informação relativa aos parâmetros de segurança, controlo e procedimentos de auditoria;
c) Toda a informação de carácter pessoal proporcionada ao NOSI CA durante o processo de registo dos subscritores de certificados, salvo se houver autorização explícita para a sua divulgação e/ou se a mesma não for incluída no conteúdo do certificado emitido;
d) Planos de continuidade de negócio e recuperação;
e) Registos de transações, incluindo os registos completos e os registos de auditoria das transações;

f) Informação de todos os documentos relacionados com o NOSI CA (regras, políticas, cerimónias, formulários e processos), incluindo conceitos organizacionais, informação financeira/comercial secreta, confidencial e/ou privilegiada, sendo propriedade do NOSI EPE;
g) Estes documentos são confiados aos recursos humanos dos Grupos de Trabalho do NOSI CA 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 NOSI CA;
h) Todas as palavras-chave, PINs e outros elementos de segurança relacionados com ao NOSI CA;
i) A identificação dos membros dos grupos de trabalho do NOSI CA;
j) A localização dos ambientes do NOSI CA e seus conteúdos.

9.3.2. 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) CRL, e
d) Toda a informação classificada como “pública” (informação não expressamente considerada como “pública” será considerada confidencial).

O NOSI CA permite o acesso a informação não confidencial sem prejuízo de controlos de segurança necessários para proteger a autenticidade e integridade da mesma.

9.3.3. 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 NOSI EPE.

9.4. Privacidade dos dados pessoais

9.4.1. Medidas para garantia da privacidade

O NOSI EPE é responsável pela implementação das medidas que garantem a privacidade dos dados pessoais, de acordo com a legislação cabo-verdiana.

9.4.2. Informação privada

É considerada informação privada toda a informação fornecida pelo titular do certificado que não seja disponibilizada no certificado digital do titular.

9.4.3. Informação não protegida pela privacidade

É considerada informação não protegida pela privacidade, toda a informação fornecida pelo titular do certificado que seja disponibilizada no certificado digital do titular.

9.4.4. Responsabilidade de proteção da informação privada

De acordo com a legislação cabo-verdiana.

9.4.5. Notificação e consentimento para utilização de informação privada

De acordo com a legislação cabo-verdiana.

9.4.6. Divulgação resultante de processo judicial ou administrativo

De acordo com a legislação cabo-verdiana.

9.4.7. Outras circunstâncias para revelação de informação

De acordo com a legislação cabo-verdiana.

9.5. Direitos de propriedade intelectual

Todos os direitos de propriedade intelectual, incluindo os que se referem a certificados, CRL emitidos, OID, DPC e PC, bem como qualquer outro documento, propriedade do NOSI CA pertencem ao NOSI EPE.

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

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

9.6. Representações e garantias

9.6.1. Representação e garantias das entidades certificadoras

O NOSI CA está obrigado a:

a) Efetuar as suas operações de acordo com esta DPC,
b) Declarar de forma clara todas as suas Práticas de Certificação no documento apropriado,
c) Proteger as suas chaves privadas,
d) Emitir certificados de acordo com o *standard* X.509,
e) Emitir certificados que estejam conformes com a informação conhecida no momento de sua emissão e livres de erros de entrada de dados,
f) Garantir a confidencialidade, no processo da geração dos dados da criação da assinatura e na 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, extinguiu 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 “Suspensão e Revogação de Certificados” deste documento e publicar os certificados revogados na LRC do repositório do NOSI CA, com a frequência estipulada na secção 2.3,
m) Publicar a sua DPC e as Políticas de Certificado aplicáveis no seu repositório garantindo o acesso às versões atuais,
n) Disponibilizar, desde que devidamente justificado o pedido de acesso, às versões anteriores da sua DPC assim como das suas Políticas de Certificados,
o) Notificar com a rapidez necessária, por correio eletrónico os titulares dos certificados em caso da EC proceder à revogação ou suspensão dos mesmos, indicando o motivo que originou esta ação,
p) Colaborar com as auditorias dirigidas pela Autoridade Credenciadora, para validar a renovação das suas próprias chaves,
q) Operar de acordo com a legislação aplicável,
r) Proteger em caso de existirem as chaves que estejam sobre sua custódia,
s) Garantir a disponibilidade da LRC de acordo com as disposições da secção 4.9,
t) Comunicar com uma antecedência mínima de dois meses a todos os titulares dos certificados emitidos assim como à Autoridade Credenciadora, em caso de cessar a sua atividade,
u) Cumprir com as especificações contidas na norma sobre Proteção de Dados Pessoais,
v) Conservar toda a informação e documentação relativa a um certificado reconhecido e as Declarações de Práticas de Certificação vigentes em cada momento e durante pelo menos vinte anos desde o momento da emissão e,
w) Disponibilizar os certificados do NOSI CA.

9.6.2. Representação e garantias das entidades de registo

As Entidades de Registo estão obrigadas a:

a) Efetuar as suas operações de acordo com esta Política,
b) Permitir a emissão de certificados livres de erros de entrada de dados,
c) Garantir a confidencialidade, no processo da geração dos dados da criação da assinatura e na sua entrega por um procedimento seguro ao titular,

d) Utilizar sistemas e produtos fiáveis que estejam protegidos contra toda a alteração e que garantam a segurança técnica e criptográfica dos processos de certificação,
e) Arquivar sem alteração os certificados emitidos,
f) Empregar pessoal com qualificações, conhecimentos e experiência necessárias para a prestação de serviços de certificação,
g) Revogar os certificados nos termos da secção “Suspensão e Revogação de Certificados” deste documento e publicar os certificados revogados na LRC do repositório do NOSI CA, com a frequência estipulada na secção 2.3,
h) Colaborar com as auditorias dirigidas pela Autoridade Credenciadora,
i) Operar de acordo com a legislação aplicável, nomeadamente de acordo com o decreto regulamentar nº18/2007 de 24 de Dezembro,
j) Proteger em caso de existirem as chaves que estejam sobre sua custódia,
k) Comunicar com uma antecedência mínima de três meses a todos os titulares dos certificados emitidos assim como à Autoridade Credenciadora, em caso de cessar a sua atividade,
l) Cumprir com as especificações contidas na legislação sobre Proteção de Dados Pessoais,
m) Conservar toda a informação e documentação relativa a um certificado reconhecido e durante pelo menos vinte anos desde o momento da emissão.

9.6.3. Representação e garantias dos titulares

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 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 4.9,
d) Não utilizar um certificado digital que tenha perdido a sua eficácia, quer por ter sido revogado, suspendido ou por ter expirado o período de validade,

e) Submeter às Entidade de Certificação (ou de Registo) a informação que considerem exata e completa em 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, do NOSI CA.

9.6.4. Representação e garantias das partes confiantes

É obrigação das partes que confiem nos certificados emitidos pelo NOSI CA:

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 e aceitar sujeitar-se às mesmas,
f) Notificar qualquer acontecimento ou situação anómala relativa ao certificado, que possa ser considerado como causa de revogação do mesmo, utilizando os meios que o NOSI CA publique no seu sítio Web.

9.6.5. Representação e garantias de outros participantes

Nada a assinalar.

9.7. Renúncia de garantias

O NOSI CA recusa todas as garantias de serviço que não se encontrem vinculadas nas obrigações estabelecidas nesta DPC.

9.8. Limitações às obrigações

A NOSI CA:

a) Responde pelos danos e prejuízos que cause a qualquer pessoa em exercício da sua atividade de acordo com o Artº 62 do DL 32/2007 de 24 de Setembro.
b) 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) Assume toda a responsabilidade mediante terceiros pela atuação dos titulares das funções necessárias à prestação de serviços de certificação.
d) A responsabilidade da administração / gestão do NOSI CA assenta sobre base objetivas e cobre todo o risco que os particulares sofram sempre que seja consequência do funcionamento normal ou anormal dos seus serviços.
e) Só responde pelos danos e prejuízos causados pelo uso indevido do certificado reconhecido, quando não tenha consignado no certificado, de forma clara reconhecida por terceiros o limite quanto ao possível uso.
f) Não responde quando o titular superar os limites que figuram no certificado quanto as suas possíveis utilizações, de acordo com as condições estabelecidas e comunicadas ao titular.
g) 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) Não assume qualquer responsabilidade no caso de perca ou prejuízo:
    i. Dos serviços que prestam, em caso de guerra, desastres naturais ou qualquer outro de força maior,
    ii. Ocasionados pelo uso dos certificados quando excedam os limites estabelecidos pelos mesmo na Política de Certificados e correspondente DPC,

iii. Ocasionado pelo uso indevido ou fraudulento dos certificados ou CRL emitidos por ela.

9.9. Indemnizações

De acordo com a legislação em vigor.

9.10. Termo e cessação da atividade

9.10.1. Termo

Os documentos relacionados com o NOSI CA (incluindo esta DPC) tornam-se efetivos logo que sejam aprovados pelo Grupo de Trabalho de Gestão e apenas são eliminados ou alterados por sua ordem.

Esta DPC entra em vigor a partir do momento da sua publicação no repositório do NOSI CA.

Esta DPC estará em vigor enquanto não for revogada expressamente pela emissão de uma nova versão ou pela renovação das chaves do NOSI CA, momento em que obrigatoriamente se redigirá uma nova versão.

9.10.2. Substituição e revogação da DPC

O Grupo de Trabalho de Gestão pode decidir em favor da eliminação ou emenda de um documento relacionado com o NOSI CA (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 ficar revogada será retirada do repositório público, garantindo-se, contudo, que será conservada durante 20 anos.

9.10.3. Consequências da cessação de atividade

Após o Grupo de Gestão decidir em favor da eliminação de um documento relacionado com a EC, o Grupo de Segurança tem 30 dias úteis para submeter para aprovação pelo Grupo de Trabalho de Gestão, um documento substituto.

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

9.11. 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, formulários assinados, ou outros, dependendo da criticidade e assunto da comunicação.

9.12. Alterações

9.12.1. Procedimento para alterações

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

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

O Grupo 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 da PKI do NOSI 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 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 e fornecido Grupo de Gestão para validação, aprovação e publicação, tornando-se as alterações finais e efetivas.

9.12.2. Prazo e mecanismo de notificação

No caso que o Grupo de Gestão 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.

9.12.3. Motivos para mudar de OID

O Grupo 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.
Nos casos em que, a julgamento do Grupo de Segurança, as alterações da DPC não afetem à aceitação dos certificados proceder-se-á ao aumento do número menor de versão do documento e o último número de Identificador de Objeto (OID) que o representa, mantendo o número maior da versão do documento, assim como o resto de seu OID associado. Não se considera necessário comunicar este tipo de modificações aos utilizadores dos certificados.
No caso em que o Grupo 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. Este tipo de modificações comunicar-se-á aos utilizadores dos certificados segundo o estabelecido no ponto 9.12.2.

9.13. Disposições para resolução de conflitos

Todas reclamações entre utilizadores e NOSI CA deverão ser comunicadas pela parte em disputa à Autoridade 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 do Tribunal da Comarca da Praia.

9.14. Legislação e normas aplicáveis

É aplicável à atividade das entidades certificadoras as seguintes legislações e standards internacional:

a) Decreto-Lei nº 33 /2007, de 24 de Setembro;
b) Decreto-Lei nº44/2009 de 9 de Novembro;
c) Portaria nº 2/2008, de 28 de Janeiro;
d) Portaria Conjunta nº 4/2008, de Fevereiro de 2008;
e) Decreto Regulamentar nº. 18/2007, de 24 de Dezembro.
f) CWA 14167- Cryptographic Module for CSP Signing Operations — Protection Profile;
g) CWA 14169:2004 - Secure signature-creation devices "EAL 4+" ;
h) ETSI EN 319 401 v2.1.1 – Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers;
i) ETSI EN 319 411-1 v1.1.1 – Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates;
   Part 1: General requirements;
j) ETSI EN 319 411-2 v2.1.1 (2016-02) Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates;
   Part. 2: Requirements for Trust Service providers issuing EU qualified certificates;
k) ETSI EN 319 412-1 v1.1.1 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles;

Part 1: Overview and common data structures;

l) ETSI EN 319 412-2 v2.1.1 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles;
Part 2: Certificate profile for certificates issued to natural persons;

m) ETSI EN 319 412-3 v1.1.1 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles;
Part 3: Certificate profile for certificates issued to legal persons;

n) ETSI EN 319 412-4 v1.1.1 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles;

o) Part 4: Certificate profile for web site certificates;

p) ETSI EN 319 412-5 v2.1.1 – Electronic Signatures and Infrastructures (ESI); Certificate Profiles;
Part 5: QCStatements;

q) ETSI EN 319 421 (v1.1.1) – Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps;

r) ETSI EN 319 422 (v1.1.1) – Electronic Signatures and Infrastructures (ESI); Time stamping protocol and time-stamp token profiles.

9.15. Conformidade com a legislação em vigor

Esta DPC é objeto de aplicação de legislação Nacional, regras, regulamentos, ordenações, e ordens incluindo, mas não limitadas a restrições na exportação ou importação de *software*, *hardware* ou informação técnica.

É responsabilidade da Autoridade Credenciadora zelar pelo cumprimento da legislação aplicável listada na secção 9.14.

9.16. Providências várias

9.16.1. Acordo Completo

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

9.16.2. Independência

No caso que uma ou mais estipulações deste documento, sejam ou tendam a ser inválidas, nulas ou irreclamáveis, em termos jurídicos, deverão ser consideradas como não efetivas. A situação anterior é válida, apenas e só nos casos em que tais estipulações não sejam consideradas essenciais. É responsabilidade da Autoridade Credenciadora a avaliação da essencialidade das mesmas.

9.16.3. Severidade

Nada a assinalar.

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

Nada a assinalar.

9.16.5. Força maior

Nada a assinalar.

9.17. Outras providências

Nada a assinalar.

10. REFERÊNCIAS BIBLIOGRÁFICAS

[1] ARME, Declaração de Práticas de Certificação da EC Raiz de Cabo Verde.
[2] ARME, Política de Certificados da ICP-CV e Requisitos mínimos de Segurança.
[3] Portaria nº 2/2008, de 28 de Janeiro;
[4] Decreto-Lei nº44/2009 de 9 de Novembro;
[5] Decreto Regulamentar nº. 18/2007, de 24 de Dezembro;
[6] Decreto-Lei nº 33 /2007, de 24 de Setembro;
[7] Portaria nº 4/2008
[8] FIPS 140-2. 1994, Security Requirements for Cryptographic Modules.
[9] ISO/IEC 3166. 1997, Codes for the representation of names and countries and their subdivisions.
[10] ITU-T Recommendation X.509. 1997, (1997 E): Information Technology - Open Systems Interconnection – The Directory: Authentication Framework.
[11] NIST FIPS PUB 180-1. 1995, The Secure Hash Algorithm (SHA-1). National Institute of Standards and Technology, "Secure Hash Standard,", U.S. Department of Commerce.
[12] RFC 1421. 1993, Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures.
[13] RFC 1422. 1993, Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management.
[14] RFC 1423. 1993, Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers.
[15] RFC 1424. 1993, Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services.
[16] RFC 2252. 1997, Lightweight Directory Access Protocol (v3).
[17] RFC 2560. 1999, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.
[18] RFC 2986. 2000, PKCS #10: Certification Request Syntax Specification, version 1.7.
[19] RFC 3161. 2001, Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).
[20] RFC 3279. 2002, Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
[21] RFC 5280. 2008, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.
[22] RFC 3647. 2003, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.
[23] RFC 4210. 2005, Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP).
[24] CABForum Baseline Requirements
[25] CABForum-EV-Guidelines –v1.7.0