Terça-feira, 21 de julho de 2020

I Série
Número 85

BOLETIM OFICIAL

ÍNDICE

CONSELHO DE MINISTROS

Decreto-lei nº 56/2020

de 21 de julho

A última família de notas do Banco de Cabo Verde data de 2014 e é composta por notas de 200 Escudos, 500 Escudos, 1000 Escudos, 2000 Escudos e 5000 Escudos. Aquando da produção desta família de notas, o Banco de Cabo Verde optou por adequar a denominação de 200 Escudos, face ao surgimento das inovações tecnológicas na indústria de produção de notas, sobretudo a nível das caraterísticas de segurança introduzidas com os novos substratos, designadamente o polímero.

Assim, a nota de 200 escudos, diferente das demais denominações da família de notas de 2014, foi alterada do substrato tradicional em fibra de algodão para o polímero. Essencialmente, a escolha pela substituição do novo substrato teve como base a resistência, a durabilidade e a incorporação de caraterísticas de segurança inovadoras quer para o público como para os profissionais que operam com o numerário.

Tratando-se a nota de 200 Escudos de uma nota de troco das denominações maiores e, consequentemente, a mais utilizada nos pagamentos de retalho, e considerando ainda o ciclo de vida curto desta nota, devido ao desgaste natural da tinta face a aderência ao polímero, o Banco de Cabo Verde, atendendo à necessidade de reforço da denominação de 200 Escudos, decidiu reformular a nota de 200 Escudos e uniformizar a família de notas de 2014 em circulação.

Assim, sob a proposta do Banco de Cabo Verde;

Ao abrigo do disposto no n.º 1 do artigo 7º da Lei Orgânica do Banco de Cabo Verde, aprovada pela Lei n.º 10/VI/2002, de 15 de julho, alterada pela Lei n.º 84/IX/2020, de 4 de abril; e

No uso da faculdade conferida pela alínea *a*) do artigo 204º da Constituição, o Governo decreta o seguinte:

Artigo 1º

Aprovação

É aprovada a emissão de uma nova nota de 200$00 (duzentos escudos), cujas características constam do anexo ao presente diploma, do qual faz parte integrante para todos os efeitos.

Artigo 2º

Curso legal e poder liberatório

A nota emitida ao abrigo do presente diploma tem curso legal e poder liberatório.

Artigo 3º

Entrada em vigor

O presente diploma entra em vigor no dia seguinte ao da sua publicação.

Aprovado em Conselho de Ministros, aos 11 de junho de 2020. — Os Ministros, *José Ulisses de Pina Correia e Silva* e *Olavo Avelino Garcia Correia*

Promulgado em 15 de julho de 2020

Publique-se.

O Presidente da República, JORGE CARLOS DE ALMEIDA FONSECA.

ANEXO

(A que se refere o artigo 1º)

Características da nova nota de 200 escudos

1 - **Frente da nota**

A frente da nota de 200 Escudos compreende:

a) A figura de HENRIQUE TEIXEIRA DE SOUSA, impressa em talho doce, a qual domina a frente da nota, suportada por um medalhão constituído por reproduções de um trecho de *pano di terra* e do mapa da ilha do fogo. O fundo, impresso em *offset*, é composto por um microtexto litográfico, não visível ao olho nu;

b) Foi aposta, do lado direito do retrato de Teixeira de Sousa, a denominação 200, de leitura vertical, de baixo para cima, encimada por uma reprodução em relevo de parte de uma caneta impressa com tinta metálica na cor verde seco e a expressão A LEI PUNE O CONTRAFACTOR, em negativo e de leitura vertical, de baixo para cima;

c) Do lado esquerdo do retrato, imediatamente por baixo do mapa da ilha do Fogo, estão apostas as assinaturas do Governador e do Administrador do Banco de Cabo Verde. Sobre o mapa da ilha, um cacho de uva da região de Chã das Caldeiras, com a inscrição BCV em microtexto, impresso em talhe doce;

d) A limitar o medalhão, na sua parte inferior, ramos de videira, impressos em talhe doce, suportam o texto BCV, de leitura na horizontal, o qual só pode ser lido desde que inclinada a nota num determinado ângulo. Encontra-se, ainda, nessa parte inferior o texto Henrique Teixeira de Sousa, 1919-2019 e a numeração da nota, de leitura na horizontal;

e) Por cima do desenho dos ramos de videira referida em d) está aposto o texto 6 de setembro de 2019, data de aniversário de Henrique Teixeira de Sousa;

f) Na parte esquerda da frente da nota, numa área de aproximadamente um terço da sua superfície, encontram-se colocados, sobre uma banda de estrutura *pyramid anti-scanner*: i) a marca de água utilizando a figura de Henrique Teixeira de Sousa; ii) as denominações BANCO DE CABO VERDE e 200 ESCUDOS, ambas de leitura em duas linhas, impressas em talhe doce; iii) um elemento de identificação da nota por deficientes visuais; iv) a numeração da nota, de leitura na vertical, de cima para baixo, com fluorescência quando usada luz ultravioleta; e v) parcelas de desenhos de grãos de café, de cores diferentes, que coincidem com outras tantas parcelas no verso, reproduzindo a silhueta de grãos de café, quando vista a nota em transparência.

2 - **Verso da nota**

O verso da Nota de 200 Escudos compreende:

a) Uma perspetiva do PICO DO VULCÃO DO FOGO, impressa em *offset*, como elemento principal do verso da nota, aplicada sobre o medalhão constituído por um trecho de *pano di terra;*

b) A denominação 200, aposta na parte superior esquerda do medalhão, a qual também aparece, em negativo, no canto inferior direito;

c) Um cacho de uva da região de Chã das Caldeiras, colocado no canto inferior esquerdo do medalhão, o qual, à luz ultravioleta, aparece em duas cores diferentes;

d) Numa área de aproximadamente um terço da superfície: i) a marca de água com a imagem de Teixeira de Sousa; ii) as denominações BANCO DE CABO VERDE e DUZENTOS ESCUDOS, ambas de leitura em duas linhas, bem como o dístico 200, impressos em talhe doce; iii) parcelas de grãos de café, de cores diferentes, que quando vistas em transparência coincidem com outras tantas parcelas na frente da nota, reproduzindo a silhueta de grãos de café.

3 - **Marca de água**

A marca de água conseguida a partir de um retrato de Henrique Teixeira de Sousa, com aproximadamente 25,3 mm de altura, encontra-se localizada na parte esquerda da frente da nota, numa área de aproximadamente um terço da sua superfície.

4 - **Papel**

O papel será de fios de algodão com fibras invisíveis à luz ultravioleta e com 96 g/m².

5 - **Filete de segurança**

Introduzido no verso da nota, o filete de segurança tem 2mm de espessura, fluorescência tipo arco-íris, magnético, leitura automática e comporta o texto BCV 200.

6 - **Cor**

A cor dominante é o vermelho, tanto na frente como no verso da nota. Foram também aplicadas outras cores vivas em tonalidade verde, amarela e rosa.

7 - **Dimensões**

A nota de 200 Escudos tem 124 mm x 62 mm de dimensão e sentido de orientação horizontal.

———

Decreto-lei nº 57/2020

de 21 de julho

No âmbito do exercício das suas funções legais, a Polícia Judiciária possui um conjunto de dados pessoais, suscetíveis de gerarem informações úteis que, informatizados, constituem um recurso de grande valia para o melhor desempenho das suas atribuições legais.

Os sistemas de informação vêm assumindo, cada vez mais, grande importância no seio das instituições, entre as quais os órgãos da polícia criminal e científica.

Para melhor prevenir, detetar e reprimir esses fenómenos criminais, torna-se indispensável que a Polícia Judiciária possa recorrer às novas tecnologias de informação e comunicação para, de entre outros, ter um Sistema Informatizado de Informação Criminal, seguro e regulado por lei, constituído por um conjunto variado de dados pessoais, nomeadamente, de abertura de processos, de salvados, de dados biográficos e pessoas a procurar, de sistema de apoio à investigação criminal, de desaparecidos, de dados lofoscópicos, e de exames do Laboratório de Polícia Científica.

Outrossim, tendo a Polícia Judiciária um Sistema Informatizado de Informação Criminal (SIIC), a mesma pode, nos termos da lei de segurança interna, da lei de prevenção criminal, da lei de cooperação judiciária internacional em matéria penal e da lei de proteção de dados pessoais de pessoas singulares, cooperar, de uma forma célere e segura, com outras forças, serviços e organismo de segurança, a nível nacional e internacional, através da comunicação recíproca de dados não sujeitos a regime especial de reserva ou proteção, que sejam necessários à realização das finalidades de cada uma dessas forças.

Para o efeito, torna-se indispensável a aprovação de um diploma que regule a Rede Informática da Polícia Judiciária (RIPJ), e que defina, ainda, as responsabilidades de cada utilizador neste sistema, as regras que devem ser observadas na recolha, tratamento, armazenamento e partilha de dados, a defesa dos direitos fundamentais dos cidadãos relacionados com os dados e informações, bem como os instrumentos de fiscalização necessários.

Ainda, no quadro das obrigações assumidas entre Cabo Verde e a União Africana e aquele com a CEDEAO, com a AFRIPOL, com a INTERPOL e com a EUROPOL, pode ser solicitada a Cabo Verde a transferência de dados pessoais, com vista à prevenção e investigação criminal.

Com vista a regular a forma de recolha, tratamento, armazenamento e partilha de dados pessoais pela Polícia Judiciária, o presente diploma define os princípios de segurança da informação para a gestão da RIPJ, bem como a proteção de dados pessoais na implementação, manutenção, operacionalização e administração da Rede. Regula igualmente o setor responsável pela gestão, as normas de segurança e acesso de toda a informação armazenada, processada e transmitida pela RIPJ.

Foi ouvida a Comissão Nacional de Proteção de Dados.

Assim,

No uso da faculdade conferida pela alínea *a*) do n.º 2 do artigo 204º da Constituição, o Governo decreta o seguinte:

CAPÍTULO I

DISPOSIÇÕES GERAIS

Secção I

Objeto, âmbito e definições

Artigo 1º

Objeto

O presente diploma estabelece as normas e regras de segurança para a utilização e gestão da Rede Informática da Polícia Judiciária, adiante designado RIPJ.

Artigo 2º

Âmbito de aplicação

1 - O presente diploma aplica-se a todos os órgãos e serviços da Polícia Judiciária.

2 - O diploma aplica-se, ainda, aos demais entidades e serviços que integram a RIPJ.

Artigo 3º

Definições

Para efeitos do disposto no presente diploma, entende-se por:

a) «Ambiente de desenvolvimento de sistemas», o ambiente computacional destinado ao desenvolvimento, manutenção e alteração dos sistemas de informação relativo aos serviços prestados pelo departamento responsável pela gestão do RIPJ, sendo que as informações des-te ambiente têm por objetivo possibilitar a construção de programas, realização de testes e simulação de situações de erro que possam ser identificadas e visam garantir qualidade funci-onal adequada dos programas e aplicativos utilizados;

b) «Ambiente físico», o ambiente que abriga os equipamentos físicos que fazem parte da RIPJ e sejam necessários para o armazenamento, processamento e transmissão de dados e da informação;

c) «Ambiente de produção de sistemas», o ambiente computacional disponibilizado pelo departamento responsável pela gestão da RIPJ para a gestão dos conteúdos específicos;

d) «Autenticação do utilizador», o procedimento executado pelo ambiente computacional de forma automatizada, com base em mecanismo que garanta a autenticidade da identificação do utilizador, podendo consistir em código de utilizador e palavra-passe, autenticação biométrica ou na utilização de certificado digital qualificado;

e) «Cópia de segurança», a cópia das informações de um determinado ambiente computaci-onal e/ou sistemas, que tem por finalidade a recuperação dos correspondentes dados quando haja ocorrência de situações que tenham indisponibilizado as informações originais;

f) «Desastre físico», a indisponibilidade ou alteração indevida de recursos de informação, causada por elementos da natureza ou equipamentos e ambientes construídos pelo homem;

g) «Desastre lógico», a indisponibilidade ou alteração indevida de recursos de informação, causada por ação no ambiente computacional, através de programas ou ações que alterem indevidamente as informações;

h) «Gestor da informação», a pessoa responsável pela autorização ou negação do acesso do utilizador a uma determinada informação;

i) «Gestor de acesso», a pessoa designada pelo Diretor Nacional da Polícia Judiciária como responsável pela gestão do acesso à RIPJ e aos serviços disponíveis, bem como pelo acompanhamento da validade das autorizações de acessos;

j) «Identificação do utilizador», a sequência de carateres que permite identificar o utilizador quando este estabelece a sua conexão com a RIPJ;

k) «Internet», o ambiente virtual exterior à RIPJ, onde diferentes computadores de várias partes do mundo comunicam através de protocolos de entendimento comum, permitindo a tro-ca de informações;

l) «Intranet», ambiente virtual interior à RIPJ, integrada pela rede de computadores da Polícia Judiciária, que só pode ser acessado pelos seus utilizadores e colaboradores internos ou utilizadores externos autorizados;

m) «Recurso computacional», o recurso ou serviço de tecnologia que possibilita ao utilizador a realização de tarefas;

n) «Recurso de informação», qualquer recurso que tenha a capacidade de receber, armazenar, transmitir ou processar a informação;

o) «Rede Informática da Polícia Judiciária (RIPJ)», o conjunto integrado dos recursos físicos e lógicos, propriedade da Polícia Judiciária de Cabo Verde, relativos às tecnologias de infor-mação e comunicação, nomeadamente hardware, software, conteúdos de qualquer natureza, data centers, Service Centers, plataformas e arquiteturas tecnológicas, redes de comunicação, serviços de terceiros, metodologias, normas e outros recursos de natureza semelhante, legalmente adquiridos, desenvolvidos ou mantidos pela Polícia Judiciária;

p) «Regras de proteção da informação», os procedimentos de segurança da informação defi-nidos e instituídos dos quais o utilizador deve ter conhecimento explícito;

q) «Requisitos de segurança», as condições para o uso da informação de forma segura des-critas nos regulamentos de segurança de informação e em documentos técnicos relativos à pro-teção de informação;

r) «Utilizador profissional», o utilizador autenticado que, no desempenho das suas funções e atribuições profissionais, tem autorização de acesso aos sistemas de informação disponibili-zados através da RIPJ;

s) «Utilizador técnico», os profissionais devidamente autorizados e credenciados pelo depar-tamento responsável pela gestão do RIPJ que, no desempenho das suas funções e atribuições profissionais, têm acesso à RIPJ para efeito, nomeadamente de gestão do parque tecnológico, desenvolvimento, implementação e manutenção de sistemas de informação da Polícia Judiciária.

Secção II

Atributos e princípios de segurança da informação

Artigo 4º

Integridade

O RIPJ é um sistema eletrónico configurado de modo a não sofrer alterações durante um processo de comunicação eletrónica ou durante o acesso a esse mesmo objeto ou documento, e manter as caraterísticas originais estabelecidas pelo proprietário da informação.

Artigo 5º

Autenticidade

A identidade de todos os intervenientes no processo de comunicação eletrónica ou de acesso à RIPJ deve ser verdadeira, autêntica e previamente reconhecida.

Artigo 6º

Confidencialidade

1 - O acesso à informação, e bem assim às transações ou comunicações eletrónicas efetuadas na RIPJ, é confidencial, sendo limitado ao utilizador que dela necessita para o desempenho das suas atividades profissionais, autorizado pelo Diretor Nacional da Polícia Judiciária.

2 - A confidencialidade da informação deve ser mantida durante todo o seu processo de uso e pode ter níveis diferentes ao longo da vida da informação.

Artigo 7º

Privacidade

A informação ou conteúdos de um determinado documento ou as caraterísticas de um processo de transação eletrónica devem ser preservados como "privados" para quem tenha autorização para o seu acesso.

Artigo 8º

Disponibilidade

Toda a informação disponibilizada na RIPJ deve estar sempre acessível para o utilizador autorizado.

Artigo 9º

Legalidade

O uso da informação deve ser feito em conformidade com as leis, com as políticas e normas estabelecidas para a RIPJ.

Artigo 10º

Auditabilidade

Todas as operações efetuadas ou informações veiculadas na RIPJ são passíveis de auditoria.

CAPÍTULO II

REDE INFORMÁTICA DA POLÍCIA JUDICIÁRIA

Secção I

Recursos da Rede Informática da Polícia Judiciária

Artigo 11º

Utilizadores

Os utilizadores da informação, enquanto agentes que interagem com outros recursos da RIPJ para a realização das suas atividades profissionais ou técnicas, constituem recursos da RIPJ.

Artigo 12º

Ambiente físico

1 - O ambiente físico deve ser protegido dos riscos de acesso e produção de eventuais danos ou destruições.

2 - O acesso ao ambiente físico da RIPJ deve ser controlado de acordo com níveis de segurança operacional e física adequados aos recursos de informação e outros que ele contém.

Artigo 13º

Dados e informações

1 - Os dados são os recursos de base da RIPJ que representam factos, conceitos ou instruções e constituem os elementos de partida que, processados, possibilitam a geração de informação.

2 - As informações, enquanto resultado de processamento e interpretação de dados para fins diversos relacionados com processos de negócios e operações, constituem recursos da RIPJ.

Artigo 14º

Infraestrutura

A infraestrutura da RIPJ, suportada pela rede pública de transmissão de dados, é formada pela rede de telecomunicações, infraestruturas de base tecnológicas que possibilitam que os demais recursos funcionem adequadamente.

Artigo 15º

Tecnologia

A tecnologia da RIPJ compreende os computadores de qualquer porte, periféricos, acessórios, softwares ou scripts, e quaisquer outros equipamentos tecnológicos, com suporte, tendencionalmente, em meios eletrónicos que possibilitam a realização do negócio, através da utilização da informação, ou qualquer outro tipo de tratamento de dados ou informação disponível no sistema.

Artigo 16º

Processos

Os processos operacionais aplicáveis, incluindo procedimentos, manuais, normas, instruções, sobretudo de instalações, configurações e testes de funcionamento correto, entre outros, são também considerados recursos de informação e da RIPJ.

Secção II

Gestão da Rede Informática da Polícia Judiciária

Artigo 17º

Responsável pela Gestão da Rede Informática da Polícia Judiciária

O Setor de Telecomunicações, Informática e Apoio Tecnológico, adiante designado STIAT, junto da Direção Nacional da Polícia Judiciária, é o responsável pela implementação, manutenção, operacionalização e administração da RIPJ.

Artigo 18º

Competência

Compete ao STIAT, enquanto entidade gestora da RIPJ, designadamente:

a) Garantir a segurança e operacionalidade da RIPJ e promover a unificação de métodos e processos;

b) Implementar as políticas e normas de segurança de toda a informação armazenada, processada e transmitida pela RIPJ;

c) Implementar o processo de segurança da informação, considerando as orientações deste diploma, com o objetivo de alcançar os níveis adequados de segurança;

d) Implementar as normas e políticas de segurança da informação em todos os recursos disponibilizados na RIPJ;

e) Desenvolver e implementar projetos e ações que permitam à RIPJ alcançar o nível de segurança adequado ao tipo de informação e às caraterísticas dos serviços prestados;

f) Operacionalizar a segurança da informação na RIPJ;

g) Garantir que os requisitos de segurança sejam respeitados no desenvolvimento, manutenção ou alteração de sistemas de informação;

h) Monitorar os acessos, através de registo e atividades de segurança da informação; e

i) O mais que lhe for cometido por lei ou regulamento.

Secção III

Gabinete de Segurança da Informação

Artigo 19º

Missão

1 - O Gabinete de Segurança da Informação, adiante designado GSI, é o órgão responsável pela gestão do processo de segurança e proteção da informação armazenada, processada e transmitida na RIPJ.

2 - O GSI deve garantir o cumprimento por todos os utilizadores da RIPJ das políticas e normas de segurança da informação estabelecidas por lei ou regulamentos e nas recomendações da ISSO/IEC 27001 e 270002.

Artigo 20º

Natureza e funcionamento

1 - O GSI é um serviço da Direção Nacional, que funciona na dependência direta do Diretor Nacional, podendo este delegar a função no Diretor do Departamento de Informação Criminal, Polícia Técnica e Apoio Tecnológico (DICPAT).

2 - A estrutura organizacional, o funcionamento e o quadro de pessoal do GSI constam de regulamento interno próprio, aprovado pelo Diretor Nacional da Polícia Judiciária.

Artigo 21º

Competências

1- Compete nomeadamente ao GSI:

a) Propor medidas de segurança da informação, tendo em conta as melhores práticas internacionais e as recomendações da ISSO/IEC 270001 e 270002;

b) Coordenar o processo de segurança da informação;

c) Controlar, acompanhar e avaliar a implementação das políticas e normas de segurança;

d) Verificar a adequação dos controlos, acompanhar auditorias de sistemas e acompanhar revisões do processo de segurança da informação, procurando garantir que os pontos de vulnerabilidades identificados sejam avaliados mais detalhadamente e que soluções adequadas sejam implementadas;

e) Avaliar a funcionalidade organizacional do sistema, face aos objetivos propostos em relação à segurança da informação;

f) Desenvolver ações para a consciencialização dos utilizadores em matéria de segurança da informação;

g) Avaliar e dar tratamento adequado às questões que estejam indefinidas nas políticas e normas;

h) Interagir com outros órgãos, serviços de segurança e empresas nacionais e internacionais, para a troca de experiências relativas ao processo de segurança da informação, garantindo sua evolução;

i) Assistir a Direção Nacional da Polícia Judiciária no tratamento das questões que não estejam definidas nas políticas e normas de segurança da informação; e

j) O que mais lhe for cometida por lei ou determinação superior.

2 - No exercício das suas competências, o GSI deve interagir com todos os departamentos e serviços da Polícia Judiciária, com vista a garantir o nível de capacitação adequada para cada utilizador dos sistemas de informação.

Seção IV

Acesso à Rede Informática da Polícia Judiciária

Artigo 22º

Recursos da Rede Informática da Polícia Judiciária

A RIPJ compreende um conjunto de recursos físicos e lógicos que têm por objetivo garantir a disponibilização de serviços privativos eletrónicos aos utilizadores e colaboradores internos da Polícia Judiciária para realização de suas atividades funcionais.

Artigo 23º

Utilizadores da Rede Informática da Polícia Judiciária

1 - São utilizadores da RIPJ os dirigentes e funcionários da Polícia Judiciária, sendo que autoridades judiciárias e órgãos da polícia criminal, devidamente autorizados, podem aceder aos recursos da rede e sistemas de informação, seja no exercício de sua atividade profissional, seja para exercer o seu direito de acesso à informação e a serviços públicos eletrónicos.

2 - Cada utilizador deve ter o seu gestor de acesso que deve garantir que existem apenas utilizadores validados na RIPJ.

3 - Os utilizadores da RIPJ, definidos no artigo 3º, são agrupados em duas categorias, a saber:

a) Utilizador profissional, que pode revestir-se com as caraterísticas de:

i. Dirigente e funcionário, agentes de autoridades judiciárias e órgãos de polícia criminal;

ii. Prestador de serviço;

iii. Auditor interno ou externo e;

iv. Consultor.

b) Utilizador técnico.

Artigo 24º

Gestor de acesso

1 - Gestor de acesso é a pessoa responsável pela autorização ou negação do acesso à RIPJ, bem como pelo acompanhamento da validade das autorizações de acesso.

2 - O Gestor de acesso é designado, a nível central, pelo Diretor Nacional, e nível a regional, pelo Diretor do Departamento de Investigação Criminal, e, ainda, pelo responsável máximo do serviço público ou entidade referido n.º 1 do artigo 23º, e tem a responsabilidade de limitar e/ou gerir o acesso aos utilizadores da respetiva instituição.

3 - Compete ao Gestor de acesso:

a) Definir e atribuir o tipo de acesso a ser autorizado;

b) Definir a criação de grupos de utilizadores com a mesma necessidade de autorização de acesso e criar um perfil de acesso para grupo;

c) Autorizar acesso apenas às pessoas que necessitam do mesmo para o desempenho das suas atividades profissionais, no âmbito das atribuições e responsabilidades cometidas pela instituição;

d) Fazer a gestão dos acessos, de acordo com as normas e regras de segurança estabelecidos;

e) Rever, a cada período definido, os acessos existentes dos utilizadores autorizados para efeitos de revalidação; e

f) Retirar o acesso quando o utilizador perde a prerrogativa do mesmo.

4 - A qualificação, a certificação e a credenciação do Gestor de acesso devem ser operacionalizadas pelo Administrador de Sistema da RIPJ.

Artigo 25º

Acesso do utilizador profissional

1 - O acesso do utilizador profissional aos recursos da RIPJ é autorizado e operacionalizado pelo gestor de acesso da respetiva instituição, nos termos do n.º 2 do artigo 24º.

2 - A atribuição do acesso ao utilizador profissional é feita mediante a leitura e assinatura pelo agente ou funcionário público do "Termos de Acesso", que contém as condições e as responsabilidades inerentes ao uso da RIPJ.

3 - A operacionalização do acesso é feita através do cadastramento do interessado nos sistemas de gestão de acesso ao RIPJ.

4 - O acesso à RIPJ é retirado ao utilizador profissional quando este cessa as funções que o tivessem determinado.

Artigo 26º

Acesso do utilizador técnico

1 - O utilizador técnico tem acesso à RIPJ mediante autorização expressa do STIAT, para o exercício restrito das suas funções e atribuições.

2 - A atribuição do acesso é feita pelo Administrador de Sistemas da RIPJ, em razão das suas atribuições, funções e responsabilidades técnicas na RIPJ.

3 - A operacionalização do acesso é feita através do cadastramento do interessado nos sistemas de gestão de acesso ao RIPJ.

4 - O acesso à RIPJ é retirado ao utilizador técnico quando este cessa as funções que o tivessem determinado.

Artigo 27º

Registo do acesso

1 - Todos os acessos realizados devem ser registados na RIPJ e guardados pelo prazo estabelecidos em regulamentos e normas.

2 - Os utilizadores devem ser informados de que os seus acessos ficam registados.

Artigo 28º

Responsabilidades

1 - O utilizador da RIPJ é responsável pelo acesso realizado com identificação e autenticação próprias.

2 - São responsabilidades do utilizador:

a) Solicitar acesso apenas para o desempenho das suas atividades profissionais através da RIPJ;

b) Eximir-se de aceder à RIPJ, quando as suas atividades profissionais não exigirem mais esse acesso.

Artigo 29º

Uso do correio eletrónico

1 - O correio eletrónico é um recurso atribuído ao utilizador conjuntamente com o acesso à RIPJ, pelo gestor de Acesso.

2 - Os endereços de correio eletrónico disponibilizados aos utilizadores, bem como as mensagens e outros conteúdos associados a cada endereço de correio eletrónico, são propriedade do Estado de Cabo Verde, mais precisamente da Polícia Judiciária, e são cedidos aos utilizadores para o desempenho exclusivo das suas atividades profissionais.

3 - A entrega do endereço de correio eletrónico ao utilizador deve ser feita de forma controlada e segura, com o objetivo de garantir que, a partir desse momento, apenas o utilizador tenha possibilidade de aceder ao seu endereço eletrónico.

4 - Os limites ao uso do correio eletrónico pelo utilizador da RIPJ, em termos de volume e capacidade, devem ser fixados pela STIAT, de acordo com os limites estipulados na Rede Tecnológica Privativa do Estado (RTPE).

Artigo 30º

Acesso e uso da Internet

1- O acesso e uso da internet pelos utilizadores da RIPJ devem ser feitos em estrita observância ao disposto no artigo 33º do Decreto-lei n.º 19/2010, de 14 de junho, que estabelece as políticas, normas e regras de segurança da informação para a gestão da Rede Informática Privativa do Estado.

2 - Para a navegação na Internet, devem ser utilizados apenas os softwares e versões homologados pelo serviço responsável pela gestão da RIPJ.

3 - Todos os arquivos recebidos a partir do ambiente da Internet para o ambiente da RIPJ, devem ser varridos por produto antivírus homologado pelo serviço responsável pela gestão da RIPJ e em uso na RIPJ.

4 - É proibido ao utilizador alterar a configuração do navegador da sua máquina, no que diz respeito aos parâmetros de segurança.

5 - Havendo necessidade de alteração da configuração, o serviço responsável pela gestão da RIPJ deve ser acionado para promover o procedimento a ser seguido.

6 - No uso da Internet, o utilizador não deve aceder a endereços ou executar ações que possam violar direitos de autor, marcas, licenças de software ou patentes existentes.

7 - É proibido o alojamento de páginas pessoais ou qualquer outra propaganda comercial pessoal no ambiente da Internet utilizando recursos da RIPJ.

8 - É vedada a transferência de material ofensivo ou hostil nos endereços na Internet utilizando recursos da RIPJ.

9 - É vedada e considerada abusiva a utilização dos recursos da RIPJ para:

a) A visualização, transferência, cópia, distribuição ou qualquer outro tipo de acesso a *sites:*

i. Com conteúdo pornográfico, pedofilia, violência;

ii. Que promovem atividades ilegais; e

iii. Que menosprezem, depreciem ou incitem preconceitos relacionados com o género, raça, orientação sexual, idade, religião, nacionalidade, deficiência física e outros.

b) A transferência ou cópia de conteúdos multimédia com volumes superiores aos definidos pelo STIAT, serviço responsável pela gestão da RIPJ, salvo exceção fixadas pelo próprio GSI;

c) A participação em salas de "chat", grupos de discussão, ou outros recursos de comunicação interativas sobre assuntos não relacionados com as funções e atribuições do utilizador; ou

d) Distribuição, pela Internet, de informações confidenciais.

Artigo 31º

Recurso computador e periféricos

1 - O computador, seja de mesa ou portátil, acompanhado de seus periféricos, disponibilizados ao utilizador, é propriedade do Estado, mais precisamente da Polícia Judiciária e, como tal, sujeito ao registo patrimonial.

2 - O utilizador é o gestor desse recurso e deve zelar e garantir a sua integridade, correto funcionamento, bem como, a confidencialidade das informações neles contidas.

3 - Nos casos em que este recurso seja partilhado por mais de um utilizador, cabe ao superior hierárquico que tenha atribuído o recurso, a designação do responsável para zelar e garantir a integridade, o correto funcionamento, bem como, a confidencialidade das informações nele contidas.

4 - Ao cessar as suas funções, definitivamente ou por transferência para outro serviço, o respetivo computador deve permanecer no serviço de origem.

5 - O computador portátil deve ser mantido em lugar seguro, devendo essa responsabilidade ser formalmente assumida pelo utilizador respetivo.

6 - Em caso algum, o utilizador pode alterar os componentes físicos nem a configuração lógica do recurso computador.

7 - Em caso algum, é permitido ao utilizador instalar e/ou executar códigos aplicativos ou outros executáveis em qualquer recurso da RIPJ sem a autorização prévia e expressa do STIAT.

8 - A alteração dos componentes físicos e a configuração lógica do computador é uma atribuição exclusiva do STIAT.

Artigo 32º

Conexão com ambientes externos

1 - A comunicação do ambiente da RIPJ com outras redes ou ambientes de tecnologia externas deve ser necessária e adequada à prossecução da finalidade legal ou estatutária e de interesse legítimo do responsável pelo tratamento, e realizada de forma segura, controlada e de modo a que sejam mínimos os riscos de invasão ao ambiente da RIPJ.

2 - São proibidos quaisquer atitudes e/ou comportamentos dos utilizadores que visem a invasão danosa do ambiente computacional de terceiros, sob pena de se tornar alvo de procedimento disciplinar e criminal, nos termos da lei.

3 - Apenas produtos (softwares) homologados e autorizados pela instituição responsável pela gestão da RIPJ devem ser utilizados para a comunicação com ambientes externos.

4 - É igualmente proibido ao utilizador baixar e/ou executar códigos aplicativos ou outros executáveis disponíveis na Internet para a RIPJ.

5 - Todos os sítios da Internet mantidos pelo STIAT devem ser periodicamente testados para garantir a atualização das informações tipo endereço e também para garantir que o serviço está em atividade normal.

CAPÍTULO III

INFORMAÇÃO E SISTEMAS DE INFORMAÇÃO

Secção I

Princípios e atributos

Artigo 33º

Valor da Informação

A informação disponível na RIPJ é um recurso de valor que permite a Polícia Judiciária, enquanto órgão de polícia criminal e científica, de realizar adequadamente as suas atribuições no âmbito da prevenção e investigação criminal, em conformidade com a lei que define a sua orgânica, a lei de investigação criminal e a lei de proteção de dados pessoais das pessoas singulares.

Artigo 34º

Sistema de informação

O sistema de informação (SI) é um conjunto de procedimentos organizados que, uma vez executado, provêm informações de suporte à organização, mediante processamento de dados de forma informatizada, e disponibiliza informação aos utilizadores.

Artigo 35º

Titularidade do direito de propriedade da Informação

O Estado de Cabo Verde é proprietário das informações armazenadas, processadas e transmitidas na RIPJ, com a exceção dos dados pessoais definidos no regime jurídico geral da proteção de dados pessoais das pessoas singulares e sem prejuízo dos níveis de classificação da informação.

Secção II

Ambientes de sistemas de informação

Artigo 36º

Ambiente de desenvolvimento e ambiente de teste de sistemas

1 - Os ambientes de desenvolvimento e teste de sistemas são utilizados exclusivamente para o desenvolvimento, manutenção, alteração e teste de sistemas de informação.

2 - Os dados utilizados nestes ambientes são, preferencialmente, não reais ou dados reais mascarados.

3 - A utilização de dados reais nestes ambientes carece de autorização formal do respetivo gestor de informação.

4 - A passagem de programas do ambiente de testes de sistemas para o ambiente de produção de sistemas deve ser feita de forma planeada, controlada, registada e autorizada pelo dirigente do serviço responsável pelo ambiente de produção de sistemas, de forma a garantir a integridade e disponibilidade da RIPJ.

Artigo 37º

Ambiente de produção de sistemas

1 - As informações do ambiente de produção de sistemas são reais, válidas, verdadeiras e possuem valor legal.

2 - É proibida a utilização do ambiente de produção de sistemas para execução de manutenção, alteração e testes de programas ou sistemas.

3 - É vedada a utilização de qualquer solução tecnológica na RIPJ, sem a prévia certificação, qualificação e autorização do STIAT, e, em particular, do seu Núcleo de Segurança de Informação.

Secção III

Classificação da informação

Artigo 38º

Finalidade

A classificação da informação tem por finalidade definir os requisitos e as regras de segurança referentes ao nível de confidencialidade ou sigilo da informação disponibilizado na RIPJ.

Artigo 39º

Processo de classificação da Informação

1 - Toda a informação, disponibilizada pela RIPJ, deve ser classificada pelo respetivo gestor da informação em relação ao seu nível de confidencialidade.

2 - Na definição do nível de classificação da informação, deve-se considerar:

a) As pessoas ou entidades que devem ter acesso à informação; e

b) Os procedimentos que devem ser seguidos na utilização da informação.

3 - A classificação da informação deve estar escrita em local visível do suporte em que esteja incluída.

Artigo 40º

Níveis de classificação da informação

Podem ser fixados dois níveis de confidencialidade para a classificação da informação:

a) Informação interna, que pode ser caraterizada em função da sua abrangência, podendo ser restrita a uma parte de pessoas ou de grupos, conforme abrangência definida:

i. Dados digitais, que podem ser acedidos pelos utilizadores da RIPJ autorizados, conforme abrangência definida;

ii. Cópia, que pode ser feita sem restrição;

iii. Correio eletrónico, que pode ser lido ou enviado sem restrição.

b) Informação Confidencial, toda a informação que tem forte restrição de acesso, nomeadamente em relação a:

i. Dados digitais, que podem ser acedidos somente pelos utilizadores autorizados;

ii. Cópia, que somente pode ser feita para fins do serviço ou para existência de cópia de segurança;

iii. Correio eletrónico, cujas informações confidenciais devem ser transmitidas de forma segura, em conformidade com as melhores práticas tecnológicas.

Secção IV

Proteção e segurança da informação

Artigo 41º

Proteção da informação

1 - Toda a informação disponibilizada pela RIPJ deve ser protegida, cuidada e gerida, visando a sua confidencialidade, integridade e disponibilidade, de forma que não seja acedida, alterada e destruída indevidamente.

2 - A informação armazenada no ambiente de tecnologia deve ser protegida contra desastre físico e lógico.

Artigo 42º

Documentação

Todos os procedimentos relacionados com o uso e a segurança da informação devem ser inscritos em regulamentos e manuais, de forma a possibilitar a continuidade dos mesmos procedimentos, mesmo na ausência dos responsáveis diretos.

Artigo 43º

Responsabilidade dos utilizadores

1 - Os utilizadores da RIPJ devem proteger, adequadamente, a informação na RIPJ, pelo que são obrigados a participar no processo contínuo de qualificação e treinamento em segurança de informação, organizado pelo GSI.

2 - O STIAT deve interagir com todas as instituições conectadas, com vista a garantir o nível de capacitação adequado para cada utilizador dos sistemas de informação.

Artigo 44º

Confidencialidade da informação

1 - O gestor da informação classifica o nível de confidencialidade e proteção da informação, baseando-se nas políticas e normas de Segurança de Informação.

2 - A confidencialidade da informação deve ser mantida durante todo o processo de uso da informação, podendo ter níveis diferentes ao longo da vida da informação.

Secção V

Gestão de sistemas de informação

Artigo 45º

Gestor de informação

O STIAT é o gestor geral da informação, sendo que compete a cada departamento e/ou serviço central ou local integrado na RIPJ, nomear o respetivo gestor da informação.

Artigo 46º

Competência do gestor de informação

1 - Cabe ao gestor da informação, em articulação com o GSI da RIPJ, definir o conjunto das funcionalidades dos Sistemas de Informação instalados, atribuídas a cada serviço, utilizador ou grupo de utilizador.

2 - Compete ao gestor da informação, em estreita articulação com o GSI da RIPJ, nomeadamente:

a) Definir o nível de classificação de confidencialidade da informação;

b) Avaliar o impacto para o serviço, nas situações de indisponibilidade dos sistemas de informação;

c) Definir o nível de continuidade de negócio referente ao SI sob sua responsabilidade, avaliando as soluções para situações de desastre e de contingência;

d) Definir para os sistemas e serviços sob a sua responsabilidade, a necessidade de cópias de segurança, bem como seu tempo de guarda e avaliar as soluções implementadas;

e) Mobilizar os recursos que permitam a implementação e manutenção do nível de proteção e disponibilidade desejado para os sistemas ou serviços sob a sua responsabilidade;

f) Atribuir ao utilizador credenciado, o direito a operar a respetiva funcionalidade no SI;

g) Retirar o acesso do utilizador ao SI quando perde a prerrogativa de uso do mesmo, nomeadamente quando cessa as funções que determinaram esse acesso.

3 - O gestor da informação deve monitorar o funcionamento do SI e os acessos efetuados, no sentido de verificar se os utilizadores têm acesso somente às funcionalidades a que são autorizadas por força das suas atribuições e responsabilidades.

Secção VI

Acesso a Sistemas de Informação

Artigo 47º

Acesso à informação

1 - O acesso à informação armazenada e processada na RIPJ é individual e intransmissível.

2 - Para aceder a qualquer informação, o utilizador deve estar devidamente autorizado e previamente autenticado.

3 - O utilizador deve ter acesso exclusivamente às informações necessárias para o seu desempenho profissional, no âmbito das suas atribuições e responsabilidades cometidas pela instituição respetiva.

4 - O tipo de acesso deve ser compatível com a necessidade do utilizador profissional e a confidencialidade da informação.

Artigo 48º

Acesso à informação

Todos os acessos realizados pelo utilizador devem ser registados na RIPJ e guardados pelo prazo estabelecido nos regulamentos.

CAPÍTULO IV

FINALIDADES, TIPOS E DESCRIÇÃO DO CONTEÚDO DE ALGUNS FICHEIROS

Artigo 49º

Finalidades dos ficheiros informáticos

Os ficheiros informáticos existentes nos SI têm por finalidade organizar e manter atualizada a informação necessária ao exercício das funções que são atribuídas nos termos da Lei Orgânica e da lei de investigação criminal à Polícia Judiciária.

Artigo 50º

Tipos de ficheiros informáticos

Nos SI da Polícia Judiciária existem um conjunto de ficheiros informáticos, nomeadamente, os ficheiros *logs,* os *scripts* de instalação, configuração e de teste de segurança do sistema; os ficheiros de abertura de processo; os de registos biográfico; os de pessoas a procurar; os de salvados; os de desaparecidos; os de dados lofoscópicos; os de dados estatísticos; os de exames forenses; entre outros, necessários para garantir a segurança dos sistemas e registos de dados e informações pessoais recolhidos e tratados, de acordo com o disposto no presente diploma e nas demais legislação aplicáveis.

CAPÍTULO V

GARANTIAS DO TITULAR DO REGISTO, DE SEGURANÇA, PROTEÇÃO DE DADOS PESSOAIS, DIREITO À INFORMAÇÃO, ACESSO E RETIFICAÇÃO

Artigo 51º

Declaração de compromisso

As instituições e serviços competentes que, no âmbito do presente diploma, tenham sido autorizados a aceder a RIPJ, devem declarar o seu comprometimento em relação aos requisitos e procedimentos para a proteção dos direitos de privacidade dos utilizadores e da informação individual identificável armazenada, processada e transmitida na RIPJ.

Artigo 52º

Princípios básicos

1 - O STIAT e as autoridades envolvidas na gestão e tratamento de dados pessoais, observam a privacidade individual dos utilizadores da RIPJ e têm a responsabilidade de proteger os dados pessoais sob sua custódia de que são fiéis depositários, nos termos estabelecidos na lei.

2 - A política de privacidade de dados pessoais é assegurada, nomeadamente, através da observância dos seguintes princípios básicos:

a) O STIAT não pode acumular ou manter dados pessoais ou outros que não aqueles estritamente necessários à realização das atribuições da Polícia Judiciária;

b) Todos os dados pessoais sob a guarda do serviço responsável pela gestão da RIPJ são confidenciais e, por isso, sujeitos a medidas previstas na lei para evitar a divulgação indevida ou não autorizada desses dados;

c) Os dados pessoais que estejam sob a guarda da instituição responsável pela gestão da RIPJ não devem ser disponibilizados a terceiros, salvo nos casos e modos previstos na lei;

d) As autoridades judiciárias competentes, devidamente autorizados, podem ter acesso à informação criminal contida no SI da Polícia Judiciária, de acordo com o nível de perfil de acesso, relativamente as matérias que, estando no âmbito das respetivas atribuições e competências, tiveram, em cada caso, necessidade de conhecer;

e) O fornecimento de dados e informações deve limitar-se àquilo que for considerado relevante e necessário para o êxito da prevenção ou da investigação criminal, no caso concreto;

f) As pessoas que, no exercício das suas funções, tenham tido acesso ao SI da Polícia Judiciária estão obrigadas ao sigilo profissional, nos termos da legislação nacional da proteção de dados pessoais e das demais normas legais aplicáveis, mesmo após o termo daquelas.

Artigo 53º

Garantias de segurança

1 - A RIPJ, suportada pela rede pública de transmissão de dados, é constituída por circuitos permanentes e linhas dedicadas, que impedem a conexão com quaisquer outros sistemas ou utilizadores não autorizados pela Polícia Judiciária.

2 - A instituição responsável pela gestão da RIPJ deve tomar todas as medidas necessárias para que os dados pessoais, sob a sua custódia, sejam protegidos contra as operações de leitura, modificação, supressão, escrita, apagamento ou comunicação de dados não autorizados nos termos dos números seguintes.

3 - Cada utilizador do sistema possui uma conta pessoal, protegida por senha, que lhe possibilita o acesso à informação em função dos privilégios que lhe estão atribuídos, definidos pelo gestor da informação, face às normas do serviço e às funções do utilizador.

4 - Sem prejuízo do disposto no número anterior, podem ser estabelecidas proteções baseadas em tabelas de controlo automático de acesso e, quando a informação esteja registada em base de dados, existem mecanismos adicionais de proteção inerentes ao *software* gestor da base de dados.

5 - O mecanismo de controlo automático de acessos aos ficheiros permite verificar por quem, onde e quando o sistema foi operado, bem como o tipo de operação realizada.

6 - Podem ser realizados controlos aleatórios periódicos da legalidade das consultas e tentativas de consulta, cujos relatórios de análise devem ser conservados por um período de dois anos, findo o qual devem ser apagados.

7 - Podem aceder aos registos e relatórios de análise a que se referem os n.ºs 5 e 6, as autoridades judiciárias para fins de investigação de eventuais violações, sem prejuízo das competências da Comissão Nacional de Proteção de Dados.

Artigo 54º

Garantias do titular do registo

1- Devem constar do registo as razões que levaram à sua criação ou, se for caso disso, à sua manutenção e, quando a ela haja lugar, os resultados da investigação.

2 - Sendo instaurado procedimento criminal, deve constar do registo o conteúdo da decisão que lhe pôs termo.

3 - Independentemente dos prazos de conservação dos dados pessoais registados, estes devem ser imediatamente apagados logo que sejam considerados infundadas as razões que levaram à sua criação.

4 - Nos casos de extinção do procedimento criminal e quando ocorra sentença absolutória, terão de justificar-se, se necessário, para fins de investigação e, caso a caso, as razões que levam à manutenção das informações registadas, nunca podendo estas ultrapassar, porém, os prazos máximos de conservação previstos nos regulamentos.

Artigo 55º

Fluxos transfronteiriços de dados pessoais

1 - No quadro das obrigações assumidas entre Cabo Verde e a União Africana e aquele com a CEDEAO, com a AFRIPOL, com a INTERPOL e com a EUROPOL, pode ser solicitada a Cabo Verde a transferência de dados pessoais, com vista à prevenção e investigação criminal.

2 - Os dados pessoais, objeto de transferência, são as referentes à prevenção e investigação criminal, relativamente aos processos de droga, tráfico de pessoas, tráfico de armas, terrorismo, organização criminosa transnacional, cibercriminalidade, lavagem de capitais e de dados lofoscópico.

3 - As transferências de dados pessoais devem ser feitas com observância dos princípios estatuídos na lei que define o regime jurídico geral de proteção de dados pessoais de pessoas singulares.

Artigo 56º

Entidade responsável

1 - Para efeitos do regime jurídico de proteção de dados pessoais, o Diretor Nacional da Polícia Judiciária é a entidade responsável pelo tratamento da base de dados.

2 - Cabe ao Diretor Nacional da Polícia Judiciária assegurar o direito de informação e de acesso aos dados pelos respetivos titulares, a correção de inexatidões, o complemento de omissões, a supressão de dados indevidamente registados, velar pela legalidade da consulta ou da comunicação da informação, bem como definir os termos do controlo necessário a segurança da informação.

Artigo 57º

Direito à informação, acesso e retificação

1 - Por solicitação escrita dirigida à Polícia Judiciária, que pode ser transmitida por meios informáticos, a pessoa identificada nos termos do presente diploma, ou o seu representante legal ou voluntário, pode conhecer o conteúdo do registo dos seus dados pessoais, nos termos da legislação nacional de proteção de dados.

2 - De igual modo, a pessoa identificada nos termos do presente diploma, ou seu representante legal ou voluntário, tem direito de exigir a retificação, a supressão ou o bloqueio de informações inexatas e o suprimento das omissões, bem como a supressão das que tenham sido obtidas por meios ilícitos ou enganosos ou cujo registo ou conservação não sejam permitidos, após consulta dos demais órgãos de polícia criminal.

CAPÍTULO VI

CÓPIAS DE SEGURANÇA

Artigo 58º

Continuidade do uso de informação

1 - Toda a informação crítica para o funcionamento dos sistemas de informação da Polícia Judiciária deve possuir, pelo menos, uma cópia de segurança atualizada e guardada em local remoto, com o nível de proteção equivalente ao nível de proteção original.

2 - Para a definição das cópias de segurança, devem ser considerados os aspetos legais, históricos, de auditoria e de recuperação de ambiente.

3 - Os recursos tecnológicos, de infraestrutura e os ambientes físicos utilizados para suportar os sistemas de informação, devem ser sujeitos a controlo de acesso físico, condições ambientais adequadas e devem ser protegidos contra situações de indisponibilidade causadas por desastres ou contingências.

4 - Para cada serviço prestado pelo SI, deve haver definição do nível de disponibilidade em situações de desastre e contingências e, para tal, a solução deve considerar os adequados recursos de tecnologia, humanos e de infraestrutura existentes.

Artigo 59º

Cópia de segurança

1 - Devem ser sempre mantidas cópias das informações dos ambientes computacionais ou de sistemas.

2 - As cópias de segurança devem ter:

a) Informações utilizadas para a recuperação do ambiente computacional, em caso de falhas ou perdas;

b) Informações legais, designadamente as que, mesmo isentas de obrigatoriedade legal, o serviço público tenha interesse em manter e aceder; e

c) Informações para auditoria, designadamente as destinadas a facilitar e a concorrer para a realização de investigações e/ou auditorias aos recursos da RIPJ.

3 - O prazo para a realização da cópia de segurança deve ser definido em regulamentos, em razão da natureza e importância da informação.

4 - Para atender a necessidades específicas de segurança, podem ser guardadas cópias específicas.

5 - As cópias de segurança devem ser mantidas e guardadas no ambiente físico principal.

Artigo 60º

Plano de continuidade operacional

1 - Para a continuidade operacional do acesso e utilização da informação na RIPJ, os recursos de informação alternativos e os processos utilizados em situação de contingência devem ter o mesmo nível de segurança, proteção e sigilo dos elementos utilizados, em conformidade com as orientações da ISSO/IEC 27001 e 27002.

2 - O desenvolvimento de planos de continuidade operacional para garantir os níveis de disponibilidade da informação e/ou serviço é coordenado pelo Gabinete de Segurança da Informação da RIPJ.

3 - Em periodicidade definida pelo GSI, o plano de continuidade deve ser testado de forma estruturada, documentado e com possibilidade de ser sujeito a auditabilidade.

4 - Os testes do plano de continuidade devem ocorrer com a participação das pessoas que normalmente são envolvidas nos casos em que uma situação real possa acontecer.

Artigo 61º

Nível de disponibilidade

1 - O nível de disponibilidade é o indicado para a solução de continuidade operacional referente aos serviços prestados através da RIPJ.

2 - Os níveis de disponibilidade dos recursos de informação utilizados pelos serviços prestados pela RIPJ são definidos em regulamentos próprios.

3 - O GSI, com a colaboração do STIAT, é responsável pela definição dos níveis de disponibilidade dos sistemas de informação.

4 - Na fixação dos níveis de disponibilidade devem ser avaliadas as potencialidades tecnológicas e os custos inerentes.

CAPÍTULO VII

FORMAÇÃO E CERTIFICAÇÃO, UTILIZADORES, PONTO DE CONTATO E FISCALIZAÇÃO

Artigo 62º

Formação e certificação

1 - A certificação de competências dos funcionários da Polícia Judiciária, bem como de agentes de outros órgãos de polícia criminal autorizados a recolher amostras, a registar e a tratar dados nos Sistemas de Informação da Polícia Judiciária, é procedida de aprovação em curso de formação adequada, de responsabilidade de cada órgão de polícia criminal.

2 - As competências dos formadores dos cursos referidos no número anterior são certificadas pela Polícia Judiciária, através do Centro de Formação da Polícia Judiciária, ou por outra entidade estrangeira, legalmente competente.

3 - Os conteúdos das formações previstas no n.º 1 são certificados pela Polícia Judiciária, através do Centro de Formação da Polícia Judiciária, em coordenação com os órgãos de polícia criminal devidamente autorizados para aceder e provisionar os ficheiros diretamente.

4 - A designação dos funcionários e agentes certificados para o exercício das funções de tratamento de dados nos sistemas de Informação da Polícia Judiciária, no âmbito de cada órgão de polícia criminal envolvido, efetua-se nos termos dos respetivos normativos orgânicos e estatutários.

Artigo 63º

Perfis de acesso

1 - O acesso ao RIPJ faz-se de acordo com os seguintes perfis:

a) Perfil 1 – reservado a Direção Nacional da PJ;

b) Perfil 2 – reservado aos Coordenadores de Investigação Criminal;

c) Perfil 3 - Reservado aos Inspetores Chefes das brigadas de investigação criminal;

d) Perfil 4 – Reservado aos Inspetores; e

e) Perfil 5 - Reservado aos utilizadores que desempenham funções de analistas.

2 - São estabelecidos, simultaneamente, perfis estruturados horizontalmente, por forma a que o acesso aos sistemas de informação tenha em conta as distintas atribuições e competências do pessoal de chefia de investigação criminal, previstos na Lei Orgânica da Polícia Judiciária e demais legislações aplicáveis.

3 - São aprovados pela Direção Nacional da Polícia Judiciária, com a colaboração do GSI, os mecanismos institucionais apropriados de atribuição de perfis, as regras de registo do uso e de auditoria de acessos, bem como os demais procedimentos de segurança que garantam o cumprimento do disposto no artigo 53º.

4 - As autoridades judiciárias podem, a todo o momento e relativamente aos processos-crimes de que sejam titulares, aceder à informação constante do da RIPJ através do Sistema Integrado de Informação Criminal, nos termos da lei.

Artigo 64º

Utilizadores

1 - O acesso aos ficheiros é efetuado em tempo real, através de consulta automatizada.

2 - As autoridades de polícia criminal que foram autorizadas para acessar e provisionar o ficheiro de dados lofoscópicos devem comunicar à Polícia Judiciária a identificação dos utilizadores com acesso ao ficheiro lofoscópico, designadamente, à plataforma do Sistema Automático de Identificação de Impressões Digitais (AFIS, sigla inglesa de *Automated Fingerprint Identification System*), mediante indicação do nome, do endereço de correio eletrónico institucional, da categoria e função, tendo em vista a atribuição de nomes de utilizador (*usernames)* e respetivas senhas (*passwords)* de acesso ao sistema, no âmbito do processo penal ou de uma ação de prevenção criminal, em razão das funções desempenhadas e das competências atribuídas.

Artigo 65º

Fiscalização

1- A Comissão Nacional de Proteção de Dados é a entidade que compete verificar as condições de funcionamento dos sistemas de informação da Polícia Judiciária, bem como as condições de recolha, armazenamento e transmissão das informações neles constantes, nos termos das disposições relativas a proteção de dados pessoais e exercício das demais competências, previstas na legislação nacional de proteção de dados pessoais.

2- O disposto no número anterior não prejudica as competências da Procuradoria da República e do Conselho Superior da Magistratura Judicial, enquanto entidades responsáveis pelo tratamento de dados relativos às instruções em processo penal e dos processos penais nos tribunais judiciais.

CAPÍTULO VIII

DISPOSIÇÕES SANCIONATÓRIAS

Artigo 66º

Sanções

Os utilizadores da RIPJ que, no exercício das suas funções ou fora dele, apropriar, destruir ou modificar a informação ou violar qualquer dos preceitos mencionados no presente diploma, respondem civil e criminalmente, em função da gravidade e consequências dos seus atos, nos termos da lei civil e penal vigentes, sem prejuízo da responsabilidade disciplinar a que der origem.

CAPÍTULO IX

DISPOSIÇÃO FINAL

Artigo 67º

Regulamentação

Para garantir a implementação das políticas e normas de segurança na utilização dos recursos da RIPJ, devem ser aprovados e fixados manuais e procedimentos internos pelo Diretor Nacional da Polícia Judiciária, com a colaboração do Gabinete de Segurança da Informação e da entidade responsável pela gestão da RIPJ e parecer prévio da Comissão Nacional de Proteção de Dados.

Artigo 68º

Entrada em vigor

O presente diploma entra em vigor no dia seguinte ao da sua publicação.

Aprovado em Conselho de Ministros, aos 2 de julho de 2020. — Os Ministros, *José Ulisses de Pina Correia e Silva*, *Janine Tatiana Santos Lélis* e *Paulo Augusto Costa Rocha*

Promulgado em 16 de julho de 2020

Publique-se.

O Presidente da República, JORGE CARLOS DE ALMEIDA FONSECA

Decreto-legislativo nº 5/2020

de 21 de julho

Cabo Verde é um país arquipelágico e uma Nação diaspórica. Estes dois elementos estruturantes do que somos desde cedo recomendaram uma especial configuração do sistema de Administração Pública que pudesse corresponder às expectativas e necessidades legítimas dos cidadãos e das empresas. Na verdade, nessas condições, o acesso dos cidadãos e empresas aos serviços públicos implica uma multiplicação significativa de postos físicos ou então um sistema que em larga medida permita solicitar e usufruir de serviços públicos à distância, sempre que possível.

Pretendendo dar corpo à segunda alternativa, em 2004, foi aprovada a Lei n.º 39/VI/2004 (Lei da Modernização Administrativa), com o objetivo de modernizar a Administração Pública Cabo-verdiana e de melhorar a prestação dos serviços públicos, de modo a torna-la mais célere, tendo sido estabelecido um conjunto de medidas de modernização e simplificação administrativa, designadamente relativas ao acolhimento e atendimento dos cidadãos em geral e dos agentes económicos em particular, à comunicação administrativa, à simplificação de procedimentos, à audição dos utentes e ao sistema de informação para a gestão.

O desenvolvimento das tecnologias de informação e comunicação, permite cada vez mais o desenvolvimento e a implementação de mecanismos eletrónicos, adequados a uma melhor interação entre os cidadãos, as empresas e a Administração Pública. Mecanismos que facilitam a solicitação de serviços públicos e aceleram e melhoram a qualidade de sua prestação e consequentemente da Administração Pública.

Assim, prosseguindo os objetivos delineados na Lei de Modernização Administrativa, procede-se, através do presente diploma, à implementação de um conjunto de medidas de simplificação e de modernização administrativa, em particular quanto aos mecanismos administrativos de interação dos cidadãos com os serviços públicos e vice-versa, designadamente a previsão da possibilidade de apresentação de requerimentos *online*, do atendimento ao público e à possibilidade de prestação de serviços *online* por parte da Administração Pública através da adoção de um sistema alternativo e voluntário de autenticação de cidadãos nos portais e sítios na internet da Administração Pública.

Pretende-se com esta iniciativa assegurar a solicitação de serviços públicos por parte dos cidadãos e a sua prestação por parte da Administração Pública, *online*, nomeadamente, a emissão de documentos eletrónicos assinados digitalmente, aos quais seja possível aceder através de código de barras unidimensional e bidimensional (*QR Code*) e a possibilidade de realização de videochamadas destinadas ao atendimento ao público.

O presente diploma procede, assim, à reengenharia dos processos, com reforma substancial no sistema de atendimento e de prestação de serviços através da integração e reengenharia das aplicações que devam ser utilizadas pelos serviços da Administração Pública; à simplificação e uniformização de procedimentos; introduz um novo modelo de gestão e de oferta de serviços e disponibilização de uma significativa gama de serviços *online*, designadamente em matéria de emissão de passaportes eletrónicos, emissão de certidões, transcrição de registos, validação de cartas de condução e de outros documentos essenciais para os cidadãos Cabo-verdianos, no país e na diáspora.

Com a implementação das medidas previstas no presente diploma, espera-se contribuir para a obtenção de ganhos de curto prazo na prestação do serviço aos utentes, na redução substancial do tempo de espera para o atendimento, bem como na melhoria significativa da qualidade no atendimento e no serviço final prestado, adequando o modo de funcionamento da Administração Pública a um paradigma de prestação digital de serviços públicos.

Os objetivos acima identificados implicam a construção de plataformas de maior aproximação aos utentes e maior interatividade no relacionamento entre o Estado e os cidadãos, contribuindo-se, assim, para a aproximação dos cidadãos ao Estado, objetivo que seguramente se alcançará através das diversas medidas consagradas no presente diploma.

Foram ouvidos o Sistema Nacional de Identificação e Autenticação Civil, a Agência Reguladora Multissectorial da Economia, o Núcleo Operacional para a Sociedade de Informação, a Unidade de Gestão da Casa do Cidadão, a Direção Nacional da Administração Pública e a Comissão Nacional de Proteção de Dados.

Assim,

Ao abrigo da autorização legislativa concedida pela Lei n.º 87/IX/2020, de 7 de maio de 2020; e

No uso da faculdade concedida pela alínea *b*) do n.º 2 do artigo 204º da Constituição, o Governo decreta o seguinte:

Artigo 1º

Objeto

O presente diploma aprova as medidas de simplificação, modernização administrativa em particular quanto aos procedimentos administrativos, necessários à interação pela via digital dos cidadãos com os serviços públicos, ao atendimento público e à prestação de serviços *online* por parte da Administração Pública e cria a Chave Móvel Digital de Cabo Verde como um mecanismo alternativo e voluntário de autenticação dos cidadãos nos portais e sítios da *Internet* da Administração Pública e como meio de assinatura eletrónica qualificada.

Artigo 2º

Âmbito de aplicação

1 - Os procedimentos administrativos, os mecanismos tecnológicos e a prestação de serviços *online* nos termos previstos no presente diploma aplicam-se:

a) A todos os serviços, organismos e instituições da Administração Pública direta e indireta do Estado; e

b) Aos serviços, organismos e instituições da Administração Autárquica, incluindo os seus serviços e fundos, personalizados ou não, e as empresas públicas municipais, sem prejuízo da competência dos respetivos órgãos próprios.

2 - O presente diploma aplica-se, ainda, aos serviços, organismos e instituições que estejam na dependência orgânica e funcional da Presidência da República, da Assembleia Nacional, das Instituições Judiciárias, das Forças Armadas e das Forças e Serviços de Segurança, bem como aos Serviços de Informação da República que, nos termos da respetiva legislação específica, não estejam expressamente excluídos do âmbito do presente diploma.

Artigo 3º

Acesso a serviços públicos *online*

1 - A todos os cidadãos nacionais ou estrangeiros, com idade igual ou superior a dezasseis anos, que não se encontrem interditados ou inabilitados é permitido o acesso à prestação de serviços *online* previstos no presente diploma.

2 - O acesso dos cidadãos nacionais ou estrangeiros à prestação de serviços *online* pode depender da prévia autenticação nos portais e sítios na *Internet,* de diferentes serviços da Administração Pública consoante a natureza dos serviços.

Artigo 4º

Sistemas de autenticação eletrónica

1 - A autenticação dos interessados na prestação digital de serviços públicos, faz-se através de um sistema simples ou multifator, de acordo com a natureza dos serviços a prestar ao utilizador.

2 - Caso seja exigida a autenticação através de certificado digital e o cidadão não disponha do documento de identificação eletrónica necessário para a autenticação deve solicitar, junto dos serviços competentes, a respetiva emissão.

3 - Os documentos de identificação eletrónica referidos no presente diploma são os previstos no âmbito da Lei que cria e regula o Sistema Nacional de Identificação e Autenticação Civil (SNIAC).

Artigo 5º

Sistema de autenticação simples

1 - A autenticação simples consiste na autenticação efetuada através de um número de identificação ou nome de utilizador e uma palavra-chave permanente.

2 - A autenticação simples é regulada em diploma próprio.

Artigo 6º

Sistema de autenticação multifator

1- A autenticação multifator consiste na autenticação efetuada através de um documento de identificação civil ou do número de passaporte para o cidadão nacional, e do número de identificação civil para o cidadão estrangeiro, associado a um único número de telemóvel e/ou a um endereço de correio eletrónico.

2 - A autenticação multifator faz-se através do cartão nacional de identificação ou passaporte para os cidadãos nacionais, ou do título de residência para cidadãos estrangeiros que residam no território nacional, através de um outro meio de identificação eletrónica validamente reconhecido em Cabo Verde ou através de outro meio de autenticação que venha a ser previsto por diploma próprio.

3 - O reconhecimento dos meios de identificação referidos no número anterior é regulado em diploma próprio.

Artigo 7º

Chave Móvel Digital de Cabo Verde

1 - A Chave Móvel Digital de Cabo Verde (CMDCV) é um sistema de autenticação multifator seguro dos utentes dos serviços públicos disponibilizados *online*, composto por uma palavra-chave permanente, escolhida e alterável pelo cidadão, bem como por um código numérico de utilização única e temporária por cada autenticação.

2 - Aquando da introdução da identificação do cidadão e da palavra-chave a ela associada nos mencionados portais e sítios na *Internet*, o sistema de autenticação eletrónico gera automaticamente um código numérico, que é enviado por *Short Message Service* (SMS) ou por correio eletrónico, ou aplicação dedicada instalada no seu telemóvel, ou outros meios eletrónicos que permitam o envio de mensagens privadas para o respetivo número de telemóvel ou endereço de correio eletrónico registados e validados pelo cidadão.

3 - A CMDCV pode ser utilizada como meio de autenticação segura em portais e sítios na *Internet*, mediante protocolo celebrado com a entidade gestora da CMDCV, com homologação do membro do Governo responsável pela área da Modernização Administrativa, com possibilidade de delegação.

4 - Para assegurar a gestão da CMDCV a entidade gestora utiliza, no âmbito das suas funções, uma plataforma eletrónica dedicada para o efeito.

Artigo 8º

Obtenção da Chave Móvel Digital de Cabo Verde

1 - Para obtenção da CMDCV o cidadão deve associar o número de identificação civil ou o número passaporte para o cidadão nacional, e do número de identificação civil para o cidadão estrangeiro, a um único número de telemóvel e/ou a um endereço de correio eletrónico.

2 - A associação prevista no número anterior destina-se exclusivamente à obtenção da CMDCV, como mecanismo voluntário e alternativo de autenticação perante serviços públicos prestados de forma digital para todo o utilizador, nacional ou estrangeiro, não podendo os dados assim obtidos ser utilizados para qualquer outro fim.

3 - O cidadão que pretenda obter a CMDCV pode:

a) Solicitar *online* a associação prevista no n.º 1 e escolher a sua palavra-chave permanente, mediante prévia confirmação de identidade por autenticação eletrónica através do certificado digital constante do cartão nacional de identificação, do título de residência de estrangeiros ou de outro meio de identificação eletrónica legalmente previsto e reconhecido; ou

b) Solicitar presencialmente a associação prevista no n.º 1 e escolher a sua palavra-chave permanente, junto dos serviços e entidades credenciadas para a receção dos pedidos de emissão, substituição e cancelamento do cartão nacional de identificação, do título de residência de estrangeiros ou de outro meio de identificação eletrónica legalmente previsto e reconhecido e aí, após confirmação de identidade por conferência com o documento de identificação civil de que for titular, obter a associação acima prevista e escolher a sua palavra-chave permanente.

4 - No caso da associação através do passaporte eletrónico o cidadão deve dirigir-se aos serviços e entidades credenciadas para a receção de pedidos de emissão, substituição e cancelamento desse documento, e aí, após confirmação de identidade por conferência com este documento de identificação civil obter a associação acima prevista e escolher a sua palavra chave permanente.

5 - Todo o cidadão nacional ou estrangeiro que não esteja presente em território nacional pode apresentar o seu pedido junto das missões diplomáticas credenciadas para a receção de pedidos de emissão, substituição e cancelamento desses documentos, e aí, após confirmação de identidade por conferência com o documento de identificação civil de que for titular, obter a associação acima prevista e escolher a sua palavra chave permanente.

Artigo 9º

Interconexão de dados

1 - Para o processo de atribuição da CMDCV, a entidade gestora relaciona, valida e regista nomeadamente os seguintes dados:

a) Nome próprio e apelidos;

b) Número de identificação civil e número de documento do cartão nacional de identificação, do título de residência de estrangeiros ou número de passaporte;

c) Data de nascimento;

d) Verificação da sua capacidade jurídica;

e)Validade do documento utilizado para obtenção da CMDCV; e

f) Existência de medidas cautelares sobre o passaporte.

2 - Na utilização da CMDCV podem ainda ser relacionados, validados e registados, nomeadamente os seguintes dados:

a) Número de identificação fiscal;

b) Número de previdência social;

c) Número de utente do sistema nacional de saúde;

d) Número de carta de condução; e

e) Nacionalidade.

3 - Os dados são relacionados e validados entre o sistema informático da entidade gestora e os sistemas informáticos dos respetivos responsáveis pelo tratamento, mediante assinatura de protocolo.

4 - A comunicação e validação dos dados são expressa e previamente autorizadas pelo respetivo titular, nos termos da Lei que aprova o Regime Geral de Proteção de Dados Pessoais.

5 - Os dados fornecidos pelo cidadão em conjunto com os dados obtidos nos termos dos números anteriores são apresentados ao cidadão para confirmação.

6 - O protocolo previsto no n.º 3 relativo à comunicação dos dados é submetido à consulta da Comissão Nacional de Proteção de Dados.

Artigo 10º

Comunicação de dados

1- Para efeitos do cancelamento previsto no artigo 14º são comunicados à entidade gestora o cancelamento do documento de registo por motivos associados à fraude de identidade, a morte ou a incapacidade superveniente do titular de CMDCV.

2 - Para efeitos da suspensão e reativação da CMDCV previstas no n.º 2 do artigo 15º são comunicados à entidade gestora além dos dados previstos no n.º 1, o cancelamento e a revogação do cartão nacional de identificação.

3 - A comunicação de dados é feita através do sistema informático.

Artigo 11º

Utilização da Chave Móvel Digital de Cabo Verde para autenticação

1 - O cidadão que tenha obtido a CMDCV pode autenticar-se nos portais e sítios na *Internet* dos serviços da Administração Pública mediante a introdução:

a) Da identificação ou número de telemóvel;

b) Da sua palavra-chave permanente; e

c) Do código numérico de utilização única e temporária automaticamente gerado, que receba do sistema de autenticação eletrónico por SMS, ou através do seu correio eletrónico, ou aplicação dedicada instalada no seu telemóvel, ou outros meios eletrónicos que permitam o envio de mensagens privadas.

2 - No caso de ter associado, para além de um número de telemóvel, um endereço de correio eletrónico, o cidadão pode escolher em cada autenticação por qual dos meios pretende receber o código numérico único e temporário.

3 - O processo de autenticação previsto nos números anteriores respeita todas as garantias em matéria de proteção de dados pessoais, designadamente as previstas na Lei que aprova o Regime Geral de Proteção de Dados Pessoais, não sendo permitido o rastreamento e o registo permanente das interações entre os cidadãos e a Administração Pública processadas através da CMDCV, sem prejuízo do disposto no artigo 17º.

4 - É da responsabilidade do cidadão garantir a utilização adequada da CMDCV para autenticação e tomar as medidas de segurança para o efeito.

Artigo 12º

Utilização da Chave Móvel Digital de Cabo Verde para assinatura eletrónica qualificada

1 - O cidadão que tenha obtido a CMDCV pode assinar documentos eletrónicos através da aposição de uma assinatura eletrónica qualificada, mediante introdução:

a) Da sua identificação ou número de telemóvel;

b) Da sua palavra-chave permanente; e

c) Do código numérico de utilização única e temporária automaticamente gerado, que receba do sistema de autenticação eletrónico por SMS, ou através do seu correio eletrónico, ou aplicação dedicada instalada no seu telemóvel, ou aplicação dedicada instalada no seu telemóvel, ou outros meios eletrónicos que permitam o envio de mensagens privadas.

2 - A utilização da chave móvel para assinatura eletrónica qualificada referida nos números anteriores respeita as disposições legais previstas no diploma que regula o uso da assinatura eletrónica e o reconhecimento da sua eficácia jurídica.

3 - É da responsabilidade do cidadão garantir a utilização adequada da CMDCV para assinatura eletrónica qualificada e tomar as medidas de segurança para o efeito.

Artigo 13º

Presunção de autoria

1 - Os atos praticados por um cidadão ou agente económico nos portais e sítios na *Internet* da Administração Pública presumem-se ser da sua autoria, dispensando-se a sua assinatura, sempre que sejam utilizados meios de autenticação segura para o efeito.

2 - Para efeitos do número anterior, consideram-se meios de autenticação segura:

a) O uso de nome de utilizador e palavra-chave; e

b) O uso de certificado digital, designadamente a constante do cartão nacional de identificação e do título de residência de estrangeiros;

c) A utilização da CMDCV.

3 - A presunção referida no n.º 1 é ilidível nos termos gerais de direito.

4 - A aposição de uma assinatura eletrónica qualificada a um documento eletrónico equivale, para todos os efeitos legais, à aposição de assinatura autógrafa dos documentos com forma escrita sobre suporte de papel e cria a presunção de que:

a) A pessoa que apôs a assinatura eletrónica qualificada é o titular desta ou é representante da pessoa coletiva titular da assinatura eletrónica qualificada, tendo poderes bastantes para o efeito;

b) A assinatura eletrónica qualificada foi aposta com a intenção de assinar o documento eletrónico em causa; e

c) O documento eletrónico assinado não sofreu qualquer alteração desde o momento da aposição da assinatura eletrónica qualificada.

Artigo 14º

Bloqueio automático, suspensão, cancelamento e revogação da Chave Móvel Digital de Cabo Verde

1 - Por motivos de segurança, a palavra-passe permanente pode ser bloqueada após a subsequente introdução de códigos alfanuméricos errados.

2 - O desbloqueio da CMDCV é efetuado nos termos previstos para a sua obtenção, por meio presencial ou por meio eletrónico, de acordo com o disposto no artigo 8º.

3 - Quando se verifique a utilização abusiva da CMDCV pode haver lugar à sua suspensão temporária por períodos de vinte e quatro horas.

4 - A CMDCV é cancelada quando exista conhecimento que o documento de identificação utilizado para sua obtenção tenha sido cancelado por motivos associados à fraude de identidade.

5 - A CMDCV e o certificado eletrónico de assinatura da CMDCV são cancelados:

a) Nos casos de morte do titular ou da sua incapacidade superveniente, através de informação enviada pela Direção-Geral dos Registos, Notariado e Identificação;

b) No caso de o passaporte perder a respetiva validade; ou

c) Em caso de inatividade superior a cinco anos.

6 - Pode ser solicitada, a todo o tempo, por meio eletrónico, a revogação da CMDCV ou da assinatura qualificada, implicando o respetivo cancelamento.

Artigo 15º

Validade e suspensão temporária

1- A validade da CMDCV coincide:

a) Com a validade do documento de identificação civil cabo-verdiano, ou do título de residência de estrangeiro, no caso de cidadão estrangeiro, acrescida de trinta dias; ou

b) Com a validade do passaporte no caso de cidadão nacional.

2 - A aplicação dos prazos referidos no número anterior não pode conduzir à atribuição de uma CMDCV com validade superior ao prazo de documento de identificação utilizado para a sua obtenção, acrescido de trinta dias.

3 - Findo o prazo de validade previsto na alínea *a*) do n.º 1, a CMDCV é suspensa até à renovação do mesmo documento.

Artigo 16º

Finalidades do tratamento de dados

1 - O tratamento de dados do cidadão visa as seguintes finalidades:

a) Execução de pedidos de registo de CMDCV;

b) Prestação de serviços online;

c) Prestação de serviço por teleconferência ou videoconferência; e

d) Execução de pedidos de cancelamento, suspensão e reativação da CMDCV.

2 - O tratamento dos dados necessários às operações referidas no número anterior só pode ser realizado por entidades ou serviços do Estado e da Administração Pública competentes e respetivos funcionários.

3 - O tratamento de ficheiros com dados pessoais a realizar por força do presente diploma tem por finalidade confirmar a identidade do cidadão no âmbito da prestação de serviços *online*.

Artigo 17º

Segurança de dados

1- No desenho e operação dos sistemas de informação nos quais se baseia a CMDCV a entidade responsável pela gestão e segurança da infraestrutura tecnológica que suporta a CMDCV garante o cumprimento de todas as exigências em matéria de proteção de dados pessoais, designadamente as previstas na Lei que aprova o Regime Geral de Proteção de Dados Pessoais, em especial, a adequada separação entre as diversas bases de dados utilizadas por aqueles sistemas de informação, sendo a informação das interações concretas realizadas entre os cidadãos e os serviços ou organismos da Administração Pública apenas guardada nos sistemas de informação desses serviços ou organismos.

2 - O registo das autenticações dos cidadãos através da CMDCV é eliminado no prazo de um ano após a respetiva ocorrência.

3 - O registo das assinaturas realizadas através da CMDCV é eliminado no prazo de um ano após a revogação ou cancelamento da respetiva CMDCV.

4 - Os cidadãos utilizadores da CMDCV podem monitorizar o seu histórico de autenticações e assinaturas.

5 - Os dados relativos ao registo de atribuição da CMDCV são apagados imediatamente após o cancelamento.

Artigo 18º

Direitos de informação, de acesso e de retificação

1 - O titular de CMDCV tem o direito de, a todo o tempo, verificar os dados pessoais inscritos no respetivo registo e conhecer o conteúdo da respetiva informação.

2 - O titular de CMDCV tem, desde o momento de apresentação do pedido de registo, o direito de exigir a correção de eventuais inexatidões, a supressão de dados indevidamente recolhidos ou indevidamente comunicados e a integração das omissões, nos termos previstos no Regime Geral de Proteção de Dados.

Artigo 19º

Regulamentação da CMDCV

Por portaria dos membros do Governo responsáveis pelas áreas da Modernização Administrativa e da Administração Pública, da Justiça e da Administração Interna, procede-se à regulamentação necessária ao desenvolvimento do mecanismo de autenticação previsto no presente diploma, à identificação dos serviços disponibilizados em função do meio de autenticação, ao modelo de sustentabilidade, devendo as regras de segurança da utilização deste serviço *online* ser adequadamente divulgadas junto dos utilizadores.

Artigo 20º

Documentos eletrónicos emitidos pelos serviços da Administração Pública

1 - Os serviços da Administração Pública podem emitir documentos eletrónicos com assinatura eletrónica qualificada aposta em conformidade com as normas do presente diploma, com o disposto no diploma, que regula o uso da assinatura eletrónica, o reconhecimento da sua eficácia jurídica, a atividade de certificação, bem como a contratação eletrónica e com as normas regulamentares relativas aos requisitos a que devem obedecer estes documentos, a emitir por portaria dos membros do Governo responsáveis pelas áreas da Modernização Administrativa e da Administração Pública.

2 - Para os fins do presente diploma, entende-se por documento eletrónico a declaração ou informação elaborados mediante processamento eletrónico de dados e contidos numa mensagem de dados, nos termos e para os efeitos do disposto na legislação supra referenciada que regula o uso da assinatura eletrónica e o reconhecimento da sua eficácia jurídica.

3 - Os documentos eletrónicos emitidos pelos serviços são assinados digitalmente com recurso a assinatura eletrónica qualificada destinada a comprovar o serviço ou entidade emitente ou a função ou cargo desempenhado pela pessoa signatária de cada documento emitido, consoante o caso.

4 - A aposição de uma assinatura eletrónica qualificada a um documento eletrónico emitido pelos serviços da Administração Pública equivale, para todos os efeitos legais, à aposição de assinatura autógrafa dos documentos com forma escrita sobre suporte de papel e cria a presunção prevista no n.º 4 do artigo 13º para os documentos assinados eletronicamente por pessoas singulares ou coletivas.

5 - Nos documentos eletrónicos emitidos deve constar um código de barras bidimensional (código QR) ou unidimensional e um código único de documento, que permitam o acesso digital ao documento, por qualquer interessado a quem sejam facultados os dados, nos termos a definir por portaria dos membros do Governo responsáveis pelas áreas da Modernização Administrativa e da Administração Pública.

6 - Os documentos eletrónicos emitidos nos termos do presente artigo são documentos autênticos, nos mesmos termos e para os mesmos efeitos que os documentos em papel.

7 - Os serviços públicos podem emitir certidões eletrónicas de forma automatizada com base na informação constante dos sistemas de Informação do Estado de Cabo Verde que servem de suporte à sua atividade, sendo-lhe aposto mecanismo de autenticação pelo sistema informático, o qual dispensa, para todos os efeitos legais, a aposição de assinatura eletrónica qualificada.

8 - As condições de armazenamento, em segurança, dos documentos assinados digitalmente são definidas por portaria dos membros do Governo responsáveis pelas áreas das Finanças, da Administração Pública, da Modernização Administrativa, dos Negócios Estrangeiros e da Justiça.

9 - Aos documentos eletrónicos previstos no presente artigo aplicam-se as regras relativas às mensagens de dados previstas no Decreto-lei que regula o uso da assinatura eletrónica, o reconhecimento da sua eficácia jurídica, nomeadamente no que diz respeito à sua eficácia legal e à sua forma e força probatória, devendo ser aceites por todas as entidades públicas e privadas às quais sejam apresentados.

10- Os modelos de documentos com código QR e assinados digitalmente, emitidos pelos serviços são aprovados por portaria do membro do Governo responsável pela área em causa e dos membros do Governo responsáveis pelas áreas da Modernização Administrativa e da Administração Pública.

Artigo 21º

Requerimentos apresentados *online*

1 - Os cidadãos podem requerer, nos portais e sítios na *Internet* dos serviços da Administração Pública, a emissão de documentos eletrónicos que se enquadrem no âmbito das respetivas competências.

2 - As condições de apresentação de requerimentos, são regulamentadas por portaria dos membros do Governo responsáveis pelas áreas da Modernização Administrativa e da Administração Pública.

3 - Os atos praticados por um cidadão ou agente económico nos portais e sítios da *Internet* dos serviços da Administração Pública presumem-se ser da sua autoria, dispensando-se a sua assinatura, sempre que sejam utilizados meios de autenticação segura para o efeito, nomeadamente os previstos no presente diploma ou outros meios de autenticação consagrados em diploma próprio.

4 - A presunção referida no número anterior é ilidível nos termos gerais de direito.

Artigo 22º

Serviços prestados *online*

A identificação dos serviços a prestar *online* pelos serviços públicos e das condições subjacentes à sua prestação é disponibilizada nos respetivos portais e é permanentemente atualizada.

Artigo 23º

Atendimento por teleconferência ou videoconferência

1 - Os serviços da Administração Pública realizam atendimento *online* ao público, através de sistema de teleconferência ou videoconferência.

2 - Depois de devidamente autenticado nos portais e sítios na *Internet*, nos termos definidos no presente diploma, os cidadãos podem solicitar o agendamento de atendimento através de teleconferência ou videoconferência, no respetivo site dos serviços competentes.

3 - O agendamento referido no número anterior depende da prévia disponibilidade dos serviços e do expresso e prévio consentimento do cidadão para que os serviços procedam à gravação da teleconferência ou da videoconferência.

4 - A gravação da teleconferência ou da videoconferência tem o valor de ata do respetivo atendimento pelos serviços, devendo ser conservada pelo período de seis meses.

Artigo 24º

Meios de pagamento

1- As taxas devidas pela prestação dos serviços previstos no presente diploma são fixadas por portaria dos membros do Governo responsáveis pelas áreas das Finanças, e do membro de Governo responsável pela área em causa.

2 - O pagamento da taxa devida nos termos do número anterior é efetuado através de sistema eletrónico de pagamentos, nos termos definidos na portaria referida no número anterior.

Artigo 25º

Regulamentação

Todos os diplomas regulamentares previstos no presente diploma são aprovados no prazo de noventa dias a contar da sua publicação.

Artigo 26º

Aplicação subsidiária

Em tudo o que não se encontrar expressamente regulado no presente diploma aplicam-se as normas relativas às mensagens de dados, aos documentos eletrónicos e às assinaturas eletrónicas, previstas no diploma que regula o uso da assinatura eletrónica, o reconhecimento da sua eficácia jurídica, a atividade de certificação, bem como a contratação eletrónica a assinatura eletrónica e o reconhecimento da sua eficácia jurídica.

Artigo 27º

Disposições finais e transitórias

1 - Até à criação da entidade gestora da CMDCV, a gestão da mesma é da responsabilidade do Conselho de Gestão do SNIAC, nos termos do diploma que cria e regula o Sistema Nacional de Identificação e Autenticação Civil.

2 - Nas missões diplomáticas, os serviços e procedimentos adotados no presente diploma são prestados através do respetivo Portal Consular.

3 - De forma a concretizar o objetivo de generalizar as soluções administrativas, técnicas e /ou tecnológicas que resultam do presente diploma, fica a Embaixada de Cabo Verde em Portugal incumbida de proceder à necessária articulação com as demais missões diplomáticas e consulares de Cabo Verde, no exterior, transmitindo-lhes os mecanismos previstos e auxiliando o seu processo de implementação.

4 - Os serviços consulares e diplomáticos de Cabo Verde e a Direção Geral dos Assuntos Consulares e Comunidades do Ministério de Negócios Estrangeiros e Comunidades que adotem os mecanismos eletrónicos previstos no presente diploma devem divulgá-los, de imediato, junto dos cidadãos, nomeadamente emitindo guias de utilização que facilitem e promovam o acesso a estes mecanismos.

5 - A Embaixada de Cabo Verde em Portugal deve criar as condições necessárias de aceitação e armazenamento, em segurança, dos respetivos documentos assinados digitalmente, nos termos a definir por Portaria do membro do Governo responsável pela área dos Negócios Estrangeiros.

Artigo 28º

Entrada em Vigor

O presente diploma entra em vigor no dia seguinte ao da sua publicação.

Aprovado em Conselho de Ministros, aos 4 de junho de 2020. — Os Ministros, *José Ulisses de Pina Correia e Silva, Olavo Avelino Garcia Correia, Luís Filipe Lopes Tavares, Janine Tatiana Santos Lélis* e *Paulo Augusto Costa Rocha*.

Promulgado em 15 de julho de 2020

Publique-se.

O Presidente da República, JORGE CARLOS DE ALMEIDA FONSECA.

I SÉRIE

BOLETIM OFICIAL

Registo legal, nº 2/2001, de 21 de Dezembro de 2001

Endereço Electronico: *www.incv.cv*

IMPRENSA NACIONAL DE CABO VERDE

Av. da Macaronésia,cidade da Praia - Achada Grande Frente, República Cabo Verde
C.P. 113 • Tel. (238) 612145, 4150 • Fax 61 42 09
Email: kioske.incv@incv.cv / incv@incv.cv

I.N.C.V., S.A. informa que a transmissão de actos sujeitos a publicação na I e II Série do *Boletim Oficial* devem obedecer as normas constantes no artigo 28º e 29º do Decreto-Lei nº 8/2011, de 31 de Janeiro.