Decreto-Lei nº 19/2010

de 14 de Junho

A estratégia para a adopção do sistema de Governação electrónica em Cabo Verde está centrada em três componentes fundamentais que derivam das relações: Administração Pública-cidadão; Administração Pública -operadores económicos; Administração Pública – servidores públicos.

As duas primeiras componentes estão viradas para o público – pessoas individuais ou colectivas. Com efeito, a nova postura dos agentes públicos, seja na formulação de políticas seja na prestação de serviços, está cada vez mais focalizada nas necessidades dos cidadãos utentes. Para tal foi encetado um processo de reformulação da maneira de lidar com o «cliente» e com os «negócios», numa reengenharia dos processos e do desenvolvimento de uma cultura de efectiva colaboração horizontal entre os departamentos.

A terceira componente visa criar as condições organizacionais, humanas e tecnológicas para a qualificação da máquina pública de forma a, por um lado, responder aos novos paradigmas da prestação pública e, por outro, conferir eficiência e eficácia na Administração Pública.

Nessa perspectiva, torna-se necessário estabelecer políticas, padrões e normas que ofereçam, para cada um dos agentes envolvidos nas relações acima descritas, o conforto necessário e suficiente para evolução e consolidação do modelo de governação em implantação.

A etapa actual de construção da Sociedade da Informação no País exige mais formalidades e, em consequência, a formatação de instrumentos de regulação que sejam atentos a temas como direito de propriedade, autoria intelectual, preservação de direitos individuais, segurança da informação, entre outros.

À medida que os Sistemas de Informação assumem um papel de maior preponderância, tanto ao nível dos processos como dos objectivos gizados pelo Governo, a pertinência da sua segurança aumenta consideravelmente, despertando o interesse de todos os intervenientes nos processos decisórios, estratégicos e técnicos.

A informação é muito mais do que um conjunto de dados. Os dados em si têm pouco significado e só a sua transformação em informação é que os torna num recurso de valor para a vida de qualquer instituição ou organização.

A informação é, pois, um bem que tem valor primordial para as organizações e como tal deve ser protegida e cuidada através de políticas e regras da mesma forma e intensidade que os recursos financeiros, materiais e outros.

Como activo crítico que é, deve estar sujeito a regras e procedimentos e ter uma estrutura de protecção.

Assim, a protecção da informação é da responsabilidade de cada um dos agentes utilizadores competentes das instituições integradas na Rede Tecnológica Privativa do Estado, independentemente do seu nível hierárquico.

A segurança dos sistemas de informação não é um simples produto ou tecnologia que se pode adquirir e aplicar. Deverá ser encarada de forma integrada com o "negócio" do Estado, como um processo em permanente evolução que requer uma enorme capacidade para provocar e gerir mudanças, tanto nos hábitos e comportamentos como nas infra-estruturas organizativas e tecnológicas.

Urge assim estimular todos os actores envolvidos a olhar para além da sua área particular de actividade e de conhecimento e a trabalhar a segurança de forma uniforme e transversal a todas as áreas, fornecendo estratégias para a criação, implementação e manutenção de um plano de segurança assente em três eixos importantes: gestão, técnica e tecnologia.

Por outro lado, a Segurança de Informação está relacionada com a protecção existente ou necessária sobre dados que possuem valor para o Estado e para o cidadão. Possui aspectos básicos como confidencialidade, integridade e disponibilidade da informação que ajudam a entender as necessidades de sua protecção e que não se aplica ou está restrita a sistemas computacionais, nem a informações electrónicas ou qualquer outra forma mecânica de armazenamento.

Ela aplica-se a todos os aspectos de protecção e armazenamento de informações e dados, em qualquer forma. O nível de segurança de um sistema operacional de computador pode ser tipificado pela configuração de seus componentes.

A Segurança da Informação refere-se, assim, à protecção existente sobre as informações tratadas na Rede do Estado, isto é, aplica-se tanto a informações corporativas quanto a informações pessoais.

Outrossim, a segurança de uma determinada informação pode ser afectada por factores comportamentais e de uso de quem a utiliza, pelo ambiente ou infra-estrutura que a cerca ou por pessoas mal intencionadas que têm o objectivo de furtar, destruir ou modificar a informação.

A Confidencialidade, Integridade e Disponibilidade representam as principais propriedades que, actualmente, orientam a análise, o planeamento e a implementação da segurança para as informações que se deseja proteger.

A realização de transacções comerciais em todo o mundo, através de redes electrónicas, públicas ou privadas, implicam o envolvimento de outras propriedades como a legitimidade e autenticidade.

É também de ter presente ainda que as políticas de segurança da informação assentam basicamente em duas filosofias complementares: a proibitiva – tudo o que não é expressamente permitido é proibido – e a permissiva – tudo o que não é expressamente proibido é permitido.

Por outro lado, os mecanismos de segurança tratados no âmbito das políticas devem apoiar-se em dois níveis de controlo – o físico e o lógico.

Deste modo, as políticas de segurança devem ter implementação realista, e definir claramente as áreas de

responsabilidade de todos e cada um dos actores envolvidos na gestão dos sistemas e redes. Devem fornecer o enquadramento para a implementação de mecanismos de segurança, definir procedimentos de segurança adequados, processos de auditoria à segurança e estabelecer uma base para os procedimentos de diversa ordem que encerram os sistemas de informação.

Em resumo, neste diploma sobre "Políticas de Segurança da Informação" pretende-se consubstanciar um conjunto de orientações, normas, procedimentos, e outras acções que visam proteger o recurso informação e que devem ser seguidas pelos utilizadores dos recursos da Rede Tecnológica Privativa do Estado, com vista a garantir os níveis de segurança desejados e necessários para a realização dos objectivos preconizados.

Assim,

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

CAPÍTULO I

Disposições gerais

Secção I

Objecto, âmbito e definições

Artigo 1º

Objecto

O presente diploma estabelece as políticas, normas e regras de segurança da informação para a gestão da Rede Tecnológica Privativa do Estado (RTPE).

Artigo 2º

Âmbito de aplicação

1. O presente diploma aplica-se a todos os serviços da Administração Central e Local do Estado, e bem assim, aos Institutos Públicos que revistam a natureza de serviços personalizados do Estado.

2. O diploma aplica-se ainda aos demais órgãos de soberania e outros serviços que integrem a RTPE.

Artigo 3º

Exclusão do âmbito de aplicação

O presente diploma não é aplicável à segurança de dados e conteúdos qualificados da competência exclusiva das Forças Armadas e das forças de Segurança que são objecto de tratamento em diploma próprio.

Artigo 4º

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 relativos aos serviços prestados pela instituição responsável pela gestão da RTPE, sendo que as informações deste ambiente têm por objectivo possibilitar a construção dos programas, realização de testes e simulação de situações de erro que possam ser identificadas e visam garantir qualidade funcional adequada dos programas aplicativos utilizados;

b) «*Ambiente de produção de sistemas*», o ambiente computacional disponibilizado pela instituição responsável pela gestão da RTPE para a gestão dos conteúdos específicos;

c) «*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;

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

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

f) «*Desastre lógico*», a indisponibilidade ou alteração indevida de recursos de informação causada por acção no ambiente computacional, através de programas ou acções que alteram indevidamente as informações;

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

h) «*Gestor de Acesso*», a pessoa designada pelo dirigente competente do departamento governamental ou organismo público integrado na RTPE como responsável pela gestão do acesso à RTPE e aos serviços disponíveis, bem como pelo acompanhamento da validade das autorizações dos acessos;

i) «*Identificação do utilizador*», a sequência de caracteres que permite identificar o utilizador quando este estabelece a sua conexão com a RTPE;

j) «*Internet*», o ambiente virtual exterior à RTPE, onde diferentes computadores de várias partes do mundo comunicam através de protocolos de entendimento comum, permitindo a troca de informações;

k) «*Programa-produto*», o programa desenvolvido e disponibilizado no mercado para uso geral;

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

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

n) «*Rede Tecnológica Privativa do Estado (RTPE)*», o conjunto integrado dos recursos físicos e lógicos, propriedade do Estado de Cabo Verde, relativos às tecnologias da informação e comunicação, nomeadamente hardware, software, conteúdos de qualquer natureza, *data centers*, *Service Centers*, plataformas e arquitecturas tecnológicas, redes de comunicação, serviços de terceiros, metodologias, normas e outros recursos de natureza semelhante legalmente adquiridos, desenvolvidos ou mantidos pelo Estado;

o) «*Regras de protecção da informação*», os procedimentos de segurança da informação definidos e instituídos dos quais o utilizador deve ter conhecimento explícito;

p) «*Requisitos de segurança*», as condições para o uso da informação de forma segura descritas nos regulamentos de segurança da informação e em documentos técnicos relativos à protecção da informação;

q) «*Utilizador comum*», a pessoa singular ou colectiva que utiliza ou acede aos sistemas de informação, disponibilizados ao público pelas instituições públicas através da RTPE;

r) «*Utilizador Profissional*», o utilizador autenticado que, no desempenho das suas funções e atribuições profissionais, tem autorização de acesso aos sistemas de informação disponibilizados pelas instituições públicas através da RTPE;

s) «*Utilizador Técnico*», os profissionais devidamente autorizados e credenciados pela instituição responsável pela gestão da RTPE que, no desempenho das suas funções e atribuições profissionais, têm acesso à RTPE para efeito, nomeadamente, de gestão do parque tecnológico, desenvolvimento, implementação e manutenção de sistemas de informação.

Secção II

Atributos e princípios de Segurança da Informação

Artigo 5º

Integridade

Um documento electrónico ou sistema electrónico deve ser configurado de modo a não sofrer alterações durante um processo de comunicação electrónica ou durante o acesso a esse mesmo objecto ou documento, e manter as características originais estabelecidas pelo proprietário da informação.

Artigo 6º

Autenticidade

A identidade de todos os intervenientes num processo de comunicação electrónica ou de acesso a um sistema electrónico deve ser verdadeira, autêntica e previamente reconhecida.

Artigo 7º

Confidencialidade

1. O acesso à informação, e bem assim às transacções ou comunicações electrónicas efectuadas na RTPE, é confidencial, sendo limitado ao utilizador autorizado pelo proprietário da informação e que dela necessite para o desempenho das suas actividades profissionais.

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 8º

Privacidade

A informação ou conteúdos de um dado documento ou as características de um processo ou transacção electrónica devem ser preservados como "privados" para quem tenha autorização para o seu acesso.

Artigo 9º

Disponibilidade

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

Artigo 10º

Legalidade

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

Artigo 11º

Auditabilidade

Todas as operações efectuadas ou informações veiculadas na RTPE são passíveis de auditoria.

CAPÍTULO II

Rede Tecnológica Privativa do Estado – RTPE

Secção I

Recursos da RTPE

Artigo 12º

Utilizadores

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

Artigo 13º

Ambiente físico

1. O ambiente físico é o recurso que abriga os equipamentos físicos que fazem parte da RTPE e sejam necessários para o armazenamento, processamento e transmissão de dados e da informação.

2. O ambiente físico deve ser protegido dos riscos de produção de eventuais danos ou destruições.

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

Artigo 14º

Dados e Informação

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

Artigo 15º

Infra-estrutura

A infra-estrutura da RTPE é formada pela rede de telecomunicações, infra-estruturas de base e tecnológicas que possibilitam que os demais recursos funcionem adequadamente.

Artigo 16º

Tecnologia

A tecnologia da RTPE compreende os computadores de qualquer porte, periféricos e quaisquer outros equipamentos tecnológicos com suporte tendencialmente em meios electrónicos que possibilitam a realização do negócio, através da utilização da informação.

Artigo 17º

Processos

Os processos operacionais aplicáveis são também considerados recursos de informação e da RTPE.

Secção II

Gestão da RTPE

Artigo 18º

Instituições intervenientes

1. A gestão da RTPE é confiada, pelo Governo, a uma instituição pública ou privada, que tenha todas as competências técnicas e tecnológicas necessárias ao seu desenvolvimento e manutenação em linha com as permanentes conquistas e aquisições no domínio das tecnologias de informação e comunicação e ainda para garantir os níveis de segurança adequados e definidos.

2. A gestão global da segurança e protecção da informação armazenada na RTPE é atribuida a um Gabinete de Segurança da Informação (GSI) a funcionar junto do Gabinete do Primeiro-ministro.

Subsecção I

Instituição responsável pela gestão da RTPE

Artigo 19º

Missão

A instituição responsável pela gestão da RTPE é responsável pela implantação, manutenção, operacionalização e administração da RTPE.

Artigo 20º

Competência

Compete à instituição responsável pela gestão da RTPE, designadamente:

a) Promover a aplicação de medidas de política na área da sociedade de informação e da governação electrónica e coordenar todas as acções que visem a implementação da governação electrónica;

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

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

d) Auxiliar na definição e execução de normas que visam a implementação das políticas de segurança da informação;

e) Auxiliar o Governo na definição de normas e políticas de segurança da informação;

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

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

h) Desenvolver e implementar, projectos e acções que permitam à RTPE alcançar o nível de segurança adequado ao tipo de informação e às características dos serviços prestados;

i) Operacionalizar a segurança da informação na RTPE;

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

k) Monitorar os acessos através de registo e actividades de segurança da informação;

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

Subsecção II

Gabinete de Segurança da Informação

Artigo 21º

Missão

1. O Gabinete de Segurança da Informação (GSI) é o órgão responsável pela gestão do processo de segurança e protecção da informação armazenada, processada e transmitida na RTPE.

2. O GSI deve garantir o cumprimento por todos os utilizadores da RTPE das políticas e normas de segurança da informação estabelecidas por lei ou regulamentos.

Artigo 22º

Natureza e funcionamento

1. O GSI é um serviço central da administração directa do Estado, dotado de autonomia administrativa, que funciona na directa dependência do Primeiro-Ministro ou do membro do Governo em quem aquele delegar.

2. A estrutura organizacional, o funcionamento e o quadro do pessoal do GSI constam de regulamento interno próprio, aprovado por portaria do membro do Governo responsável pela área da sociedade de informação.

Artigo 23º

Competências

1. Compete nomeadamente ao GSI:

a) Propor políticas de Segurança da Informação;

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 vulnerabilidade identificados sejam avaliados mais detalhadamente e que soluções adequadas sejam implementadas;

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

f) Desenvolver acções 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 e empresas nacionais e internacionais para a troca de experiências relativas ao processo de segurança da informação, garantindo sua evolução;

i) Assistir o Governo no tratamento das questões que não estejam definidas nas políticas e normas de segurança da informação.

2. No exercício das suas competências, o GSI deve interagir com todos os departamentos governamentais e demais instituições do Estado com vista a garantir o nível de capacitação adequada para cada utilizador dos sistemas de informação.

Secção III

Acesso à RTPE

Artigo 24º

Recursos da RTPE

A Rede Tecnológica Privativa do Estado compreende um conjuto de recursos físicos e lógicos que têm por objectivo garantir a dispobilização de serviços públicos electrónicos aos cidadãos e empresas e a realização de actividades funcionais dos agentes públicos.

Artigo 25º

Utilizadores da RTPE

1. Os utilizadores da RTPE podem ser instituições públicas, agentes públicos, cidadãos e empresas que, devidamente autorizados, podem aceder aos recursos da rede e aos sistemas de informação, seja no exercício de sua actividade profissional, seja para exercer o seu direito de acesso à informação e a serviços públicos electrónicos.

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

3. Os utilizadores da RTPE são agrupados nas seguintes três categorias, cada um deles definido no artigo 4º:

a) Utilizador comum;

b) Utilizador profissional, que pode revestir-se com as características de:

i. Funcionário, agente e trabalhador da Administração directa e indirecta do Estado e das Autarquias Locais;

ii. Prestador de serviço;

iii. Auditor interno ou externo e;

iv. Consultor.

c) Utilizador técnico.

Artigo 26º

Gestor de Acesso

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

2. O Gestor de acesso é designado pelo responsável máximo do serviço da Administração Central, Local ou Instituto Público e tem responsabilidade limitada aos utilizadores da respectiva instituição.

3. Compete ao Gestor de acesso:

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

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

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

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;

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 Sistemas da RTPE.

Artigo 27º

Acesso do utilizador comum

1. O acesso do utilizador comum, cidadão ou empresa, a serviços públicos de informação ou outros não classificados, não carece de qualquer tipo de autorização.

2. O acesso a serviços públicos qualificados e personalizados, através da RTPE, só pode ser feito mediante autenticação do utilizador.

3. Para efeitos de autenticação, o utilizador comum, cidadão ou empresa, deve cadastar-se junto dos serviços competentes da Administração Pública.

4. O Gestor de acesso do utilizador comum é a Casa do Cidadão ou outra instituição pública devidamente qualificada e credenciada para tal, cabendo-lhe prestar, entre outros, o serviço de cadastramento.

Artigo 28º

Acesso do Utilizador Profissional

1. O acesso de qualquer agente público ou funcionário do Estado aos recursos da RTPE é autorizado e operacionalizado pelo gestor de acesso da respectiva instituição, conforme previsto no artigo 26º.

2. A atribuição do acesso é feita mediante a leitura e assinatura pelo agente público ou funcionário do Estado de um documento designado "Termos de Acesso", que contém as condições e as responsabilidades inerentes ao uso da RTPE.

3. A operacionalização do acesso é feita através do cadastramento do interessado nos sistemas de gestão de acesso da RTPE.

4. Ao utilizador profissional é retirado o acesso quando perde as prerrogativas de acesso à RTPE, nomeadamente quando cessa as funções que o tivessem determinado.

Artigo 29º

Acesso do Utilizador Técnico

1. O utilizador técnico tem acesso à RTPE mediante autorização expressa da instituição responsável pela gestão da RTPE, para o exercício restrito das suas funções e atribuições.

2. A atribuição do acesso é feita pelo Administrador de Sistemas da instituição responsável pela gestão da RTPE, em razão das suas atribuições, funções e responsabilidades técnicas nessa instituição.

3. A operacionalização do acesso é feita através do cadastramento do interessado nos sistemas de gestão de acesso da RTPE.

4. Ao utilizador técnico é retirado o acesso quando perde as prerrogativas de acesso à RTPE, nomeadamente quando cessa as funções que o tivessem determinado.

Artigo 30º

Registo do acesso

1. Todos os acessos realizados devem ser registados na RTPE e guardados pelo prazo estabelecido em regulamentos e normas.

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

Artigo 31º

Responsabilidade

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

2. São responsabilidades do utilizador:

a) Solicitar acesso apenas para o desempenho das suas actividades profissionais através da RTPE;

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

Artigo 32º

Uso do Correio Electrónico

1. O Correio Electrónico é um recurso atribuído ao utilizador conjuntamente com o acesso à RTPE, pelo Gestor de Acesso.

2. Os endereços de correio electrónico disponibilizados aos utilizadores, bem como as mensagens e outros conteúdos associados a cada endereço de correio electrónico, são propriedade do Estado de Cabo Verde e são cedidos aos utilizadores para o desempenho das suas actividades profissionais.

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

4. Os limites ao uso do Correio Electrónico, em termos de volume e capacidade, são fixados pela instituição responsável pela gestão da RTPE em normas e regulamentos, em função das capacidades tecnológicas disponíveis na RTPE.

Artigo 33º

Acesso e uso da Internet

1. O acesso à Internet é um recurso atribuído automaticamente ao utilizador conjuntamente com o acesso à RTPE, pelo Gestor de Acesso.

2. Para a navegação na Internet devem ser utilizados apenas os softwares e versões homologados pela instituição responsável pela gestão da RTPE.

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

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, a instituição responsável pela gestão da RTPE deve ser accionada para promover o procedimento a ser seguido.

6. No uso da Internet, o utilizador não deve aceder a endereços ou executar acções 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 Internet utilizando recursos da RTPE.

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

9. É vedada e considerada abusiva a utilização dos recursos da RTPE para:

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

i) Com conteúdo pornográfico, pedofilia, violência;

ii) Que promovam actividades ilegais;

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 pela instituição responsável pela gestão da RTPE, salvo excepções fixadas pelo próprio Gabinete de Segurança da Informação;

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

d) Distribuição, pela Internet, de informações confidenciais.

Artigo 34º

Recurso Computador e Periféricos

1. O computador, seja de mesa ou portátil, acompanhado de seus periféricos, disponibilizado ao utilizador é propriedade do Estado e, como tal, sujeito ao registo patrimonial.

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

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

4. Ao cessar as suas funções, definitivamente ou por transferência para outro serviço do Estado, o recurso 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 respectivo.

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 RTPE sem a autorização prévia e expressa da instituição responsável pela gestão da RTPE.

8. A alteração dos componentes físicos e a configuração lógica do computador é uma atribuição exclusiva da instituição responsável pela gestão da RTPE.

9. O utilizador é responsável por perdas e extravios dos recursos móveis sob sua responsabilidade.

Artigo 35º

Conexão com ambientes externos

1. A comunicação do ambiente da RTPE com outras redes ou ambientes de tecnologia externos deve ser realizada de forma segura, controlada e de modo a que sejam mínimos os riscos de invasão ao ambiente da RTPE.

2. São proibidas quaisquer atitudes e comportamentos dos utilizadores que visem a invasão danosa do ambiente computacional de terceiros, sob pena de procedimento disciplinar nos termos da lei.

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

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

5. Todos os sítios da Internet mantidos pela instituição responsável pela gestão da RTPE devem ser periodicamente testados para garantir a actualização das informações tipo endereço e também para garantir que o serviço está em actividade normal.

Artigo 36º

Proibições

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

2. É vedada a transferência de material ofensivo ou hostil nos endereços da Internet através de recursos da RTPE.

CAPÍTULO III

Informação e sistemas de informação

Secção I

Princípios e atributos

Artigo 37º

Valor da informação

A informação disponível na RTPE é um recurso de valor que permite às diversas instituições do Estado realizar adequadamente os serviços no âmbito de suas atribuições, bem como o atendimento das necessidades dos cidadãos.

Artigo 38º

Sistemas de informação

1. Sistema de Informação (SI) é um conjunto de procedimentos organizados que, quando executados, provêem informações de suporte à organização, mediante processamento de dados de forma informatizada e disponibiliza informação aos utilizadores.

2. O modelo de definição de SI adoptado classifica os SI em três categorias:

a) SI Transaccional;

b) SI para a Gestão;

c) SI de apoio à Decisão.

Artigo 39º

Titularidade do direito de propriedade da Informação

O Estado de Cabo Verde é o proprietário das informações armazenadas, processadas e transmitidas na RTPE, sem prejuízo do estabelecido no artigo 55º relativamente ao tratamento dos dados pessoais e níveis de classificação da informação.

Secção II

Ambientes de Sistemas de Informação

Artigo 40º

Ambiente de desenvolvimento e ambiente de teste de sistemas

1. Os ambientes de desenvolvimento e teste de sistemas são utilizados exclusivamente para 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 respectivo 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 pela chefia responsável pelo ambiente de produção de sistemas, de forma a garantir a integridade e disponibilidade da RTPE.

Artigo 41º

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 RTPE sem a prévia certificação, qualificação e autorização da instituição responsável pela gestão da RTPE e em particular do seu departamento de Segurança.

Secção III

Classificação da Informação

Artigo 42º

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 disponibilizada na RTPE.

Artigo 43º

Processo de classificação da informação

1. Toda informação deve ser classificada pelo respectivo 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, áreas organizacionais ou entidades que devem ter acesso à informação;

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

3. A classificação da informação deve estar escrita em local visível no suporte em que esteja incluída.

Artigo 44º

Níveis de classificação da informação

Podem ser fixados 3 (três) níveis de confidencialidade para a classificação da informação:

a) Informação pública, que pode ser acedida sem restrições por qualquer Utilizador da RTPE:

i. Dados digitais, que podem ser acedidos sem restrição;

ii. Cópia, pode ser feita sem restrição;

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

b) Informação interna, caracterizada, em função da sua abrangência, podendo ser restrita a uma instituição ou grupo de instituições ou ainda, a toda a RTPE, designadamente em relação a:

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

ii. Cópia, que pode ser feita sem restrição;

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

c) Informação Confidencial, que tem forte restrição de acesso, nomeadamente em relação a:

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

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

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

Secção IV

Protecção e Segurança da Informação

Artigo 45º

Protecção da informação

1. Toda informação deve ser protegida, cuidada e gerida visando 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 46º

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 directos.

Artigo 47º

Responsabilidade dos utilizadores

1. Deve existir um processo constante de qualificação e treinamento dos utilizadores em segurança da informação, com o objectivo de capacitá-los a proteger adequadamente a informação na Rede Privada do Estado.

2. A instituição responsável para a Gestão da RTPE deve interagir com todas as Instituições conectadas com vista a garantir o nível de capacitação adequado para cada utilizador dos sistemas de informação.

Artigo 48º

Confidencialidade da informação

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

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

Secção V

Gestão de Sistemas Informação

Artigo 49º

Gestor de Informação

Compete a cada serviço da administração central, local ou instituto público integrado na RTPE, nomear o respectivo Gestor de Informação.

Artigo 50º

Competências do Gestor de Informação

1. Cabe ao Gestor da Informação, em articulação com o departamento de segurança da Instituição Responsável para a Gestão da RTPE, definir o conjunto das funcionalidades dos Sistemas de Informação instalados, atribuidas a cada serviço, utilizador ou grupo de utilizadores.

2. Compete ao Gestor da Informação, em estreita articulação com o departamento de segurança da instituição responsável pela gestão da RTPE, 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 protecção e disponibilidade desejado para os sistemas ou serviços sob a sua responsabilidade;

f) Atribuir ao Utilizador credenciado da sua instituição, o direito a operar a respectiva funcionalidade no sistema de informação;

g) Retirar o acesso do utilizador ao SI quando este 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 efectuados 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 Informação

Artigo 51º

Acesso à informação

1. O acesso à informação armazenada e processada na RTPE 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 atribuições e responsabilidades cometidas pela Instituição respectiva.

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

Artigo 52º

Registo do acesso

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

Artigo 53º

Responsabilidade

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

2. São responsabilidades do utilizador profissional:

a) Solicitar acesso apenas para as informações de que necessita para as suas actividades profissionais nos serviços realizados através da RTPE;

b) Eximir-se de aceder à informação, quando suas actividades profissionais realizadas através da RTPE não mais exigirem esse acesso.

CAPÍTULO IV

Dados pessoais e privacidade

Artigo 54º

Declaração de Compromisso

As organizações envolvidas no âmbito do presente diploma devem declarar o seu comprometimento em relação aos requisitos e procedimentos para a protecção dos direitos de privacidade dos utilizadores e da informação individual identificável armazenada, processada e transmitida na RTPE.

Artigo 55º

Princípios básicos

1. A instituição responsável pela gestão da RTPE e as autoridades públicas envolvidas na gestão e tratamento de dados pessoais observam a privacidade individual dos utilizadores da RTPE e tem 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) A instituição responsável pela gestão da RTPE não pode acumular ou manter intencionalmente dados pessoais ou outros que não aqueles relevantes na condução dos seus serviços e adopta as medidas necessárias para garantir a integridade dos dados pessoais sob sua custódia;

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

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

Artigo 56º

Segurança

Os dados pessoais sob a custódia da instituição responsável pela gestão da RTPE devem estar protegidos por políticas e procedimentos, visando:

a) Evitar o uso ou o acesso não autorizado aos sistemas de informações;

b) Manter a integridade, disponibilidade e privacidade das informações confidenciais;

c) Evitar perda ou destruição.

Artigo 57º

Uso restrito e sob autorização

Em casos excepcionais, os dados pessoais podem ser utilizados para fins diversos daqueles a que se destinam, desde que haja consentimento do seu titular.

Artigo 58º

Direito de Acesso

O titular dos dados pessoais pode solicitar, por escrito, a sua consulta e actualização junto do serviço que tenha responsabilidade institucional de gerir os respectivos dados pessoais, conforme previsto na lei geral.

Artigo 59º

Direito de oposição

Qualquer indivíduo pode opor que os seus dados pessoais sejam objecto de tratamento e reclamar junto das instâncias competentes pelo seu uso indevido, nos termos previstos na lei geral.

CAPÍTULO V

Cópias de segurança

Artigo 60º

Continuidade do uso da informação

1. Toda informação crítica para o funcionamento dos sistemas de informação deve possuir, pelo menos, uma cópia de segurança actualizada e guardada em local remoto, com o nível de protecção equivalente ao nível de protecção da informação original.

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

3. Os recursos tecnológicos, de infra-estrutura 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 sistema de informação, deve haver definição do nível de disponibilidade em situações de desastre e contingência e, para tal, a solução deve considerar os adequados recursos de tecnologia, humanos e de infra-estrutura existentes.

Artigo 61º

Cópias de segurança

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

2. As cópias de segurança devem conter:

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

b) Informações legais, designadamente as que devem ser mantidas e guardadas por expressa determinação legal;

c) Informações históricas, designadamente as que, mesmo isentas de obrigatoriedade legal, o serviço público tem interesse em manter e aceder;

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

3. O prazo para a realização de cópia de segurança deve ser definido nos regulamentos internos, 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.

CAPÍTULO VI

Continuidade operacional

Artigo 62º

Plano de continuidade operacional

1. Para a continuidade operacional do acesso e utilização da informação na RTPE, os recursos de informação alternativos e os processos utilizados em situação de contingência devem ter o mesmo nível de segurança, protecção e sigilo dos elementos utilizados.

2. O desenvolvimento de planos de continuidade operacional para garantir os níveis de disponibilidade da informação e/ou serviço é coordenado pelo departamento de Segurança da instituição responsável pela gestão da RTPE.

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 63º

Nível de disponibilidade

1. Nível de disponibilidade é o indicador para a solução de continuidade operacional referente aos serviços prestados através da RTPE.

2. Os níveis de disponibilidade dos recursos de informação utilizados pelos serviços prestados através da RTPE são definidos através de regulamento.

3. O GSI, com a colaboração dos Gestores da Informação, 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

Disposições sancionatórias

Artigo 64º

Sanções

Os utilizadores da RTPE que por meio das suas condutas objectivem furtar, destruir ou modificar a informação ou violar qualquer dos preceitos mencionados no presente decreto-lei, respondem civil e criminalmente em função da gravidade e consequência dos seus actos, nos termos das leis civil e penal vigentes, sem prejuízo da responsabilidade disciplinar a que der origem.

CAPÍTULO VIII

Disposições finais e transitórias

Artigo 65º

Norma transitória

Até a implementação da instituição responsável pela gestão da RTPE, o Núcleo Operacional da Sociedade de Informação (NOSI) desempenha as funções que àquela estão atribuídas.

Artigo 66º

Regulamentação

Para auxiliar os utilizadores dos recursos da RTPE na implementação das políticas e normas de segurança adoptadas por este diploma, são aprovados e fixados manuais de procedimentos a nível interno da instituição responsável pela gestão da RTPE.

Artigo 67º

Entrada em vigor

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

Visto e aprovado em Conselho de Ministros.

José Maria Pereira Neves - Maria Cristina Lopes de Almeida Fontes Lima - Cristina Isabel Lopes da Silva Monteiro Duarte - Janira Isabel Fonseca Hopffer Almada

Promulgado em 3 de Junho de 2010

Publique-se.

O Presidente da República, PEDRO VERONA RODRIGUES PIRES

Referendado em 3 de Junho de 2010

O Primeiro-Ministro, *José Maria Pereira Neves*

———

Decreto-Lei nº 20/2010

de 14 de Junho

Vários são os dispositivos constitucionais que deixam transparecer a importância que o Estado de Cabo Verde atribui à educação e à formação profissional. Um deles é o n.º 1 do artigo 77º da Constituição da República, que, conjugado com o disposto no seu n.º 2, reconhece a todos o direito à educação, deixando ainda claro que a educação deve preparar e qualificar os cidadãos para o exercício da actividade profissional, com vista à participação cívica e democrática na vida activa e para o exercício pleno da cidadania.

A preparação, formação e a qualificação dos indivíduos para o exercício de uma actividade profissional constitui uma vertente da educação, de grande alcance e significado social, da qual ela não pode dissociar-se.

O Programa do Governo para a Legislatura em curso absorve na íntegra as aspirações do legislador constitucional cabo-verdiano ao colocar na linha da frente dos desafios a vencer, o principal problema nacional que é o desemprego. Assim, a adopção de medidas de políticas públicas favorecedoras do investimento privado, da densificação do tecido empresarial e da inovação, com vista a acelerar o ritmo da geração de empregos, é uma das grandes metas a atingir. Aliado aos esforços que vêm sendo dispendidos nos domínios da educação e qualificação dos recursos humanos para o emprego, na melhoria da qualidade do ensino, assim como, na extensão do ensino técnico e da formação profissional, está-se a dar um grande passo para a implementação dos importantes eixos do processo de construção da competitividade da economia cabo-verdiana, quer em termos de qualidade, quer em termos de produtividade.

O presente diploma regula o Regime Jurídico Geral do Sistema Nacional de Qualificações, definindo os instrumentos, as acções e as estruturas necessárias ao seu funcionamento e desenvolvimento.

O SNQ deve ser configurado como um conjunto de instrumentos e acções necessários à promoção, desenvolvimento e integração das ofertas da formação profissional, através do Catálogo Nacional das Qualificações Profissionais, assim como, a permitir a evolução e certificação das correspondentes competências profissionais, de modo a favorecer o desenvolvimento humano, social e profissional da pessoa e satisfazer as necessidades do sistema produtivo.

Algumas balizas norteam a implementação do SNQ, de entre as quais merecem destaque especial, a orientação escolar, vocacional e profissional centrada no desenvolvimento humano e pessoal, tanto para a livre escolha da profissão como para o exercício do direito ao trabalho, de modo a satisfazer as necessidades individuais, sociais e económicas, o acesso em condições de igualdade, de todos os cidadãos, ao reconhecimento de suas competências, independente do modo como os tenha adquirido, a adequação da formação à qualificação de modo a satisfazer às exigências do mercado e a mobilidade dos trabalhadores, entre outros.

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

Artigo 1º

Objecto

O presente diploma regula o Regime Jurídico Geral do Sistema Nacional de Qualificações (SNQ) e define os instrumentos, acções e estruturas necessárias ao seu funcionamento e desenvolvimento.