Accelerating
the **Digital Transition**
in **São Tomé and Príncipe**

Quadro Nacional de Interoperabilidade de São Tomé e Príncipe

(QNI 0.1 – Novembro 2021)

UNDP

UNITED NATIONS UNIVERSITY
UNU-EGOV

O Quadro Nacional de Interoperabilidade (QNI) foi desenvolvido conjuntamente pelo Programa das Nações Unidas para o Desenvolvimento (PNUD) São Tomé e Príncipe e pela Unidade Operacional em Governação Eletrónica da Universidade das Nações Unidas (UNU-EGOV) em consulta com o Instituto Nacional de Inovação e Conhecimento (INIC) e demais agências governamentais de São Tomé e Príncipe.

Questões sobre o QNI podem ser dirigidas a:

Instituto de Inovação e Conhecimento (INIC)
Telefone: (+239) 2242650
E-mail: inic@inic.gov.st

Todo o conteúdo deste documento de referência está publicado no portal do Instituto de Inovação e Conhecimento (INIC) na Internet (www.inic.gov.st), garantindo acesso público às informações de interesse geral e transparência intrínseca à iniciativa. A responsabilidade da publicação, atualização e gestão dos recursos disponíveis desse site é do INIC.

Índice

Índice de Tabelas

Acrónimos

CCG	Comité de Coordenação e Gestão
CTI	Comité Técnico de Interoperabilidade
GT	Grupo de Trabalho
ITU	*International Telecommunication Union*
QNI	Quadro Nacional de Interoperabilidade
TIC	Tecnologias da Informação e Comunicação
UNU-EGOV	*United Nations University Operating Unit on Policy-Driven Electronic Governance*

1. Enquadramento

1.1 Contexto

A construção de uma Plataforma de Interoperabilidade para São Tomé e Príncipe foi idealizada durante a elaboração da Estratégia de Governação Digital do país, aprovada pela Resolução 35/2020 do Conselho de Ministros em sua 73ª Sessão Ordinária, em 16 de julho de 2020, ocasião na qual também foi criado o comitê para Governação Digital (CGD) com o objetivo de monitorizar e garantir a sua execução. O documento foi fruto de um trabalho conjunto entre o Governo de São Tomé e Príncipe, representado pelo Instituto de Inovação e Conhecimento (INIC), e a Unidade Operacional em Governação Eletrónica da Universidade das Nações Unidas (UNU-EGOV).

Naquela ocasião, ressaltou-se que "o desenvolvimento de uma estratégia para a Governação Digital tem a si associado um importante conjunto de requisitos que abrange, entre outros, as necessidades de integração, coordenação, reengenharia, desenho, manutenção e evolução de uma multiplicidade de serviços existentes e propostos, de reconhecimento e validação de múltiplas identidades do cidadão, e de monitorização e garantia de elevada confiabilidade e escalabilidade de toda esta infraestrutura." Uma plataforma de interoperabilidade visa, portanto, oferecer uma resposta eficaz a este conjunto de requisitos da governação digital.

De facto, a governação digital possui propósitos que serão profundamente facilitados a partir da existência dessa Plataforma de Interoperabilidade, nomeadamente:

i. melhorar o desempenho do Governo;

ii. aumentar a efetividade dos serviços públicos;

iii. diminuir a assimetria informacional entre Governo e sociedade;

iv. fortalecer a interação entre Governo e sociedade;

v. aumentar a participação da sociedade nas decisões governamentais; e

vi. promover um Governo aberto, transparente e responsável.

A Estratégia de Governação Digital do país preconizou, portanto, uma plataforma central, monitorizada, orientada a serviços, com potencial para dotar a Administração Pública de ferramentas partilhadas, transversais para a interligação de sistemas, federação de identidades, fornecimento de autenticação, envio de mensagens, pagamentos, entre outras, que permitam de forma ágil e econômica, a disponibilização de serviços digitais mais próximos das necessidades do cidadão e das empresas. Teria ainda o objetivo de permitir a disponibilização de serviços a entidades privadas, contribuindo para

fomentar a modernização e transformação digital não só do sector público, mas também do tecido económico são-tomense.

Tal plataforma exige um correspondente enquadramento regulatório, necessário para assegurar e dar sustentabilidade legal e administrativa para sua plena funcionalidade. É nesse contexto que o Quadro Nacional de Interoperabilidade (QNI) se insere, incluindo também uma lei que deverá instituí-lo, determinando sua vigência, alcance e amplitude.

A proposta do Quadro Nacional de Interoperabilidade de São Tomé e Príncipe busca seguir princípios estipulados na Estratégia de Governação Digital, em especial o da "Liderança Robusta", retratado no protagonismo do Instituto de Inovação e Conhecimento (INIC); o das "Parcerias Internacionais Favoráveis", no qual figura o Programa das Nações Unidas para o Desenvolvimento (PNUD); bem como o princípio dos "Recursos Tecnológicos Partilhados", consubstanciado neste projeto em que as instituições governamentais privilegiam a partilha de capacidades tecnológicas, evitando a proliferação de silos que tardem a transformação digital do país.

1.2 Conceito de Interoperabilidade

Interoperabilidade[1] é a capacidade de diversos sistemas e organizações trabalharem em conjunto (interoperar) em prol de objetivos comuns mutuamente benéficos e acordados, de maneira eficaz e eficiente, e envolve a partilha de informação e conhecimento entre as organizações, através dos processos de negócio que suportam, por meio da troca de dados entre os seus respetivos sistemas de informação.

Da definição anterior decorre que o conceito de interoperabilidade deve compreender, para além da dimensão técnica habitualmente associada ao termo, uma dimensão semântica e organizacional conforme se descrevem de seguida[1]:

Interoperabilidade Organizacional

Esta camada de interoperabilidade refere-se à maneira como a administração pública alinha os seus processos de negócio, responsabilidades e expetativas para alcançar objetivos comuns e mutualmente benéficos. Na prática, a interoperabilidade organizacional significa a documentação e a integração ou o alinhamento de processos de negócio e a troca de informações relevantes. A interoperabilidade organizacional também visa atender as necessidades da comunidade de utilizadores, ao tornar os serviços disponíveis, facilmente identificáveis, acessíveis e focados no utilizador.

Interoperabilidade Semântica

A interoperabilidade semântica garante que o formato e o significado exato dos dados e informações trocadas são preservados e compreendidos durante as trocas entre as partes envolvidas, ou seja, "o que é enviado é compreendido". A interoperabilidade semântica pode cobrir tanto aspetos semânticos quanto sintáticos. O aspeto semântico refere-se ao significado dos elementos dos dados e a relação entre eles, incluindo o desenvolvimento de vocabulários e esquemas para descrever as trocas de dados e garante que os elementos dos dados são compreendidos da mesma maneira por todas as partes que estão se comunicando. O aspeto

[1] Conceito adaptado dos apresentados nos Quadros de Interoperabilidade da Estónia, do Brasil e da União Europeia.

[1] European Commission. *New European Interoperability Framework*.2017. Disponível em: https://ec.europa.eu/isa2/eif_en

sintático refere-se à descrição do formato exato da informação a ser trocada em termos de gramática e formato.

Interoperabilidade Técnica

A interoperabilidade técnica envolve as aplicações e infraestruturas que conectam os sistemas e os serviços. Dentre os aspetos de interoperabilidade técnica, incluem-se as especificações de interface, os serviços de interconexão, os serviços de integração de dados, a apresentação e a troca de dados, e os protocolos de comunicação segura. A interoperabilidade técnica deve ser garantida, sempre que possível, por meio da utilização de especificações técnicas formais.

2. Definição, Propósito e Abrangência do Quadro Nacional de Interoperabilidade

O Quadro Nacional de Interoperabilidade é concebido como uma estrutura básica para a estratégia de governo eletrónico, aplicada a toda a Administração Pública de São Tomé e Príncipe, abrangendo os três Poderes do governo nacional – Poder Executivo, Poder Legislativo e Poder Judiciário e os poderes regionais e locais, não restringindo a participação, por adesão voluntária, de outras organizações.

Um Quadro Nacional de Interoperabilidade consiste em um acordo interorganizacional, em que é definido um conjunto de políticas, padrões técnicos e orientações e serve como uma ferramenta para alcançar a interoperabilidade de sistemas de informação e de serviços do setor público.

Assim, o QNI define um conjunto mínimo de premissas, políticas, recomendações e especificações técnicas que regulamentam a utilização da Tecnologia de Informação e Comunicação (TIC) na interoperabilidade de serviços de governo eletrónico, estabelecendo as condições de interação com os demais Poderes e esferas de governo e com a sociedade em geral.

O Quadro Nacional de Interoperabilidade de São Tomé e Príncipe contempla as três camadas de interoperabilidade mencionadas na Secção 1.2: Interoperabilidade Organizacional, Interoperabilidade Semântica e Interoperabilidade Técnica.

O QNI contribui para a universalização de acesso e utilização da informação, para a preservação dos documentos eletrónicos e simultaneamente para uma redução de custos de licenciamento de *software*.

O Quadro Nacional de Interoperabilidade aqui apresentado inclui especificamente:

- Conceitos e definições utilizados no contexto da interoperabilidade digital
- Políticas utilizadas na construção do QNI e que fundamentam as escolhas das especificações técnicas
- O regime de cumprimento das normas estabelecidas pelo QNI
- A definição do processo de governança, gestão e revisão do QNI e responsabilidades para:
  - Estabelecimento, aprovação e revisão das normas de interoperabilidade
  - Avaliação da conformidade dos sistemas de informação com as normas técnicas de interoperabilidade
- O conjunto de normas relativos a:

- Normas técnicas para interconexão, segurança, meios de acesso, organização e troca de informação entre os sistemas da infraestrutura governamental de TIC, e áreas de integração para governo eletrónico
- Formatos de dados para permitir a troca de dados entre os sistemas de informação do governo.

3. Políticas Gerais e por Dimensão do Quadro Nacional de Interoperabilidade

Relacionam-se de seguida as políticas gerais utilizadas na construção do Quadro Nacional de Interoperabilidade e que fundamentam as especificações técnicas de cada segmento, que serão indicadas no capítulo 4 deste documento, além de orientar os órgãos na implementação de sistemas interoperáveis.

P1. Adoção Preferencial de Normas Abertas

O Quadro Nacional de Interoperabilidade define que serão adotadas, preferencialmente, normas abertas nas especificações técnicas.

Uma norma aberta é aquela destinada à publicação, transmissão e armazenamento de informação em suporte digital que cumpra cumulativamente os seguintes requisitos:

- A sua adoção decorra de um processo de decisão aberto e disponível à participação de todas as partes interessadas;
- O respetivo documento de especificações tenha sido publicado e livremente disponibilizado, sendo permitida a sua cópia, distribuição e utilização, sem restrições;
- O respetivo documento de especificações não incida sobre ações ou processos não documentados;
- Os direitos de propriedade intelectual que lhe sejam aplicáveis, incluindo patentes, tenham sido disponibilizados de forma integral, irrevogável e irreversível à República Democrática de São Tomé e Príncipe;
- Não existem restrições à sua implementação.

Normas proprietárias são aceites nas seguintes condições:

- De forma transitória, em soluções de TIC do legado. O âmbito do Quadro Nacional de Interoperabilidade não atinge o legado, mas no caso de manutenção/atualização de qualquer solução de TI, o órgão deve se preocupar em seguir os padrões do Quadro Nacional de Interoperabilidade e substituir as normas padrões proprietárias dessa solução pelas definidas nesse documento de referência.
- Quando da inexistência de norma aberta, na qual poderão ser adotadas normas proprietárias até que uma norma aberta esteja disponível.

Sem prejuízo dessas metas, serão respeitadas as situações em que haja necessidade de consideração de requisitos de segurança e integridade de informações.

P2. Uso de Software Público e/ou Software Livre

A implementação das normas de interoperabilidade deve priorizar o uso de software público e/ou software livre.

P3. Existência de Suporte de Mercado

Todas as especificações contidas no Quadro Nacional de Interoperabilidade contemplam soluções amplamente utilizadas pelo mercado. O objetivo a ser alcançado é a redução dos custos e dos riscos na conceção e produção de serviços nos sistemas de informações governamentais.

P4. Continuidade

O avanço da interoperabilidade é um processo contínuo e deve ser gerido por meio de um planeamento de longo prazo, dinâmico e ágil, e por essa razão é essencial prever formas de atualizar as normas técnicas adotadas pelo QNI e gerenciar o processo de revisão constante do documento.

O Quadro Nacional de Interoperabilidade considera que a interoperabilidade envolve elementos técnicos, semânticos e organizacionais, sendo políticas gerais direcionadoras dessas camadas:

Camada Técnica

- Ampliar o acesso aos sistemas de informação
- Como meio de acesso, todos os sistemas de informação de governo deverão ser acessíveis por meio de qualquer tecnologia que se mostrar a mais adequada dentre as tecnologias disponíveis, ao nível de segurança requerido pelo serviço.
- Escalabilidade
- As especificações selecionadas deverão ter a capacidade de atender alterações de utilização do sistema, tais como, mudanças em volumes de dados, quantidade de transações ou quantidade de utilizadores. As normas estabelecidas não poderão ser fator restritivo, devendo ser capazes de fundamentar o desenvolvimento de serviços que atendam desde necessidades mais localizadas, envolvendo pequenos volumes de transações e de utilizadores, até demandas de abrangência nacional, com tratamento de grande quantidade de informações e envolvimento de um elevado contingente de utilizadores.

Camada Semântica

- Desenvolvimento e manutenção de ontologias e outros recursos de organização da informação.

  Visando facilitar o cruzamento de dados de diferentes fontes de informação, aquando da sua utilização por outras organizações integrantes da administração pública, por organizações da sociedade civil ou pelo cidadão, devem ser utilizados recursos tais como vocabulários controlados, taxonomias, ontologias e outros métodos de organização e recuperação de informações. Tais recursos podem ser desenvolvidos colaborativamente por pessoas com conhecimento na área específica e/ou em metodologias de modelagem específicas, e os

resultados devem ser compartilhados, reaproveitados e disponibilizados em um repositório de vocabulários e ontologias de governo eletrónico.

- Desenvolvimento e adoção de uma norma de modelação de dados para Governo

  Baseada em notação simples, objetiva e facilmente utilizável, a modelagem deve: evidenciar as integrações atuais e as integrações necessárias entre os dados; apoiar as interações do governo em suas diversas secretarias e órgãos; apoiar o alinhamento com os processos de negócios governamentais; promover a melhoria na gestão pública; e servir como arquitetura de interoperabilidade para o Governo.

- Desenvolvimento e adoção de uma política de disseminação de dados e informações

  Deve-se adotar uma política que promova a incorporação do conceito de Dados Abertos (*Open Data*) de modo a orientar a incorporação de processos de disponibilização dos dados públicos, permitindo assim a adequada transparência e seu melhor uso pela sociedade, alinhada com as diretrizes específicas do Quadro Nacional de Interoperabilidade para que tenhamos a efetiva interação do Governo com a sociedade.

Camada Organizacional

- Simplificação administrativa

  A aplicação do Quadro Nacional de Interoperabilidade visa contribuir para que as interações do governo com a sociedade sejam realizadas de forma simples e direta, sem prejuízo da legislação vigente.

- Promoção da colaboração entre organizações

  Por meio da integração entre objetivos institucionais e processos de negócio de organizações com estruturas internas e processos internos diferentes.

- Garantia à privacidade de informação

  Todos os órgãos responsáveis pelo oferecimento de serviços de governo eletrónico devem garantir as condições de preservação da privacidade das informações do cidadão, empresas e órgãos de governo, respeitando e cumprindo a legislação que define as restrições de acesso e divulgação.

4. Regime de Cumprimento do Quadro Nacional de Interoperabilidade

O QNI é normativo, sendo a adoção das normas, recomendações e políticas contidos no Quadro Nacional de Interoperabilidade prescritiva e a conformidade obrigatória para os órgãos da Administração Pública abrangendo os três Poderes do governo nacional – Poder Executivo, Poder Legislativo e Poder Judiciário – e os poderes regionais e locais, não restringindo a participação, por adesão voluntária, de outras organizações, nomeadamente organizações privadas.

No âmbito das entidades anteriormente mencionadas, é obrigatória a adoção das especificações contidas no Quadro Nacional de Interoperabilidade para:

- Todos os novos sistemas de informação que vierem a ser desenvolvidos e implantados na Administração Pública, e que se enquadram no âmbito de interação, dentro da Administração Pública e com a sociedade em geral;
- Sistemas de informação legados que sejam objeto de implementações que envolvam provimento de serviços de governo eletrónico ou interação entre sistemas; e
- Aquisição ou atualização de sistemas e equipamentos de TIC.

5. Governança e Gestão do Quadro Nacional de Interoperabilidade

A elaboração e adoção de forma sustentável do QNI em São Tomé e Príncipe, requer o estabelecimento de um modelo de governança que elenque e descreva os atores (papéis e responsabilidades) relevantes para a sua operacionalização e gestão. Requer igualmente que se estabeleça um processo de revisão do próprio QNI que permita manter o seu conteúdo, nomeadamente as normas e especificações técnicas que prevê, atualizado, de forma a refletir a evolução tecnológica existente e o desenvolvimento das práticas de interoperabilidade do país. As secções seguintes reúnem estes elementos.

5.1 Papéis e responsabilidades no âmbito do QNI

Nesta secção são elencados vários papéis e responsabilidades que se vislumbram como essenciais para uma adoção, implementação e evolução bem-sucedida do QNI.

Comité de Coordenação e Gestão do QNI

O Comité de Coordenação e Gestão (CCG) do QNI tem um papel central no âmbito do QNI, com responsabilidade e autoridade de tomada de decisão relativa ao desenvolvimento e gestão contínuos do Quadro Nacional de Interoperabilidade. São atribuições desta entidade:

- Definir as orientações do QNI e deliberar sobre as políticas e especificações técnicas;
- Liderar o processo de revisão e atualização do QNI, providenciando a infraestrutura de gestão necessária para suportar todo o processo, bem como deliberar sobre os ajustes que decorram da revisão e atualização;
- Elaborar e divulgar orientações técnicas, nomeadamente na forma de manuais e outros materiais de instrução;
- Definir objetivos, identificar projetos, promover a colaboração entre as agências e propor medidas relativas à implementação do QNI;
- Manifestar-se sobre questões relacionadas com a adoção e a conformidade com o QNI por agências governamentais;
- Constituir e apoiar a atividade dos grupos de trabalho para a elaboração de propostas, diretrizes e especificações técnicas, de acordo com a necessidade;

- Disponibilizar e manter atualizado os recursos associados ao QNI: páginas, catálogos, gestão de comunidades, respostas às consultas públicas realizadas e outros serviços e informações relacionadas com o QNI;
- Instigar a partilha e a cooperação técnica nacional e internacional na área de normas de interoperabilidade; e
- Promover iniciativas de divulgação e de capacitação de funcionários públicos para a aplicação do QNI.

No contexto atual de São Tomé e Príncipe, e face ao seu papel e atribuições definidas na Resolução do Conselho de Ministros nº 35/2020, o INIC vislumbra-se como a entidade que potencialmente poderia assumir o papel de coordenação e gestão do QNI.

Comité Técnico de Interoperabilidade

O Comité Técnico de Interoperabilidade (CTI) é presidido por representante do Comité de Coordenação e Gestão do QNI e constituído por representantes das várias agências governamentais que adotam ou que são potenciais adotantes do QNI, criando-se desta forma a oportunidade para que todas as agências possam participar e ter um papel ativo na governança do QNI. Este Comité atua com o intuito de garantir:

- O valor do QNI como um "ativo coletivo", que apoia a capacidade e o desempenho das várias agências individuais e do setor público como um todo, fomentando uma cultura de interoperabilidade na Administração Pública de São Tomé e Príncipe.
- Que o QNI é mantido e aprimorado ao longo do tempo em alinhamento com as necessidades globais do domínio e particulares de todas as entidades;
- Que os benefícios que podem ser aportados pelo QNI (maior capacidade, desempenho, eficiência e eficácia de cada agência e do setor público) superam os seus custos (diminuição da autonomia da agência, custos de administração, etc.);
- Que o desenvolvimento das estratégias, iniciativas, e práticas das várias agências decorre em conformidade com as normas e recomendações do QNI.

Grupos de Trabalho

Os Grupos de Trabalho (GT) são grupos constituídos por peritos de diferentes setores, oriundos de instituições governamentais, do setor público, de organizações técnicas e profissionais, da academia, da sociedade civil, de organizações internacionais, ou do setor privado, estabelecidos para rever regularmente as normas e especificações de cada um dos segmentos técnicos do QNI, bem como para refletirem sobre outros aspetos relevantes do QNI. Os grupos são estabelecidos e encerrados pelo Comité de Coordenação e Gestão do QNI e a ele reportam os resultados da sua atividade.

5.2 Processo de Revisão do QNI

O QNI é um documento dinâmico, que necessita de ser revisto com determinada periodicidade, de forma a acomodar e refletir a evolução tecnológica e o desenvolvimento das práticas de interoperabilidade do país.

Sugere-se que um processo de revisão estruturado seja conduzido a cada 3 anos, sem prejuízo de poderem ser revistas e mantidas atualizadas as tabelas de normas em periodicidade inferior.

O processo de revisão deve compreender a sequência de fases proposta na Figura 1, culminando com a publicação de uma nova versão do QNI. A primeira versão aprovada do QNI é designada por QNI *1.0*. As versões seguintes aprovadas deverão seguir uma numeração sequencial (*2.0*, *3.0* e assim por diante). Sugere-se ainda um forte envolvimento e intervenção de diversos atores através de processos consultivos de diferentes naturezas (consultas públicas, grupos de trabalho, envio de contributos por email e redes sociais) no decorrer do processo. Instituições governamentais, do setor público, organizações técnicas e profissionais, do setor privado, academia, sociedade civil e cidadãos, todos devem ter oportunidade de participar no processo de revisão.

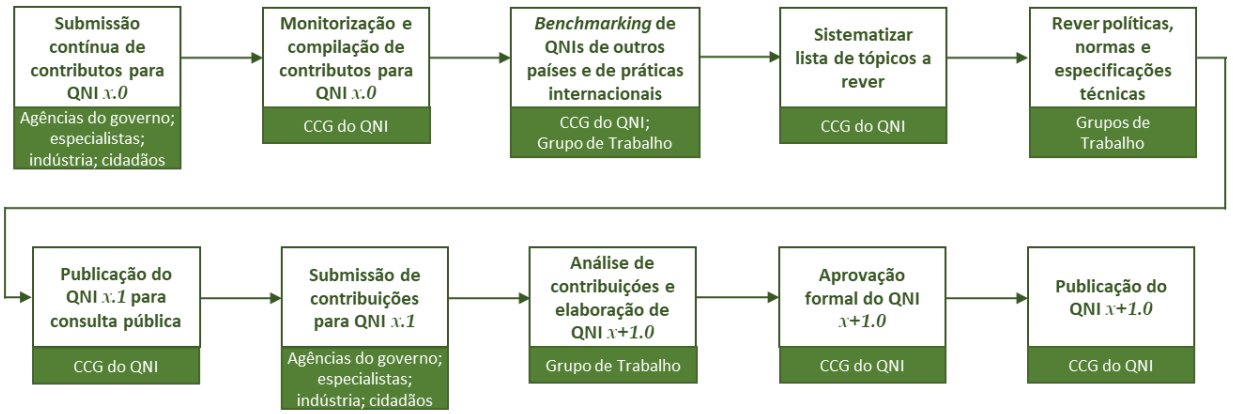

Figura 1: Processo de revisão do QNI: fases e atores.

O processo prevê a existência de mecanismos que permitam a recolha, de forma contínua, de contributos (sugestões, comentários, etc.) por parte de diversas entidades para a versão publicada e em aplicação. Os contributos, que cheguem de forma aberta e continuada, devem ser compilados e analisados pelo Comité de Coordenação e Gestão (CCG) do QNI. Em simultâneo, e sob orientação do CCG do QNI, deve ser constituído um grupo de trabalho para analisar e identificar as melhores práticas internacionais adotadas por outros países na elaboração dos seus QNI. Os contributos recebidos e as práticas identificadas são sistematizados e partilhados com grupos de trabalho específicos, constituídos por especialistas nos segmentos em análise, que os analisarão e se pronunciarão sobre os mesmos, fazendo os ajustes necessários ao QNI. A nova versão ajustada do QNI é publicada para consulta pública formal. As contribuições feitas à proposta de novo QNI são analisadas e uma nova versão do QNI produzida. Esta nova versão é preparada e aprovada pelo CCG do QNI e divulgada publicamente para adoção.

Todas as versões do QNI bem como documentação afim relevante deverá estar publicamente disponível num website mantido para o efeito. Todas as consultas públicas realizadas às várias versões do QNI deverão também ser devidamente publicitadas quer no website oficial do QNI quer pelos canais considerados adequados para promover convenientemente as iniciativas e permitir os melhores níveis possíveis de participação dos diversos atores.

6. Especificação Técnica dos Componentes do Quadro Nacional de Interoperabilidade

O Quadro Nacional de Interoperabilidade de São Tomé e Príncipe está segmentado em cinco partes, com a finalidade de organizar as definições das normas.

Os cinco segmentos – "Interconexão", "Segurança", "Meios de Acesso", "Organização e Troca de Informação" e "Áreas de Integração para Governo Eletrónico" – estão subdivididos em **componentes**, para os quais foram estabelecidas as especificações técnicas a serem adotadas pelos órgãos governamentais abrangidos pelo Quadro Nacional de Interoperabilidade.

As especificações técnicas indicadas são classificadas em dois níveis de situações que caracterizam o grau de obrigatoriedade de adoção:

- **Obrigatório (O)**: item adotado pelo governo como norma no QNI, tendo sido submetido a um processo formal de homologação conforme descrito no capítulo 5 deste documento. Os componentes com nível **Obrigatório** devem ser obrigatoriamente adotados em novos produtos/projetos de TI;
- **Recomendado (R)**: item que atende às políticas técnicas do QNI, é reconhecido como um item que deve ser utilizado no âmbito das instituições de governo, mas ainda não foi submetido a um processo formal de homologação. Os componentes de nível **Recomendado** não são obrigatórios, porém sugeridos para adoção em novos produtos/projetos de TI;

Apresenta-se, a seguir, uma breve descrição dos segmentos e respetivos componentes.

6.1 Interconexão – Segmento 1

Interconexão consiste na ligação de redes de telecomunicações funcionalmente compatíveis, de modo que os utilizadores de serviços de uma das redes possam comunicar com utilizadores de serviços de outra rede ou, ainda, aceder a serviços nela disponíveis. Logo, esse segmento estabelece as condições para que as redes dos órgãos de governo se possam interligar e, assim, promover a interoperabilidade.

Tabela 1: Aplicação[2]

Componente	Especificação	Situação
Transporte de mensagem eletrónica	Utilizar produtos de mensagem eletrónica que suportam interfaces em conformidade com SMTP/MIME para transferência de mensagens. RFC correlacionadas: RFC 5321, RFC 5322, RFC 2045, RFC 2046, RFC 3676, RFC 2047, RFC 2231 (atualização das RFC 2045, 2047 e 2183), RFC 2183, RFC 4288, RFC 4289, RFC 3023 e RFC 2049.	O
Acesso à caixa postal	*Post Office Protocol* – POP3 para acesso remoto a caixa postal. RFC correlacionada: RFC 1939 (atualizada pela RFC 1957 e RFC 2449).	R
	Internet Message Access Protocol – IMAP para acesso remoto à caixa postal. RFCs correlacionadas: RFC 2342 (atualizada pela RFC 4466), RFC 2910 (atualizada pela RFC 3380, RFC 3381, RFC 3382, RFC 3510 e RFC 3995), RFC 2971, RFC 3501, RFC 3502 e RFC 3503.	O
Mensagens em Tempo Real	O modelo e requisitos para *Instant Messaging and Presence Protocol* (IMPP) são definidos pela RFC 2778 e RFC 2779.	R
	O modelo e requisitos para *Extensible Messaging and Presence Protocol* (XMPP) são definidos pela RFC 6120 e atualizada pela RFC 6122.	O
AntiSpam – Gerenciamento da Porta 25	Implementar submissão de e-mail via porta 587/TCP com autenticação, reservando a porta 25/TCP apenas para transporte entre servidores SMTP.	R
Protocolo de transferência de hipertexto	Utilizar HTTP/1.1 (RFC 2616, atualizada pelas RFCs 2817, 5785, 6266 e 6585).	O
	Utilizar HTTP/2 (RFC 7540).	R
Protocolos de transferência de ficheiros	FTP (com reinicialização e recuperação) conforme RFC 959 (atualizada pela RFC 2228, RFC 2640, RFC 2773, RFC 3659 e RFC 5797) e HTTP conforme RFC 2616 (atualizada pelas RFCs 2817, 5785, 6266 e 6585) para transferência de arquivos. SFTP (*Secure File Transfer Protocol*) conforme RFC 913.	O
Diretório	LDAP v3 deverá ser utilizado para acesso geral ao diretório OpenLDAP, conforme RFC 4510.	O
Sincronismo de tempo	RFC 5905 IETF - Network Time Protocol – NTP version 4.0[3].	O
Serviços de Nomeação de Domínio	O DNS deve ser utilizado para resolução de nomes de domínios Internet, conforme a RFC 1035 (atualizada pela RFC 1183, RFC 1348, RFC 1876, RFC 1982, RFC 1995, RFC 1996, RFC 2065, RFC 2136, RFC 2181, RFC 2137, RFC 2308, RFC 2535, RFC 1101, RFC 3425, RFC 3658, RFC 4033, RFC 4034, RFC 4035, RFC 4343, RFC 5936, RFC 5966 e RFC 6604). DNSec (Domain Name System Security Extensions), RFC 4033.	O
Protocolos de sinalização	Uso do Protocolo de Inicialização de Sessão (SIP), definido pela RFC 3261 (atualizada pela RFC3265, RFC4320, RFC4916, RFC5393, RFC5621, RFC5626, RFC5630, RFC5922, RFC5954 e RFC6026), como protocolo de controle na camada de aplicação (sinalização) para criar, modificar e terminar sessões com um ou mais participantes.	O
	Uso do protocolo H.323 em sistemas de comunicação multimídia baseado em pacotes, definido pela ITU-T (*International Telecommunication Union Telecommunication Standardization* sector).	R
Protocolos de gerenciamento de rede	Uso do protocolo SNMP, definido pelas RFC 3411 (atualizada pela RFC 5343 e RFC 5590) e 3418, como protocolo de gerência de rede. Versão 2	R
	Uso do protocolo SNMP, definido pelas RFC 3411 (atualizada pela RFC 5343 e RFC 5590) e 3418, como protocolo de gerência de rede. Versão 3	R
Protocolo de troca de informações estruturadas em plataforma descentralizada e/ou distribuída	Ver Tabela 17 – Especificações para a Área de Integração para Governo Eletrónico – *Web Services*.	
Protocolo de análise de fluxo de rede	IPFIX, conforme RFC 5101, sFlown (RFC 3176).	R
Protocolo de Rede Definida por Software	Software-Defined Networking (RFC 7426) ITU-T JCA-SDN-D-001 Rev.6 http://www.itu.int/en/ITU-T/jca/sdn/Documents/deliverable/jca-sdn-	R

[2] As RFCs (*Request for Comments*) podem ser acedidas em http://www.ietf.org/rfc.html

[3] O *Simple Network Time Protocol* – SNTP *version* 4.0 está definido na seção 14 da RFC 5905.

	D-001_R6-sdn_standard-roadmap_31082017.docx	
Infraestrutura como Serviço – (serviços em nuvem)	Serviço em nuvem prestado por provedor compreendendo processamento, armazenamento (*storage*), rede e outros recursos computacionais, nos quais o órgão contratante pode implementar e executar softwares ou aplicações. O serviço é realizado mediante responsabilidade compartilhada, entre provedor e contratante do serviço. Cabe, por exemplo, ao provedor do serviço gerenciar a infraestrutura do serviço em nuvem, e ao contratante gerenciar sistemas operacionais. Referência: NIST Definition of Cloud Computing – Special Publication 800-145	R
Software como Serviço (serviços em nuvem)	Serviço de consumo de aplicação ou software executados por um provedor. As aplicações são acessíveis por navegador web ou por interfaces web – *Software as a Service* (SaaS). O serviço é realizado mediante responsabilidade compartilhada, entre provedor e contratante do serviço. Cabe, por exemplo, ao provedor do serviço gerenciar a infraestrutura do serviço em nuvem, e ao contratante gerenciar as configurações do software/aplicação relacionadas aos utilizadores. Referência: NIST Definition of Cloud Computing – Special Publication 800-145	R
Serviços em Nuvem	**Nuvem Privada** – A infraestrutura do serviço em nuvem é provida para uso exclusivo de uma única organização, a qual pode ter múltiplos usuários. Pode ser da própria organização ou operada por terceiros, ou uma combinação. Referência: NIST Definition of Cloud Computing – Special Publication 800-145	R
	Nuvem Pública – A infraestrutura do serviço em nuvem é provida para uso do público em geral. Pode ser da própria organização ou operada por terceiros, ou uma combinação. Referência: NIST Definition of Cloud Computing – Special Publication 800-145	R
	Nuvem Híbrida – A infraestrutura do serviço em nuvem é composta de duas ou mais estruturas de nuvem distintas, mas estão unidas por tecnologia padronizada ou proprietária que permite portabilidade dos dados e aplicações. Referência: NIST Definition of Cloud Computing – Special Publication 800-145	R
Interface de gerenciamento de dados em nuvem	Interface para gerenciamento de dados em nuvem. Referência: utilizar CDMI (RFC 6208)	R
Interface aberta para computação em nuvem	Interface aberta para computação em nuvem (OCCI). Referência: GFD.221, GFD.222, GFD.223, GFD.224, GFD.226, GFD.227, GFD.228 e GFD.229 (occi-wg.org/about/specification/). A versão atual das especificações é a 1.2.	R

Tabela 2: Rede/Transporte

Componente	Especificação	Situação
Transporte	TCP (RFC 793)	O
	UDP (RFC 768) quando necessário, sujeito às limitações de segurança.	O
Intercomunicação LAN/WAN	IPv6 conforme RFC 2460 (atualizada pela RFC 5085, RFC 5722 e RFC 5871).	O
	IPv4 conforme RFC 791 (atualizada pela RFC 1349).	R
Comutação por Label	Quando necessário, o tráfego de rede pode ser otimizado pelo uso do MPLS (RFC 3031), devendo este possuir, no mínimo, quatro classes de serviço. No caso de interconexão com a rede pública com comutação por Label, não haverá troca de Label entre a rede privada do governo e a rede pública. Neste caso deve-se adotar interface NNI (Option A) entre a rede do governo e a rede pública.	O
Qualidade de serviço	Adoção de uma arquitetura para serviços diferenciados pelo uso do Diffserv (RFC 2475, atualizada pela RFC 3260).	O

Tabela 3: Enlace/Físico

Componente	Especificação	Situação
Rede local sem fio	IEEE 802.11 b, em conformidade com as determinações do *Wi-Fi Alliance* (http://www.wi-fi.org)	R
	IEEE 802.11 g, em conformidade com as determinações do *Wi-Fi Alliance* (http://www.wi-fi.org)	O
	IEEE 802.11 n, em conformidade com as determinações do *Wi-Fi Alliance* (http://www.wi-fi.org)	R
	IEEE 802.11ac	R

	IEEE 802.11ad http://standards.ieee.org/findstds/standard/802.11ad-2012.html	R
Rede de acesso por cabeamento elétrico	*Power Line Communication* (PLC)	R
Qualidade de Serviço – 802.1p	https://standards.ieee.org/findstds/standard/802.1Q-2014.html	R
Virtual LAN	VLAN (IEEE 802.1Q)	R
Resiliência Layer2	Spanning tree protocol (802.1d, 802.1w, 802.1s)	R
	Shortest Path Bridging	R
	DCB – Data Center Bridging	R

6.2 Segurança – Segmento 2

Trata dos aspetos de segurança de TIC que o governo deve considerar.

6.2.1 Políticas Técnicas

a) Os dados, informações e sistemas de informação do governo devem ser protegidos contra ameaças, de forma a reduzir riscos e garantir a integridade, confidencialidade, disponibilidade e autenticidade.

b) Os dados e informações devem ser mantidos com o mesmo nível de proteção, independentemente do meio em que estejam sendo processados, armazenados ou trafegando.

c) As informações classificadas e sensíveis que trafegam em redes inseguras, incluindo as sem fio, devem ser criptografadas de modo adequado, conforme os componentes de segurança especificados neste documento.

d) Os requisitos de segurança da informação dos serviços e de infraestrutura devem ser identificados e tratados de acordo com a classificação da informação, níveis de serviço definidos e com o resultado da análise de riscos.

e) A segurança deve ser tratada de forma preventiva. Para os sistemas que apoiam processos críticos, devem ser elaborados planos de continuidade, nos quais serão tratados os riscos residuais, visando atender aos níveis mínimos de produção.

f) A segurança é um processo que deve estar inserido em todas as etapas do ciclo de desenvolvimento de um sistema.

g) Os sistemas devem possuir registos históricos (*logs*) para permitir auditorias e provas materiais, sendo imprescindível a adoção de um sistema de sincronismo de tempo centralizado, bem como a utilização de mecanismos que garantam a autenticidade dos registos armazenados, se possível, com assinatura digital.

h) Nas redes sem fio metropolitanas recomenda-se a adoção de valores aleatórios nas associações de segurança, diferentes identificadores para cada serviço e a limitação do tempo de vida das chaves de autorização.

i) A documentação dos sistemas, dos controles de segurança e das topologias dos ambientes deve ser mantida atualizada e protegida, mantendo-se grau de sigilo compatível.

j) Os utilizadores devem conhecer suas responsabilidades com relação à segurança e devem estar capacitados para a realização de suas tarefas e utilização correta dos meios de acesso.

6.2.2 Especificações Técnicas

Tabela 4: Comunicação de dados

Componente	Especificação	Situação
Transferência de dados em redes inseguras	TLS – Transport Layer Security, RFC 5246 (atualizada pela RFC 5746 e RFC 5878). Caso seja necessário o protocolo TLS v1 pode emular o SSL v3.	R
Algoritmos para troca de chaves de sessão, durante o *handshake*	RSA, Diffie-Hellman RSA, Diffie-Hellman DSS, DHE_DSS, DHE_RSA;	R
Algoritmos para definição de chave de cifração	RC4, IDEA, 3DES e AES	R
Certificado Digital	X.509 v3, SASL – *Simple Authentication and Security Layer*, RFC 4422	R
Hipertexto e transferência de ficheiros	RFC 2818 (atualizada pela RFC 5785)	R
Transferência de ficheiros	SSH FTP	R
	Securing FTP with TLS, RFC 4217	R
Segurança de redes IPv4	*IPSec Authentication Header* RFC 4303 e RFC 4835[4] para autenticação de cabeçalho do IP. IKE – *Internet Key Exchange*, RFC 4306 (atualizada pela RFC5282), deve ser utilizado sempre que necessário para negociação da associação de segurança entre duas entidades para troca de material de chaveamento. ESP – *Encapsulating Security Payload*, RFC 4303 Requisito para VPN – *Virtual Private Network*.	O
Segurança de redes IPv4 para protocolos de aplicação	O S/MIME v3, RFC 5751[5] deverá ser utilizado quando for apropriado para segurança de mensagens gerais de governo.	O
Segurança de redes IPv6 na camada de rede	O IPv6 definido na RFC 2460 (atualizada pela RFC 5095), RFC 5722 e RFC 5871 apresenta implementações de segurança nativas no protocolo. As especificações do IPv6 definiram dois mecanismos de segurança: a autenticação de cabeçalho AH (*Authentication Header*) RFC 4302 ou autenticação IP, e a segurança do encapsulamento IP, ESP (*Encrypted Security Payload*) RFC 4303[6].	R

Tabela 5: Correio Eletrónico

Componente	Especificação	Situação
Acesso a caixas postais	O acesso à caixa postal deverá ocorrer através do cliente do software de correio eletrônico utilizado, considerando as facilidades de segurança nativas do cliente. Quando não for possível utilizar o cliente específico ou for necessário aceder à caixa postal através de redes não seguras (por exemplo: Internet) deve-se utilizar HTTPS de acordo com os padrões de segurança de transporte descritos na RFC 2595 (atualizada pela RFC 4616)[7], que trata da utilização do TLS com IMAP, POP3 e ACAP.	O
Conteúdo de e-mail	O S/MIME V3 deverá ser utilizado quando for apropriado para segurança de mensagens gerais de governo. Isso inclui RFC 5652, RFC 3370 (atualizada	O

[4] Consultar errata para RFC 4303 e RFC 4306.

[5] Consultar errata para RFC 5751.

[6] Consultar errata para RFC 4302 e RFC 4303.

[7] Consultar errata para a RFC 2595.

	pela RFC 5754), RFC 2631, RFC 5750, RFC 5751 e RFC 5652[8].	
Transporte de e-mail	Utilizar SPF (*Sender Policy Framework*) nos termos da RFC 4408, e reservar a porta 25, do protocolo SMTP, exclusivamente para transporte de mensagens entre MTAs; para comunicação entre MUAs e MTAs, utilizar a porta 587 (*Submission*), nos termos das RFCs 4409 e 5068[9].	O
Identificação de e-mail	Utilizar DKIM (*DomainKey Identified Mail*) nos termos da RFC 6376[10] http://datatracker.ietf.org/doc/rfc6376/	R
Transporte seguro de e-mail	Usar SMTP seguro sobre TLS para transporte de emails entre MTA's nos termos da RFC 3207 e SMTP AUTH nos termos da RFC 4954[11].	R

Tabela 6: Criptografia

Componente	Especificação	Situação
Algoritmo de cifração	3DES ou AES	R
Algoritmo para assinatura/*hashing*	SHA-256 ou SHA-512[12]	R
	SHA-224 ou SHA-238	R
Algoritmo para transporte de chave criptográfica de conteúdo/sessão	RSA	O
Algoritmos criptográficos baseados em curvas elípticas	ECDSA 256 e ECDSA 512 (RFC 5480)[13]. ECIES 256 e ECIES 512.	O
	ECMQV e ECDH, ambos para acordo de chaves, conforme RFC 5753.	R
Requisitos de segurança para módulos criptográficos	FIPS 140-1 e FIPS 140-2.	R

Tabela 7: Desenvolvimento de Sistemas

Componente	Especificação	Situação
Assinaturas XML	Sintaxe e Processamento de assinatura XML (XMLsig) conforme definido pelo W3C http://www.w3.org/TR/xmldsig-core/	O
Cifração XML	Sintaxe e Processamento de Cifração XML (XMLenc) conforme definido pelo W3C http://www.w3.org/TR/xmlenc-core/	R
Assinatura e cifração XML	Transformação de decifração para assinatura XML conforme definido pelo W3C http://www.w3.org/TR/xmlenc-decrypt	R
Principais gerenciamentos XML quando um ambiente PKI é utilizado	XML – *Key Management Specification* (XKMS 2.0) (Especificações de Gerenciamento de Chave XML) conforme definido pelo W3C http://www.w3.org/TR/xkms2/	R
Autenticação e autorização de acesso XML	SAML – conforme definido pelo OASIS quando um ambiente ICP é utilizado http://www.oasisopen.org/committees/security/index.shtml	R
Intermediação ou Federação de Identidades	WS-Security 1.1 – arcabouço de padrões para garantir integridade e confidencialidade em mensagens SOAP. (http://www.oasisopen.org/standards#wssv1.1. WS-Trust 1.4 – extensões para a norma WSSecurity, definindo o uso de credenciais de segurança e gerência de confiança distribuída. (http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/os/wstrust-	R

[8] Consultar errata para RFC 5652, RFC 3370, RFC 5754, RFC 2631, RFC 5751 e RFC 5652.

[9] Consultar errata para RFC 4408.

[10] Consultar errata para RFC 4871.

[11] Ver http://www.ietf.org/rfc/rfc3207.txt e http://www.ietf.org/rfc/rfc4954.txt

[12] Os sistemas devem ter suporte para o algoritmo de *hash* MD5 com RSA, para garantir compatibilidade com implementações anteriores.

[13] ECDSA, para assinaturas digitais, e ECIES para cifração e transporte seguro de chaves criptográficas.

	1.4-spec-os.pdf).	
Navegadores	Somente utilizar testemunhas de conexão de caráter permanente (*cookies*) com a concordância do utilizador.	O

Tabela 8: Serviços de Rede

Componente	Especificação	Situação
Diretório	LDAPv3 RFC 4510, RFC 4511, RFC 4512 e RFC 4513[14]. LDAP v3 extensão para TLS RFC 4510, RFC 4511 e RFC 4513.	R
Mensagem instantânea	RFC 2778, RFC 3261 (atualizada pela RFC 3265, RFC 3853, RFC 4320, RFC 4916, RFC 5393, RFC 5621, RFC 5626, RFC 5630, RFC 5922), RFC 3262, RFC 3263, RFC 3264 e RFC 3265 (Atualizada pela RFC 5367 e RFC 5727)[15]	R
Carimbo do tempo	RFC 3628 TSAs – *Policy Requirements for Time-Stamping Authorities, Time-Stamp Protocol*, RFC 3161 ETSI TS101861 (*Time-Stamping Profile*) (atualizada pela RFC 5816)[16].	R
Prevenção de DDoS	Usar métodos para inibir o uso de *IP spoofing* em ataques de DDoS nos termos do RFC 2827[17].	R

Tabela 9: Redes Sem Fio

Componente	Especificação	Situação
MAN[18] sem fio 802.16-2004[19] 802.16.2-2004[20] 802.16e[21] e 802.16f[22]	Utilizar PKM-EAP (*Privacy Key Management – Extensible Autentication Protocol*) com: • EAP – TLS ou TTLS; • AES[23] (*Advanced Encryption Standard*).	R
LAN sem fio 802.11	Usar a especificação WPA2 (*Wi-Fi Protect Access*) com criptografia AES	R

Tabela 10: Resposta a Incidentes de Segurança da Informação

Componente	Especificação	Situação
Preservação de Registos	*Guidelines for Evidence Collection and Archiving*, RFC 3227.	R
Gerenciamento de incidentes em redes computacionais	*Expectations for Computer Security Incident Response*, RFC 2350.	O
Informática Forense	*Guide to Integrating Forensic Techniques into Incident Response* – NIST – *Special Publication* 800-86 – (http://csrc.nist.gov/publications/nistpubs/800-86/SP800-86.pdf).	O
Comunicação entre Equipas e entre Centros de tratamento e resposta a incidentes	Representação para o compartilhamento de informações entre Equipes e entre Centros de Resposta a Incidentes de Segurança em Redes de Computadores: *Incident Object Description Exchange Format* (IODEF) – RFC 5070[24] http://datatracker.ietf.org/doc/rfc5070/	R

[14] Consultar errata para RFC 4511 e RFC 4512.

[15] Consultar errata para RFC 3261, RFC 3262, RFC 3264, RFC 3265 e RFC 5727.

[16] Consultar errata para RFC 3161.

[17] Ver http://www.ietf.org/rfc/rfc2827.txt

[18] O 802.16 é definido pelo IEEE como uma interface tecnológica para redes de acesso sem fio metropolitanas ou WMAN (*Wireless Metropolitan Access Network*).

[19] https://standards.ieee.org/standard/802_16-2004.html

[20] https://standards.ieee.org/standard/802_16_2-2004.html

[21] https://standards.ieee.org/standard/802_16e-2005.html

[22] https://standards.ieee.org/standard/802_16f-2005.html

[23] http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[24] Deverão ser realizados estudos a respeito de procedimentos e ferramentas para a possível adoção desta norma.

	Extensão do formato IODEF para suportar a comunicação de eventos do tipo "*phishing*". http://datatracker.ietf.org/doc/rfc5901/ Guia para a extensão do formato IODEF. http://datatracker.ietf.org/doc/rfc6684/	
Comunicação entre Sistemas de detecção e resposta a intrusão	Formato para compartilhamento de dados entre sistemas de detecção e resposta a incidentes de segurança computacionais: *Intrusion Detection Message Exchange Format* (IDMEF) – RFC 4765[25] http://datatracker.ietf.org/doc/rfc4765/	R

Tabela 11: Segurança para Alguns Serviços em Nuvem

Componente	Especificação	Situação
Serviços em Nuvem	Arquitetura de Referência para Segurança. NIST *Special Publication* 500-299 e 800-144.	R
Interface de gestão de dados em nuvem	Arquitetura de segurança: metodologia de análise e modelo formal. RFC 6208, capítulo 6.	R

6.3 Meios de Acesso – Segmento 3

São explicitadas as questões relativas aos padrões dos dispositivos de acesso aos serviços de governo eletrónico.

6.3.1 Especificações Técnicas

Tabela 12: Meios de Publicação

Componente	Especificação	Situação
Conjunto de caracteres	The Unicode Consortium. The Unicode Standard, Version 10.0.0 http://www.unicode.org/versions/Unicode10.0.0/ UTF-8 ISO/IEC 10646:2014 Obs: A versão ISO também está em atualização (https://www.iso.org/standard/69119.html).	R
Formato de troca de hipertexto	W3C XML versões 1.0 ou 1.1 (.xml) http://www.w3.org/TR/xml/	O
	W3C HTML 5 conforme especificações do W3C http://www.w3.org/TR/html5/	O
	W3C HTML versão 4.01 (.html ou .htm) http://www.w3.org/TR/html4/	R
	W3C XHTML versões 1.0 ou 1.1 (.xhtml) http://www.w3.org/TR/xhtml1	R
Mobile	W3C Mobile Web Application Best Practices http://www.w3.org/TR/mwabp/	R
	W3C Metadata API for Media Resources 1.0 http://www.w3.org/TR/mediaont-api-1.0/	R
	W3C Geolocation API Specification 2nd Edition http://www.w3.org/TR/geolocation-API/	R
Ficheiros do tipo documento/publicação	Texto puro (ficheiro .txt)	O
	Open Documento ODF 1.2 (.odt) – conforme especificação da OASIS[26]	O
	EPUB 3.0.1 http://idpf.org/epub/301	R
	Portable Document Format - PDF ISO 32000-1:2008	R

[25] Deverão ser realizados estudos a respeito de procedimentos e ferramentas para a possível adoção desta norma.

[26] Disponível em: http://docs.oasis-open.org/office/v1.2/OpenDocument-v1.2.html

	Portable Document Format - PDF/A ISO 19005-1:2005[27], quando necessária a preservação digital de documentos	R
Ficheiros do tipo folha de cálculo	Open Document ODF 1.2 (.ods) - conforme especificação da OASIS	O
Ficheiros do tipo apresentação	Open Document ODF 1.2 (.odp) – conforme especificação da OASIS	O
	HTML (.html ou .htm), conforme especificações do W3C.	R
Ficheiros do tipo "base de dados" para estações de trabalho[28]	Texto puro (.txt).	O
	CSV (Comma-Separated Values), conforme definido pela IETF no RFC 4180	O
	XML (-xml), conforme especificações do W3C.	R
Troca de informações gráficas e imagens estáticas	W3C PNG (.png), ISO/IEC 15948:2003 (E) http://www.w3.org/TR/PNG/	O
	SVG (.svg), gerado conforme especificações do W3C[29].	R
	JPEG File Interchange Format (.jpeg, .jpg ou .jfif)[30].	R
Gráficos vetoriais	SVG (.svg), gerado conforme especificações do W3C.	R
Animação	SVG (.svg), gerado conforme especificações do W3C.	R
Áudio	Ogg Vorbis (.ogg, .oga)[31].	R
	Ogg FLAC (.ogg, .oga)	R
	FLAC (.flac)	R
Vídeo	Ogg Theora (.ogg, .ogv)[32].	R
	Matroska (.mkv)	R
	Áudio e vídeo MPEG-4, Part 14 (.mp4)[33].	R
Compactação de ficheiros	ZIP (.zip)	R
	GNU ZIP (.gz).	R
	Pacote TAR (.tar)	R
Informações georreferenciadas	GML versão 2.0 ou superior[34].	O
	ShapeFile[35].	O
	GeoTIFF[36].	O
	GeoJSON, como definido em http://www.geojson.org/geojsonspec. Html	R

6.4 Organização e Troca de Informação – Segmento 4

Aborda os aspetos relativos ao tratamento e à transferência de informação nos serviços de governo eletrónico. Inclui normas de vocabulários controlados, taxonomias, ontologias e outros métodos de organização e recuperação de informações.

---

[27] http://www.pdfa.org/competence-centers/pdfa-competence-center/

[28] No caso de texto plano "txt" e "csv", deve ser incluído o leiaute dos campos, de forma a possibilitar o seu tratamento.

[29] *Scalable Vector Graphics* (SVG) 1.1 *Specification*. W3C Recommendation 14 January 2003. Disponível em: http://www.w3.org/TR/2003/REC-SVG11-20030114/.

[30] JPEG *File Interchange Format* (version 1.02) 1 September 1992. Disponível em: http://www.jpeg.org/public/jfif.pdf

[31] Xiph.Org Foundation. Especificação disponível em: http://xiph.org/vorbis/doc/Vorbis_I_spec.html.

[32] Theora. Especificação disponível em: http://www.theora.org/.

[33] ISO/IEC 14496-14:2003 – *Information Technology – Coding of audio-visual objects* – Part 14: MP4 file format.

[34] *Geography Markup Language*. Especificações disponíveis em: http://www.opengeospatial.org/standards/gml. Indicado para estruturas vetoriais complexas, envolvendo primitivas geográficas como polígonos, pontos, linhas, superfícies, coleções, e atributos numéricos ou textuais sem limites de número de caracteres.

[35] ESRI *Shapefile Technical Description*. Disponível em: http://www.esri.com/library/whitepapers/pdfs/shapefile.pdf. Indicado para estruturas vetoriais limitadas a linhas, pontos e polígonos, cujos atributos textuais não ultrapassem 256 caracteres. Pode armazenar também as dimensões M e Z.

[36] GeoTIFF *Format Especification*. Disponível em: http://remotesensing.org/geotiff/geotiff.html. Indicado para estruturas matriciais limitadas a matrizes de pixel.

6.4.1 Especificações Técnicas

Tabela 13: Tratamento e transferência de Dados

Componente	Especificação	Situação
Linguagem para troca de dados	XML (*Extensible Markup Language*) como definido pelo W3C http://www.w3.org/XML	O
	JSON (*Javascript Object Notation*) Como definido pela IETF http://www.ietf.org/rfc/rfc4627.txt	O
	CSV (*Comma-Separated Values*), conforme definido pela IETF no RFC 4180	O
Transformação de dados	XSL (Extensible Stylesheet Language) como definido pelo W3C http://www.w3.org/TR/xsl XSL Transformation (XSLT) como definido pelo W3C http://www.w3.org/TR/xslt	O
Definição dos dados para troca	XML Schema como definido pelo W3C: – XML Schema Part 0: Primer http://www.w3.org/TR/2004/REC-xmlschema-0-20041028/ – XML Schema Part 1: Structures http://www.w3.org/TR/xmlschema-1/structures – XML Schema Part 2: Datatypes http://www.w3.org/TR/xmlschema-2/datatypes	O
Especificação para informações de transporte público	GTFS (*General Transit Feed Specification*) como definido em https://developers.google.com/transit/gtfs/	R
Especificação para informações de transporte público em tempo real	GTFS-Realtime como definido em https://developers.google.com/transit/gtfs-realtime/	R

Tabela 14: Especificações para Organização e Troca de Informação – Vocabulários e Ontologias

Componente	Especificação	Situação
Descrição de recursos	RDF (*Resource Description Framework*) como definido pela W3C.	R
Sintaxe RDF	• JSON-LD, como definido em http://www.w3.org/TR/json-ld/ • Turtle, como definido em http://www.w3.org/TR/turtle/ • RDFa Primer, como definido em http://www.w3.org/TR/rdfa-primer/	R
Especificação de vocabulários para RDF	*Resource Description Framework* (RDF) *Schema*, como definido pelo W3C em http://www.w3.org/TR/rdf-schema/	R
Vocabulários	Lista de vocabulários recomendados pela W3C como definido em http://www.w3.org/2011/rdfacontext/rdfa-1.1	R
Sistemas de Organização do Conhecimento	SKOS (*Simple Knowledge Organization System*) como definido pelo W3C http://www.w3.org/2004/02/skos/	R
Linguagem de definição de ontologias na web	OWL (*Web Ontology Language*) Como definido pelo W3C	R
Linguagem de consulta semântica	SPARQL (*Sparql Protocol and RDF Query Language*) como definido pelo W3C	R

6.5 Áreas de Integração para Governo Eletrónico – Segmento 5

Estabelece a utilização ou construção de especificações técnicas para sustentar a troca de informação em áreas transversais da atuação governamental, cuja padronização seja relevante para a interoperabilidade de serviços de governo eletrónico, tais como Dados e Processos, Informações Contábeis, Geográficas, Estatísticas e de Desempenho, entre outras.

6.5.1 Especificações Técnicas

Tabela 15: Temas Transversais às Áreas de Atuação de Governo

Componente	Especificação	Situação
PROCESSOS – Linguagem para Execução de Processos	BPEL4WS V1.1, conforme definido pelo OASIS http://www.oasisopen.org/committees/download.php/2046/BPEL%20V1-1%20May%205%202003%20Final.pdf	R
PROCESSOS – Notação de Modelagem de Processos	BPMN – *Business Process Model and Notation* versão 1.2, definido pelo OMG http://www.omg.org/spec/BPMN/1.2/	O
	BPMN – *Business Process Model and Notation* versão 2.0, definido pelo OMG http://www.omg.org/spec/BPMN/2.0/	R
Troca de Informação Financeira	XBRL – *eXtensible Business Reporting Language* http://www.xbrl.org/SpecRecommendations/	O
Legislação, Jurisprudência e Proposições Legislativas	LexML v. 1.0[37] http://projeto.lexml.gov.br	O
Informações Georreferenciadas – Interoperabilidade entre sistemas de informação geográfica	WMS versão 1.0 ou posterior http://www.opengeospatial.org/standards/wms	O
	WFS versão 1.0 ou posterior http://www.opengeospatial.org/standards/wfs	O
	WCS versão 1.0 ou posterior http://www.opengeospatial.org/standards/wcs	O
	CSW versão 2.0 ou posterior http://www.opengeospatial.org/standards/cat	O
	WFS-T versão 1.0 ou posterior[38] http://www.opengeospatial.org/standards/wfs	R
	WKT[39] http://www.opengeospatial.org/standards/sfa	R
	Filter Encoding versão 1.0 ou posterior[40] http://www.opengeospatial.org/standards/filter	O
	Symbology Encoding versão 1.1.0 ou posterior[41] http://www.opengeospatial.org/standards/se	R
Troca de Dados Estatísticos	SDMX – Statistical Data and Metadata Exchange http://sdmx.org/wpcontent/uploads/2011/04/SDMX_2-1_SECTION_1_Framework.pdf	R

Tabela 16: *Web Services*

Componente	Especificação	Situação
Infraestrutura de registo	Especificação UDDI v3.0.2 (*Universal Description, Discovery and Integration*) definida pela OASIS http://uddi.org/pubs/uddi_v3.htm	R
	ebXML (*Electronic Business using eXtensible Markup Language*). A especificação pode ser encontrada em http://www.ebxml.org/specs/index.htm	R
Linguagem de definição do serviço	WSDL 1.1 (*Web Service Description Language*) como definido pelo W3C. A especificação pode ser encontrada em http://www.w3.org/TR/wsdl	O
	WSDL 2.0 (*Web Service Description Language*) como definido pelo W3C. A especificação pode ser encontrada em	R

[37] Projeto LexML define recomendações para a identificação e estruturação de documentos legislativos e jurídicos.

[38] Observar padrões e políticas de segurança indicados pelo Segmento Segurança, principalmente WS-Security.

[39] Para codificar coordenadas em serviços Web convencionais. As coordenadas devem estar em Lat/Long utilizando o datum SIRGAS2000 (EPSG:4674) ou WGS-84 (EPSG:4326). Usar GML sempre que possível.

[40] Especificação acessória para codificar expressões de filtro

[41] Para codificar estilos em mapas

	http://www.w3.org/TR/wsdl20/	
Protocolo para acesso a Web Service	SOAP v1.2, como definido pelo W3C http://www.w3.org/TR/soap12-part1/ http://www.w3.org/TR/soap12-part2/ Especificações do protocolo SOAP podem ser encontradas em http://www.w3.org/TR/soap12-part0/	O
	HTTP/1.1 (RFC 2616)[42]	O
Perfil básico de interoperabilidade	Basic Profile 2.0 Second Edition, como definido pela WS-I http://ws-i.org/Profiles/BasicProfile-2.0-2010-11-09.html	R
Portlets remotos	WSRP 1.0 (*Web Services for Remote Portlets*) como definido pela OASIS http://www.oasis-open.org/committees/wsrp	R

Tabela 17: Arquitetura Corporativa

Componente	Especificação	Situação
Linguagem de modelagem	ArchiMate versão 3 http://pubs.opengroup.org/architecture/archimate3-doc/	R

[42] Utilizado para desenvolvimento de projetos baseados em REST.

7. Glossário de Siglas e Termos Técnicos

Apresentan-se de seguida os significados dos principais termos técnicos utilizados no QNI. Os termos encontram-se organizados por ordem alfabética.

***Browser* (navegador) –** Programa de computador que habilita seus utilizadores a interagirem com documentos virtuais da Internet, também conhecidos como páginas da web. Como exemplo de *browser* temos o Google Chrome, o Microsoft Edge e o Mozilla Firefox.

Criptografia – Técnica de proteção de informação que consiste em cifrar o conteúdo de uma mensagem ou um sinal, transformando-o em um texto ilegível, por meio da utilização de algoritmos matemáticos complexos.

***Handshake* –** Em uma comunicação via telefone, troca de informações entre dois modems e o resultante acordo sobre que protocolo utilizar antes de cada conexão telefónica.

***Hashing* –** Transformação de uma cadeia de caracteres em um valor de tamanho fixo normalmente menor ou em uma chave que representa a cadeia original. É utilizada para indexar e recuperar itens em uma base de dados, porque é mais rápido encontrar o item utilizando a menor chave transformada do que o valor original. Também é utilizada em algoritmos de criptografia.

IEEE – ***Institute of Electrical and Electronics Engineers*** (Instituto de Engenheiros Elétricos e Eletrónicos) – Fomenta o desenvolvimento de padrões e normas que frequentemente se tornam nacionais e internacionais.

IETF – ***Internet Engineering Task Force*** (Força Tarefa de Engenharia da Internet) – Entidade que define protocolos operacionais padrão da Internet, como o TCP/IP.

LAN – ***Local Area Network*** **(Rede Local) –** Grupo de computadores e dispositivos associados que compartilham uma mesma linha de comunicação e normalmente recursos de um único processador ou servidor em uma pequena área geográfica. Normalmente, o servidor possui aplicações e armazenamento de dados compartilhados por vários utilizadores em diferentes computadores.

Mensagens em Tempo Real ou Mensagem Instantânea – Tipo de comunicação que permite que um utilizador troque mensagens em tempo real com outro utilizador também conectado à rede.

Metadados – Conhecido como "dados sobre dados", metadados são utilizados para registar atributos sobre um recurso informacional visando facilitar a recuperação, a gestão a interoperabilidade, dar suporte à identificação digital e dar suporte ao arquivamento e preservação.

***Middleware* –** Termo geral que serve para mediar dois programas separados e normalmente já existentes. Aplicações diferentes podem comunicar-se através do serviço de *Messaging*, proporcionado por programas *middleware*.

OGC – *Open Geospatial Consortium* (consórcio internacional *Open Geospatial*) – Possui a missão de "desenvolver especificações para interfaces espaciais que serão disponibilizadas livremente para uso geral".

Ontologia – Na filosofia, ontologia é o estudo da existência ou do ser enquanto ser, ou seja, a maneira de compreender as identidades e grupos de identidades. Na ciência da computação, é um modelo de dados que representa um conjunto de conceitos sob um domínio e seus relacionamentos, ou, mais formalmente, especifica uma conceitualização dele.

RFC – *Request for Comments* (Solicitação de Comentários) – Documento formal da IETF, resultante de modelos e revisões de partes interessadas. A versão final do RFC tornou-se uma norma em que nem comentários nem alterações são permitidos. As alterações podem ocorrer, porém, por meio de RFCs subsequentes que substituem ou elaboram em todas as partes dos RFCs anteriores.

W3C – *World Wide Web Consortium* (Consórcio da Rede Mundial *Web*) – Associação de indústrias que visa promover padrões para a evolução da *web* e interoperabilidade entre produtos para WWW produzindo softwares de especificação e referência.

WAN – *Wide Area Network* (Rede de Grande Área) – Rede de computadores que abrange extensas áreas geográficas como um estado, um país ou um continente.

***Web Services* –** Aplicação lógica, programável, que torna compatíveis entre si os mais diferentes aplicativos, independentemente do sistema operacional, permitindo a comunicação e troca de dados entre diferentes redes.

UNITED NATIONS
UNIVERSITY

UNU-EGOV

Operating Unit on Policy-Driven
Electronic Governance

UNU-EGOV
Campus de Couros,
Rua de Vila Flor 166
4810-445 Guimarães,
Portugal

egov.unu.edu
egov@unu.edu
+351 253 510 850