Segunda - feira, 29 de Janeiro de 2024

Número 07
I SÉRIE

SÃO TOMÉ E PRÍNCIPE

DIÁRIO DA REPÚBLICA

SUMÁRIO

ASSEMBLEIA NACIONAL

Lei n.º 01/2024

Quadro Nacional de Interoperabilidade

Preâmbulo

O Quadro Nacional de Interoperabilidade (QNI) é concebido como uma estrutura básica para a estratégia de governação electrónica aplicada a toda a Administração Pública de São Tomé e Príncipe e abrange todos os poderes do Estado, sem restringir a participação, por adesão voluntária, de outras organizações.

Um Quadro Nacional de Interoperabilidade consiste num acordo interorganizacional, em que é definido um conjunto de políticas, normas técnicas e orientações, e serve como uma ferramenta para alcançar a interoperabilidade de sistemas de informação e de serviços do sector 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 electrónico, estabelecendo as condições de interacção com os demais poderes, esferas do Governo e com a sociedade em geral.

Para alcançar tal objectivo, é crucial a elaboração de um instrumento normativo para a governação que permita a adopção do QNI em São Tomé e Príncipe.

No contexto do Projecto de Aceleração da Transição Digital em São Tomé e Príncipe, no âmbito do Programa de Modernização do Sistema de Justiça, desenvolvido conjuntamente pelo Programa das Nações Unidas para o Desenvolvimento (PNUD), São Tomé e Príncipe e pela Unidade Operacional em Governação Electrónica 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, foram realizadas interacções com diversos actores-chave de todos os sectores governamentais de São Tomé e Príncipe, tanto no formato de entrevistas com pontos focais de 12 departamentos governamentais, como via Workshop presencial, em que participaram todas as entidades envolvidas no desenvolvimento do Projecto.

Durante os processos de interacções institucionais, foram identificadas e definidas as características desejadas para o instrumento normativo ora apresentado, em especial o nível hierárquico do instrumento, sendo prevalecente o entendimento que deveria tratar-se de uma lei aprovada pela Assembleia Nacional, de maneira a garantir a sua observância por todas as esferas de poder instaladas na República Democrática de São Tomé e Príncipe.

A Assembleia Nacional decreta, nos termos da alínea b) do artigo 97.º da Constituição, o seguinte:

Artigo 1.°
Objecto

A presente Lei institui o Quadro Nacional de Interoperabilidade (QNI) de São Tomé e Príncipe, doravante designado por QNI, que define um conjunto mínimo de premissas, políticas e especificações técnicas que regulamentam a utilização de Tecnologias de Informação e Comunicação (TIC) na interoperabilidade dos serviços de governo electrónico.

Artigo 2.°
Âmbito de aplicação

1. O QNI é aplicável a todas as instituições públicas e abrange todos os poderes do Estado, sem restringir a participação, por adesão voluntária, de outras organizações.

2. Para efeitos da presente Lei, são instituições públicas as pessoas colectivas de direito público, a administração directa, indirecta e autónoma do Estado.

Artigo 3.°
Comité de Coordenação e Gestão

1. É criado o Comité de Coordenação e Gestão (CCG) do QNI, com responsabilidade e autoridade para supervisionar e tomar decisão relativamente ao desenvolvimento e gestão contínua do Quadro Nacional de Interoperabilidade.

2. Compete ao CCG:

a) Definir as orientações, especificações técnicas do QNI e propor as políticas a serem adoptadas;

b) Liderar o processo de revisão e actualização futuras do QNI, providenciando a infra-estrutura de gestão necessária para suportar todo o processo, bem como deliberar sobre eventuais ajustes que decorram da revisão e actualização;

c) Elaborar e divulgar orientações técnicas, nomeadamente na forma de manuais e outros materiais de instrução;

d) Definir objectivos, identificar projectos, promover a colaboração entre os organismos da Administração Pública e propor medidas relativas à implementação do QNI;

e) Dar parecer e informações sobre questões relacionadas com a adopção e a conformidade com o QNI por organismos da Administração Pública;

f) Constituir e apoiar a actividade dos grupos de trabalho para a elaboração de propostas, directrizes e especificações técnicas, de acordo com a necessidade;

g) Disponibilizar e manter actualizados os recursos associados ao QNI: páginas, catálogos, gestão de comunidades, respostas às consultas públicas realizadas e outros serviços e informações relacionados;

h) Instigar a partilha e a cooperação técnica nacional e internacional na área de normas de interoperabilidade; e

i) Promover iniciativas de divulgação e de capacitação de funcionários públicos para a aplicação do QNI.

3. A composição, funcionamento e coordenação do CCG é definido por despacho conjunto do Ministro encarregado da área de Tecnologia e de Administração Pública.

Artigo 4.°
Comité Técnico de Interoperabilidade

1. É instituído o Comité Técnico de Interoperabilidade (CTI), cuja função é acompanhar, supervisionar e coordenar o apoio técnico para a implementação e cumprimento dos regulamentos e legislação associada ao QNI.

2. O CTI é presidido pelo representante indicado pelo CCG.

3. Compete ao CTI:

a) Garantir o valor do QNI como um «activo colectivo», com apoio à capacitação e ao desempenho dos organismos do sector público, fomentando uma cultura de interoperabilidade na Administração Pública de São Tomé e Príncipe;

b) Assegurar a manutenção e o aprimoramento do QNI ao longo do tempo, em alinhamento com as necessidades de todas as entidades que o utilizem;

c) Actuar para que os benefícios que possam ser aportados pelo QNI, de maior capacidade, desempenho, eficiência e eficácia de cada organismo do sector público, superem os custos associados;

d) Promover o desenvolvimento das estratégias, iniciativas e práticas dos organismos do sector público, em conformidade com as normas e recomendações do QNI.

4. O CTI é composto por cinco técnicos com valências na área de Tecnologia de Informação e Comunicação como se discrimina:

a) Dois indicados pelo Ministro encarregado da área de tecnologias;

b) Um indicado pelo Ministro encarregado da área da Administração Pública;

c) Um indicado pela associação representativa das Autarquias;

d) Um indicado pela Câmara de Comércio.

5. O CTI deve apresentar e publicar, em formato digital, o Relatório Anual de Acções de Interoperabilidade Digital, com detalhamento de sua actuação.

Artigo 5.°
Modelo e processo de revisão

1. É instituído o modelo do QNI no formato do anexo 1 da presente Lei, que dela é parte integrante.

2. O QNI deve ser revisto a cada intervalo de 3 anos, sem prejuízo de alterações técnicas pontuais às tabelas que o integram, sempre que tal se justifique pela evolução das normas técnicas, que são aprovadas pelo Comité Técnico de Interoperabilidade.

3. As propostas de alteração ao QNI são submetidas à consulta pública, que é conduzida pelo Comité de

Coordenação e Gestão do Quadro Nacional de Interoperabilidade.

Artigo 6.°
Norma transitória

Os actuais sistemas de apoio à prestação dos serviços públicos continuam válidos até que sejam actualizados ou substituídos para estarem em conformidade com o Quadro Nacional de Interoperabilidade.

Artigo 7.°
Entrada em vigor

A presente Lei entra em vigor 30 dias após a sua publicação no Diário da República.

Assembleia Nacional, em São Tomé, aos 03 de Novembro de 2023.- A Presidente da Assembleia Nacional, *Celmira de Almeida do Sacramento dos Santos Lourenço.*

Promulgada em 30 de Novembro de 2023. - O Presidente da República, *Carlos Manuel Vila Nova.*

ANEXO

O QNI 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 Electrónico" - estão subdivididos em componentes, para as quais foram estabelecidas as especificações técnicas a serem adoptadas pelos órgãos governamentais abrangidos pelo QNI.

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

Obrigatório (O): item adoptado 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 adoptados em novos produtos/projectos 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 do Governo, mas ainda não foi submetido a um processo formal de homologação. Os componentes de nível Recomendado não são obrigatórios, porém sugeridos para adopção em novos produtos/projectos de TI;

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

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 aos serviços nela disponíveis. O segmento estabelece as condições para que as redes dos órgãos do Governo se possam interligar e, assim, promover a interoperabilidade.

Tabela 1: Aplicação [1]

Componente	Especificação	Situação
Transporte de mensagem eletrócnica	Utilizar produtos de mensagem electrónica 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 (actualizada 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 actualizada 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 (actualizada pela RFC 2228, RFC 2640, RFC 2773, RFC 3659 e RFC 5797) e HTTP conforme RFC 2616 (actualizada 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[2]**.**	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

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

[2] O Simple Network Time Protocol-SNTP version 4.0 está definido na secção 14 da RFC 5905.

Protocolo de troca de informações estruturadas em plataforma descentralizada e/ou distribuída	Ver Tabela 17 – Especificações para a Área de Integração para Governo Electrónico – 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-D-001_R6-sdn_standard-roadmap_31082017.docx	R
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 1: 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 adoptar interface NNI (Option A) entre a Rede do Governo e a Rede Pública.	O
Qualidade de serviço	Adoção de uma arquitectura para serviços diferenciados pelo uso do Diffserv (RFC 2475, atualizada pela RFC 3260).	O

Tabela 2: 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

Segurança – Segmento 2

Trata dos aspectos de segurança de TIC que o Governo deve considerar.

i. 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 adopção 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 adopção 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 actualizada 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 correcta dos meios de acesso.

ii. 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[3] 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	O S/MIME v3, RFC 5751[4] deverá ser utilizado quando for apropriado para segurança de mensagens gerais do Governo.	O

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

[4] Consultar errata para RFC 5751.

aplicação		-
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[5].	R

Tabela 5: Correio Electrónico

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)[6], 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 do Governo. Isso inclui RFC 5652, RFC 3370	O

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

[6] Consultar errata para a RFC 2595.

	(atualizada pela RFC 5754), RFC 2631, RFC 5750, RFC 5751 e RFC 5652[7].	
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[8].	O
Identificação de e-mail	Utilizar DKIM (*DomainKey Identified Mail*) nos termos da RFC 6376[9] 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[10].	R

Tabela 6: Criptografia

Componente	Especificação	Situação
Algoritmo de cifração	3DES ou AES	R
Algoritmo para assinatura/*hashing*	SHA-256 ou SHA-512[11]	R
	SHA-224 ou SHA-238	R
Algoritmo para transporte de chave criptográfica de conteúdo/sessão	RSA	O
Algoritmos criptográficos baseados em curvas	ECDSA 256 e ECDSA 512 (RFC 5480)[12].	O

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

[8] Consultar errata para RFC 4408.

[9] Consultar errata para RFC 4871.

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

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

elípticas	ECIES 256 e ECIES 512.	
	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	WS-Security 1.1 – arcabouço de padrões para garantir integridade e confidencialidade em mensagens SOAP.	R

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

de Identidades	(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-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[13]. 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)[14]	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)[15].	R
Prevenção de DDoS	Usar métodos para inibir o uso de *IP spoofing* em ataques de DDoS nos termos do RFC 2827[16].	R

Tabela 9: Redes Sem Fio

Componente	Especificação	Situação
MAN[17] sem fio 802.16-2004[18]	Utilizar PKM-EAP (*Privacy Key Management – Extensible Autentication Protocol*) com: • EAP – TLS ou TTLS;	R

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

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

[15] Consultar errata para RFC 3161.

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

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

802.16.2-2004[19] · 802.16e[20] e 802.16f[21]	• AES[22] (*Advanced Encryption Standard*).	
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[23] http://datatracker.ietf.org/doc/rfc5070/	R

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

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

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

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

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

[23] 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[24] 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

Meios de Acesso – Segmento 3

São explicitadas as questões relativas aos padrões dos dispositivos de acesso aos Serviços do Governo Electrónico.

i. Especificações Técnicas

Tabela 12: Meios de Publicação

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

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[25]	O
	EPUB 3.0.1 http://idpf.org/epub/301	R
	Portable Document Format - PDF ISO 32000-1:2008	R
	Portable Document Format - PDF/A ISO 19005-1:2005[26], quando necessária a preservação	R

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

	digital de documentos	
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[27]	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[28].	R
	JPEG File Interchange Format (.jpeg, .jpg ou .jfif)[29].	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)[30].	R
	Ogg FLAC (.ogg, .oga)	R
	FLAC (.flac)	R

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

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

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

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

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

Vídeo	Ogg Theora (.ogg, .ogv)[31].	R
	Matroska (.mkv)	R
	Áudio e vídeo MPEG-4, Part 14 (.mp4)[32].	R
Compactação de ficheiros	ZIP (.zip)	R
	GNU ZIP (.gz).	R
	Pacote TAR (.tar)	R
Informações georreferenciadas	GML versão 2.0 ou superior[33].	O
	ShapeFile[34].	O
	GeoTIFF[35].	O
	GeoJSON, como definido em http://www.geojson.org/geojsonspec. Html	R

Organização e Troca de Informação – Segmento 4

Aborda os aspetos relativos ao tratamento e à transferência de informação nos Serviços do Governo Electrónico. Inclui normas de vocabulários controlados, taxonomias, ontologias e outros métodos de organização e recuperação de informações.

i. Especificações Técnicas

Tabela 13: Tratamento e transferência de Dados

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

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

[33] *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.

[34] 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.

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

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: Especificação 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

Área de Integração para Governo Electrónico – Segmento 5

Estabelece a utilização ou construção de especificações técnicas para sustentar a troca de informação em áreas transversais da actuação governamental, cuja padronização seja relevante para a Interoperabilidade de Serviços do Governo

Electrónico, tais como Dados e Processos, Informações Contábeis, Geográficas, Estatísticas e de Desempenho, entre outras.

i. Especificações Técnicas

Tabela 15: Temas Transversais às Áreas de Actuação do 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[36] http://projeto.lexml.gov.br	O
Informações Georreferenciadas – Interoperabilidade entre sistemas de informação	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

[36] Projecto LexML define recomendações para a identificação e estruturação de documentos legislativos e jurídicos.

geográfica	CSW versão 2.0 ou posterior http://www.opengeospatial.org/standards/cat	O
	WFS-T versão 1.0 ou posterior[37] http://www.opengeospatial.org/standards/wfs	R
	WKT[38] http://www.opengeospatial.org/standards/sfa	R
	Filter Encoding versão 1.0 ou posterior[39] http://www.opengeospatial.org/standards/filter	O
	Symbology Encoding versão 1.1.0 ou posterior[40] 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.	O

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

[38] 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.

[39] Especificação acessória para codificar expressões de filtro

[40] Para codificar estilos em mapas

	A especificação pode ser encontrada em http://www.w3.org/TR/wsdl	
	WSDL 2.0 (*Web Service Description Language*) como definido pelo W3C. A especificação pode ser encontrada em http://www.w3.org/TR/wsdl20/	R
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)[41]	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

[41] Utilizado para desenvolvimento de projectos baseados em REST.