PROGRAMA REGIONAL DE INTEGRAÇÃO DIGITAL DA ÁFRICA OCIDENTAL DA GUINÉ-BISSAU

O GOVERNO DA GUINÉ-BISSAU

PROGRAMA REGIONAL DE INTEGRAÇÃO DIGITAL DA ÁFRICA OCIDENTAL SOP1

SERVIÇOS DE CONSULTORIA PARA ESTUDO DE VIABILIDADE PARA O DESENVOLVIMENTO DE UM QUADRO DE INTEROPERABILIDADE, CAMADA DE TROCA DE DADOS E PLATAFORMA DE SERVIÇOS E PLANO DE AÇÃO PARA A DIGITALIZAÇÃO DOS PRINCIPAIS SERVIÇOS PÚBLICOS

QUADRO DE INTEROPERABILIDADE, PLATAFORMA DE INTEROPERABILIDADE E ARQUITETURA EMPRESARIAL

Apresentado por:
DevEmerge Global Consultancy Private Limited, India em consórcio com JV with Qualisys Consulting Limited, Senegal

INFORMAÇÕES DO PROJETO

Projeto	Estudo de Viabilidade para o Desenvolvimento de um Quadro de Interoperabilidade, Camada de Troca de Dados e Plataforma de Serviços e Plano de Ação para a Digitalização dos Principais Serviços Públicos
Cliente	Programa Regional de Integração Digital da África Ocidental Guiné-Bissau (WARDIP – Guiné-Bissau)
País	Guiné-Bissau
Duração do projeto	Fevereiro – Julho de 2024
Nome do Documento	Estrutura de interoperabilidade, plataforma de interoperabilidade e arquitetura empresarial
Versão do documento	2.0
Data da versão	31 de Julho de 2024
Histórico de Revisão	Versão 1.0 Documento em Rascunho 12 de Abril de 2024

AGRADECIMENTO

A DevEmerge Global e a Qualisys Consulting agradecem sinceramente ao Programa Regional de Integração Digital da África Ocidental (WARDIP), ao Banco Mundial, ao Instituto Tecnológico para a Modernização Administrativa (ITMA), ao Ministério dos Transportes, Telecomunicações e Economia Digital (MTTDE) e à Autoridade Reguladora Nacional (RNA), pela seleção dos serviços do nosso Consórcio para realizar o "Estudo de Viabilidade para o Desenvolvimento de um Quadro de Interoperabilidade, Camada de Intercâmbio de Dados e Plataforma de Serviços e Plano de Ação para a Digitalização dos Principais Serviços Públicos na Guiné-Bissau".

A equipa de consultoria expressa a mais profunda gratidão e apreço a todas as partes interessadas que forneceram apoio, sem o qual o estudo não teria sido realizado.

Agradecemos especialmente às equipas WARDIP, ITMA e MTTDE, por suportarem este estudo de viabilidade e nos guiarem em todas as etapas que foi necessário suporte administrativo e operacional. Agradecemos todas as informações e apoio por parte de todas as partes interessadas chave.

INDÍCE

LISTA DE MESAS

LISTA DE FIGURAS

ACRÓNIMOS E ABREVIATURAS

ADM	Método de desenvolvimento de arquitetura
API	Interface de programação de aplicativos
BPA	Análise de processos de negócios
BPEL	Linguagem de execução de processos de negócios
BPM	Gestão de processos de negócios
BPMN	Notação de linguagem de modelagem de processos de negócios
BRS	Especificações de requisitos de negócios
CA	Autoridade Certificadora
CFE	Centro De Formalizacao de Emprego
CIA	Confidencialidade, integridade e disponibilidade da
CIAN	Confidencialidade, integridade, disponibilidade e não repúdio da
DFS	Serviço Financeiro Digital
DSS	Padrões de serviço digital
EA	Arquitetura Empresarial
eGIF -GW	eGovernment Interoperability Framework para Guiné-Bissau
eID	Identificação eletrónica
ERP	Planejamento de recursos empresariais de
G2B	Governo 2 Negócios
G2C	Governo 2 Cidadãos
G2G	Governo 2 Governo
GoGB	Governo da Guiné Bissau
IAM	Gestão de identidade e acesso
TIC	Tecnologia de Informação e Comunicação
IM	Mediador de informações de
ITMA	Instituto Tecnológico de Modernização Administrativa
MDA	Ministérios, Departamentos e Agências do
MTTDE	Ministério dos Transportes, Telecomunicações e Economia Digital
OOP	Uma Vez
PDPRM	Modelo de referência da plataforma digital pública
PKI	Infraestrutura de chave pública
QoS	Qualidade de Serviços de
SOA	Arquitetura Orientada a Serviços
SRS	Especificações de requisitos do sistema
TOGAF,	a estrutura de arquitetura de grupo aberto
TWG	Grupo de trabalho técnico do

SUMÁRIO EXECUTIVO

A Guiné-Bissau tem um elevado potencial para a transformação digital, a qual poderá transformar todas as partes do país através implementação de soluções digitais eficientes, transparentes, eficazes, oportunas e integradas. Ter um quadro denominado "Quadro de Interoperabilidade do Governo Eletrónico para a Guiné-Bissau (eGIF-GW)" é um passo essencial para alcançar uma transformação digital geral do governo para serviços públicos.

O Governo da Guiné-Bissau (GoGB) recebeu apoio financeiro do Banco Mundial para implementar o Programa Regional de Integração Digital da África Ocidental (WARDIP). O objetivo geral do WARDIP é apoiar os países da África Ocidental no desenvolvimento conjunto de um mercado digital único, reforçando, conforme necessário, aspetos específicos do ambiente necessário, como as competências digitais e o ambiente de inovação. O objetivo do WARDIP é apoiar a Guiné-Bissau a desenvolver-se como uma economia digital e garantir um ambiente propício à transformação digital, promovendo a inovação e a competitividade no mercado digital regional único.

Um mercado único online permitirá que governos, empresas e indivíduos tenham acesso e forneçam serviços públicos e privados online, bem como façam vendas e compras online sem restrições a partir de qualquer lugar da região. Os principais facilitadores da camada online são os serviços financeiros digitais (DFS), o quadro de interoperabilidade e as assinaturas eletrónicas como parte da Infraestrutura de Chave Pública (PKI).

A interoperabilidade permite que diversos sistemas desenvolvam uma compreensão sobre certos dados específicos num determinado domínio, sem a qual os sistemas não podem interpretar e utilizar dados para atingir objetivos comuns. Na verdade, o eGIF-GW é uma parte importante das atividades de construção da Arquitetura Empresarial (EA) do governo da Guiné-Bissau, a qual fornece a estrutura dos componentes do governo eletrónico, as suas inter-relações e os princípios e diretrizes que regem o seu desenho e evolução ao longo do tempo.

Os benefícios esperados do eGIF-GW são: relação custo-benefício, troca contínua de dados, transparência de processos, infraestrutura partilhada, disciplina tecnológica, segurança da informação, concorrência saudável e minimização de custos.

Os princípios do eGIF-GW são:

- Padronização de Sistemas de TI. Os sub-princípios são: abertura, reutilização, transparência e portabilidade.
- Integração de processos de negócios. Os sub-princípios são: segurança e privacidade.
- Eficiência na prestação de serviços. Os sub-princípios são: flexibilidade, acessibilidade, escalabilidade e heterogeneidade.
- Design Centrado no Utilizador
- Soberania, residência e localização dos dados
- Integração, Escalabilidade e Flexibilidade

Os fatores críticos para a verificação de interoperabilidade na prestação de serviços públicos e administrativos integrados entre os MDAs são: "Identificação de Processos"; "Conformidade com Padrões"; "Colaboração de Sistemas de TI"; e "Instituição de Estrutura Legal", sendo também evidente que que termos gerais, fatores humanos e tecnológicos são fundamentais para alcançar resultados significativos na interoperabilidade dos sistemas informáticos.

1. QUADRO DE INTEROPERABILIDADE

1.1 Introdução

Um Quadro é um elemento fundacional que dá suporte a uma entidade mais relevante. Por outro lado, a interoperabilidade de acordo com o Quadro Europeu de Interoperabilidade (QIR) [1]é definida pela União Europeia como "*a capacidade das organizações interagirem no sentido de objetivos mutuamente benéficos, envolvendo a partilha de informação e conhecimento entre estas organizações, através dos processos de negócio que os suportam, através do intercâmbio de dados entre os seus sistemas TIC.*". No entanto, no contexto deste documento, a interoperabilidade é definida como a capacidade de diversos sistemas de informação (SI) geridos por várias organizações ou MDAs se inter-relacionarem através da comunicação, interpretação e troca de informações de uma forma impactante para fornecer serviços públicos que envolvem vários MDAs ou organizações, de forma integrada e coesa.

Os guineenses aproveitam cada vez mais os dados e as tecnologias digitais para melhorar as suas vidas, mas é necessário mais para soltar as oportunidades do digital. Sendo uma nação pequena, rica em recursos naturais inexplorados, a Guiné-Bissau tem a maior proporção de riqueza natural per capita na região da África Ocidental. Apesar do seu enorme potencial de desenvolvimento – graças às suas terras agrícolas, pescas, florestas e habitats naturais – a Guiné-Bissau continua a ser um dos países menos desenvolvidos do mundo. Isto deve-se em parte à significativa fragmentação e instabilidade política e institucional do país (a Guiné-Bissau é também um dos países mais frágeis do mundo), que dificultam o desenvolvimento e a implementação de reformas políticas tão necessárias[2].

A recentemente concluída Avaliação Nacional da Economia Digital da Guiné-Bissau [3]faz um balanço das conquistas recentes ao longo das cinco áreas fundamentais da economia digital do país – infraestruturas digitais, plataformas públicas, serviços financeiros, negócios e competências – e propõe recomendações priorizadas e sequenciadas para garantir o seu desenvolvimento dinâmico, seguro e inclusivo. Destaca também que a transformação digital pode contribuir muito para resolver vários dos fatores de fragilidade do país, nomeadamente através do reforço da inclusão financeira; desenvolvimento de novas oportunidades de emprego fora do comércio de castanha de caju; e ligar populações vulneráveis (especialmente raparigas e mulheres) à Internet.

A Guiné-Bissau pode orgulhar-se de várias conquistas recentes no domínio da transformação digital, com muitas mais no horizonte. Por exemplo, esperava-se que a ligação direta do cabo submarino da Costa Africana à Europa (ACE) do país fosse entregue em novembro de 2022 (embora entregue, mas ainda não operacional à data deste relatório devido à não comercialização do SCGB – Sociedade de Cabos da Guiné-Bissau), juntamente com um ponto de troca de Internet, devendo ambos conduzir a uma diminuição significativa no preço retalhista do acesso e utilização da Internet de banda larga.

As principais funções governamentais estão a tornar-se digitalizadas e os guineenses podem agora declarar e pagar os seus impostos online, através da plataforma KONTAKTU[4]. Nos últimos dois anos, o número e a quantidade de transações de dinheiro móvel aumentaram mais rapidamente na Guiné-Bissau do que em qualquer outro país da União Económica e Monetária da África Ocidental (UEMOA). O cenário emergente de empreendedorismo digital do país está a crescer e o seu principal centro de inovação e tecnologia, o InnovaLab, está a trazer o dinamismo do setor privado para o setor público.

A partir destas conquistas e esforços orientados para alcançar a transformação digital no país, podemos constatar que a Guiné-Bissau tem um elevado potencial para a transformação digital poder transformar

[1] https://ec.europa.eu/isa2/sites/isa/files/eif_brochure_final.pdf
[2] https://blogs.worldbank.org/en/digital-development/digitalizing-guinea-bissau-future-starts-now
[3] https://documents.worldbank.org/en/publication/documents-reports/documentdetail/099745006262216743/p177016084979202b08dd501a5690c82506
[4] https://kontaktu.mef.gw/?lang=en

todas as partes da vida do país através do fornecimento de soluções digitais, eficientes, transparentes, eficazes, atempadas e integradas. As plataformas públicas digitais servirão como catalisadores para o desenvolvimento de novos segmentos da economia e para a redução do custo de fazer negócios através de maior conveniência e poupança. Ter um quadro denominado "**Quadro de Interoperabilidade do Governo Eletrónico para a Guiné-Bissau (eGIF-GW)** " é um passo essencial para alcançar a criação de plataformas públicas digitais e a transformação digital geral do governo, ao mesmo tempo que se superam obstáculos específicos, tais como a conetividade limitada ou recursos tecnológicos reduzidos.

Na verdade, o eGIF-GW é uma parte importante das atividades de construção da Arquitetura Empresarial (EA) do governo da Guiné-Bissau que fornece a estrutura dos componentes do governo eletrónico, as suas inter-relações e os princípios e diretrizes que regem o seu desenho e evolução ao longo do tempo. A estrutura eGIF-GW específica conceitos, princípios, políticas, recomendações, padrões e práticas para que os MDAs trabalhem em conjunto, no sentido da prestação coletiva de serviços públicos abrangendo todas as agências governamentais. O objetivo do eGIF-GW é garantir que os serviços que requerem dois ou mais processos de negócio das MDAs sejam entregues de forma integrada e a um custo acessível, aproveitando as TIC. Outro objetivo da interoperabilidade e da transformação digital é garantir a melhoria da prestação de serviços públicos aos cidadãos e às empresas, o aumento da eficiência governamental e o impacto positivo na vida dos cidadãos, a promoção da inclusão social e o crescimento económico. Por último, o eGIF-GW reforçará o compromisso com a segurança dos dados e o conformidade com os standards nacionais e internacionais de proteção de dados, essenciais para manter a confiança do público nas plataformas digitais governamentais.

1.1.1 Objetivo e benefícios

A interoperabilidade permite que diversos sistemas desenvolvam uma compreensão sobreposta de dados específicos de uma determinada área. Sem interoperabilidade, os sistemas não podem interpretar e utilizar dados para atingir objetivos comuns. Por exemplo, os médicos do Ministério da Saúde da Guiné-Bissau não podem utilizar dados de imagem diretamente de aparelhos de ressonância magnética ao mesmo tempo que realizam o processo de atualização do registo de saúde de um paciente sem um quadro comum de troca de dados.

O objetivo do eGIF-GW compreende:

- Estrutura de base: A estrutura serve como base com a qual todos os sistemas de informação (SI) pertencentes e geridos por organizações governamentais necessitam de interoperar.
- Padronização de Especificações: A estrutura define um conjunto de especificações padrão e melhores práticas para a implementação de sistemas de informação, a fim de garantir a troca contínua de informações.
- Janela única de prestação de serviços (one-stop shop): O quadro promove a prestação de serviços entre entidades através da implementação de sistemas de informação e garante interações contínuas entre o governo, as empresas e os cidadãos, ao mesmo tempo que aproveita as ferramentas TIC para a prestação de serviços.

Os benefícios esperados do eGIF-GW incluem:

- Custo-benefício: Aumentar a eficiência, a flexibilidade e o valor dos investimentos existentes em sistemas de TI.
- Troca de dados facilitada: Promover a troca perfeita de dados entre MDAs.
- Transparência do Processo: Incentivar uma visão transparente dos processos governamentais comuns.
- Infraestrutura Partilhada: Promover infraestrutura, aplicativos e serviços partilhados de governo eletrónico/TI.
- Disciplina de Tecnologia: Garantir a disciplina tecnológica na implementação de TI pelos MDAs.

- Segurança da Informação: Garantir a integridade e a segurança dos dados e processos partilhados mantendo a tríade da CIA.
- Competição Saudável: Promover a concorrência entre fornecedores e serviços eletrónicos inovadores por parte dos MDAs.
- Minimização de custos: Minimizar o custo dos investimentos em TI e evitar a dependência de fornecedores.

Especificamente para os cidadãos, que serão os beneficiários finais do processo, os benefícios da interoperabilidade são os seguintes:

- Princípio uma vez (Once Only Principle - OOP): Garantir que os cidadãos, instituições e empresas só devem fornecer determinadas informações padrão às autoridades e administrações uma única vez.
- Maior acesso aos serviços: Os cidadãos podem melhor e mais convenientemente aceder aos serviços governamentais a partir do conforto das suas casas ou de qualquer lugar do país.
- Melhor Serviço Público: A interoperabilidade assegura que os cidadãos beneficiam de um melhor serviço público através da abertura, transparência e participação.
- Valor e Satisfação do Cidadão: Os cidadãos estão mais bem informados e a qualidade dos serviços públicos é melhorada, levando a um aumento do valor e da satisfação dos utilizadores.

1.1.2 Escopo

O Quadro de Interoperabilidade do Governo Eletrónico para a Guiné-Bissau (eGIF-GW) deverá fornecer diretrizes e especificações que permitam a prestação de serviços públicos entre entidades pelos MDAs. Visa detalhar os princípios nos quais a interoperabilidade se baseará, os níveis e as etapas para alcançar a interoperabilidade, os desafios de adoção, bem como as medidas de conformidade e os processos de revisão. Como parte das estratégias globais para a implementação da Arquitetura Empresarial da Guiné-Bissau, o eGIF-GW define diretrizes básicas de interoperabilidade na forma de princípios, modelos e recomendações comuns para a interação entre MDAs ou organizações.

1.1.3 Resultados esperados

Com a implementação e cumprimento da disponibilização do eGIF-GW, ao nível dos princípios que visam alcançar a interoperabilidade na vertente legal, organizacional, semântico e técnico; modelos como o modelo conceptual e as recomendações do serviço público, de seguida encontram-se os resultados que se espera que sejam alcançados pelo governo da Guiné-Bissau:

- Sinergias melhoradas: O quadro irá estimular comunicação facilitada e troca de dados, aumentando sinergias entre as entidades governamentais.
- Integração Total: O quadro garantirá a integração total dos sistemas de TI do setor público para uma prestação eficiente de serviços em várias entidades governamentais.
- Acessibilidade: O quadro permitirá que os cidadãos, as empresas e outras partes interessadas tenham acesso fácil aos serviços de governo eletrónico e de uma forma economicamente acessível.
- Interação perfeita: O quadro permite uma comunicação online tranquila e transfronteiriça entre organizações governamentais, empresas e cidadãos.
- Maior participação dos cidadãos na governação: O quadro irá garantir que os cidadãos da Guiné-Bissau, independentemente de onde estejam, realizem a sua contribuição para o governo, uma vez que podem aceder a todos os serviços governamentais online.
- Atualização de Políticas: As políticas governamentais para aumentar o acesso dos cidadãos aos serviços administrativos e públicos, promover a sensibilização e a transparência, abordar as queixas dos cidadãos, ajudar a resolver um dos principais fatores de fragilidade e exclusão social

do país, minimizar a corrupção, facilitar a realização de negócios, etc. poderão ser atingidas através deste quadro.

- Infraestrutura Tecnológica Melhorada: A implementação do quadro de interoperabilidade e os esforços de transformação digital irão melhorar as infraestruturas digitais e outras infraestruturas de TI.
- Melhor inclusão financeira: Ao superar conetividade e recursos tecnológicos limitados em todo o país, o quadro garantirá que mais cidadãos sejam cobertos em termos de serviços financeiros.
- Apoio à Educação/Competências Digitais: O quadro garantirá competências digitais e iniciativas educativas que promovam a utilização de tecnologias digitais para melhorar o ensino, a aprendizagem e a avaliação e, ainda, apoiarão os trabalhadores do GoGB e os cidadãos.
- Inclusão Social e Promoção do Crescimento Económico: O crescimento económico aliado à inclusão social será promovido através do quadro, o qual garantirá que aqueles em risco de pobreza e exclusão social tenham as oportunidades e os recursos necessários para participar plenamente na vida económica, social, política e cultural e desfrutar de um padrão de vida considerado normal na sociedade em que vivem.
- Segurança de Dados e Promoção da Conformidade: O quadro promoverá a visão nacional sobre segurança de dados através da consciencialização, parceria e responsabilidades partilhadas numa comunidade confiável de partes interessadas; bem como o cumprimento das normas nacionais e internacionais de proteção de dados.

1.1.4 Caso de uso e aplicabilidade

A interoperabilidade é essencial num ambiente em evolução digital em que as administrações públicas procuram obter informações a partir dos dados para poderem tomar decisões e alcançar o sucesso operacional. Um caso de utilização da interoperabilidade para a administração pública é a utilização da interoperabilidade para suportar abordagens administrativas sustentáveis que os governos adoptam para melhorar a prestação de serviços públicos. Permite que os MDA implementem políticas baseadas em dados através da governação eletrónica ou de iniciativas semelhantes. A aplicação de um quadro de transferência de dados partilhados também melhora a colaboração governamental, ultrapassando as barreiras linguísticas.

O Quadro de Interoperabilidade do Governo Eletrónico para a Guiné-Bissau (eGIF-GW) é aplicável à interação entre Governos (G2G), Empresas (G2B) e Cidadãos (G2C).

1.1.5 Partes interessadas e Responsabilidade

A responsabilidade é crítica para um esforço de interoperabilidade bem-sucedido. Tendo isto em conta, todas as partes interessadas devem ser consideradas co-titulares do quadro de interoperabilidade. No entanto, o ITMA pode fazer a coordenação. O ITMA também será responsável pela conceção da estrutura de interoperabilidade e documentos relacionados, tais como padrões de interoperabilidade de dados, diretrizes padrão para sites governamentais, etc.

Uma vez que a interoperabilidade bem-sucedida de todos os setores governamentais e serviços públicos será útil para todas as partes interessadas, as partes interessadas são, portanto, incentivadas a trabalhar em conjunto para garantir a implementação suave e rápida do quadro a todo o tempo nas suas respetivas organizações.

Além disso, as pessoas com as seguintes funções de nível C (C-level) e executivas sénior nos MDAs devem liderar o quadro de interoperabilidade ao nível da sua organização:

- Secretários permanentes
- Diretor Executivo (CEO)
- Diretor Financeiro (CFO) / Chefes de Finanças

- Diretor de Informação (CIO)
- Diretor de Tecnologia (CTO)
- Responsáveis pela segurança da informação (CISO)
- Gestores de TI / Diretor de TI

Dado o contexto de instabilidade política e incertezas orgânicas que caraterizam os sucessivos governos na Guiné-Bissau, é muito importante reforçar a estrutura de governança da Economia Digital para garantir a eficácia e a sustentabilidade da interoperabilidade do projeto. Isto está base da nossa decisão de ter uma estrutura de governação clara para o eGIF-GW, conforme descrito na secção 1.5.1, que inclui representantes de todos os níveis de governo e setores relevantes. Propõe-se que esta estrutura seja liderada por uma autoridade central, mas que inclua também um comité de supervisão ou conselho consultivo que reúna as partes interessadas de diferentes áreas, incluindo o setor privado e a sociedade civil.

Esta estrutura, conforme descrita na secção 1.5.1, incorpora mecanismos robustos de responsabilização e transparência para garantir que todas as ações e decisões no âmbito do quadro de interoperabilidade sejam registadas e estejam acessíveis para auditoria pública. Num contexto de instabilidade política, isto é importante porque ajuda a construir confiança no processo e não nas pessoas.

Dado o papel vital dos gestores de nível C e de TI na liderança da implementação deste quadro, é enfatizada a importância da formação contínua. A formação deve enfatizar a necessidade de flexibilidade no quadro de interoperabilidade, permitindo que estes cargos de nível C (C-suite) e executivos seniores nos MDA se adaptem às mudanças políticas e tecnológicas.

1.1.6 Fatores críticos de sucesso

Para que a implementação do eGIF-GW seja bem sucedida, há alguns fatores ou considerações que devem ser tidos em conta, uma vez que a sua falha resultará na não realização das metas, objetivos e benefícios esperados do quadro. São eles:

- Vontade política/compromisso: O Quadro estimulará comunicação fácil e transferência de dados, melhorando sinergias entre as entidades governamentais.
- Coerência nas iniciativas governamentais: Os projetos de IT e iniciativas desta natureza devem ser consistentes e em progressão, para que a mudança de política de governo ou de líder de um ministério ou de outros altos funcionários do governo não leve a que uma iniciativa seja interrompida ou abandonada.
- Apropriação e coordenação: Como já foi dito, os esforços coordenados de todas as partes interessadas no desenvolvimento das TIC no país são uma necessidade para o sucesso do quadro. Deve manter-se uma clara apropriação e coordenação da implementação e do cumprimento para alcançar o máximo impacto online com outras iniciativas digitais no país.
- Colaboração dos MDA: Os MDA devem estar imensamente envolvidos na implementação do quadro e na definição de mecanismos claros para apoiar a aplicação, de modo a ter um forte impacto no percurso de transformação digital do governo e no panorama digital do país. As funções de nível C (C-suite) e de funcionários seniores nos MDA podem ser utilizadas para impulsionar esta colaboração na sua respetiva organização.
- Apoio sistémico: Para que o quadro tenha impacto na sociedade e produza benefícios sustentáveis a longo prazo, devem existir sistemas de apoio, tais como infraestruturas comuns, como um centro de dados nacional e uma Política Nacional de TIC.
- Aliança Estratégica para a Boa Governação: O desenvolvimento de parcerias estratégicas entre o governo e entidades como universidades, instituições e organizações internacionais (PNUD, BM) poderia fornecer apoio técnico, financeiro e estratégico, essencial para a sustentabilidade a longo prazo deste projeto.

1.2 Digitalização de Serviços e Prestação de Serviços

O quadro de interoperabilidade é um meio para atingir um fim e não um fim em si. O objetivo é melhorar a prestação de serviços, através da Janela Única de Atendimento (digitalização dos serviços públicos e centralização da prestação de serviços através de uma plataforma única). Como tal, o foco deste projeto está na digitalização dos serviços – dos quais os setores podem beneficiar. O Governo, o seus ministérios, agências e departamentos necessitam de acordar na interoperabilidade para atingirem a digitalização tanto dos serviços públicos, como da prestação de serviços públicos.

Os conceitos, modelos e componentes que são relevantes para ter um serviço público digitalizado e garantir a prestação de serviços digitais estão descritos nas subsecções abaixo.

1.2.1 Standard de Serviço Digital (DSS)

Embora o governo desenvolva e opere múltiplos serviços através de serviços partilhados ou quaisquer outros meios, é importante garantir um conjunto comum de standards para estes serviços digitais. O Standard de Serviço Digital é definido como "um conjunto de princípios de melhores práticas para desenhar e fornecer serviços governamentais. Ajuda as equipas digitais a construir serviços simples, claros e rápidos."

De acordo com o Governo do Reino Unido, as principais características do Padrão de Serviço Digital estão listadas abaixo:

1. Compreender os utilizadores e suas necessidades.
2. Resolver um problema global para os utilizadores.
3. Oferecer uma experiência agrupada em todos os canais.
4. Tornar o serviço simples de usar.
5. Certificar-se de que todos possam usar o serviço.
6. Ter uma equipa multidisciplinar.
7. Utilizar formas ágeis de trabalhar.
8. Repetir e melhorar com frequência.
9. Criar um serviço seguro que proteja a privacidade dos utilizadores.
10. Definir como é o sucesso e publicar dados de desempenho.
11. Escolher as ferramentas e tecnologias certas.
12. Tornar o novo código-fonte aberto.
13. Utilizar e contribuir para padrões abertos, componentes comuns e tendências.
14. Operar um serviço confiável.

O Padrão de Serviço Digital (DSS) do Governo da Índia sugere um conjunto de padrões e princípios inter-relacionados que se aplicam a todos os aspetos de qualquer serviço digital, ao longo do seu ciclo de vida, nomeadamente, Definir, Realizar, Medir e Governar os Serviços Digitais. O DSS é um conjunto de mais de 170 standards, princípios e diretrizes organizados segundo uma taxonomia racional, que é fácil de compreender e implementar pelo ecossistema.

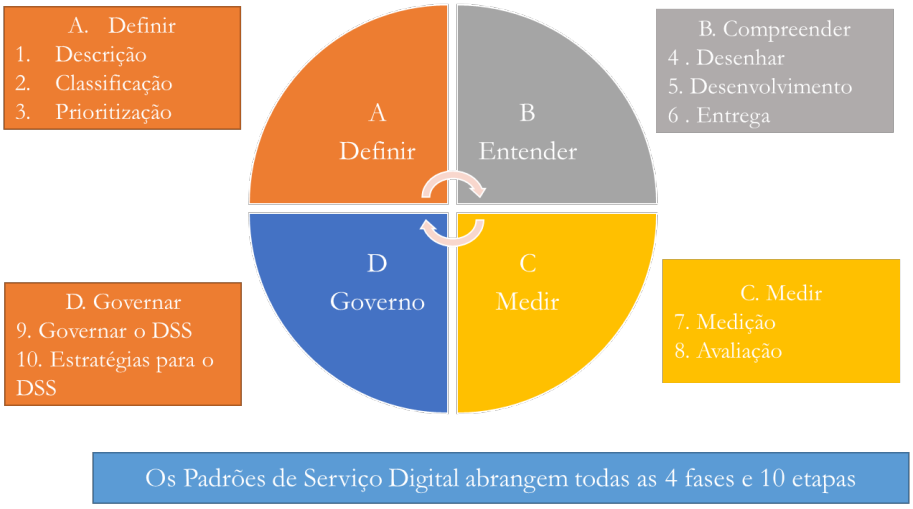

Figura 1: Ciclo de Vida dos Serviços Digitais

A estrutura DSS pode ser aplicada com benefícios a uma variedade de situações, como grandes projetos digitais inéditos, sistemas antigos que necessitam de ser migrados para a era digital, serviços pouco complexos e portfólio de serviços. O DSS fornece não apenas os padrões, princípios e diretrizes a serem seguidos, mas também o quadro para medir o desempenho dos serviços digitais e avaliar o seu impacto, e também um conjunto de estratégias para superar os desafios na adoção do DSS.

1.2.2 Modelo de Referência de Plataforma Digital Pública (PDPRM)

Uma plataforma digital é principalmente um ecossistema de inovação focado nos negócios onde os participantes (empreendedores, agências governamentais e públicas, financiadores e investidores, prestadores de serviços, academia e pesquisadores, desenvolvedores, incubadoras, cidadãos e consumidores de serviços e reguladores) se reúnem com o objetivo comum de alargar e melhorar os serviços digitais para benefício de todos, possibilitados pelas tecnologias digitais comuns subjacentes. Quando os serviços respeitam a serviços públicos, as plataformas são denominadas Plataformas Públicas Digitais (PDPs).

O modelo de referência propõe as seguintes capacidades, não limitadas, como segue:

- Utilizadores e Canais de Acesso: Ao conceber uma PDP, o governo deve identificar os seus utilizadores e os seus canais de acesso. Os utilizadores que interagem com os sistemas podem ser Cidadãos (G2C), Governo e Regulador (G2G), Fornecedor e Intermediário, Empreendedor e Start-up, Mercado/eCommerce, Desenvolvedores, Instituições de Pesquisa/Academia, Instituições Financeiras. O acesso aos serviços digitais pode ser fornecido a partir de navegador da Web, dispositivos móveis, sistema de conversa (chat bot), sistema interativo de resposta de voz (IVRS), telefone, central de serviços, central de atendimento e assim por diante.

- Capacidades de negócio: uma combinação de funções, processos, informações e ferramentas possibilita uma capacidade de negócio. Muitas partes interessadas interagem com as PDPs e cada uma delas terá um propósito/negócio diferente para interagir com a PDP. Os potenciais recursos de negócios podem ser a integração de partes interessadas (registo de utilizador), gestão de partes interessadas, ofertas, serviços e catálogo, design de experiência (UI/UX), Acesso ao Mercado, Modelo de Cobrança e Receita, Incentivos e Subsídios, Confiança e Reputação, Promoção e Marketing, Serviços Digitais e Compras, Registo e Entrega, Confiança e Reputação, Pesquisa e Descoberta.

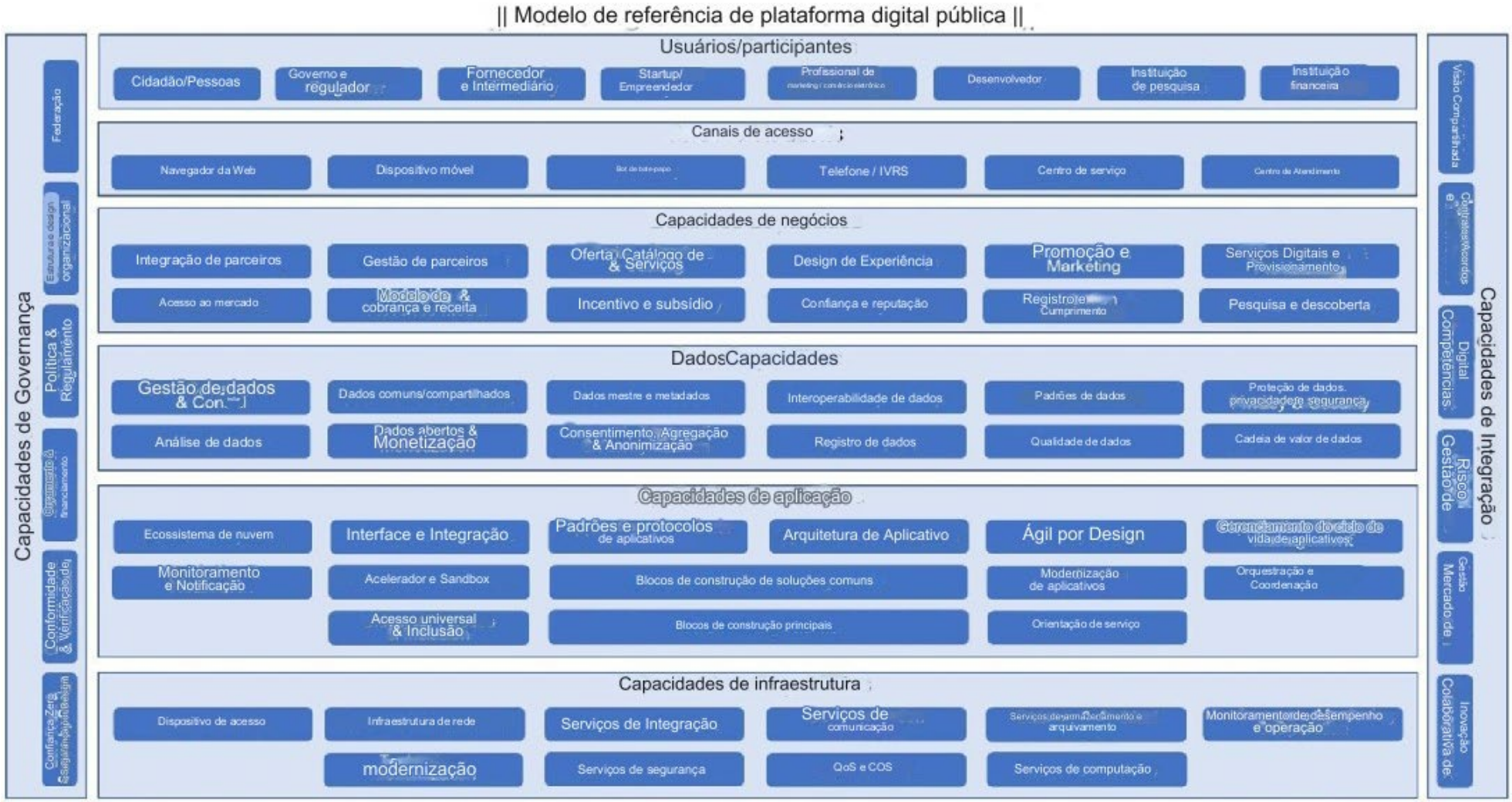

Figura 2- Modelo de referência de plataforma digital públic

- Capacidades de dados: A chave para a transformação digital é criar capacidades para gerir e aproveitar dados/informações no seu máximo potencial. Os blocos de construção apoiam a implementação destas capacidades, mas são necessárias pessoas e processos para cumprir a intenção.
- Capacidades da aplicação: As aplicações possuem diversas possibilidades e funcionalidades disponibilizadas através dos blocos em que são desenvolvidas que atingem os objetivos de negócio dos serviços digitais. Eles incluem ecossistema de nuvem (cloud), padrões e protocolos de aplicações, arquitetura de aplicações, metodologia Agile-by-Design, interface e integração, monitorização e notificação, acelerador e zona de teste (sandbox), blocos de construção de soluções comuns, como ensino online (eLearning), mercados digitais (eMarketplace), blocos de construção principais, como identidade digital, pagamentos, modernização de aplicações, Acesso Universal e Inclusão, Orientação para os Serviços.
- Capacidades de infraestruturas: As infraestruturas são o pilar fundamental do PDP. Os recursos incluem Infraestrutura de Rede, Dispositivos de Acesso, Serviços de Integração, Serviços de Comunicação, Serviços de Armazenamento e Arquivamento, Serviços de Computação, Qualidade de Serviço (QoS) e Classe de Serviços (Cos), Serviços de Segurança e Modernização Tecnológica.
- Capacidades de Governança: A ISO/IEC 38500:2015 define governança como: "um sistema que dirige e controla o estado atual e futuro". Governança é um processo de tomada de decisão com uma estrutura definida de relacionamentos que dirigem e controlam a empresa para atingir os objetivos declarados. O processo pelo qual a direção e o controlo são fornecidos deve considerar a igualdade de preocupação e a transparência, protegendo os direitos e interesses da empresa.
- Capacidades transversais: Para criar os blocos de construção, precisamos de capacidades e sub-capacidades de segurança e privacidade. Estes são transversais e devem funcionar em conjunto (muitas vezes um desafio em organizações isoladas). Por exemplo, se nos concentrarmos apenas na modelagem de ameaças a aplicações ou à privacidade. Neste caso, as informações contextuais sobre o risco para a agência governamental e a reutilização por meio da gestão adequada do conhecimento serão frequentemente não priorizados. Ao criar capacidades de segurança ou privacidade, é essencial reconhecer que elas são facilitadoras. Como tal, as pessoas envolvidas nestes grupos devem evangelizar, promover e ajudar outras equipas a reconhecer a impotência da segurança e da privacidade.
- Capacidades de integração: A interoperabilidade é uma área de capacidade fundamental para a transformação digital porque parte da transformação envolve a transformação ao longo de todo o governo. Conforme mencionado nas capacidades dos dados, partilhar, aproveitar e reutilizar é fundamental, aplicando-se o mesmo às capacidades de aplicações/soluções e às capacidades de negócios.
- Capacidades de gestão de mudanças de arquitetura: A gestão de mudanças de arquitetura envolve atingir o valor de negócio do alvo inicial. As principais capacidades incluem realização de valor, monitorização, gestão de riscos, gestão de processos de governança, implementação de mudanças, capacitação, análise de lacunas e realização dinâmica de decisões.

1.2.3 Conjunto de Blocos de construção do Governo (GovStack)

O PDPRM fornece uma visão geral de uma arquitetura de ecossistema governamental que absorve provisoriamente os blocos de construção e camadas do GovStack. O Quadro de Investimento Digital dos ODS (Objetivos de Desenvolvimento Sustentável) identificou 23 blocos de construção comuns que podem ser utilizados para apoiar uma vasta gama de casos de utilização em vários setores. Blocos de construção adicionais podem ser definidos pelos atores conforme necessário para seus casos de uso.

Alguns Blocos de Construção são Blocos de Construção 'Principais' que fornecem serviços fundacionais. Todos os outros blocos de construção usam estes blocos de construão (principais) que são necessários para qualquer implementação de blocos de construção. Conforme visto no diagrama da Arquitetura de Referência

da Plataforma Digital Pública na Seção 1.2.2 acima, os Blocos de Construção Principais sustentam os Blocos de Construção da Solução Comum.

Os Blocos de Construção da Solução Comum fornecem funcionalidades discretas que são usadas regularmente por uma ampla variedade de casos de uso. Cada Blocos de Construção de Solução Comum ligar-se-á a outros Blocos de Construção através de um Mediador de Informação (Information Mediator) e aderirá aos padrões e especificações definidos para esse Blocos de Construção, bem como aos requisitos transversais definidos nas especificações técnicas do GovStack.

Blocos de construção principais: qualquer aplicativo que aproveite a abordagem e arquitetura GovStack deve usar os blocos de construção principais que foram definidos para fornecer serviços e funcionalidades básicas.

- ***Mediador de Informação:*** O bloco de construção do Mediador de Informação (MI) fornece um gateway seguro para troca de dados e serviços entre outros blocos de construção e aplicações externas. Conecta todos os Blocos de Construção de uma aplicação e garante a interoperabilidade e implementação de standards. O MI fornece mecanismos para aplicações/Blocos de Construção publicarem e consumirem serviços e notificações de eventos, entre outros Blocos de Construção.

- ***Identidade e Verificação:*** O bloco de construção de Identidade e Verificação cria, gere e usa uma identidade digital fundacional (uma identidade funcional não está no escopo deste bloco de construção). Como parte do sistema de identidade geral, ele pode ter interface com outros blocos de construção, a fim de realizar o conjunto completo de requisitos necessários para a identificação e verificação dos outros blocos de construção e atores do GovStack.

- Segurança: O bloco de construção de Segurança pode ser dividido em requisitos de segurança transversais generalizados que qualquer bloco de construção deve aderir. Além disso, o componente básico de segurança fornece serviços básicos de gestão de identidade e acesso (IAM) ou outros componentes básicos.

Os requisitos de segurança abordam todos os problemas e preocupações transversais de segurança para qualquer plataforma digital GovStack, incluindo cada camada, cada bloco de construção e todos as aplicações. Embora outros blocos de construção abordem "alguns" aspetos de segurança, as soluções subsequentes fornecidas por todos os blocos de construção devem cumprir os standards e configurações estabelecidos nos requisitos dos blocos de construção de segurança.

Blocos de construção da solução comum: blocos de construção da solução comum implementam funcionalidades que podem ser necessárias para vários casos de uso. Eles são módulos independentes e interagem com outros componentes do Bloco de Construção da Solução Comum por meio do Bloco de Construção do Mediador de Informação.

As seguintes especificações do Bloco de Construção da Solução Comum foram lançadas como parte do GovStack versão 1.1.0:

- **Registo:** O Bloco de Construção de Registo regista identificadores e outras informações gerais sobre uma pessoa, local ou outra entidade, normalmente para fins de registo ou inscrição em serviços ou programas específicos e rastreabilidade dessa entidade ao longo do tempo.

- **Registos Digitais:** Os Registos Digitais são bancos de dados geridos centralmente que identificam de forma única pessoas, fornecedores, instalações, procedimentos, produtos e locais relacionados a uma organização, setor ou atividade.

- **Pagamentos:** O Bloco de Construção de Pagamentos implementa transações financeiras, como remessas, reclamações de seguros, compras de produtos, pagamentos de taxas de serviço, juntamente

com o registo de informações transacionais relacionadas. Ele também fornece utilitários para rastrear custos e extrair testes de auditoria.

O link a seguir fornece mais informações e especificações e requisitos detalhados para o Bloco de Construção de Pagamentos.

As seguintes especificações do Bloco de Construção estão em desenvolvimento:

- **Gestão de Consentimento:** Este Bloco de Construção gere um conjunto de políticas que permitem aos utilizadores determinar as informações que serão acessíveis a potenciais consumidores específicos de informações, para qual finalidade, por quanto tempo e se essas informações podem ser partilhadas.

- **eMarketplace:** Este Bloco de Construção fornece um espaço de marketing digital onde entidades fornecedoras podem anunciar e vender eletronicamente produtos e serviços a outras entidades (B2B) ou clientes finais (B2C).

- **Mensagens:** Este Bloco de Construção facilita notificações, alertas e comunicações bidirecionais entre aplicativos e serviços de comunicação, incluindo SMS, USSD (serviço de dados não estruturados), IVR (reconhecimento de voz), e-mail e plataformas de social media.

- **Agendamento:** Este Bloco de Construção fornece um mecanismo para configurar eventos com base em intervalos regulares ou combinações específicas do status de vários parâmetros, a fim de dar origem a tarefas específicas num processo de negócios automatizado.

- **Fluxo de Trabalho e Algoritmo:** Este Bloco de Construção otimiza e controla processos de negócios especificando regras que governam a sequência de atividades executadas e o tipo de informações trocadas para orquestrar o fluxo do processo desde o início até a conclusão.

Os blocos de construção de soluções comuns adicionais são os seguintes:

- Análise e Inteligência de Negócio
- Inteligência artificial
- Gestão de casos de clientes
- Gestão de Colaboração
- Gestão de conteúdo
- Coleção de dados
- e-learning
- Serviços de Informação Geográfica (GIS)
- Gestão de Mobilidade
- Relatórios e Painéis
- Repositórios de dados partilhados
- Terminologia

Requisitos transversais: Para além das especificações do bloco de construção da solução principal e comum, a abordagem GovStack detalha muitos requisitos transversais. Esses requisitos aplicam-se a todos os Blocos de Construção desenvolvidos no contexto de uma aplicação GovStack. Estes requisitos transversais fornecem diretrizes e princípios que garantem a adesão às melhores práticas e permitem o desenvolvimento de plataformas com desempenho, robustas, seguras e escaláveis.

Os requisitos transversais do GovStack são definidos como uma série de práticas e princípios. Esses princípios são articulados com os verbos TEM, PODE e DEVE.

Padrões relevantes: Quando aplicável, os Blocos de Construção do GovStack aderirão aos padrões existentes. É altamente recomendável que todos os Blocos de Construção do GovStack estejam alinhados com os seguintes padrões:

- Segurança: Estrutura de segurança cibernética do NIST (National Institute of Standards and Technology)
- Texto: Unicode
- Datas e carimbos de data/hora: ISO8601/UTC
- Dados: JSON e esquema JSON
- APIs: REST
- Documentação da API: OpenAPI 3.1 (Swagger)
- Contenterização: Contentores OCI

Além destas normas comuns, se estiver disponível uma norma existente, esta deverá ser utilizada, por ex. DICOM/Hl7/FHIR para cuidados de saúde. O TMForum possui uma grande biblioteca de APIs padronizadas e modelos de dados que podem ser usados.

1.2.4 Assinatura Digital e Infraestrutura de Chave Pública (PKI)

Há um bloco de segurança como parte do bloco de construção central dos blocos de construção GovStack. Este alicerce é levado mais longe aqui, considerando a assinatura digital e a PKI e como elas são cruciais para garantir a segurança, a autenticidade e a integridade dos dados trocados na plataforma de interoperabilidade.

Permitirá a criação, gestão, distribuição, utilização e armazenamento de certificados digitais e chaves públicas. Isto é fundamental para:

a) Autenticação Forte, que garante que os utilizadores sejam realmente quem dizem ser;
b) Assinatura Digital, que permite assinar digitalmente documentos e transações, oferecendo uma camada de segurança jurídica e verificabilidade; e
c) Criptografia, que garante que a comunicação entre os diferentes serviços da plataforma é segura, protegendo os dados contra acessos não autorizados.

As assinaturas digitais podem ser usadas nos seguintes cenários:

- Autenticação - para garantir a identidade de uma pessoa ou organização.
- Integridade – garantia de que as mensagens ou documentos não estão expostos a alterações não autorizadas.
- Não repúdio – uma parte que assinou um documento ou mensagem não pode posteriormente negar que o assinou.

As assinaturas digitais são baseadas na Infraestrutura de Chave Pública (PKI) e requerem um par de chaves – uma chave pública e outra chave privada – que são correspondidas. A chave privada é secreta e utilizada para autenticação e assinatura digital de documentos. A chave pública é pública e usada pelo destinatário para verificar a identidade e validade.

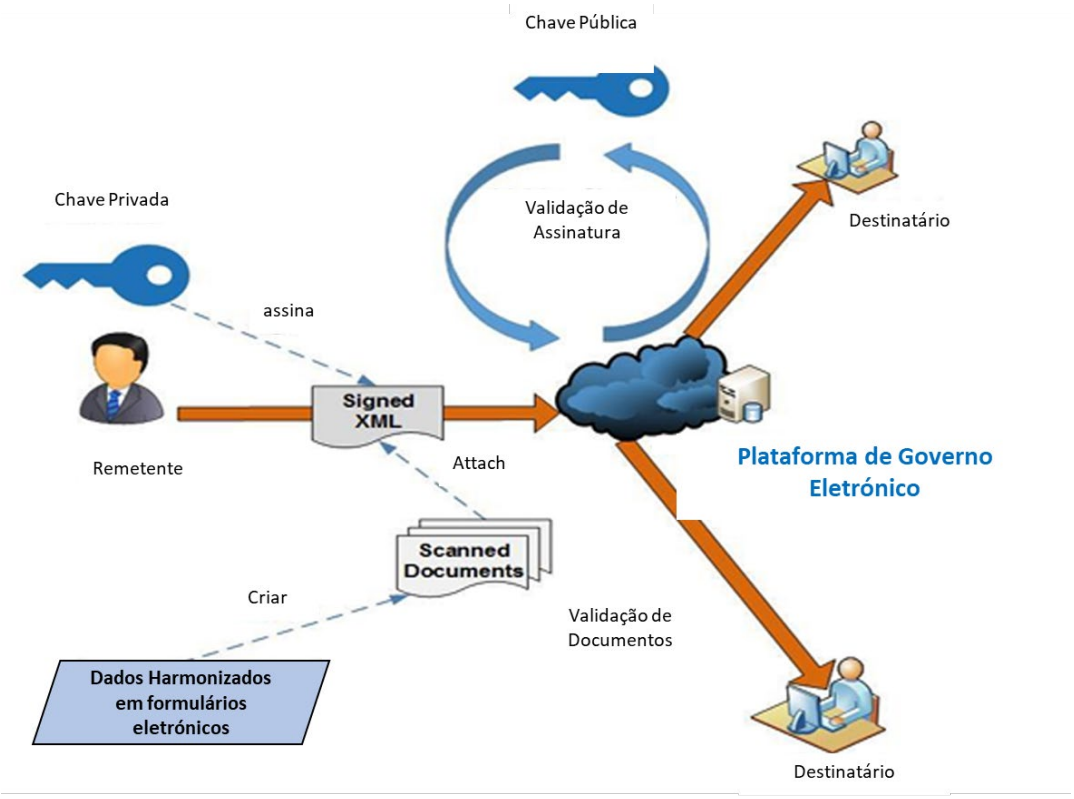

Figura 3: Assinaturas Digitais e PKI

Enquanto passo essencial para evitar fraudes, a funcionalidade de identificação e verificação dos utilizadores da Plataforma pública do Governo desempenha um papel muito importante. Antes da geração das chaves privada e pública, é essencial que o utilizador seja identificado e verificado. Para este efeito, é necessária a criação de uma Autoridade Certificadora (CA). A CA, enquanto terceira parte de confiança é responsável por verificar a identidade do utilizador e da organização antes que as chaves sejam geradas e transmitidas às partes.

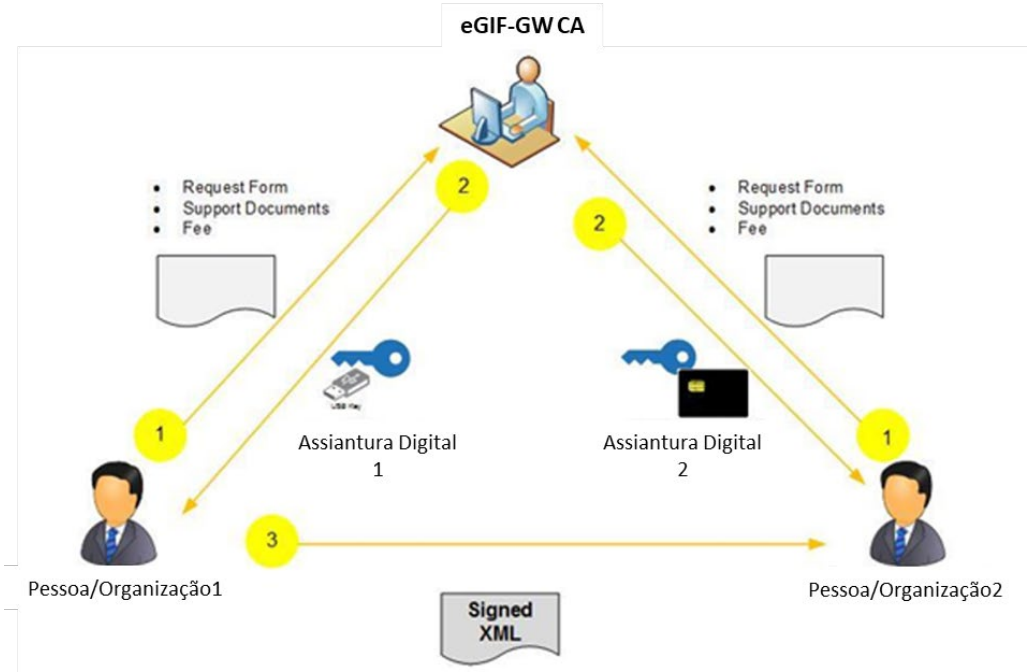

Figura 4: Processo de assinatura digital

1.2.5 Identidade Eletrónica (eID)

Uma identificação eletrónica ("eID") é uma solução digital que fornece a cidadãos ou organizações uma prova de identidade. Ela pode ser utilizada para aceder a benefícios ou serviços fornecidos por autoridades governamentais, bancos ou outras empresas, tais como pagamentos móveis. Além da autenticação e login online, muitos serviços de identidade eletrónica também oferecem aos utilizadores a opção de assinar documentos eletrónicos com uma assinatura digital.

O sistema eID é a identidade digital que cada cidadão utilizará para aceder aos serviços da plataforma governamental digital. A integração do eID na plataforma de interoperabilidade é fundamental, pois permitirá aos cidadãos aceder a um vasto conjunto de serviços públicos e privados de forma simplificada e com um único meio de identificação digital. A identificação eletrónica também mitiga significativamente as possibilidades de fraude e roubo de identidade e facilita a personalização e adaptação dos serviços às necessidades específicas dos utilizadores.

A incorporação de PKI e eID na plataforma de interoperabilidade simplifica a arquitetura geral do sistema e melhora a gestão operacional. Isto não só facilita a manutenção, mas também aumenta a segurança, uma vez que todos os componentes essenciais são integrados e geridos centralmente. Além disso, a inclusão da PKI e da eID na plataforma de interoperabilidade cria uma base sólida para uma plataforma de interoperabilidade robusta, segura e eficiente, capaz de servir eficazmente a população da Guiné-Bissau.

1.3 Conceito de interoperabilidade

1.3.1 Interoperabilidade

A interoperabilidade, enquanto capacidade de as aplicações e os sistemas trocarem dados de forma segura e automática, é um aspeto crucial das iniciativas de Governo Eletrónico. Ela permite a partilha de dados de forma coordenada entre organizações e departamentos, melhorando a pesquisa e desenvolvimento e melhorando a aperfeiçoando a experiência do utilizador final. Ao permitir que os dados fluam entre diversos sistemas com mínima intervenção humana, a interoperabilidade reduz os silos de dados e permite uma maior eficiência e qualidade de serviço.

Alguns dos benefícios de conceber, desenvolver e implementar um quadro e/ou plataformas de interoperabilidade são substanciais. Estes esforços podem levar a uma gestão de dados mais eficiente, produtividade aumentada, escalabilidade e redução de custos, as quais contribuem como um todo para a melhoria de oferta de serviços e da experiência do utilizador final.

- Racionalização da gestão de dados: A interoperabilidade permite que a informação se propague de forma mais coesa, sem ser perturbada por incompatibilidades de sistemas ou processos humanos. O Governo pode melhor gerir, monitorizar e proteger os dados através da simplificação do seu esforço de regulação do movimento de dados, gestão de utilizadores, proteção da privacidade dos dados e cumprimento da legislação de segurança dos dados.
- Aumento da produtividade: A interoperabilidade proporciona uma partilha de dados sem esforço entre sistemas díspares, o que aumenta a eficiência organizacional. Sem interoperabilidade, os sistemas díspares necessitam de manipular e transforar os dados para conseguir partilhá-los. A necessidade de recorrer a processamento de dados adicionais apresentam uma maior probabilidade de erros.
- Promover a escalabilidade: A interoperabilidade dos dados aumenta a capacidade do Governo para expandir as operações e adaptar-se às condições dinâmicas do mercado. Com sistemas interoperáveis, o Governo pode partilhar dados em grande escala sem ser restringido por limitações estruturais e operacionais.
- Redução de custos: Os sistemas não interoperáveis têm de aplicar passos adicionais para garantir uma transferência de dados fiável e preciso. Isto pode envolver a instalação de middleware, que formata e

distribui dados entre pontos de transferência. A instalação de diferentes componentes de software implica custos adicionais de desenvolvimento, operação e manutenção. Assim, as organizações mudam para sistemas com melhor interoperabilidade para reduzir as despesas correntes.

- Para alcançar a interoperabilidade necessária com o objetivo de prestar serviços públicos e administrativos integrados entre os MDAs, devem ser cumpridos os seguintes requisitos através da criação de um mecanismo:
- Identificação de processos: A identificação dos principais processos empresariais e a sua aprovação coletiva pelos MDAs é o primeiro passo para ter sistemas interoperáveis. Isto coloca a responsabilidade em cada MDA de ter um documento que regista a análise de processos empresariais (APE) dos seus respetivos serviços governamentais.
- Conformidade com Standards: A apresentação de dados através de infraestruturas e/ou aplicações de TI de forma padronizada e coesa. Isto define um nível de conformidade com as normas definidas pelo quadro.
- Colaboração de sistemas informáticos: A capacidade das infraestruturas/aplicações informáticas participantes para utilizar os dados trocados de forma compreensível para a prestação e entrega de serviços. É aqui que a interoperabilidade entre os sistemas informáticos das várias entidades governamentais comunicam entre si através de uma única fonte de dados.
- Instituição de um quadro jurídico: Capacidade para criar quadros jurídicos, políticos e regulamentares que definam o âmbito da interoperabilidade, nomeadamente no que respeita à transmissão de dados e aos requisitos em matéria de privacidade e proteção de dados.

1.3.2 eGIF-GW: Princípios fundamentais

Os princípios fundamentais subjacentes ao eGIF-GW são:

Princípio 1 - Padronização dos sistemas de TI: Este princípio assegura a eficiência na aquisição de sistemas de TI entre os MDAs e ajuda o governo a criar capacidades relevantes para apoiar a partilha de recursos e futuras inovações. A padronização da tecnologia em todos os estratos da administração pública acabará por diminuir o número de plataformas utilizadas pelo Governo reduzindo o custo dos sistemas de TI.

Dado que a standardização deve considerar as necessidades locais específicas e a capacidade da infraestrutura existente para que a implementação seja realista e prática, a standardização dos sistemas de TI aqui não se refere apenas aos sistemas/infraestruturas existentes, mas a qualquer novo projeto ou iniciativa de aquisição de sistemas de TI. Para os sistemas/infraestruturas existentes, estes necessitam de ser atualizados sempre que possível para atender aos standards, caso falharem nas verificações de conformidade com os standards, num esforço para garantir a interoperabilidade perfeita entre todos os sistemas de TI do governo.

Os sub-princípios são:

- Princípio 1.1 - Abertura: O princípio da abertura diz respeito, principalmente, a dados, especificações e aplicações. Os dados governamentais abertos aludem à ideia de tornar todos os dados públicos disponíveis de forma livre e para utilização e reutilização por terceiros, a menos que se apliquem restrições como a proteção de informações pessoais identificáveis (PII), a confidencialidade ou os direitos de propriedade intelectual (PI).
  A abertura baseia-se na utilização de , standards, protocolos e interfaces abertos. A abertura dos sistemas informáticos pode ser determinada primariamente pelo grau em que novos serviços de partilha de recursos podem ser acrescentados e disponibilizados para utilização por uma variedade de programas clientes sem comprometer a prestação de serviços.

  Recomendações:

  i. Os MDAs **devem** publicar os dados que lhes pertencem como dados abertos, exceto se certas restrições o impedirem.

ii. Os MDAs **devem** utilizar software de fonte aberta tanto quanto possível e contribuir para as comunidades de desenvolvimento destes softwares, uma vez que esta é um facilitador do subprincípio da rede, ou seja, a reutilização.

Estas recomendações pressupõem que existem políticas claras e eficientes de proteção de dados e confidencialidade de dados pessoais para promover a abertura dos dados (legislação de proteção de dados e privacidade).

- Princípio 1.2 - Reutilização: Este sub-princípio implica a capacidade de recursos do governo, por exemplo, componentes de software, API, standards, etc., e processos comuns serem reutilizados entre os MDAs, o que permite a interoperabilidade e a melhoria da qualidade.

  Por reutilização, entende-se que os MDAs confrontados com um problema específico tentam beneficiar do trabalho realizado por outros, procurando o que está disponível, avaliando a sua utilidade ou relevância para o problema em causa e, se for caso disso, adotando soluções que tenham provado o seu valor noutro local. Isto exige que o MDA esteja aberto à partilha das suas soluções de interoperabilidade, conceitos, quadros, especificações, ferramentas e componentes com outros.

  Recomendações:
  i. Os MDAs **devem** reutilizar e partilhar dados e informações, exceto se existirem indicações em sentido contrário.
  ii. Os MDAs **devem** reutilizar e partilhar soluções e estabelecer parcerias para o desenvolvimento de soluções de software.

- Princípio 1.3 - Transparência: A transparência refere-se a permitir a visibilidade dentro do ambiente administrativo de um MDA, garantindo a disponibilidade de interfaces com sistemas de informação internos e assegurando o direito à proteção dos dados pessoais. Isto implica a prestação de serviços eficazes e coerentes, reunindo recursos, processos e dados atualmente existentes em vários silos.

  Recomendações:
  i. Os MDAs **devem assegurar a** visibilidade interna e garantir o fornecimento de interfaces externas para os serviços públicos e administrativos.

- Princípio 1.4 - Portabilidade: Este princípio implica a capacidade de uma aplicação desenvolvida para um sistema informático governamental A poder ser executada, sem modificações, num sistema informático governamental B que implemente as mesmas interfaces. Isto garante a neutralidade na tomada de decisões tecnológicas, evitando assim a imposição de determinadas tecnologias ou produtos aos parceiros. Assegura igualmente que os sistemas se adaptam a um ambiente tecnológico em rápida evolução.

  Recomendações:
  i. Os MDAs devem fornecer acesso a serviços públicos e administrativos sem impor restrições a qualquer tipo de tecnologia ou produto específico.
  ii. Não deve haver legislação que imponha tecnologias específicas para os cidadãos, as empresas e os MDAs no desenvolvimento de sistemas e serviços de informação.
  iii. Os standards e especificações abertas (SOAP, REST, etc.) devem ser utilizadas na criação do interface utilizado pelos sistemas de informação, reforçando assim a neutralidade tecnológica.
  iv. Os MDAs devem garantir a facilidade de transferência de dados entre sistemas e aplicações governamentais.

Princípio 2 - Integração dos processos de negócio: A integração de processos de negócio (IPN) permite que as entidades governamentais liguem pessoas, dados e aplicações. Com a IPN, as entidades

governamentais podem coordenar-se melhor, tanto internamente como com outros MDAs, empresas e cidadãos, para alcançar melhores resultados. A padronização dos dados é uma condição prévia para uma integração eficaz dos processos. Torna a prestação de serviços mais fácil e contínua através de um mecanismo normalizado de partilha e transferência de dados/informação. O objetivo é facilitar a extração de dados de transações de aplicações governamentais díspares acessíveis e disponiveis a processos de negócio que sejam necessários para a prestação de serviços públicos. Permite uma visão standardizada dos dados e informações públicas, ao assegurar a transparência dos sistemas em silos. Os sub-princípios são os seguintes

- Princípio 2.1 - Segurança: Este princípio assegura a transferência fidedigna de dados e informações comerciais entre os sistemas da administração pública, em conformidade com as normas e políticas de segurança estabelecidas pelo Governo. Deste modo, os cidadãos e as empresas podem ter a certeza de que, quando interagem com os estabelecimentos públicos, o fazem com confiança e um sentido de segurança.

  Recomendações:

  i. O MTTDE ou uma entidade reguladora sob a sua alçada **deve** desenvolver uma política nacional de segurança/ cibersegurança que esteja alinhada com os standards, o quadro e a estratégia de segurança do governo.
  ii. Os sistemas de informação dos MDAs **devem** respeitar a tríade **CIDN (confidencialidade, integridade, disponibilidade e não repúdio)** relativamente aos dados e serviços.

- Princípio 2.2 - Privacidade: O NIST[5] define privacidade como a garantia de que a confidencialidade e o acesso a determinadas informações sobre uma entidade estão protegidos. Os MDAs devem assegurar que os sistemas de informação do governo garantem a confidencialidade das informações do governo, das empresas e dos cidadãos, tal como previsto nas leis/regulamentos, normas, políticas ou diretrizes respetivas em matéria de proteção de dados e privacidade.

  Recomendações:

  i. Os MDAs com sistemas que prestam serviços públicos e administrativos **devem** publicar uma política de privacidade para os cidadãos e as empresas, que indiquem claramente a forma como os seus dados são recolhidos, armazenados, utilizados, divulgados, acedidos e a corrigidos e o direito de oposição ao tratamento.

Princípio 3 - Eficiência na prestação de serviços: Este princípio engloba o principal objetivo do eGIF-GW, que consiste em garantir a prestação eficiente de serviços públicos e administrativos em todos os organismos para-estatais do governo. A transformação digital integral do governo implica a capacidade de alavancar as TIC de forma a digitalizar eficazmente os processos governamentais, a fim de prestar um serviço público de excelência aos cidadãos a um custo razoável. Os sub-princípios são os seguintes

- Princípio 3.1 - Flexibilidade: Refere-se à capacidade dos sistemas de informação para se adaptarem à situação e às necessidades actuais sem comprometer o objetivo global da interoperabilidade.
- Princípio 3.2 - Acessibilidade: Assegura que os recursos informáticos de um MDA são acessíveis e utilizáveis de forma segura por outros MDA autorizados para efeitos de prestação de serviços públicos e administrativos.
- Princípio 3.3 - Escalabilidade: Refere-se à capacidade dos sistemas de informação da administração pública para lidar com uma quantidade crescente de trabalho de uma forma capaz ou à sua capacidade de aumentar a sua produção total sob uma carga crescente, quando são adicionados recursos (normalmente hardware).

[5] https://csrc.nist.gov/glossary/term/privacy

- Princípio 3.4 - Heterogeneidade: Refere-se à capacidade de os sistemas da administração pública interoperarem eficazmente, independentemente dos vários tipos de dispositivos e redes, do hardware informático, dos sistemas operativos, das linguagens de programação e da implementação pelos programadores.

Recomendação:

i. Os MDAs **devem** avaliar a eficácia e a eficiência dos diferentes serviços de interoperabilidade e opções tecnológicas, tendo em conta os requisitos de negócio e o equilíbrio entre custos e benefícios.

Princípio 4 – Design Centrado no Utilizador: Este princípio garante que os sistemas e serviços digitais sejam desenvolvidos com uma abordagem centrada no utilizador, melhorando a acessibilidade e a experiência do utilizador em todos os serviços governamentais digitais. Uma vez que os Utilizadores dos serviços públicos governamentais são qualquer MDA, cidadão ou empresa que aceda e beneficie da utilização destes serviços, as necessidades destas diferentes categorias de utilizadores devem ser consideradas ao determinar quais os serviços públicos que devem ser prestados e como devem ser prestados e entregues.

As necessidades e exigências dos utilizadores devem orientar a conceção e o desenvolvimento dos serviços públicos, de acordo com as expectativas de uma abordagem de prestação de serviços multicanal; existência de um ponto único de contato para todos os utilizadores; recolha e avaliação sistemática do feedback dos utilizadores para informar sobre o desenho de novos serviços públicos e a melhoria dos serviços públicos existentes; e fornecimento ao utilizador apenas das informações necessárias para obter um determinado serviço público.

Recomendação:

i. Os MDA **devem** trabalhar em conjunto para fornecer serviços agregados através do portal do cidadão, funcionando como ponto de contacto único para os serviços públicos.
ii. Os utilizadores **podem** escolher um tipo de canal de serviço de sua preferência, por exemplo: agência de atendimento, correios, telefone, e-mail e outros canais de internet.
iii. Os utilizadores que se candidatem a qualquer serviço público eletrónico **poderão** fazê-lo através de uma identidade eletrónica (e-ID) ou outro meio seguro.
iv. **Deve** ser criado um mecanismo para a análise, conceção, desenvolvimento e melhoria dos serviços públicos com base na recolha e avaliação sistemática do feedback dos utilizadores.
v. Os utilizadores **devem** fornecer os dados uma vez e todos os MDA que necessitem dos dados devem aceder a esses dados e partilhá-los também quando necessário, em estrita conformidade com as leis e regulamentos de proteção de dados.

Princípio 5 – Soberania, Residência e Localização de Dados: Este princípio centra-se na capacidade de aplicar os direitos legais locais e requisitos de proteção para os dados em relação ao armazenamento e processamento dos dados. A soberania dos dados é uma política ou lei governamental que chama a atenção para o facto de que os dados estão sujeitos às leis de dados e privacidade de uma localização geográfica específica. Residência de dados é a localização física ou geográfica onde os dados são armazenados. A residência de dados exige que tanto uma cópia de determinados dados ou todos os dados sejam armazenados e processados no país ou região onde foram recolhidos.

Recomendação:

i. Devem ser definidas regras claras sobre localização, residência e soberania dos dados para garantir que os dados dos cidadãos são protegidos de acordo com as leis nacionais e contribuam para a segurança e a privacidade.

Princípio 6 – Integração, Escalabilidade e Flexibilidade: Este princípio promove flexibilidade, escalabilidade e permite a integração de serviços escritos em diferentes linguagens de programação. A busca por escalabilidade, flexibilidade e facilidade de manutenção deve resultar na consideração e adoção de vários caminhos arquiteturais. Sem escalabilidade, uma atividade governamental pode ter dificuldade em satisfazer a crescente procura, levando à insatisfação dos cidadãos e à potencial perda de confiança na capacidade do governo para prestar um serviço público eficiente. A flexibilidade, por outro lado, é a capacidade de um governo se adaptar às mudanças no ambiente de negócios que conduzem à introdução de novos serviços públicos ou à melhoria dos serviços públicos existentes.

Recomendação:

i. As soluções tecnológicas devem ser integráveis, escaláveis e flexíveis, permitindo ajustes rápidos e eficientes em resposta a mudanças na procura ou condições.

1.3.3 eGIF-GW: Requisitos técnicos

A adoção de standards abertos e a definição de standards de metadados são os dois principais requisitos técnicos para alcançar a interoperabilidade entre os MDAs. O pilar fundacional da interoperabilidade é a adoção de standards abertos, incluindo as especificações da Internet e da World Wide Web (W3c), para todos os sistemas governamentais.

- Standards abertos: Não existe uma definição globalmente aceite de standards abertos. No entanto, algumas características-chave dos standards abertos incluem a acessibilidade (livremente disponível para qualquer pessoa sem restrições), a interoperabilidade (entre diferentes sistemas, tecnologias ou aplicações de software) e a capacidade de evolução (concebidas para serem adaptáveis e evoluírem ao longo do tempo para satisfazerem os requisitos em mudança e os avanços tecnológicos).

  Recomendações:

  i. Os MDAs **devem** adotar de forma extensiva standards abertos e utilizar as tecnologias da Web e da Internet para o desenvolvimento de plataformas de serviços eletrónicos.
  ii. Os MDAs **devem** apresentar os recursos Web nos formatos XML ou JSON.

- Standards de metadados: Os standards de metadados é um requisito que se destina a estabelecer um entendimento comum do significado ou da semântica dos dados, para assegurar a utilização e interpretação corretas e adequadas dos dados pelos seus proprietários e utilizadores. Para alcançar este entendimento comum, é necessário definir um certo número de características ou atributos dos dados, também conhecidos como metadados. O objetivo deste standard é apoiar a interoperabilidade entre todos os MDAs para a descoberta, utilização e gestão de dados online.

  Recomendação:

  i. Recomenda-se a adoção dos standards abertos internacionais constantes do **Apêndice 1 - Standards de metadados** para standards de metadados em áreas específicas da implementação dos serviços online, a fim de garantir a interoperabilidade dos sistemas (transferência de informações) e a descoberta de recursos na Web.

1.3.4 eGIF-GW: Requisitos gerais

Com base nos requisitos de interoperabilidade para a prestação de serviços públicos e administrativos integrados entre os MDAs, que são a **"identificação dos processos"**, a **"conformidade com as normas"**, a **"colaboração dos sistemas informáticos"** e a **"instituição de um quadro jurídico"**, é evidente que, de um modo geral, os fatores humanos e tecnológicos são fundamentais para obter resultados significativos da interoperabilidade dos sistemas informáticos.

A Tabela 1 mapeia os requisitos de interoperabilidade e as áreas de foco aos fatores correspondentes.

Tabela 1: Requisitos de interoperabilidade

Área de foco da interoperabilidade	Descrição	Fator
Identificação do processo	Definição de processos dentro e entre MDA(s) para prestar um serviço integrado, ou seja, identificar e acordar os processos necessários	Humano
Conformidade com a norma	Apresentação dos dados entre sistemas informáticos/administração eletrónica díspares de forma padronizada e significativa, ou seja, a capacidade dos sistemas informáticos cooperantes para compreenderem da mesma forma o significado dos dados trocados	Tecnologia
Colaboração em sistemas informáticos	A capacidade de os sistemas de TI comunicarem de forma contínua e utilizarem os dados transferidos de forma compreensível para uma prestação eficientes de serviços públicos, ou seja, uma transferência de dados sem descontinuidades através da infraestrutura informática	Tecnologia
Instituição do quadro jurídico	Capacidade de criar quadros regulamentares que definam o âmbito da interoperabilidade, ou seja, identificar os domínios em que o quadro jurídico pode ter de ser alterado ou atualizado.	Humano

Além disso, a Tabela 2 mapeia os requisitos de interoperabilidade e os domínios de foco nas camadas de interoperabilidade correspondentes:

Tabela 2: Requisitos de interoperabilidade e áreas de foco para as camadas de interoperabilidade correspondentes

Área de foco da interoperabilidade	Camada de interoperabilidade	Descrição
Identificação do processo	Organização	A capacidade dos MDAs para definir, implementar e gerir processos e outros obstáculos organizacionais para a prestação de serviços entre entidades, ou seja, reengenharia de processos, incluindo alterações de processos, estruturas organizacionais, etc.
Conformidade com a norma	Semântica	A capacidade de apresentar os dados de forma padronizada, partilhada e significativa aos sistemas e infraestruturas de TI que cooperam entre si, permitindo a transferência de dados, ou seja, que os dados sejam interpretados e processados com o mesmo significado
Colaboração em sistemas informáticos	Técnica	A capacidade de cooperação das infraestruturas/aplicações de TI para comunicarem sem problemas e utilizarem os dados transferidos de forma compreensível para a prestação e o fornecimento de serviços públicos, ou seja, preocupações técnicas como questões técnicas na interconexão de sistemas e serviços TIC, armazenamento e arquivo de informações,

		protocolos para a transferência de informações e ligação em rede, segurança, etc.
Instituição do quadro jurídico	Jurídico	Capacidade de efetuar "controlos de interoperabilidade", analisando a legislação existente para identificar os obstáculos à interoperabilidade, a coerência e a aplicabilidade digital; e, na ausência de legislação, criar uma para apoiar legalmente a interoperabilidade.

Em suma, pode dizer-se que a interoperabilidade da governação eletrónica exige fatores humanos e tecnológicos. No que respeita aos fatores tecnológicos, as diferentes tecnologias devem basear-se em standards abertos e na definição de metadados.

1.3.5 Quadro de Interoperabilidade da Governação Eletrónica

A fim de desenvolver um quadro prático de interoperabilidade da governação eletrónica, os fatores humanos e tecnológicos da interoperabilidade para a prestação de serviços integrados entre os MDAs acima mencionados devem ser analisados na globalidade. Por conseguinte, para garantir o êxito dos projetos de governação eletrónica, todos os interesses relacionados com o fator humano devem estar em equilíbrio. Isto inclui os interesses e a estrutura política, as posições das leis e dos quadros regulamentares que regem os serviços públicos e o governo em geral, e as competências de gestão e as ferramentas necessárias para trazer eficiência na governação devem ser geridas adequadamente.

O quadro de interoperabilidade da governação do e-GIF-GB está representado na Figura 1.

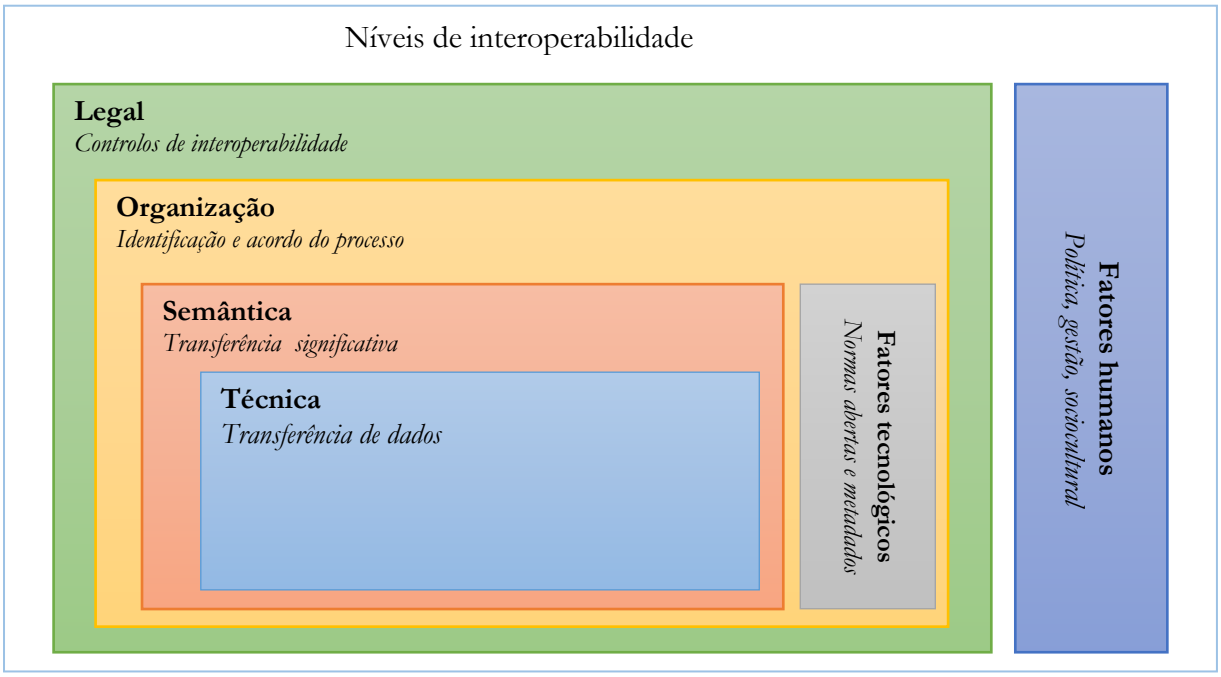

Figura 5 - Quadro de Interoperabilidade da Governação Eletrónica eGIF-GW

Considera os fatores humanos e tecnológicos na construção de um quadro de interoperabilidade torna-se prático e sustentável. Estes fatores atravessam os níveis de interoperabilidade, do organizacional ao jurídico ao semântico e técnico. Conforme está representado na figura 5 acima.

Conforme indicado na figura, a Interoperabilidade Legal é apoiada pela Interoperabilidade Organizacional, que por sua vez é apoiada pela Interoperabilidade Semântica, que por si só é apoiada pela Interoperabilidade Técnica. Consequentemente, a interoperabilidade técnica constitui a base para o eGIF-GW. A governança facilita e reforça a implementação do eGIF-GW.

Os fatores humanos podem ainda ser divididos em:

- Política: Para questões relacionadas com a estratégia. No contexto político, espera-se o apoio e o empenho das autoridades, a definição de políticas/orientações e estratégias para os diferentes níveis de interoperabilidade.
- De gestão: Para questões como a formação, a motivação e a reorientação das pessoas afetas aos MDAs.
- Económico: Para questões relacionadas com o financiamento.
- Social cultural: Para as características sociais/culturais dos intervenientes no sistema. Os fatores sociais/culturais, como as diferenças culturais, as práticas de trabalho, as questões de confiança, os prazos e as questões de exclusão social, têm mais influência.

1.4 Camadas de interoperabilidade

Existem quatro camadas de interoperabilidade que precisam ser definidas. Estas camadas de interoperabilidade estão detalhadas no modelo de interoperabilidade (Figura 6) que é aplicável a todos os serviços públicos e administrativos do governo.

Figura 6 - Modelo de interoperabilidade

Os quatro níveis de interoperabilidade são: jurídico, organizacional, semântico e técnico. No topo destes níveis está a estrutura da governação eletrónica, que inclui

1.4.1 Interoperabilidade Legal

Cada MDA que tem um papel a desempenhar na prestação de serviços públicos e administrativos é obrigado a trabalhar no âmbito de um quadro jurídico nacional específico. A interoperabilidade jurídica assegura que as organizações que funcionam com diferentes quadros jurídicos, políticas e estratégias possam colaborar. Para tal, é necessário garantir que as legislações existentes não bloqueiam o estabelecimento de serviços públicos e administrativos e que existam acordos claros sobre a forma de lidar com as diferenças nas legislações, incluindo a opção de adotar nova legislação.

A principal atividade para verificar o requisito legal de interoperabilidade consiste em efetuar **"verificações de interoperabilidade"**, examinando as legislações existentes para identificar possíveis áreas que constituam barreiras à interoperabilidade. A coerência entre as legislações, no que diz respeito à garantia da

interoperabilidade, deve ser efetuada antes da sua adoção e através de uma avaliação regular do desempenho dessas legislações, uma vez comecem a ser utilizadas.

A Guiné-Bissau não dispõe do quadro jurídico e regulamentar adequado necessário para sustentar uma transformação digital e as leis existentes estão geralmente desatualizadas, algumas das quais datam do período colonial. A maioria dos instrumentos jurídicos tem mais de 20 anos e não abordam os principais desafios socioeconómicos, tecnológicos, ambientais e políticos que a nova era da transformação digital trouxe ao país. Apesar dos princípios estabelecidos na Constituição, a verdade é que não existem diplomas legais publicados sobre proteção de dados e privacidade, interoperabilidade, utilização e reutilização de dados, assinatura eletrónica, comércio eletrónico, contratação pública eletrónica, acesso e partilha de informação e não existem mecanismos eficazes para garantir a cibersegurança ou combater o cibercrime.

Tendo em conta a falta de um quadro jurídico adequado que permita a interoperabilidade, a Guiné-Bissau deve desenvolver legislação nos seguintes domínios

- Lei de propriedade intelectual;
- Lei de Inclusão Digital;
- Lei de Governança Eletrónica;
- Legislação sobre Crimes Digitais;
- Regulamentação sobre a Economia Digital (regulamentação sobre aspetos como moedas digitais, serviços financeiros digitais e comércio eletrónico transfronteiriço, etc.);
- Lei de Responsabilidade do Fornecedor de Serviços Digitais;
- Lei da Neutralidade da Rede;
- Regulamento sobre Transformação Digital no Sector Público;
- Proteção de dados;
- Arquivamento;
- Combate à cibercriminalidade;
- Assinaturas eletrónicas e validade dos contratos eletrónicos;
- Legislação da concorrência;
- Acesso à informação, nomeadamente o acesso aos registos públicos;
- Contratos públicos eletrónicos; e
- Regime-quadro de interoperabilidade.

Recomendações:

A conceção e a elaboração de um regime de interoperabilidade podem ser realizadas por vários meios. As diferentes vias possíveis incluem vários elementos. Como ponto de partida, é importante notar que existem vários níveis de estatutos, como as leis emitidas pelo Parlamento ou os decretos emitidos pelo Conselho de Ministros, etc. De um ponto de vista pragmático, quanto mais elevado for o nível do diploma que vai estabelecer a interoperabilidade, maior será a necessidade de todos os outros diplomas de nível hierárquico inferior o respeitarem. Por conseguinte, uma lei aprovada pelo Parlamento é de longe a solução mais adequada.

Tendo em conta o atual panorama jurídico, é importante que qualquer legislação, quer setorial quer geral, seja preparada de modo a permitir a partilha de informações entre ministérios, caso contrário haverá limitações no quadro da interoperabilidade.

No que respeita ao conteúdo do diploma que estabelece o regime de interoperabilidade, este pode ser mais ou menos pormenorizado. Tendo em conta a rapidez da evolução tecnológica, é aconselhável que o diploma contenha certos princípios obrigatórios, permitindo, ao mesmo tempo, abranger a evolução tecnológica.

1.4.2 Interoperabilidade organizacional

A interoperabilidade organizacional assegura a gestão e a aplicação eficazes dos processos necessários para a prestação de serviços entre entidades. Identifica e aborda eventuais obstáculos, incluindo questões de propriedade dos dados, estrutura do serviço público, requisitos das tecnologias da informação e gestão dos processos, etc.

A interoperabilidade organizacional está relacionada com a coordenação e o alinhamento de processos empresariais e estruturas de informação que abrangem fronteiras intra e interorganizacionais (como a reengenharia de processos, incluindo ordens governamentais, alterações de processos e estruturas organizacionais). O seu objetivo é promover a colaboração entre diferentes linhas de ministérios que pretendem trocar informações e que podem ter estruturas e processos internos diferentes. Trata de métodos comuns, processos e serviços partilhados para a colaboração, incluindo o fluxo de trabalho, tomada de decisões e a partilha de informações.

Standards rígidos de segurança e privacidade devem ser incorporados desde o início do desenho do processo, a fim de garantir que todas as fases de automação respeitem a confidencialidade e integridade dos dados.

A prestação de serviços públicos e administrativos transversais aos MDAs exige, pelo menos, as seguintes etapas

i. Identificação/Descoberta de serviços inter-entidades: Esta etapa identifica ou descobre serviços cujas prestações requerem duas ou mais entidade governamentais. Estes serviços podem ter sido prestados manual ou digitalmente, separadamente, por dois ou mais MDAs. No entanto, esses serviços devem ser digitalizados e prestados de forma integrada.
   Por outro lado, o sub-serviço do MDA "A" necessário para fornecer o serviço integrado do MDA "1" pode ser acedido pelo MDA "2" através de um serviço Web/API aberta da Entidade "A".

   Um MDA interessado ou qualquer parte interessada pode iniciar um serviço inter-entidades se esse serviço for benéfico para os cidadãos, empresas (promovendo uma maior facilidade em fazer negócios) e o país em geral.

ii. Identificação dos MDAs para a prestação de serviços: A prestação de um serviço integrado exige a identificação dos MDAs e/ou de terceiros envolvidos. A cooperação e a adesão dos MDAs são fundamentais para o êxito das outras etapas. Conhecer os MDAs envolvidos e as suas responsabilidades é muito importante para a prestação de serviços inter-entidades.

iii. Identificação e definição dos processos cruzados: Esta etapa identifica e define os processos cruzados exigidos pelos diferentes MDA para fornecer o serviço inter-entidades. Cada MDA envolvido deve definir especificamente os processos a digitalizar a partir do seu lado. Estes processos são sub-processos que devem ser integrados noutros subprocessos pelos MDAs cooperantes. Os processos podem ser descritos em termos narrativos e/ou sob a forma de um gráfico.

iv. Acordo de Processo: Esta etapa facilita a cooperação entre os MDAs participantes e define o papel de participação de cada parte interessada. A questão em torno do acordo do processo é que ele é de natureza humana. Requer o envolvimento activo dos MDAs participantes para chegarem a acordo sobre como automatizar os sub-processos de cada um dos MDAs. O envolvimento poderia acontecer através da estrutura de governação discutida na secção 1.5.1.

Basicamente, as seguintes questões devem ser resolvidas no acordo sobre o processo:

a. Propriedade dos dados
b. Identificação dos utilizadores
c. Questões jurídicas
d. Infraestrutura informática/aplicações necessárias.

e. Procedimentos Operacionais Normalizados
f. Acordos de nível de serviço
g. Mecanismos de transferência de processos.
h. Orientações e lista de controlo de conformidade
i. Gestão das alterações (deve ser elaborado um plano de gestão das alterações).

v. Standardização dos processos: Esta etapa identifica os Standards Abertas necessários para facilitar a integração dos sub-processos e a interoperabilidade entre diferentes MDAs. Isto exige a utilização de conceitos e standards de **gestão de processos empresariais (GPE)**. O objetivo dos standards GPE é assegurar a reutilização, a clareza das definições, a interoperabilidade e a portabilidade.

A padronização dos processos visa também unificar os procedimentos para um serviço comum entre os MDAs que utilizam diferentes etapas/métodos para o realizar. Isto facilita a integração de dados entre sistemas. Baseia-se principalmente na **Business Process Modelling Language Notation (BPMN)** como standard aberto para coordenar a sequência de processos e as mensagens que fluem entre diferentes processos em vários MDAs num conjunto de actividades relacionadas.

A BPMN descreve diretamente a **Business Process Execution Language (BPEL)**, que é um método de cálculo standardizado/formal para processos dinâmicos. A BPEL é uma linguagem baseada em XML utilizada para definir processos empresariais no âmbito de serviços Web. Garante que os processos empresariais podem ser diretamente mapeados para qualquer linguagem de modelação empresarial para execução imediata.

vi. Digitalização e automatização de processos: A identificação dos standards abertos necessários para a padronização dos processos facilita a automatização/digitalização dos processos conexos, como se indica a seguir, sendo os três primeiros realizados por cada MDA cooperante para automatizar os seus subprocessos necessários à prestação dos serviços integrados, enquanto os três últimos são implementados conjuntamente pelos MDAs cooperantes, seguindo os standards abertos em cada fase.

- *Desenho do processo*: A conceção de processos engloba a identificação dos processos existentes, a reengenharia de processos empresariais e a conceção de processos TO-BE. Inclui a identificação de processos que podem ser candidatos à automatização, a descrição das diferentes actividades que constituem cada um dos processos, a identificação de áreas de melhoria, se for caso disso, a reformulação da forma como o trabalho é realizado para reduzir os custos e corresponder melhor à visão da MDA, a documentação da conceção TO-BE em modelos e ferramentas de standards abertos para garantir uma gestão adequada dos processos. Deve indicar adequadamente o fluxo do processo e os intervenientes no mesmo. Se o sub-processo interno envolver um sub-processo de outro(s) MDAs, este facto deve ser indicado na conceção do fluxo do processo.
- *Modelação do processo:* Esta fase inclui a seleção de ferramentas de Standards Abertos e a implementação de um protótipo de processo de negócio. A criação de protótipos também ajuda a identificar as diferentes funções que estarão envolvidas no processo, as etapas específicas e, mais importante, quaisquer sub-processos que possam ser candidatos à reutilização.
- *Automatização do processo:* Nesta fase, o desenvolvimento de processos automatizados de início ao fim começará juntamente com quaisquer outras funcionalidades que possam ser necessárias para a visibilidade e a automatização. A automatização de processos implica a visualização e simulação completas dos sub-processos que podem ser replicados na fase de conceção e desenvolvimento do software/aplicação.
- *Execução do processo:* Esta fase inclui a integração de processos e a garantia de qualidade. Implica a integração dos sub-processos cooperantes para fornecer serviço(s) e garantia(s) integrados. Esta fase implica a ligação das bases de dados, aplicações ou sistemas dos MDAs que colaboram, incluindo sistemas antigos, sistemas de planeamento de recursos empresariais (ERP) e software de gestão das

relações com os clientes (CRM), etc. Nesta fase, o processo integrado deve estar pronto para ser implementado no ambiente de produção.

- *Monitorização do processo de negócio:* Esta fase centra-se na monitorização do comportamento do processo comercial automatizado entre os MDAs cooperantes para identificar áreas onde existem estrangulamentos e para delinear uma correção de problemas de desempenho, correções de erros, juntamente com a identificação de melhorias futuras.
- *Otimização do processo de negócio:* Esta fase refere-se à garantia de que as questões identificadas durante a fase de monitorização são resolvidas; e que qualquer área de melhoria no processo é modificada para satisfazer as necessidades de prestação de serviços integrados.

vii. Prestação de serviços: A prestação de serviços é o último passo para a prestação de serviços inter-entidades. Nesta fase, o processo integrado está pronto para ser implementado no ambiente de produção.

A interoperabilidade organizacional envolve muito mais elementos humanos do que tecnológicos. Por forma a atingir uma interoperabilidade com impacto, as questões relacionadas com a estrutura e a cultura das instituições de serviço público, os territórios e a reivindicação de funções que se sobreponham devem ser abordadas corretamente.

A nível organizacional, devem ser abordados os seguintes desafios:

i. Quem detém a propriedade, é responsável pela segurança e utiliza os dados deve ser identificado e acordado pelos MDAs colaborantes. Além disso, os desafios em torno de quem paga o serviço, a fórmula de partilha de pagamentos e os requisitos de infraestruturas, etc., devem ser resolvidos a nível organizacional.
ii. Deve ser tido em conta um orçamento adicional para a conformidade com a interoperabilidade.
iii. Os processos não transparentes e a resistência à mudança para novos processos e dados de processos existentes devem ser geridos adequadamente através de um processo de gestão da mudança.
iv. As questões políticas e jurídicas devem ser resolvidas em torno da prestação de um serviço integrado; e
v. As competências e os conhecimentos especializados necessários devem ser fornecidos através do reforço das capacidades e da sensibilização para a importância da interoperabilidade.

Recomendações:

- Um sistema de feedback/reclamações dos utilizadores da plataforma.
- Programas de formação e desenvolvimento de competências para funcionários de MDAs, com foco em gestão de mudança e capacidades de colaboração interdepartamental, além de competências técnicas.
- No seguimento do ciclo de vida da Gestão de Processos de Negócio (BPM), é recomendado que em cada fase se utilize Business Process Modeling Language Notation (BPMN) e Business Process Execution Language (BPEL) para se atingir o processo de automação. A razão para isso é porque o BPMN pode ajudar a modelar um BPEL antes de ele ser implementado ou ajudar a explicar um fluxo BPEL. Isso pode ser realizado utilizando ferramentas de código aberto em lugar de proprietárias.
- O uso da arquitetura/abordagem correta para uma organização deve basear-se na consideração cuidadosa dos requisitos e restrições do projeto. As opções são Arquitetura Orientada a Serviços (SOA), Arquitetura Orientada a Eventos (EDA), Arquitetura Orientada a Mensagens (MDA) e Arquitetura de Microsserviços (MSA). Consulte o Apêndice 3 – Abordagens Arquitetónicas: Prós e Contras para obter vantagens e compensações dessas opções.

1.4.3 Interoperabilidade semântica

A interoperabilidade semântica permite que os dados sejam interpretados e processados com o mesmo significado, informação, etc. A interoperabilidade semântica é vista como um aspeto fundamental na via da

integração da administração pública online e da melhoria da qualidade dos serviços. Aproveita tanto a estruturação como a codificação da transferência de dados, incluindo o vocabulário, para que os sistemas recetores possam interpretar os dados da mesma forma.

A integração semântica dos serviços de administração pública online significa que toda a informação relevante processada ou partilhada se baseia numa mediação e/ou tradução bem-sucedida do significado de início ao fim para os prestadores de serviços ou utilizadores (cidadãos, empresas, prestadores de serviços da administração pública), bem como para as aplicações de administração pública online/TI.

A interoperabilidade semântica inclui o seguinte, que deve ser informado pelos standards de interoperabilidade de dados (DIS - Data Interoperability Standards) a serem formuladas:

i. A capacidade das organizações para compreenderem os dados trocados de forma semelhante;
ii. A capacidade dos sistemas de software para utilizarem adequadamente os dados recebidos de outros sistemas de software;
iii. A forma como os elementos das estruturas de dados trocados estão relacionados com objetos, relações e eventos do mundo real;
iv. Transferência de informações sobre o contexto dos dados, ou seja, relações, operações e funcionamento em geral; e
v. Transferência de metadados entre organizações/entidades

Os standards de interoperabilidade de dados (DIS), a serem formuladas, devem também alcançar a interoperabilidade semântica, afirmando que

1. Os parceiros de transferência de dados têm um entendimento comum do significado dos dados partilhados;
2. As transferências de dados aderem ao entendimento partilhado; e
3. Os dados são trocados sem erros de interpretação.

Em termos de propriedade e manutenção dos dados, os MDAs que pretendam prestar um serviço inter-entidades com o objetivo de integrar diferentes recursos Web que contenham informações de serviços de sistemas antigos e torná-los acessíveis através de uma única plataforma devem deixar os dados e a sua manutenção a cargo das organizações proprietárias.

Os MDAs devem ter em conta os seguintes aspectos para alcançar a interoperabilidade semântica, de modo a integrar os serviços públicos e administrativos e outras iniciativas de governação eletrónica :

Activos de interoperabilidade semântica: De um modo geral, os ativos de interoperabilidade semântica centram-se no empacotamento dos dados (sintaxe) e na transmissão do significado dos dados (semântica). Eles tratam da estrutura dos dados, enquanto os ativos de interoperabilidade semântica explicam como os dados devem ser interpretados, ou seja, a estrutura e a interpretação dos dados.

Os ativos sintáticos estão relacionados com o bloco de construção **Esquemas** e a sua principal função é definir estruturas de dados de uma forma formal. Isto inclui esquemas (formato compatível com XML) e esquemas de metadados. O nível sintático de interoperabilidade é a primeira fase para alcançar a interoperabilidade semântica, porque proporciona um nível de formalização em torno de temas de dados conhecidos. Normalmente, isto é conseguido através da criação de repositórios de ativos para esquemas comuns e do estabelecimento de uma política de utilização a nível de todo o sector público. Isto é abordado na camada de interoperabilidade técnica de dados.

Os ativos semânticos estão relacionados com o bloco de construção **do Catálogo de Normas de Dados** e a sua principal função é fornecer uma terminologia central para garantir que os elementos de dados são interpretados da mesma forma pelas partes comunicantes. Estes ativos denotam recursos de informação que foram criados para garantir a interoperabilidade dos sistemas de informação. Os ativos semânticos para a interoperabilidade semântica estão divididos da seguinte forma

- Dicionários
- Thesauri
- Nomenclaturas
- Taxonomias
- Tabelas de mapeamento
- Ontologias
- Registos de serviços.

Note-se que a interoperabilidade semântica se centra aqui mais nos ativos semânticos, ao passo que a camada de dados na secção de interoperabilidade técnica aborda os ativos sintáticos.

Seguem-se as etapas para obter ativos de interoperabilidade semântica:

- *Análise da informação sobre o serviço inter-entidades:* Nesta etapa, são recolhidas e analisadas as informações relacionadas com o serviço integrado a ser prestado por dois ou mais MDAs. Esta fase descreve em pormenor a recolha e a análise do que, quem, onde (localizações dos MDAs), tempo, canais, natureza, requisitos, especificações, processos e legislação/regulamentação, etc., do serviço.

  Esta etapa pode ser realizada através da especificação de cenários e casos de utilização em modo de texto livre. O texto livre deve ser transformado num formato de tabela mais estruturado, contendo as necessidades de informação identificadas e o(s) serviço(s) correspondente(s), bem como o que os utilizadores do serviço têm de fazer para obter o serviço.

  A tabela que contém as entidades do serviço deve ser modelada utilizando a Linguagem de Modelação Unificada (UML) para produzir esquemas de modelação do fluxo de trabalho, tendo também em conta a BPMN.

- *Criar um glossário de tópicos e terminologias:* Esta etapa cria um glossário que contém todos os tópicos e termos relevantes necessários para descrever os serviços em questão. Cada entrada deve conter uma breve descrição do tópico, a sua relação com outros termos e as necessidades de informação correspondentes.
- *Criar um vocabulário controlado e agrupar os termos relacionados:* Com base no glossário, deve ser criado um vocabulário controlado. Cada serviço e tópico geral a ser descrito deve ser representado por um termo principal e, possivelmente, por termos relacionados adicionais. Todos os itens do vocabulário controlado devem ser agrupados em subgrupos hierárquicos através de relações definidas. Esta é uma forma de classificação de elementos relacionados chamada Taxonomia.
- *Conceber uma Ontologia:* A ontologia resolve o significado dos termos e as suas relações de uma forma formal. A descrição informal no glossário deve ser verificada para assegurar que reflecte o significado formal (e vice-versa).
- *Implementar a Semântica:* A implementação da ontologia consiste na utilização das construções acima referidas para a descrição e operação de serviços (por exemplo, criação de perfis de serviços na WSMO). A Linguagem de Modelação de Serviços Web (WSML) fornece a sintaxe e a semântica para a Ontologia de Modelação de Serviços Web (WSMO).

Recomendações:

- Recomenda-se que os standards de interoperabilidade de dados sejam formuladas de modo a abordar mais a interoperabilidade semântica.
- Os standards de metadados especificados no **Apêndice 1 - Standards de metadados** são recomendadas como standards para descrições de tópicos e terminologias de serviços.

- A Ontologia de Modelação de Serviços Web (WSMO)6 é recomendada como norma para fornecer um quadro baseado em ontologias, que apoia a implementação e a interoperabilidade de serviços Web semânticos.
- Recomenda-se a utilização da Web Service Modeling Language (WSML)7 para fornecer a sintaxe e a semântica do WSMO.
- Os desenvolvedores de TI, arquitetos de sistemas governamentais, legisladores e reguladores devem ser responsáveis por alcançar e garantir a interoperabilidade semântica.

1.4.4 Interoperabilidade técnica

A interoperabilidade técnica trata das questões técnicas da interconexão de sistemas e serviços TIC, armazenamento e arquivo de informações, protocolos para transferência de informações e ligação em rede, segurança, etc.); em geral, a interoperabilidade técnica foi considerada para classificar as normas em vários níveis ou domínios (por exemplo, domínio da apresentação, domínio da rede, domínio da transferência de dados, etc.)

A interoperabilidade técnica examina os elementos tecnológicos que ligam os sistemas de informação. Inclui especificações de interface, protocolos de comunicação seguros, serviços de interligação, apresentação e transferência de dados, aplicação e integração de dados para a prestação integrada de serviços públicos.

O objetivo da interoperabilidade técnica é utilizar uma série de standards e especificações técnicas para combinar uma variedade de infraestruturas, aplicações e serviços com vista à interoperabilidade dos sistemas e plataformas de governo eletrónico.

Modelo concetual de prestação integrada de serviços públicos: O modelo conceptual para a prestação integrada de serviços públicos é necessário para especificar uma visão clara dos componentes que constituem o ambiente integrado, apoiado por requisitos e procedimentos de interoperabilidade. O modelo conceptual promove a ideia de interoperabilidade desde a conceção. O modelo é apresentado na figura seguinte. Como se pode ver na figura, os serviços dos MDAs devem ser concebidos de acordo com o modelo acima e em conformidade com os princípios fundamentais do e-GIF-GB, alguns dos quais são reiterados no modelo conceptual para a prestação integrada de serviços públicos.

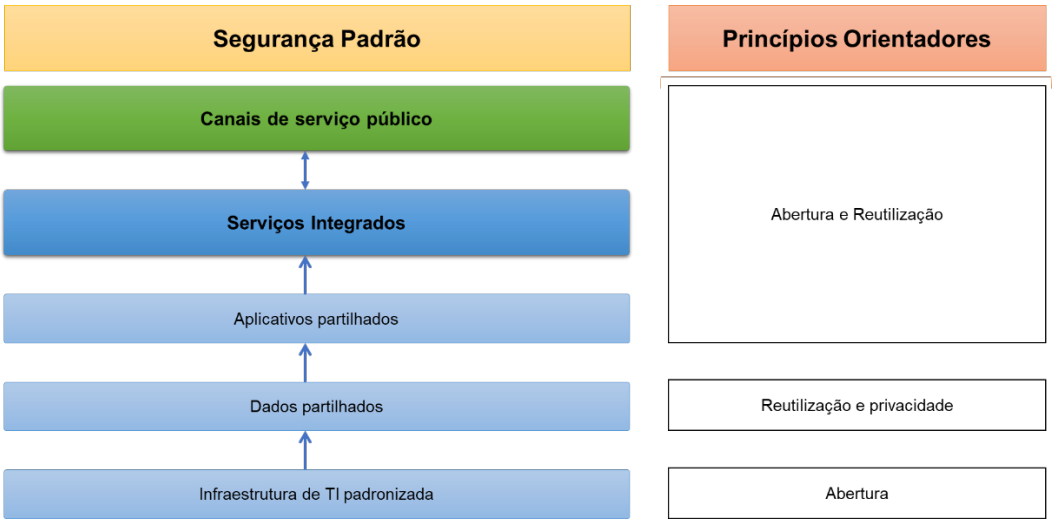

Figura 7 - Modelo integrado de prestação de serviços públicos

[6] https://www.w3.org/submissions/WSMO/
[7] https://www.w3.org/submissions/WSML/

Os domínios da arquitetura técnica de interoperabilidade explicados na secção seguinte devem ser observados para garantir que as infraestruturas/aplicações de governação eletrónica /TI cooperantes comuniquem sem problemas. Assegurará também que os dados trocados sejam utilizados de forma compreensível para a prestação de serviços públicos, de acordo com os requisitos e especificações de interoperabilidade organizacional e semântica. Os domínios da arquitetura de interoperabilidade técnica a observar são discutidos na secção seguinte.

Domínios da arquitetura de interoperabilidade técnica: Os domínios da arquitetura de interoperabilidade técnica criam uma lógica de organização para os dados, as aplicações e a infraestrutura, capturada num conjunto de relações, normas técnicas e escolhas para alcançar a padronização e a integração técnicas desejadas. O domínio da arquitetura de interoperabilidade técnica que reflete o modelo conceptual está representado na figura abaixo:

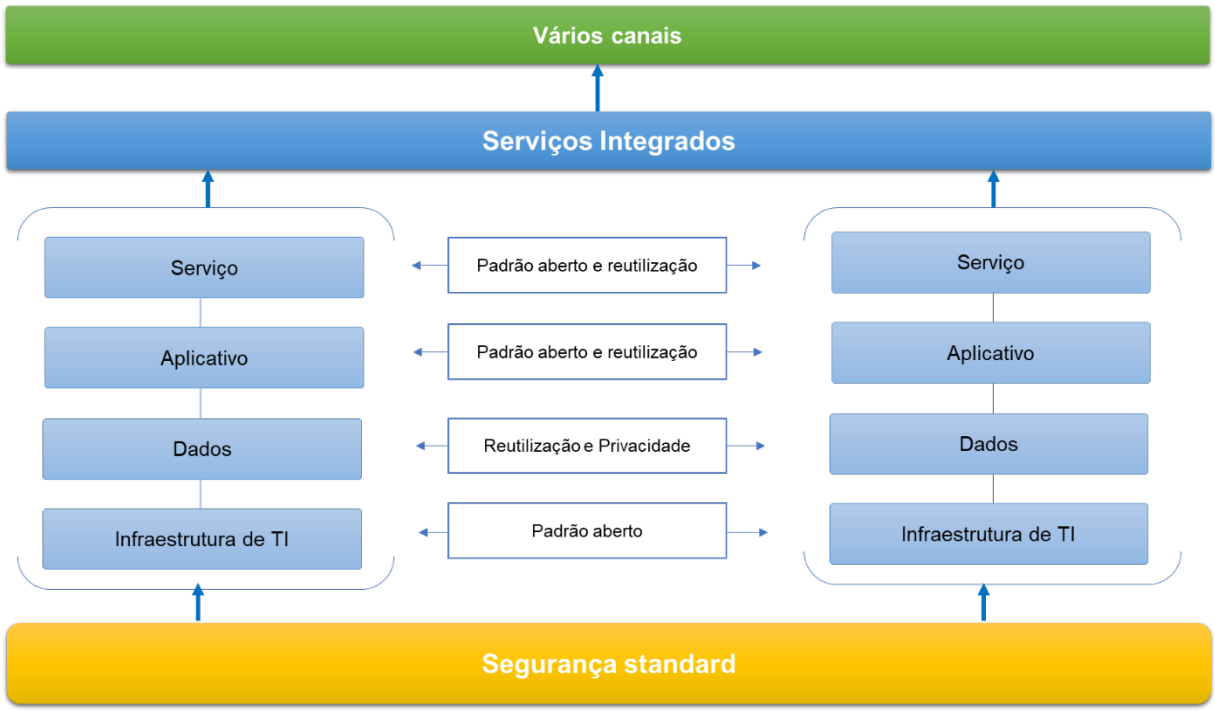

Figura 8 - Domínios arquitetónicos de interoperabilidade

Os domínios críticos da arquitetura de interoperabilidade considerados para uma interoperabilidade eficaz dos sistemas de governo eletrónico /TI são o canal, o serviço, a aplicação, os dados, a infraestrutura e a segurança. Estes são, em certa medida, capturados e alinhados com o Quadro de Arquitetura de Grupo Aberto (TOGAF)[8] , um domínio de arquitetura amplamente aceite para a arquitetura empresarial. Abrange a arquitetura de negócio, de dados, de aplicações e tecnológica como os quatro domínios de arquitetura comumente aceites como subconjuntos de uma arquitetura empresarial no seu canal de exclusão de ADM.

Para a segurança, o TOGAF vê-a como uma preocupação transversal. Como uma preocupação transversal, o TOGAF[9] descreve a Arquitetura de Segurança como impactando e informando as Arquiteturas de Negócios, Dados, Aplicativos e Tecnologia, conforme mostrado no diagrama abaixo.

[8] https://www.opengroup.org/togaf
[9] A Norma TOGAF, 10ª Edição - Um Guia de Bolso por Andrew Josey, e Dave Hornford.

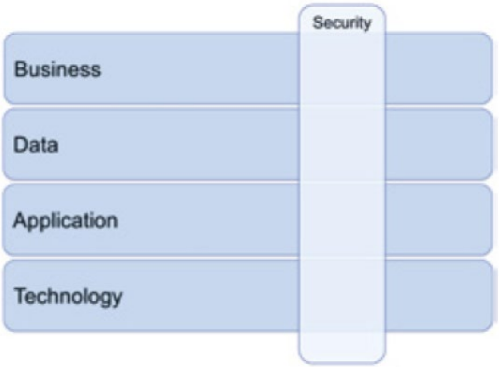

Figura 9 - A segurança como uma preocupação transversal à arquitetura

No entanto, a arquitetura empresarial no Método de Desenvolvimento da Arquitetura TOGAF (ADM) pode ser comparada ao domínio da interoperabilidade organizacional que já foi descrito na secção do documento relativa à interoperabilidade organizacional.

Os cinco grandes domínios arquitetónicos estão a ser especificados para satisfazer os requisitos de interoperabilidade tecnológica para a prestação de serviços integrados por dois ou mais MDAs.

- *Canal*: Os canais são o interface através da qual são prestados serviços públicos integrados. São fundamentais para o êxito da governação eletrónica e a prestação de serviços multicanais deve ser uma consideração de conceção. A adoção de multicanais para serviços integrados é um pré-requisito para a acessibilidade, a conveniência e a prestação de serviços a um custo acessível. Espera-se que todos os canais sejam interoperáveis entre si e com quaisquer dispositivos utilizados pelos utilizadores do serviço.

  Recomendações:

  - Recomenda-se que os centros de serviços comuns, os sítios Web/Portais, as plataformas móveis e o centro de contacto/centro de atendimento do Governo sejam canais que façam parte do serviço integrado. Consulte **o Apêndice 2 - Canal de serviços eletrónicos** para mais informações sobre estes canais de serviços eletrónicos.
  - Para os canais, recomenda-se que os MDAs elaborem e respeitem um documento contendo "Normas e diretrizes para sítios Web governamentais".
  - Para os canais móveis, os MDAs devem aderir às normas para aplicações Web em dispositivos móveis do W3C.

- *Serviço:* O domínio da arquitetura dos serviços é muito importante para a prestação de serviços integrados. A maioria dos serviços integrados deve ser fornecida através da Web, utilizando a Internet como meio de comunicação, devido à sua abertura, avanço e ampla adoção. A disponibilização de serviços através da Web, utilizando a Internet como meio de comunicação, trouxe o conceito de arquitetura orientada para os serviços (SOA) e de serviços Web.

  Recomendações:

  - Os MDAs devem adotar standards abertos para o desenvolvimento de API para aceder às suas infraestruturas/aplicações/serviços.
  - A adoção da abordagem REST para a implementação de serviços Web é recomendada devido à flexibilidade da abordagem.
  - As mensagens do consumidor de serviços (cliente) para o fornecedor (editor) e vice-versa devem ser apresentadas em XML ou JSON.

- *Aplicação:* Para além da SOA e dos serviços Web para a prestação de serviços integrados com base na Web, o Middleware pode integrar aplicações empresariais autónomas e de sistemas legados. Exemplos de serviços de middleware incluem a integração de aplicações empresariais (EAI), a integração de dados, o middleware orientado para as mensagens (MOM), os mediadores de pedidos de objetos (ORB) e o serviços empresariais de gestão de pedidos (ESB – Entreprise Service Bus).

  Além disso, o middleware facilita e gere a interação entre aplicações em plataformas informáticas heterogéneas e funciona como uma camada abstrata que esconde as complexidades da criação de aplicações distribuídas. Fornece serviços que facilitam a transferência de dados num formato standardizado.

  O Apêndice 4 - Serviços de middleware enumera os tipos de middleware com exemplos e uma breve descrição de cada um. Qualquer um destes middleware identificados pode ser adotado em função das necessidades e dos requisitos. O quadro geral é o mesmo, mas a arquitetura e a implementação variam.

  Recomendação:
  - A categoria de serviços de middleware que podem ser utilizados pelos MDAs para a interoperabilidade das aplicações é destacada no **Apêndice 4 - Serviços de Middleware**.

- *Dados:* Os dados são o único componente da arquitetura de interoperabilidade que atravessa o tecido das TIC, alimenta as aplicações e permite a prestação de serviços. É a componente mais importante da arquitetura de interoperabilidade. Para fornecer um serviço transversal, os dados são trocados entre a infraestrutura e as aplicações de governação eletrónica /TI dos MDAs que cooperam.
  O nível sintático de interoperabilidade é a primeira fase para alcançar a interoperabilidade semântica, porque proporciona um nível de formalização em torno de temas de dados conhecidos. Normalmente, isto é conseguido através da criação de repositórios de ativos para esquemas comuns e do estabelecimento de uma política de utilização ao nível de todo o sector público.

  Recomendação:
  - Os dados de cada MDA devem ser estruturados com base em standards para garantir uma transferência de informação sem descontinuidades. Isto implica que devem ser seguidos esquemas de dados uniformes.
  - Na sua maioria, estes esquemas são XML normalizados e esquemas de metadados. Determinam os atributos de dados para activos de dados "essenciais", como uma "Pessoa" (Nome, Data de Nascimento, Números de Telefone, etc.) ou uma "Organização" (Nome, Sector, Endereço, etc.). Os esquemas comuns são os requisitos sintáticos da interoperabilidade dos dados.

- *Infraestrutura informática:* A camada de infraestrutura TI da arquitetura de interoperabilidade inclui a combinação de componentes de hardware, sistema operativo, rede e base de dados. A figura abaixo detalha estes componentes.

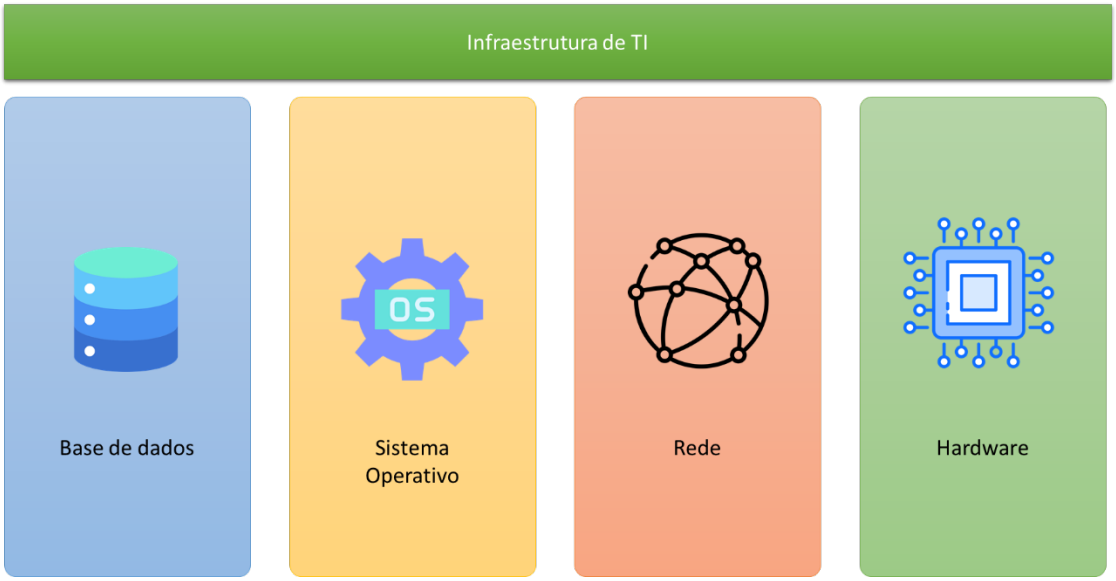

Figura 10 - Camada de infraestrutura de TI

O objetivo da arquitetura de interoperabilidade das infraestruturas de TI é garantir que o desenvolvimento de infraestruturas informáticas dos MDAs participantes utilize de forma compreensível os dados trocados para a prestação de serviços integrados ou transversais. Para atingir o objetivo, a implementação da infraestrutura informática deve basear-se em determinadas especificações, como a implementação do serviço Web.

Recomendação (Base de dados):

Recomenda-se a adoção do seguinte:

- Qualquer sistema de gestão de bases de dados relacionais (RDBMS) que suporte a SQL (Structured Query Language) da norma ANSI como linguagem padronizada de acesso.
- Qualquer sistema de gestão de bases de dados não relacionais (SGBD não relacionais), com base em requisitos específicos, que suporte a linguagem de consulta estruturada (SQL) e outras linguagens de consulta não exclusivamente SQL (NoSQL).
- O sistema de gestão de bases de dados implementado pelos MDAs deve suportar uma interface de programação de aplicações (API) padronizada para acesso à base de dados, por exemplo, conectividade aberta de bases de dados (ODBC)

Recomendação (sistema operativo):

- Recomenda-se a utilização de sistemas operativos (SO) que estejam em conformidade com os standards POSIX (Portable Operating System Interface). Exemplos de tais sistemas operativos são Unix, Linux, Windows, MacOS e Android, etc.

Recomendações (Rede):

Deve ser assegurado o seguinte:

- As redes de comunicação (LAN, WLAN, WAN, etc.) são construídas com base no modelo e protocolos TCP/IP
- As redes suportam standards abertos (por exemplo, normas com fios, sem fios e de segurança) e protocolos normalizados abertos.
- O equipamento de rede suporta a configuração com protocolos standard abertos.

Recomendações (Hardware):

O hardware deve:

- ser compatível com os sistemas operativos compatíveis com POSIX

- ser compatível com as interfaces padronizada (por exemplo, USB, SATA, Ethernet, etc.)
- ser atualizável para dar resposta a futuras necessidades.
- suportar a instalação de software de standards abertos (por exemplo, middleware)

- *Segurança:* O domínio da segurança define os serviços de segurança que são necessários em cada domínio do modelo de arquitetura de interoperabilidade. O nível de segurança é transversal a todas as camadas técnicas de interoperabilidade. Inclui standards, protocolos e tecnologias necessários para proteger a troca de informações, bem como o acesso seguro a informações e serviços do sector público.
  As medidas de segurança devem, sobretudo, garantir **a confidencialidade, a integridade, a disponibilidade e o não repúdio (tríade CIAN)** das informações e dos sistemas de informação. Estes são serviços de segurança fundamentais e os esforços de interoperabilidade não os devem comprometer. Os serviços implicam a cifragem dos dados, standards de infraestruturas de chaves públicas que suportam a utilização de chaves públicas e privadas de cifragem e decifragem, assinaturas digitais e protocolos de transmissão seguros. Incluem também o armazenamento, a utilização e a salvaguarda de informações sobre a identidade dos utilizadores, cidadãos, empregados e recursos.

  Recomendações (Hardware):

  Para atingir os standards de segurança da interoperabilidade, recomenda-se, no mínimo, o seguinte
  - O equipamento de segurança utilizado nos sistemas de administração pública online suporta protocolos e standards de segurança abertos.
  - A segurança é concebida nos sistemas de TI/e-Governo, sendo a interoperabilidade uma consideração fundamental, através da adoção de princípios de segurança desde a conceção.
  - Elaborar normas e orientações nacionais em matéria de segurança dos sistemas de informação e das redes e respeitar as suas disposições.
  - Desenvolva directrizes de proteção de dados e cumpra as suas disposições.
  - Cumprir os standards internacionais de Infraestrutura de Chave Pública (PKI).

1.5 eGIF-GW: Governação e Conformidade

A governação de uma organização refere-se a políticas, práticas e procedimentos seguidos por uma organização com base num quadro para mitigar o risco e garantir a conformidade. A conformidade, em si mesma, pode ser considerada como um subconjunto da governação, em que as organizações demonstram a conformidade com leis e regulamentos específicos ou com a residência de dados.

Para o Quadro de Interoperabilidade da Administração Pública Eletrónica para a Guiné-Bissau (eGIF-GW), o quadro de gestão da governação e da conformidade recomendado é descrito em seguida:

1.5.1 Estrutura de governação

Uma estrutura de governação é um sistema de regras, processos, funções e responsabilidades no âmbito do processo global de tomada de decisões do projeto eGIF-GW. É o quadro em que o projeto eGIF-GW é gerido e é responsável por garantir que o projeto é conduzido de acordo com a conceção do quadro de interoperabilidade.

Para governar adequadamente os quatro níveis de interoperabilidade, é necessário adotar uma estrutura de governação online, como se mostra na Figura 2 da secção 1.3. Assim, a estrutura de governação recomendada é a seguinte

- Comité Diretivo (CG): O Comité é responsável por supervisionar e fiscalizar todo o processo de prestação de serviços eletrónicos entre agências/entre serviços e deverá trabalhar para garantir o cumprimento de todos os standards.
- Grupo de Trabalho Técnico (GTT): O grupo é responsável pela implementação real do eGIF-GW e reporta ao GC como e quando necessário.

1.5.2 Gestão da conformidade

A prática da gestão da conformidade consiste na monitorização e avaliação constantes dos sistemas para garantir que cumprem os protocolos de gestão do risco e da conformidade, bem como as regras e normas empresariais e regulamentares. Uma estrutura de gestão da conformidade é uma estrutura especializada criada para gerir o nível de conformidade de uma organização relativamente a regras e regulamentos estabelecidos. Uma estrutura de conformidade define como os processos são usados para gerir a tecnologia, garantir a supervisão e assegurar a conformidade.

O desenvolvimento e a aceitação do eGIF-GW por todas as partes interessadas, sem uma adequada conformidade, não pode, por si só, atingir o seu objetivo. Assim, é fundamental que o eGIF-GW seja apoiado por uma conformidade adequada pelas partes interessadas. Atingir a interoperabilidade em conformidade com o eGIF-GW significa simplesmente que as partes interessadas cumprem com estas disposições.

O quadro de conformidade do eGIF-GW tem em conta a definição das funções e responsabilidades pela conformidade, bem como o processo de avaliação da conformidade.

I. Funções e responsabilidades em matéria de conformidade

Para garantir o cumprimento das disposições do eGIF-GW em todos os ministérios, departamentos e entidades, incluindo outras entidades parceiras não governamentais, serão definidas as seguintes funções e responsabilidades

Responsáveis pela conformidade (COs): Na qualidade de co-proprietários do eGIF-GW, espera-se que todas as partes interessadas trabalhem para garantir a aplicação efetiva do quadro. Assim, cada parte interessada, no cumprimento dos seus respetivos mandatos, responsabilidades e deveres, é instada a monitorizar, encorajar e assegurar a conformidade com os normativos,.

Tendo em conta o que precede, os seguintes responsáveis das organizações das partes interessadas serão os principais responsáveis pela conformidade:

- *Gestores de TI / Diretores de TI:* Este tipo de responsável pela conformidade deve ser o principal responsável por garantir o cumprimento das disposições do eGIF-GW, uma vez que é responsável pela aplicação efetiva das disposições técnicas. Por conseguinte, deve estudar criticamente, compreender e garantir que as suas respectivas organizações cumprem as disposições técnicas. Isto permitir-lhes-á recomendar adequadamente as especificações para a aquisição e instalação de sistemas informáticos, bem como para a atualização de sistemas antigos, em conformidade com as disposições do eGIF-GW. Além disso, permitir-lhes-á implementar eficazmente todos os projetos informáticos aprovados, em conformidade com as especificações aprovadas.
- *Chefes dos ministérios, entidade s e departamentos governamentais:* Estes responsáveis pela conformidade aprovam projetos informáticos em nome dos seus MDAs e departamentos/unidades. Por conseguinte, devem ser responsáveis por garantir a conformidade com as disposições do quadro. Assim, espera-se que estudem e compreendam cuidadosamente o eGIF-GW, bem como que assegurem que todos os projetos estão em conformidade com as disposições do quadro antes da aprovação.
- *Organismo adjudicante de projetos informáticos:* Todos os organismos envolvidos na aquisição de projetos de TI, incluindo departamentos/unidades de aquisição do governo, são igualmente responsáveis por garantir a conformidade com as disposições do eGIF-GW devido às suas posições estratégicas. Por conseguinte, são instados a estudar, compreender e garantir a conformidade com as disposições técnicas do quadro. Se estes organismos de aprovação descobrirem que um projeto proposto é suscetível de violar as disposições do FEGIF-BG, a aprovação deve ser recusada e o candidato deve ser aconselhado a cumprir as disposições.

Para além dos responsáveis pela conformidade acima referidos, os seguintes podem também ajudar a garantir a conformidade com o AEIF-GB:

- *Estrategas de negócio:* trabalham com e para o governo e são instados a estudar, compreender e fazer cumprir as disposições do eGIF-GW. A falha em assegurar que as estratégias de governo eletrónico/negócio eletrónico desenvolvidas estão em conformidade com o quadro, resultará na recusa dessa iniciativa, bem como na não atribuição de fundos governamentais para apoiar essa estratégia.
- *Programadores de aplicações:* aqueles interessados em trabalhar com ou para qualquer organização governamental no desenvolvimento dos seus sistemas, devem também estudar, compreender e cumprir com as disposições do eGIF-GW. Uma aplicação que não cumpra as disposições técnicas do quadro não será aceite ou patrocinada pelo governo.
- *Fornecedores de TIC:* os que pretendem transacionar com a administração pública ou prestar assistência a organizações governamentais na execução dos projetos destas devem garantir que todas as soluções de sistemas propostas à administração pública estão em conformidade com o eGIF-GW.

Comité Diretivo (CG): Para garantir o acompanhamento adequado da aplicação e do cumprimento das disposições do quadro, será criado um comité de trabalho denominado Comité Diretivo do eGIF-GW. O mandato do comité diretivo consiste em controlar a conformidade das partes interessadas com as disposições do quadro; reunir-se anualmente para avaliar o nível de conformidade das partes interessadas com as disposições do quadro; coordenar (se necessário) ou prestar assistência no desenvolvimento, promoção e adoção de normas, diretrizes e políticas que ajudarão a garantir a realização do objetivo deste quadro; e coordenar a revisão e atualização do quadro em conformidade com as disposições do eGIF-GW. Para que o comité diretivo possa reunir-se, o quórum é constituído quando houver 3 membros do comité mais o coordenador.

O comité deve ser composto por:

- Coordenador (representante da ITMA)
- Gestores de TI/Chefe de TI de cada uma das seguintes organizações
    - Ministério dos Transportes, das Telecomunicações e da Economia Digital
    - Ministério das Finanças
    - Ministério da Economia, Planeamento e Integração Regional
    - Ministério da Educação
    - Ministério da Saúde
    - Ministério da Agricultura
    - Ministério do Comércio e da Indústria
    - Ministério da Informação
    - Ministério das Obras Públicas
    - Ministério da Justiça
    - Ministério do Interior
    - Ministério dos Negócios Estrangeiros
    - Ministério da Administração do Território.
    - Ministério do Turismo
    - Ministério do Ambiente
    - Alfândega (DG Alfandega)
    - Receitas e impostos (Contribuições & Impostos)
    - CNE (Comissão Nacional de Eleições)
    - Autoridade Reguladora das Telecomunicações (ARN)
    - Instituto Tecnológico de Modernização Administrativa (ITMA)
    - BCEAO (Banco Central)
- Um representante da Câmara de Comércio (CCIAS) enquanto grupo da sociedade civil

- No máximo 2 profissionais de TI representando o sector privado.

Grupo de trabalho técnico (TWG): Todos os MDAs são encorajados a criar um TWG interno que garanta que todos os projetos e iniciativas de TI estão em conformidade com as disposições do eGIF-GW; aconselhe atempadamente a sua administração sobre a necessidade de realizar anualmente avaliações de conformidade com o EGIF-GW; inicie e implemente serviços inter-entidade s conforme necessário; apresentar ao Comité Diretivo do eGIF-GW um relatório sobre o estado da avaliação de conformidade do eGIF-GW realizada na sua organização, até 31 de janeiro, através dos gestores de TI / chefes de TI; e apresentar desafios, sugestões, inovações e ambiguidades, etc. e apresente os desafios, sugestões, inovações e ambiguidades, etc., encontrados no processo de implementação do eGIF-GW ao Comité Diretivo do eGIF-GW através dos Gestores de TI / Chefe de TI.

O grupo de trabalho técnico (TWG) deve ser composto por, pelo menos, 5 pessoas provenientes dos departamentos/unidades de TI e de negócios do MDA em causa. O grupo de trabalho técnico (TWG) deve ser dirigido pelos gestores de TI/chefe de TI. Após a criação do TWG, os detalhes dos seus membros devem ser comunicados ao Comité Diretivo do eGIF-GW; e todas as comunicações do TWG para o Comité Diretivo do eGIF-GW devem ser feitas através do chefe do TWG.

Uma vez que o quadro de interoperabilidade é introduzido pela primeira vez no país, é um pouco desafiador que todos os MDAs sigam os padrões exigidos e o nível de colaboração pode ser baixo, o ITMA, como agência líder, pode adotar uma estrutura de governança enxuta e ser flexível ao fazê-lo, caso a estrutura de governação proposta pareça complexa e pareça uma montanha suficientemente grande para ser superada, o que atrasa a implementação do quadro de interoperabilidade em específico e o projeto digital em geral.

II. Desafios em matéria de conformidade

Seguem-se as dificuldades que podem surgir na aplicação da conformidade com o eGIF-GW:

- Este quadro está sujeito à vontade das partes interessadas de cumprirem as especificações, políticas e normas estabelecidas. Por conseguinte, não se pode obrigar as partes interessadas a cumpri-lo, mas apenas incentivá-las. Tendo em conta o que precede, é necessário desenvolver diretrizes e normas vinculativas para garantir o cumprimento das disposições do presente quadro.
- Relativamente ao desafio acima referido, a avaliação da conformidade das partes interessadas depende da sua capacidade de efetuar a avaliação anual exigida e da sua vontade de apresentar um relatório ao GTT. O TWG não pode avaliar corretamente o nível de conformidade se as partes interessadas não conseguirem ou não tiverem capacidade para avaliar eficazmente o seu nível de conformidade com as disposições deste quadro ou se recusarem a apresentar o relatório exigido ou apresentarem um relatório falsificado.
- Nenhum MDA está autorizado a efetuar despesas num ano fiscal sem uma provisão orçamental aprovada. Assim sendo, os MDAs são incentivados a fazer provisões orçamentais adequadas para os projetos iniciados, a fim de garantir o cumprimento das disposições do eGIF-GW.

III. Avaliação do cumprimento

Para verificar o estado de conformidade das partes interessadas com as disposições do eGIF-GW, é necessário efetuar regularmente uma avaliação do sistema dos MDAs para determinar a conformidade com as disposições do quadro, bem como para verificar se violam alguma das suas especificações.

Recomenda-se que esta avaliação seja efetuada anualmente pelas partes interessadas nas suas várias organizações e que apresentem um relatório sobre o estado de conformidade ao Comité Diretivo do eGIF-GW até 31 de janeiro do ano seguinte ao da avaliação. Isto permitir-lhes-á medir e avaliar a conformidade geral com o quadro pelas partes interessadas.

2. PLATAFORMA DE INTEROPERABILIDADE

2.1 Visão geral

Uma vez estabelecido o quadro conceptual para a plataforma de interoperabilidade, deve ser proposta uma solução que permita a ligação dos sistemas, bases de dados e serviços do sector público, bem como a integração backend dos principais sistemas, registos, bases de dados e plataformas. Esta proposta deve também incluir os serviços públicos e administrativos identificados, a arquitetura de prestação de serviços e a própria plataforma de interoperabilidade de balcão único, apresentando as características, os processos de negócio, as aplicações/dados, a rede/infraestrutura, o serviço de pagamento, os relatórios, os serviços de apoio, as opções de alojamento (indicando especificamente o hardware e o software de apoio à plataforma de interoperabilidade), etc.

O conceito de middleware foi mencionado na secção 1.3.4 e pormenorizado no apêndice 4. Por conseguinte, a plataforma de interoperabilidade pode ser vista simplesmente como um middleware que se situa entre sistemas ou plataformas díspares, facilitando assim a transferência de dados entre estes sistemas de informação (SI) e assegurando um fluxo contínuo de informações ao garantir que estes sistemas comunicam e interpretam os dados num formato ou linguagem comuns. Veja uma ilustração abaixo:

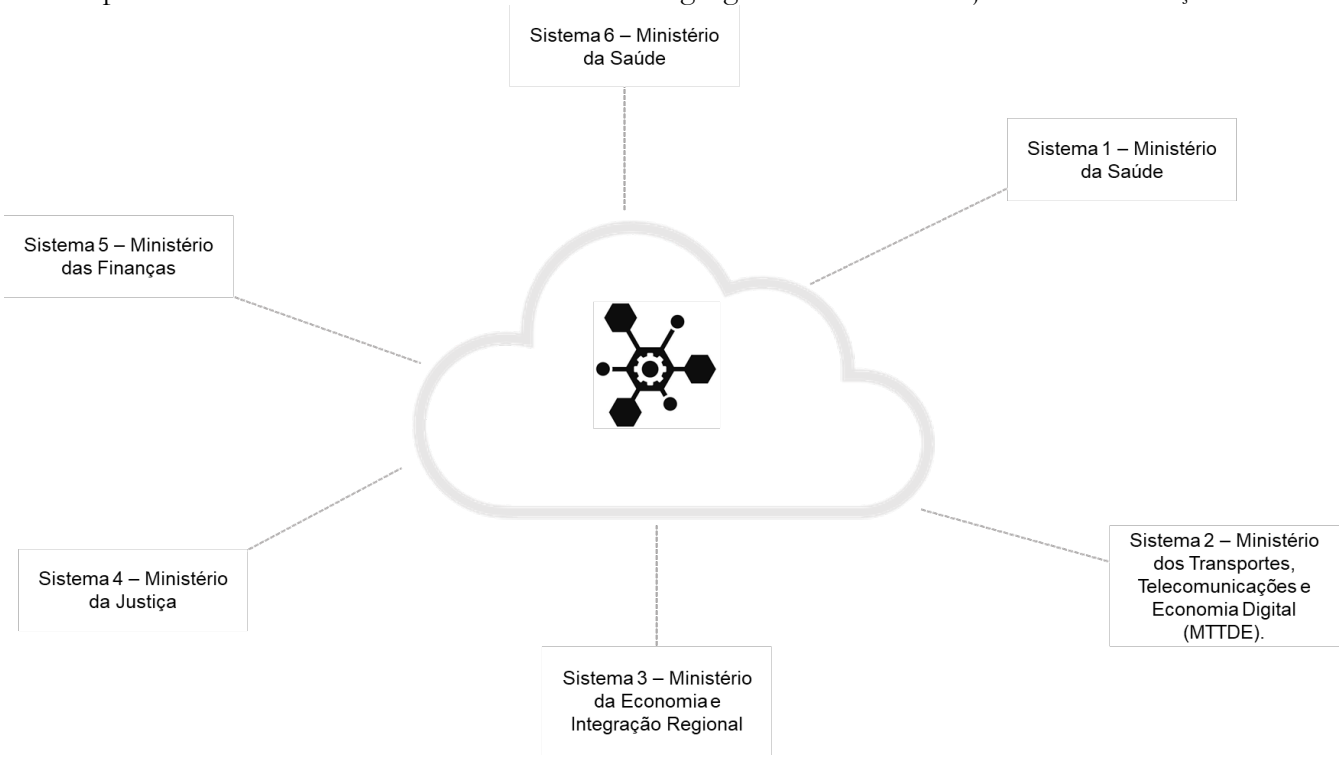

Figura 11 - Visão geral da plataforma de interoperabilidade

Nesta circunstância, todos os sistemas estão a unir-se para oferecer dados a uma única fonte que servirá agora de base para a prestação de serviços públicos e administrativos aos cidadãos e às empresas de uma forma fácil e contínua, para além das fronteiras da Guiné-Bissau.

2.2 Serviços públicos

Conteúdo aqui. No decurso da nossa avaliação diagnóstica/situacional do panorama digital, bem como das consultas das partes interessadas com os diferentes ministérios da Guiné-Bissau, foram identificados os serviços públicos e administrativos:

- Serviço de Identificação de Cidadãos

- Carta de condução
- Balcão único para as empresas/Registo de empresas
- Autorização de importação/exportação.
- Plataforma para estudantes
- Pedido de visto
- Passaporte
- Registo criminal
- Certidões de nascimento e de cidadania.
- Bilhete de identidade
- Apresentação e pagamento de encargos sociais.
- Registo de veículos
- Saúde materno-infantil e imunização
- Serviços de prevenção de complicações na gravidez
- Certidões de óbito
- Contratos públicos
- Desembaraço aduaneiro
- Contratos públicos
- Desembaraço aduaneiro
- Pagamento de direitos aduaneiros e impostos
- Apuramento fiscal.
- Apresentação e pagamento de impostos.

O quadro que se segue apresenta um mapa dos serviços públicos e administrativos para os MDAs responsáveis:

Tabela 3: Cartografia dos serviços públicos e administrativos

Ministério	Serviços
Instituto Tecnológico de Modernização Administrativa	• Serviço de Identificação de Cidadãos
Direcção Nacional de Viação e Transportes Terrestres under MTTDE	• Carta de condução
Centro De Formalizacao de Emprego (CFE) under Ministério da Economia, Planeamento e Integração Regional	• Balcão único para as empresas/Registo de Empresas
Ministério do Comércio	• Autorização de importação/exportação
Ministério da Educação, do Ensino Superior e da Investigação	• Plataforma para Estudantes
Ministério dos Negócios Estrangeiros	• Pedido de visto
Ministério do Interior	• Passaporte
Ministério da Justiça	• Registo criminal • Certidões de nascimento e de cidadania • Bilhete de identidade • Apresentação e pagamento de encargos sociais. • Registo de veículos
Ministério da Saúde	• Saúde materno-infantil e imunização • Serviços de prevenção de complicações na gravidez • Certidões de óbito

Ministério das Finanças	• Contratos públicos • Apuramento fiscal • Apresentação e pagamento de impostos
Direcção Geral das Alfândegas under MTTDE	• Desembaraço alfandegário • Pagamento de notas aduaneiras e impostos

2.3 Catálogo de Serviços Públicos

O Catálogo de Serviços Públicos é um repositório central que reúne todas as informações relevantes sobre os serviços oferecidos pelo governo. Esta centralização é desejável para evitar redundâncias e garantir informação detalhada e atualizada sobre os serviços disponíveis. Um catálogo de serviços públicos não é apenas uma ferramenta para listar serviços, mas um componente essencial para garantir a eficácia, segurança e interoperabilidade da arquitetura de prestação de serviços num ambiente de governação eletrónica. É a espinha dorsal para a integração de serviços e a base para uma plataforma de serviços governamentais coesa e orientada para o utilizador.

O Catálogo de Serviços Públicos visa promover a abertura e a transparência relativamente aos dados detidos pelo serviço público, catalogando e descrevendo os dados do serviço público. Este catálogo pode ser fornecido como um portal web separado ou como um subportal dentro do portal principal do governo eletrónico e deve ser capaz de orientar os cidadãos e as empresas sobre os dados que o serviço público do GoGB possui. Esses dados também devem ser classificados de acordo com informações pessoais, comerciais, espaciais, pessoais sensíveis ou protegidas.

O portal deverá disponibilizar um catálogo de conjuntos de dados (datasets) detidos pelo serviço público e ter uma funcionalidade de busca para conjuntos de dados com base na classificação dos setores. Além disso, devem ser transmitidos os catálogos das APIs dos serviços público da Guiné-Bissau, incluindo os standards das APIs do serviço público.

Para aproveitar os serviços públicos existentes e atingir os seus objetivos, os potenciais utilizadores de serviços públicos (cidadãos e empresas) precisam de encontrar facilmente informações executáveis e normalizadas sobre serviços públicos relevantes através de pesquisas multicanais, incluindo em portais governamentais e outros sítios Web públicos e privados; compreender de forma autónoma a informação constante nos referidos portais bem como as ações a empreender para avançar com o seu projeto; usufruir de procedimentos simplificados e normalizados que lhes permitam beneficiar de serviços públicos a todos os níveis; e receber apoio e assistência das autoridades competentes quando necessário.

Para otimizar a qualidade e eficiência dos seus serviços, os prestadores de serviços públicos (governo e seus MDAs) precisam de ser capazes de descrever os seus serviços apenas uma vez num formato legível por máquina para permitir a disseminação generalizada da informação em todos os canais; trocar informações com outras administrações públicas, em todos os níveis; ter acesso a todas as descrições de serviços públicos na Guiné-Bissau; e aproveitar as melhores práticas de outros prestadores de serviços para melhorar a sua oferta, qualidade e eficiência de serviços.

Abaixo estão as melhores práticas para criar um catálogo de serviços públicos:

- Harmonização da informação sobre serviços públicos utilizando padrões comuns e abertos: É necessário harmonizar todos os dados existentes sobre serviços públicos e mapeá-los em relação a padrões comuns para garantir a disseminação generalizada de informação qualitativa sobre serviços públicos em todo o país e otimizar a eficiência dos serviços públicos.
- Centralização da informação através de plataformas comuns: Uma vez harmonizadas as descrições dos serviços públicos utilizando padrões de dados comuns, o próximo desafio é tornar a informação facilmente acessível e pesquisável para o utilizador final. Idealmente, todas as informações sobre

serviços públicos deveriam estar disponíveis num portal único, onde os cidadãos, as empresas e as organizações possam encontrar a informação de que necessitam.

- Garantir uma experiência de utilizador consistente: As principais características de um portal de balcão único bem-sucedido abrangem aspetos como a qualidade e a disponibilidade de informações atualizadas, a disponibilidade de serviços online, a acessibilidade transfronteiriça e a facilidade de utilização do portal. Uma experiência de utilização de alta qualidade incentiva potenciais utilizadores de serviços a realizarem sistematicamente as suas pesquisas em portais governamentais, reduz a necessidade de apoio e reforça o valor acrescentado dos catálogos de serviços públicos.
- Estabelecer recursos de pesquisa fáceis de usar: Um componente vital do que torna um catálogo de serviços públicos útil e fácil de usar para os cidadãos e as empresas é a forma como permite a pesquisa de informações. Os balcões únicos e outros portais de governo eletrónico enfrentam frequentemente o desafio de terem de fornecer uma estrutura facilmente compreensível para informações complexas e em vários níveis. Para utilizadores finais não familiarizados com estruturas organizacionais ou costumes locais, uma caixa de pesquisa de texto livre pode ser quase totalmente inútil. Algumas orientações que indiquem aos utilizadores a área certa de acordo com os acontecimentos empresariais ou da vida irão ajudá-los a restringir a categoria de serviços de que necessitam e contribuir para poupar tempo.

2.4 Arquitetura de entrega dos Serviços públicos

A arquitetura da prestação dos serviços públicos define o modo como a plataforma de interoperabilidade se integra na prestação dos vários serviços públicos e administrativos identificados na lista da secção anterior.

Com base na nossa avaliação da arquitetura de prestação de serviços de vários países, e na sequência da nossa avaliação no local do panorama digital da Guiné-Bissau, a figura abaixo indica a arquitetura de prestação de serviços proposta

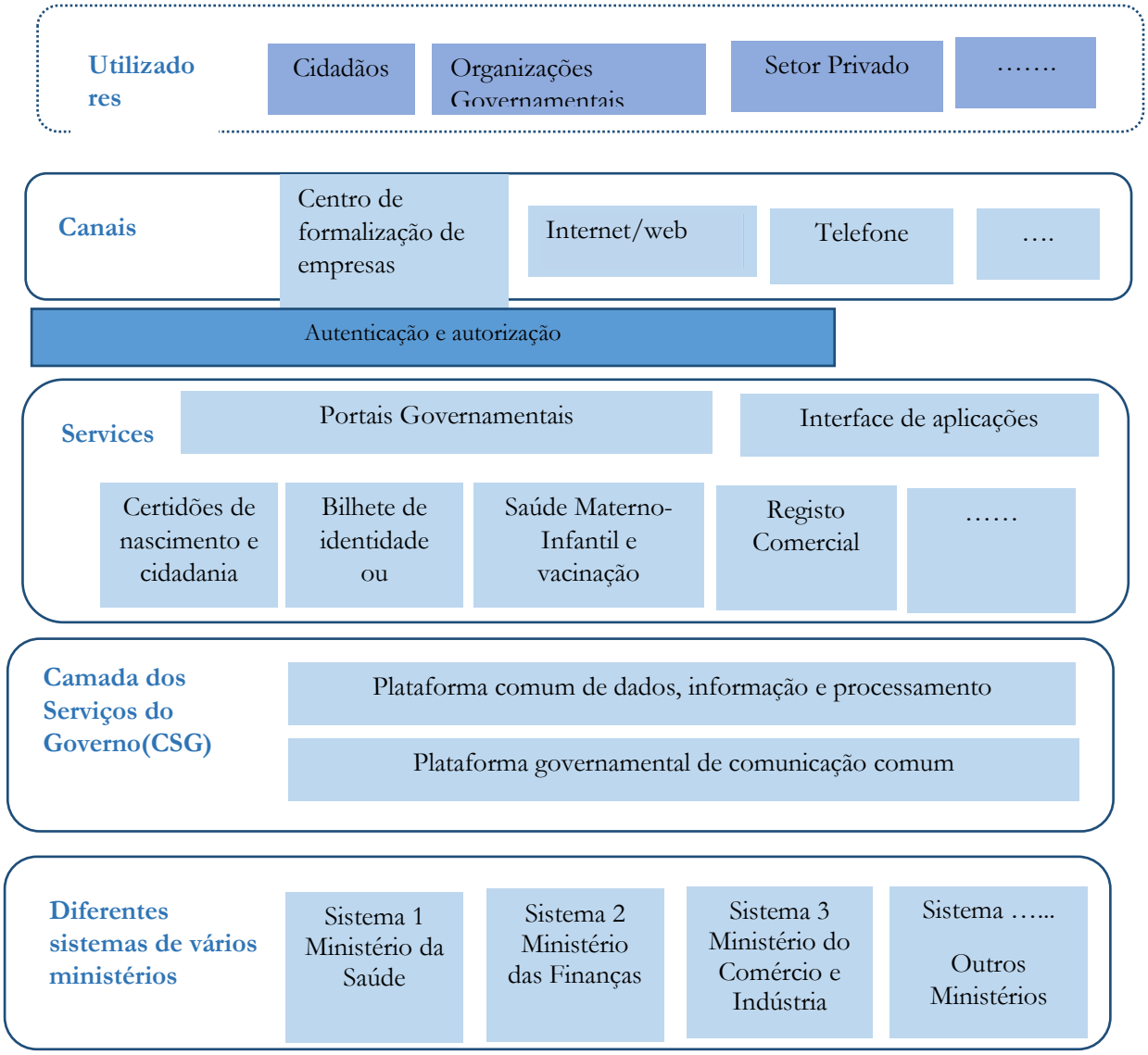

Figura 12 - Arquitetura de prestação de serviços

Na arquitetura de prestação de serviços acima, distinguimos as diferentes camadas de prestação de serviços para o governo, incluindo:

- Utilizadores: são os atuais destinatários dos serviços, incluindo os cidadãos, o sector privado/empresas, organizações do governo, etc
- Canais: são os mecanismos de prestação de serviços, tais como balcão único, plataforma web/internet, número de linha telefónica/de serviço, etc.
- Serviços: são serviços de governo eletrónico, como certidões de nascimento e cidadania; antecedentes criminais; bilhetes de identidade ou passaportes; saúde materno-infantil e imunização; etc.

No topo da camada de Serviços há um bloco para autenticação e autorização que indica que os serviços oferecidos por meio de um portal governamental ou de interfaces de aplicações podem exigir procedimentos de autenticação e autorização.

Sistema de Serviços Governamentais (GSBus): é o núcleo da interoperabilidade. É um sistema que permite às entidades governamentais trocar dados sem problemas e prestar os seus serviços de forma integrada. O sistema atende às necessidades dos cidadãos para obter o serviço sem passar de uma entidade para outra. O GSBus constitui duas componentes principais que são a plataforma comum de informação (que fornece

interoperabilidade de dados, serviços e processos) e a plataforma comum de comunicação (que fornece rede e infraestrutura).

Sistemas existentes de diferentes ministérios: representam sistemas de informação existentes dos ministérios que oferecem o serviço, que podem ser conformes com SOA ou existir como sistemas legados. Exemplos de tais sistemas são o pedido de registo comercial do Ministério da Economia e integração regional; e a aplicação de Registo do Estado Civil que funciona internamente no Ministério da Justiça.

Os padrões de interoperabilidade descritos na parte do quadro de interoperabilidade deste relatório, tais como serviços web, padrões de segurança, integração e interconexão de dados, metadados, acesso à informação e camadas de apresentação, devem ser integrados na arquitetura de prestação de serviços. Consulte o apêndice 5 para padrões de rede e infraestrutura relacionados com a interconexão e segurança; apêndice 6 para padrões de serviços da Web que visam alcançar interoperabilidade de processos; e o apêndice 7 para integração de dados, metadados, acesso à informação e camadas de apresentação para alcançar a interoperabilidade semântica dos dados; todos eles são componentes arquitetónicos que suportam a arquitetura de entrega de serviços.

2.5 Plataforma de serviços públicos

Em primeiro lugar, a plataforma de serviços públicos fornece uma base de dados única para os diferentes sistemas de silo da administração pública que são definidos na camada "Sistema existente de diferentes ministérios" na arquitetura de prestação de serviços. O diagrama de fluxo abaixo mostra como a plataforma de interoperabilidade serve como fonte central de dados para sistemas de silos díspares geridos por diferentes ministérios, entidade s e departamentos:

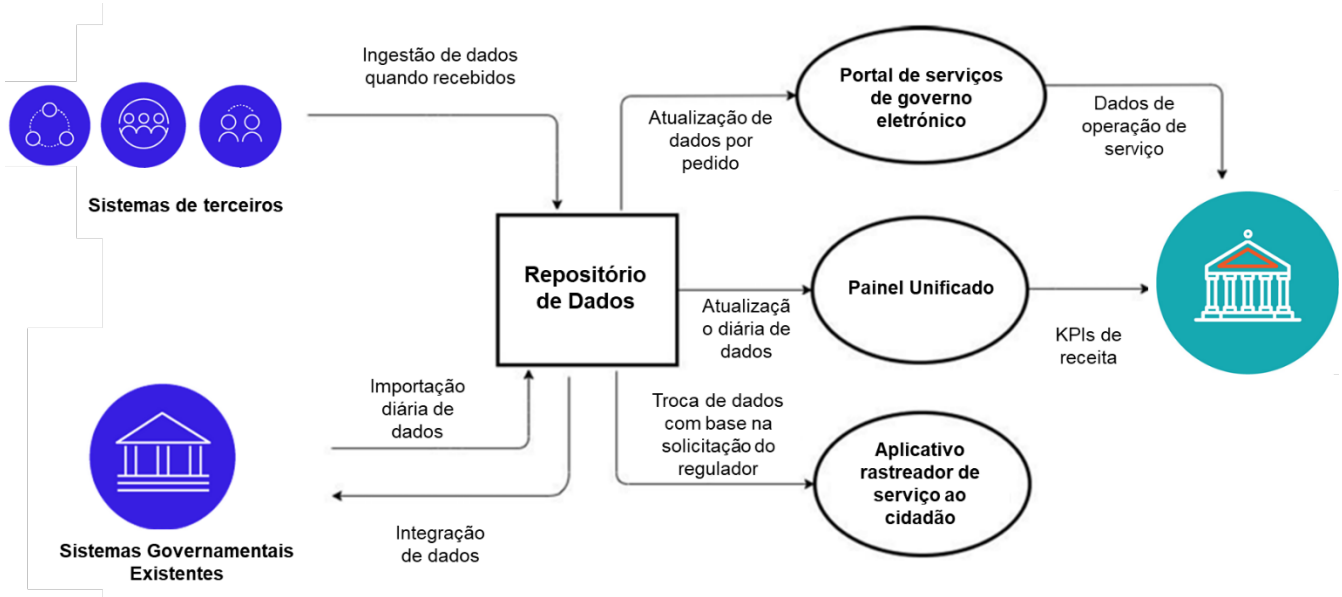

Figura 13 - Diagrama de fluxo de interoperabilidade

Em segundo lugar, a plataforma funciona como uma aplicação de balcão único para aceder aos serviços de governação eletrónica através de um portal Web ou de uma interface de programação de aplicações (API) baseada nos standards Web e nos protocolos/abordagens de serviços Web recomendados na parte do quadro de interoperabilidade do presente relatório. Esta plataforma de serviços enquadra-se na "plataforma comum de comunicação governamental" do nível do barramento de serviços governamentais (GSB) da arquitetura de prestação de serviços acima descrita. O diagrama seguinte descreve o acesso aos serviços de administração pública online e o fluxo de dados entre os utilizadores e a base de dados central da plataforma de interoperabilidade.

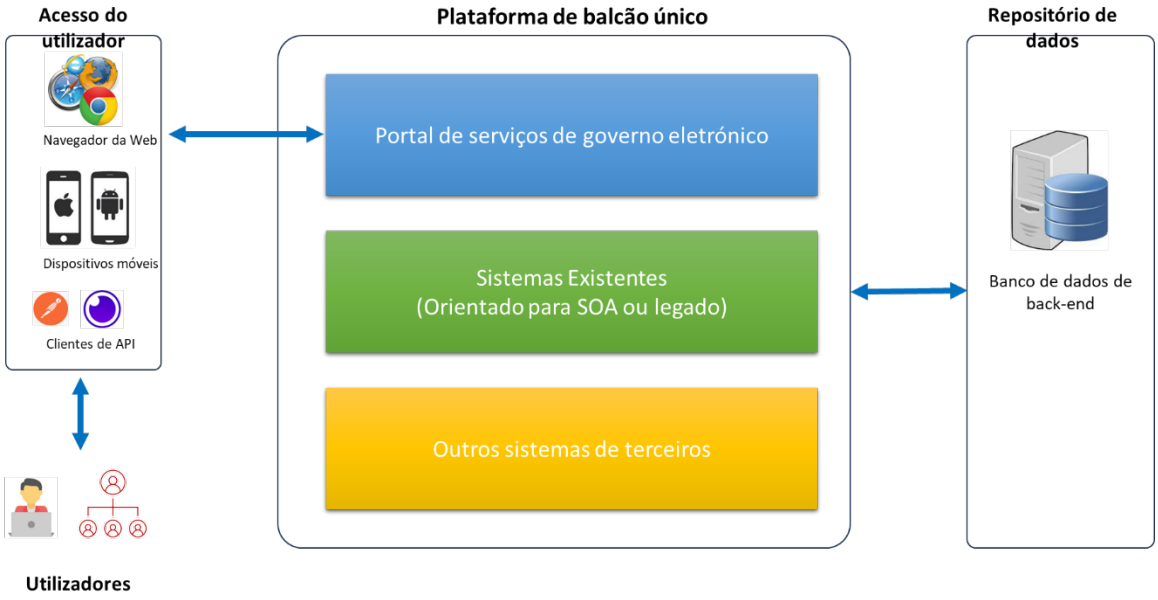

Figura 14 - Arquitetura de interoperabilidade

2.5.1 Características

Dado que a plataforma de interoperabilidade é uma plataforma informática, espera-se que mantenha um certo nível de características, algumas das quais são

- Acesso dos utilizadores: A plataforma deve gerir o acesso às aplicações de que necessita. As equipas de segurança e de administração de TI devem ver rapidamente quem tem acesso a que aplicação(ões), fazendo uma pesquisa simples utilizando o endereço de correio eletrónico da empresa do utilizador. Com isto, a plataforma verificará o acesso às aplicações ou o estado de desaprovação em todos os sistemas de TI a ela ligados.
- Registos de auditoria: A plataforma deve ter disposições para registar todas as actividades num formato normalizado e enriquecido. Por exemplo, a plataforma pode enriquecer automaticamente os dados de registo de auditoria de cada sistema informático com um endereço de correio eletrónico do utilizador, quando aplicável (quando a identidade do utilizador [UID] corresponde ao endereço de correio eletrónico do utilizador).
- Suporte para ferramentas de segurança: A plataforma deve ter suporte para soluções de segurança próprias ou outras ferramentas de segurança, como ogz.io, Netskope, NetWitness, Rapid7, Splunk, etc. Isto irá aumentar o esforço das equipas de segurança para reduzir o tempo de resposta a incidentes de segurança.
- Suporte para aplicações SaaS: A plataforma deve ter suporte para integrar outras plataformas de software as a service (SaaS) baseadas na nuvem que possam ser necessárias em qualquer altura durante a prestação de serviços públicos e administrativos.
- Suporte dos standards OCSF: A plataforma deve ter suporte para o Open Cybersecurity Schema Framework (OCSF)[10] , que é agnóstico em relação ao formato de armazenamento, recolha de dados e processos ETL. O OCSF fornece um esquema normalizado para eventos de segurança comuns, define critérios de controlo de versões para facilitar a evolução do esquema e inclui um processo de autogovernação para produtores e consumidores de registos de segurança.

2.5.2 Processo de negócio

Tal como referido na secção relativa ao quadro, a identificação dos principais processos de negócio envolvidos na lista de serviços públicos e administrativos identificados e o acordo de cada ministério

[10] https://github.com/ocsf

competente em relação a este processo é o primeiro passo para ter sistemas interoperáveis. Este acordo pode levar ao alinhamento e realinhamento dos processos, conduzindo à reengenharia dos processos de negócio. Os processos de negócio identificados por toda a linha de organismos envolvidos na oferta destes serviços públicos devem ser documentados no que se designa por relatórios de análise dos processos empresariais (BPA). Este relatório BPA servirá de base para que os fornecedores ou prestadores de serviços de implementação da plataforma de interoperabilidade desenvolvam os documentos de especificação dos requisitos de negócio (BRS) e de especificação dos requisitos do sistema (SRS).

2.5.3 Aplicação e dados

Os dados dos vários sistemas antigos devem ser agregados numa única base de dados com base nos processos de negócio identificados de todos os principais organismos da administração pública envolvidos na oferta dos serviços públicos e administrativos identificados. Os dados de outros serviços públicos e administrativos provenientes de organismos da administração pública sem sistema interno devem ser desenvolvidos com base em esquemas de dados que sigam as especificações e recomendações de interoperabilidade semântica. Devem também ser seguidas as recomendações relativas à camada de base de dados indicadas nas secções de interoperabilidade técnica.

Com isto em vigor, as aplicações, quer se trate de um interface de programação de aplicações (API), de um interface Web ou de uma aplicação móvel, devem armazenar e recuperar dados desta fonte de dados, que deve ser configurada em cluster (base de dados) e ter uma elevada disponibilidade, escalabilidade e redundância. Para tal, as aplicações devem ser implementadas como contentores num ambiente Kubernetes (K8s), oferecendo assim a portabilidade, a flexibilidade, a escalabilidade e a agilidade necessárias.

Não estamos, no entanto, alheios à situação actual na Guiné-Bissau onde os sistemas antigos proprietários em vigor podem não estar disponíveis para partilhar dados/participar na iniciativa, o desenvolvimento da plataforma deve estar ciente destas restrições e riscos e adotar resposta apropriada de gestão de risco para lidar com isso, uma das quais pode ser trabalhar de perto com os fornecedores desses sistemas antigos e obter sua adesão e compromisso com o projeto, ao mesmo tempo que acalma seus temores de qualquer conflito de interesses.

2.5.4 Redes e infraestruturas

Dado que as soluções de interoperabilidade de diferentes vendedores ou fornecedores podem ter requisitos de rede, software e hardware diferentes, não é possível fornecer requisitos específicos nesta altura. Por conseguinte, os requisitos serão de carácter geral, relacionados com a rede e a infraestrutura. A infraestrutura de rede e de hardware deve ser configurada tendo em conta a redundância e a elevada disponibilidade. A infraestrutura de rede deve ter uma rede primária com largura de banda suficiente e uma ligação à Internet de reserva (backup), em caso de interrupção do serviço de Internet, para que a reserva (backup) possa assumir o controlo. No que respeita à infraestrutura de hardware, os servidores devem ser agrupados em clusters para garantir a transferência de serviços em caso de falha de hardware. O centro de dados também deve ter um local de recuperação de desastres (DR) para recuperar e restaurar a infraestrutura tecnológica e as operações quando o centro de dados principal ficar indisponível.

2.5.5 Opções de alojamento

De um modo geral, as opções de alojamento disponíveis para as plataformas de interoperabilidade são as infraestruturas de alojamento baseadas na nuvem e no local. No entanto, para manter a segurança nacional e a soberania nacional, recomenda-se a utilização de opções de alojamento no local. Para tal, é necessário desenvolver um centro de dados nacional para alojar a interoperabilidade e outras infraestruturas críticas governamentais ou nacionais. Deverá também existir um centro de recuperação de desastre (disaster recovery - DR) para fornecer redundância ao centro primário in caso de falha deste. O centro DR deverá assegurar espaço de relocalização temporária no caso de ocorrer uma falha de segurança ou um desastre natural e

assegura que o Governo possa continuar as operações até voltar a ser seguro reiniciar os serviços no local do centro de dados primário ou numa nova localização permanente.

Deve-se notar que nossas recomendações para um centro de dados nacional e hospedagem local são baseadas nas melhores práticas para uma plataforma digital governamental desta magnitude. Apesar disso, também estamos cientes durante a nossa avaliação de que o país não possui um centro de dados nacional ou qualquer outro centro de dados em qualquer lugar para este projeto. Recentemente, o PNUD financiou o estudo de viabilidade do centro de dados nacional, mas este não pode ser totalmente dependente devido ao cronograma que não está sob o controlo do projeto.

À luz das restrições acima referidas relativamente à não preparação do centro de dados nacional, a plataforma pode, portanto, ser alojada na nuvem utilizando um dos fornecedores de alojamento em nuvem populares, como AWS, Google Cloud e Microsoft Azure. Ao fazê-lo, a região do fornecedor de nuvem e a zona de disponibilidade escolhidas para este projeto devem estar o mais próximas possível de África. Além disso, o local dos dados em caso de desastres deve estar longe da região escolhida para o local da nuvem primária.

2.5.6 Serviço de pagamento

Para pagar os serviços administrativos, a plataforma deve incorporar a capacidade de os cidadãos e as empresas efetuarem pagamentos sem problemas pelos serviços acedidos através da plataforma. Podem fazê-lo através de serviços de pagamento por cartão online ou através de pagamento bancário via agência. Isto pode ser possível através de APIs para gateways de pagamento ou das APIs de pagamento bancário do governo.

2.5.7 Relatórios

Conteúdo aqui. A plataforma deve incorporar ferramentas de report e análise. Através destas ferramentas, podem obter-se relatórios padronizados e ad-hoc, que podem ser relatórios detalhados ou resumidos. Além disso, deve ser concebido um painel de controlo (dashboard) unificado para fornecer informações sobre as receitas, incluindo indicadores-chave de desempenho (KPI), que podem ser visualizados para saber como estão as receitas do governo obtidas através da plataforma.

2.5.8 Serviços de apoio

Para a operacionalização da plataforma de interoperabilidade em relação ao portal de serviços públicos e administrativos do governo, deve haver uma formalização do serviço de apoio informático com base na ITIL (Information Technology Infrastructure Library), que é um quadro concebido para normalizar a seleção, o planeamento, a entrega, a manutenção e o ciclo de vida global dos serviços informáticos numa empresa. Um serviço de apoio fundamental neste domínio é o serviço de helpdesk, que deve ser operacionalizado com uma matriz de escalonamento e um nível de serviço suportado por um acordo de nível de serviço (SLA).

2.6 Quadro jurídico

A Guiné-Bissau não dispõe de mecanismos eficazes para garantir a cibersegurança ou combater a cibercriminalidade (ou seja, leis, quadros de governação, iniciativas, etc.). Esta falta de mecanismos persiste apesar de a CEDEAO fornecer algumas orientações sobre estas questões, nomeadamente a Estratégia Regional da Cibersegurança e da Cibercriminalidade da CEDEAO e a lei complementar sobre a lei de proteção de dados pessoais da CEDEAO.

Não obstante, existem alguns aspetos em que foram dados passos preliminares para a implementação de um quadro de interoperabilidade. Através do Decreto do Conselho de Ministros n.º 50/2021, de 1 de dezembro de 2021, foi criado o Instituto Tecnológico para a Modernização Administrativa (doravante designado por ITMA). O ITMA é uma pessoa coletiva de direito público responsável pela operacionalização da rede privada do Governo e das iniciativas de modernização tecnológica da Administração Pública. Nos termos do referido Decreto, o ITMA tem por missão desenvolver, coordenar, acompanhar e avaliar os programas e projetos de

tecnologias de informação e comunicação, governação eletrónica, interoperabilidade e a modernização tecnológica da Administração Pública, e garantir a organização, administração, gestão, operação e manutenção das infraestruturas das redes de telecomunicações administrativas, assegurando a execução e distribuição dos serviços públicos de tecnologias de informação e telecomunicações administrativas. O ITMA é formalmente controlado pelo Conselho de Ministros; no entanto, a prática informal tem sido a de o ITMA ser controlado pelo Ministério dos Transportes e Comunicações. Por esta razão, em questões operacionais, a equipa do ITMA contacta diretamente com outras entidades governamentais, no entanto, sempre que as questões requerem um aspeto mais formal e relevante, os contactos com outras entidades governamentais são realizados através de comunicações do Ministério dos Transportes e Comunicações.

O ITMA tem atualmente uma estrutura muito limitada, com apenas 4 funcionários afectos a tempo inteiro ao projeto, embora conte com o apoio de outros técnicos afectos a outros departamentos públicos. Para atingir os seus objetivos, o ITMA organiza reuniões do comité técnico a cada dois meses, com representantes de cada ministério. De acordo com o Decreto do Conselho de Ministros n.º 50/2021, estas reuniões devem ter lugar pelo menos duas vezes por ano, o que significa que o ITMA tem vindo a envidar esforços adicionais para ter todos os ministérios alinhados do ponto de vista técnico.

É importante referir que o ITMA, apesar de ter sido criado através de um diploma publicado em 2021, só começou a funcionar em outubro de 2023, o que significa que a sua existência é muito limitada. Do ponto de vista prático, tendo em conta o número limitado de recursos disponíveis, nas palavras do seu Presidente, o ITMA tem funcionado mais como um consultor do Governo e é responsável pelo PMO de determinados projetos, do que como um organismo público com competências para definir e implementar as estratégias do Governo em matéria de modernização da administração pública. O Presidente do ITMA sugeriu que, para ganhar maior relevância, deveria ter sido criado por meio de uma Lei em vez de um Decreto do Conselho de Ministros. Desta forma, o ITMA teria poderes para estabelecer relações diretas e formais com todos os ministérios, garantindo assim o cumprimento das suas instruções.

2.7 Em conclusão, recomenda-se, por conseguinte, que o ITMA seja dotado da legislação adequada para dispor do quadro jurídico necessário para impulsionar a plataforma de interoperabilidade e assumir o papel de agência designada responsável pela liderança e gestão desta iniciativa.

Segurança

A segurança da plataforma deve basear-se nos requisitos e especificações de segurança indicados na secção 1.3.4. Para além destas especificações, os protocolos de comunicação utilizados pela plataforma devem adotar a versão segura dos ports e protocolos bem conhecidos em vez da versão não segura. Ver **apêndice 7 - Protocolos/Ports seguros**.

APÊNDICES

Apêndice 1 - Standards de metadados

O estabelecimento de uma norma comum de metadados ajudará os cidadãos e as empresas a encontrar mais facilmente informações e recursos governamentais. Os standards de metadados foram desenvolvidas para apoiar tanto a interoperabilidade das máquinas (transferência de informações) como a descoberta de recursos na Web por utilizadores humanos da Web e das aplicações. A norma de metadados ajudará muito no nível dos serviços e aplicações dos domínios da arquitetura da interoperabilidade técnica, quando a informação é combinada e trocada entre diferentes sistemas informáticos para prestar serviços públicos.

O quadro seguinte descreve os standards de metadados abertos para áreas específicas:

Nome	Área	Descrição	URL
Norma de Metadados da Administração Pública online, e-GMS	Governo	A norma de metadados da administração pública online (e-Government Metadata Standard), e-GMS, é a norma de metadados da administração pública online do Reino Unido. Define a forma como os organismos do sector público do Reino Unido devem rotular conteúdos, como páginas Web e documentos, para que essas informações sejam mais facilmente geridas, encontradas e partilhadas.	https://en.wikipedia.org/wiki/E-GMS
O núcleo de Dublin	Recursos digitais ou físicos	O Dublin Core, também conhecido como Dublin Core Metadata Element Set, é um conjunto de quinze itens de metadados principais para a descrição de recursos digitais ou físicos.	https://www.dublincore.org/
ISO/IEC 19506	Ativos de software / sistemas	A norma ISO/IEC 19506:2012 define um meta-modelo para representar os ativos de software existentes, as suas associações e os ambientes operacionais, designado por Meta-modelo de Descoberta de Conhecimento (KDM).	https://www.iso.org/standard/32625.html
ISO/IEC 11179	Metadados da organização	A norma ISO/IEC 11179 de registo de metadados (MDR) é uma norma internacional ISO/IEC para a representação de metadados de uma organização num registo de metadados. Documenta a padronização e o registo de metadados para tornar os dados compreensíveis e partilháveis.	https://www.iso.org/standard/78914.html

ISO 19115	Metadados geoespaciais	A norma ISO 19115-1:2014 define o esquema necessário para descrever a informação e os serviços geográficos através de metadados.	https://www.iso.org/standard/53798.html
RDF/W3C	Recursos Web	O quadro de descrição de recursos (RDF), também designado por norma da Web semântica, é um modelo normalizado para o transferência de dados na Web.	https://www.w3.org/RDF/ https://www.w3.org/TR/rdf11-concepts/ https://www.w3.org/TR/rdf12-concepts/

Apêndice 2 - Canal dos serviços eletrónicos

Centro de serviços comum

Estes são centros ou canais de TIC designados onde serviços governamentais comuns podem ser fornecidos. É um serviço adequado a um modelo de prestação de serviços para o sector educativo e para os moradores rurais.

Site/Portal

Este é um canal online para fornecer serviços eletrónicos informativos e transacionais ao público. Os portais da Web apresentam uma forma eficaz de integrar aplicações, pessoas e negócios por meio de dois ou mais MDAs para oferecer um ponto exclusivo de acesso a serviços aos utilizadores.

Plataforma móvel

A prestação integrada de serviços através de plataformas móveis pode ser muito eficiente em termos de cobertura, conveniência, preço acessível e acessibilidade. Para garantir a interoperabilidade, a escolha da abordagem de padrão aberto é crítica.

Contato Governamental/Call Center

A prestação de serviços integrados através de call centers pode ser um modelo viável. São centros onde os clientes dos serviços governamentais podem fazer ligações diretas para solicitar serviços e informações.

Apêndice 3 – Abordagens Arquitetónicas: Prós e Contras

Arquitetura Orientada a Serviços (SOA)

A arquitetura orientada a serviços é uma abordagem de design de software que envolve a divisão de aplicações de software em componentes menores e mais modulares, conhecidos como serviços. Cada serviço pode ser considerado uma unidade independente que executa uma função comercial específica, como processamento de pedidos ou gestão de dados de clientes. Esses serviços comunicam entre si através de uma rede, utilizando protocolos e interfaces padronizados. O objetivo da SOA é criar uma arquitetura flexível e modular que possa se adaptar às mudanças nas necessidades dos negócios ao longo do tempo, dividindo uma aplicação grande e monolítica em serviços menores e mais gerenciáveis.

SOA difere da Arquitetura de Microsserviços (MA) ao nível dos princípios, um dos quais é que a "reutilização" não é incentivada em MA e isso ocorre porque MA cria dependência entre componentes de microsserviços. Embora em SOA, se existir uma funcionalidade num dos serviços, basta chamar esse serviço para fazer o trabalho, mas na Arquitetura de Microsserviços, pode-se até duplicar o código/lógica apenas para desacoplar/separar.

Um dos princípios-chave da SOA é a reutilização de serviços. Os serviços devem ser projetados para serem tão genéricos quanto possível, para que possam ser reutilizados em várias aplicações. Isto requer atenção cuidadosa ao projeto de interfaces de serviço, bem como ao uso de formatos de dados e protocolos de comunicação padrão.

Para implementar SOA, as organizações normalmente usam uma camada de "middleware" que fornece a infraestrutura para comunicação entre serviços. Essa camada de middleware pode ser baseada em diversas tecnologias, incluindo serviços web, middleware orientado a mensagens ou APIs RESTful.

Os benefícios do SOA são uma maior flexibilidade e agilidade na atualização ou substituição de serviços sem afetar todo o sistema; serviços reutilizáveis em diferentes aplicações, permitindo às organizações desenvolver novas aplicações de forma mais rápida e eficiente; melhor escalabilidade e desempenho através da divisão de aplicações em serviços menores; e redução nos custos e tempo de desenvolvimento devido ao desenvolvimento de serviços independentes uns dos outros.

Arquitetura Orientada a Eventos (EDA)

Implementação de um sistema orientado a eventos onde os serviços se comunicam através de eventos e mensagens, permitindo colaboração em tempo real e processamento assíncrono. Ele suporta acoplamento fraco e permite escalabilidade e extensibilidade. No entanto, acrescenta complexidade ao tratamento de eventos e pode exigir componentes de infraestrutura adicionais.

Arquitetura Orientada a Eventos (EDA) é um estilo de arquitetura de software que promove a produção, deteção, consumo e reação a eventos. Este paradigma tornou-se cada vez mais popular no desenvolvimento de sistemas escaláveis, fracamente acoplados e flexíveis. O EDA permite que os aplicativos se comuniquem entre si de forma assíncrona por meio de eventos, melhorando a capacidade de resposta e facilitando um comportamento mais dinâmico do aplicativo.

As vantagens do EDA são a capacidade de suportar o dimensionamento horizontal independente de componentes, garantindo assim o manuseio eficaz de cargas aumentadas; flexibilidade e agilidade na realização de alterações no sistema, como adição de novos tipos de eventos ou lógica de processamento com impacto mínimo nos componentes existentes; acoplamento frouxo de componentes, promovendo assim a modularidade e tornando o sistema mais fácil de estender e manter; capacidade de resposta a entradas ou mudanças de estado mais rapidamente por meio do processamento assíncrono de eventos; e resiliência que permite que partes do sistema falhem ou sejam atualizadas sem afetar a disponibilidade de todo o sistema.

As desvantagens do EDA são a complexidade devido à natureza assíncrona dos sistemas orientados a eventos; o desafio de garantir a consistência dos dados em diferentes serviços; e as dificuldades em gerir um grande

número de tipos de eventos, garantir a compatibilidade do esquema de eventos e lidar com o versionamento de eventos.

Arquitetura Orientada a Mensagens (MDA)

Arquitetura Orientada a Mensagens (MDA) é um conceito semelhante ao Domain Events Pattern ou Event Sourcing. Basicamente, MDA significa que uma aplicação é composta por componentes autónomos que se comunicam entre si por meio de mensagens. O MDA é muito comum em aplicações distribuídas porque cada componente fica num servidor diferente, mas mesmo assim eles ainda precisam trabalhar juntos.

Mas o que é surpreendente sobre o MDA é que ele também pode ser aplicado a aplicações locais (não distribuídas). Isso significa que um aplicativo MDA local pode facilmente se tornar um aplicativo distribuído, sendo apenas algumas configurações necessárias, mas o código do aplicativo deve permanecer intacto. O principal benefício, porém, é que torna muito fácil escrever código de alta qualidade e sustentável, ou seja, código pouco acoplado, altamente coeso e altamente testável.

A desvantagem é que é necessário um pouco de experiência para se sentir confortável com isso. Não é simples e, a princípio, parece um excesso de engenharia, mas depois de experimentá-lo, parecerá a maneira correta de implementar uma aplicação não trivial. Mas para isso é preciso entender bem o MDA.

Arquitetura de microsserviços (MSA)

A arquitetura monolítica existente, onde todas as funcionalidades estão fortemente acopladas numa única aplicação, tem a vantagem da simplicidade e do fácil desenvolvimento, mas carece de escalabilidade e tolerância a falhas. Pode tornar-se complexo e difícil de manter à medida que o sistema cresce. O uso do MSA é promovido pelo movimento DevOps.

A arquitetura de microsserviços envolve a divisão do sistema em microsserviços independentes e fracamente acoplados, cada um responsável por funcionalidades específicas. Ele oferece escalabilidade, tolerância a falhas e flexibilidade nas escolhas tecnológicas. No entanto, introduz complexidade na gestão da comunicação e implementação entre serviços.

Alguns dos princípios-chave do padrão Microserviços são Independência, Descentralização, Comunicação e Escalabilidade. Esses princípios resultam em algumas vantagens e também em compensações. Em termos de vantagens, estas são a capacidade de escalar horizontalmente com facilidade, desenvolvimento mais rápido como resultado da capacidade das equipas de trabalharem microsserviços de forma independente, diversidade de tecnologia entre programadores, resiliência devido ao isolamento de serviço facilitando a gestão de falhas e manutenção mais fácil de atualizações e correções de bugs. As desvantagens estão, portanto, no aspecto da complexidade da gestão de uma rede de serviços, na sobrecarga de comunicação devido à comunicação entre serviços, no desafio na gestão da consistência dos dados e na sincronização entre serviços e na coordenação de testes ponta a ponta para um aplicativo devido a vários composições de serviço.

NOTA: A escolha da arquitetura ideal para um cenário específico deve depender dos requisitos funcionais e não funcionais das aplicações ou sistemas de TI em questão.

Apêndice 4 - Serviços de middleware

Tipo de serviço →	Integração de aplicativos empresariais (EAI)	Integração de dados	Middleware orientado a mensagens (MOM)	Corretor de Solicitação de Objeto (ORB)	Barramento de serviço empresarial (ESB)
Descrição	Uma estrutura de integração composta por uma coleção de tecnologias e serviços que formam um middleware ou "estrutura de middleware" para permitir a integração de processos, sistemas e aplicações de uma empresa.	A integração de dados envolve combinar dados residentes em diferentes fontes e fornecer aos utilizadores uma visão unificada deles.	MOM é uma infraestrutura de software ou hardware que oferece suporte ao envio e recebimento de mensagens entre sistemas distribuídos. Ele fornece uma camada que permite que componentes de software que foram desenvolvidos de forma independente e executados em diferentes plataformas de rede interajam entre si.	ORB permite que chamadas de programas sejam feitas de um computador para outro através de uma rede de computadores, proporcionando transparência de localização por meio de chamadas de procedimentos remotos. Ele fornece uma estrutura que permite que objetos remotos sejam utilizados na rede, da mesma forma como se fossem locais e fizessem parte do mesmo processo.	O ESB implementa um sistema de comunicação entre aplicações de software que interagem mutuamente numa arquitetura orientada a serviços (SOA) baseada no modelo cliente-servidor.
Cenário	Para integração de sistemas/aplicativos de TI silos em MDAs (onde dados idênticos são armazenados em aplicativos diferentes, ou seja, independência de fornecedor e fachada comum).	Harmonização/fusão de bases de dados entre dois ou mais MDAs.	Para interação/integração de componentes de software de MDAs (aplicativos, servlets etc.) que foram desenvolvidos de forma independente e que circulam em diferentes plataformas em rede para fornecer serviços integrados. Ele permite que aplicativos distribuídos comuniquem entre si e troquem dados enviando e recebendo mensagens.	Para conectar MDAs com sistemas/plataformas de TI heterogéneos. Pode ser utilizado numa prestação de serviços integrada onde aplicações e serviços instalados no servidor do MDA 1 podem ser executados no cliente do MDA 2.	Fornecer serviços públicos reutilizáveis de TI comuns ou diferentes habilitados por diferentes MDAs.
Tecnologia / Método / Padrões	- **Mediação** (Intracomunicação) - atua como intermediário ou intermediário entre vários aplicativos - **Federação** (Intercomunicação) - atua como fachada abrangente em vários aplicativos.	Criação de Esquema Mediado (Banco de Dados Virtual). Isso faz interface com bancos de dados de origem por meio de wrappers/adaptadores.	É um sistema de troca de mensagens baseado em publicação/assinatura, por exemplo, Advanced Message Queuing Protocol (AMQP), MQ Telemetry Transport (MQTT), Object Management Group's Data Distribution Service (DDS), eXtensible Messaging and Presence Protocol (XMPP) etc.	Arquitetura Common Object Request Broker (CORBA), Internet Communications Engine (ICE), etc.	- **Proprietário** : IBM WebSphere Message Broker Integration Bus, Azure Service Bus, etc. - **Código aberto** : Apache Camel, Fuse ESB, Open ESB, etc.

Apêndice 5 - Standards relativos à rede e às infraestruturas

Categoria	Domínio	Nome	Comentários	URL
Interconexão	Protocolos de rede	IP v4 - Protocolo de Internet versão 4	Para migração para IP v6. O novo hardware deve suportar IP v4 e também IP v6.	http://www.ietf.org/rfc/rfc0791.txt
		IP v6 - Protocolo de Internet versão 6	Ao implementar o IP v6, configure os roteadores para IP v4 "fantasma"	http://www.ietf.org/rfc/rfc2460.txt
		IEEE 802.11-WLAN	IEEE 802.11 é um conjunto de padrões para comunicação de computadores em redes locais sem fio (WLAN), desenvolvido pelo IEEE LAN/MAN Standards Committee (IEEE 802) nas bandas do espectro público de 5 GHz e 2,4 GHz. Inclui: – 802.11-1997 (802.11 legado) – versão original do padrão IEEE 802.11 foi lançada em 1997 e esclarecida em 1999, mas hoje está obsoleta. – 802.11a - usa o mesmo protocolo de camada de enlace de dados e formato de quadro do	http://www.ieee802.org/11/

			padrão original, mas uma interface aérea baseada em OFDM (camada física). Ele opera na banda de 5 GHz com uma taxa de dados líquida máxima de 54 Mbit/s, além de código de correção de erros, que produz uma taxa de transferência líquida alcançável realista em meados de 20 Mbit/s – 802.11b – tem uma taxa máxima de dados brutos de 11 Mbit/s e usa o mesmo método de acesso ao media definido no padrão original. O aumento dramático no rendimento do 802.11b (em comparação com o padrão original), juntamente com reduções simultâneas substanciais de preços, levaram à rápida aceitação do 802.11b como a tecnologia definitiva de LAN sem fio. – 802.11g – funciona na banda de 2,4	

			GHz (como 802.11b), mas usa o mesmo esquema de transmissão baseado em OFDM que 802.11a. Ele opera a uma taxa de bits máxima da camada física de 54 Mbit/s, excluindo códigos de correção de erro direto, ou cerca de 19 Mbit/s em média. O hardware 802.11g é totalmente compatível com versões anteriores do hardware 802.11b e, portanto, está sobrecarregado com problemas legados que reduzem o rendimento quando comparado ao 802.11a em aproximadamente 21%.	
		IEEE 802.16-WiMax	WiMAX, que significa Interoperabilidade Mundial para Acesso por Micro-ondas, é uma tecnologia de telecomunicações que fornece transmissão de dados sem fio usando uma variedade de modos de transmissão,	http://www.ieee802.org/ https://ieeexplore.ieee.org/document/8538829

			desde links ponto a multiponto até acesso à Internet portátil e totalmente móvel. A tecnologia fornece velocidade de banda larga simétrica de até 72 Mbit/s sem a necessidade de cabos. A tecnologia é baseada no padrão IEEE 802.16 (também chamado de acesso de banda larga sem fio).	
	Protocolos de diretório	LDAP v3 - Protocolo leve de acesso a diretórios versão 3	Para acesso a serviços de diretório	http://www.ietf.org/rfc/rfc1777.txt
	Protocolos de transferência de arquivos	FTP - Protocolo de transferência de arquivos	Observe que os protocolos seguros de transferência de arquivos (como Secure Copy e SSH File Transfer Protocol) estão em revisão. Use reinicialização e recuperação.	http://www.ietf.org/rfc/rfc0959.txt
		HTTP v1.1 - Protocolo de transferência de hipertexto versão 1.1	Protocolo em nível de aplicativo. Consulte para uso seguro de HTTP (HTTPS) e TLS.	http://www.ietf.org/rfc/rfc2616.txt
		WebDAV - Criação e controlo de	Um conjunto de extensões para HTTP	http://www.ietf.org/rfc/rfc2518.txt

		versão distribuídos na World Wide Web	v1.1 que permite aos utilizadores editar e gerir arquivos remotamente de forma colaborativa, mas evita problemas de acesso com firewalls NAT.	
		Protocolo de controlo de sessão	SCP é um protocolo simples, que permite que um servidor e um cliente tenham várias conversas em uma única conexão TCP. O protocolo foi projetado para ser simples de implementar e é modelado após TCP.	https://www.w3.org/Protocols/HTTP-NG/http-ng-scp.html
		Protocolo de cópia segura	Cópia segura ou SCP é um meio de transferir com segurança arquivos de computador entre um host local e um host remoto ou entre dois hosts remotos, usando o protocolo Secure Shell (SSH).	https://winscp.net/eng/docs/scp https://www.ionos.com/digitalguide/server/know-how/scp-secure-copy/
	Protocolos de transferência de correio	SMTP - Protocolo Simples de Transferência de Correio	SMTP é um padrão da Internet para transmissão de correio eletrónico (e-mail) através de redes de protocolo da Internet (IP).	http://www.ietf.org/rfc/rfc5321.txt

			O SMTP foi definido pela primeira vez na RFC 821 (STD 10) e atualizado pela última vez pela RFC 5321 (2008), que descreve o protocolo amplamente utilizado atualmente, também conhecido como SMTP estendido (ESMTP).	
		POP3 - Protocolo Postal versão 3	POP3 é um protocolo padrão da Internet de camada de aplicação usado por clientes de e-mail locais para recuperar e-mails de um servidor remoto através de uma conexão TCP/IP. O design do POP3 e seus procedimentos oferecem suporte aos utilizadores finais com conexões intermitentes (como conexões dial-up).	http://www.ietf.org/rfc/rfc1939.txt
		IMAP - Protocolo de acesso a mensagens da Internet	O IMAP é um dos dois protocolos padrão da Internet mais comuns para recuperação de e-mail. É um protocolo de	http://www.ietf.org/rfc/rfc3501.txt

			Internet da camada de aplicação operando na porta 143 que permite que um cliente local acesse e-mail em um servidor remoto. A versão atual, IMAP versão 4 revisão 1 (IMAP4rev1), é definida pela RFC 3501. O IMAP oferece suporte aos modos de operação conectado (online) e desconectado (offline). Os clientes de e-mail que usam IMAP geralmente deixam mensagens no servidor até que o utilizador as exclua explicitamente.	
		X.400	X.400 é um conjunto de recomendações ITU-T que definem padrões para e-mail que foram usados em organizações e como parte de produtos de e-mail proprietários, como o Microsoft Exchange. Embora o X.400 tenha sido originalmente	https://www.itu.int/rec/T-REC-F.400-199906-I/en

			projetado para ser executado no serviço OSI Transport, uma adaptação para permitir a operação sobre TCP/IP, RFC 1006, tornou-se a forma mais popular de executar o X.400.	
	Protocolos de gestão de rede	SNMP – Protocolo Simples de gestão de Rede	O Simple Network Management Protocol (SNMP) é usado em sistemas de gestão de rede para monitorizar dispositivos conectados à rede em busca de condições que justifiquem atenção administrativa. O SNMP é um componente do Internet Protocol Suite conforme definido pela Internet Engineering Task Force (IETF). Consiste em um conjunto de padrões para gestão de rede, incluindo um protocolo de camada de aplicação, um esquema de banco de dados e um conjunto de objetos de dados.	http://tools.ietf.org/html/rfc3411

		Telnet – Emulação de Terminal	Telnet (rede de telecomunicações) é um protocolo de rede usado nas conexões de Internet ou de rede local (LAN). Foi desenvolvido em 1969 começando com RFC 15 e padronizado como IETF STD 8, um dos primeiros padrões da Internet. Normalmente, o Telnet fornece acesso a uma interface de linha de comando em uma máquina remota.	http://tools.ietf.org/html/rfc854
		SSH – SHell seguro	Secure Shell ou SSH é um protocolo de rede que permite a troca de dados usando um canal seguro entre dois dispositivos em rede. Usado principalmente em sistemas baseados em Linux e Unix para aceder a contas shell, o SSH foi projetado como um substituto para TELNET e outros shells remotos inseguros, que enviam informações, principalmente	http://tools.ietf.org/html/rfc4252

			senhas, em texto simples, deixando-as abertas para intercetação. A criptografia usada pelo SSH proporciona confidencialidade e integridade dos dados em uma rede insegura, como a Internet.	
	Serviços de registo	DNS - Servidor de Nomes de Domínio	Use DNS para domínio de Internet/Intranet para resolução de endereço IP.	http://www.ietf.org/rfc/rfc1035.txt
	Protocolos de tempo	NTP v4 - Protocolo de horário de rede versão 4	O Network Time Protocol (NTP) é amplamente utilizado para sincronizar relógios de computadores na Internet. O NTPv4 inclui melhorias fundamentais nos algoritmos de mitigação e disciplina que estendem a precisão potencial para dezenas de microssegundos com estações de trabalho modernas e LANs rápidas.	https://datatracker.ietf.org/doc/html/rfc5905
		UTC (MSL) - Relógio de Tempo Universal (Laboratório de Padrões de Medição)	UTC é uma escala de tempo global com um conjunto de relógios muito maior que o conjunto NIST.	https://www.nist.gov/pml/time-and-frequency-division/time-realization/utcnist-time-scale-0/introduction-utcnist

	Protocolos de mensagens	MIME - Extensão multifuncional de correio da Internet	MIME é uma forma de codificar arquivos binários para transmissão pela Internet, para que possam ser enviados como parte de mensagens de e-mail.	http://www.ietf.org/rfc/rfc2049.txt
		SOAP v1.2 - Protocolo Simples de Acesso a Objetos	Protocolo leve destinado à troca de informações estruturadas em um ambiente descentralizado e distribuído.	http://www.w3.org/TR/2007/REC-soap12-part1-20070427/
		XMPP - Protocolo Extensível de Mensagens e Presença	XMPP é o padrão aberto para mensagens e presença. O XMPP potencializa tecnologias emergentes como IoT , WebRTC , mensagens instantâneas, jogos online e redes sociais em tempo real .	https://xmpp.org/
	Protocolos de voz sobre Internet (VOIP)	SIP - Protocolo de Iniciação de Sessão	Um protocolo para iniciar, modificar e encerrar uma sessão de utilizador interativa que envolve elementos multimídia como vídeo, voz e mensagens instantâneas. Tem maior	http://www.ietf.org/rfc/rfc3261.txt

			aceitação que H.323.	
		RTP - Protocolo de Transporte em Tempo Real	Define um formato de pacote padronizado para entrega de áudio e vídeo pela Internet e é frequentemente usado em conjunto com RTSP, H.323 ou SIP.	http://www.ietf.org/rfc/rfc3550.txt
		H.323 v2 H.323 versão 2	Uma recomendação abrangente da ITU-T, que define os protocolos para fornecer sessões de comunicação audiovisual em qualquer rede de pacotes.	https://www.itu.int/rec/T-REC-H.323
		G.711	Padrão ITU-T para codificação de áudio; usado principalmente em telefonia. G.711 é um codec de áudio de banda estreita originalmente projetado para uso em telefonia que fornece áudio de qualidade a 64 kbit /s.	https://www.itu.int/rec/T-REC-G.711/
		G.729	Um codec de áudio para voz que compacta o áudio da voz em blocos de 10 milissegundos; é usado principalmente em aplicativos VOIP devido	https://www.itu.int/rec/T-REC-G.729

			ao seu baixo requisito de largura de banda.	
		IAX – Troca Inter Asterisk	IAX é o protocolo Inter-Asterisk eXchange nativo do Asterisk PBX e suportado por vários outros soft switches e PBXs. É usado para permitir conexões VoIP entre servidores, bem como comunicação cliente-servidor. IAX agora se refere mais comumente a IAX2, a segunda versão do protocolo IAX. O protocolo IAX original foi descontinuado em favor do IAX2. O protocolo IAX2 foi publicado como um RFC 5456 informativo (não padronizado) por critério do Editor da RFC em fevereiro de 2009.	https://datatracker.ietf.org/doc/rfc5456/
Segurança	línguas	WSS - Segurança de Serviços Web	Uma base técnica para implementar funções de segurança, como integridade e confidencialidade, em mensagens que	https://docs.oasis-open.org/wss/v1.1/wss-v1.1-spec-pr-SOAPMessageSecurity-01.htm

			implementam aplicativos de serviços da Web de nível superior.	
		Política de segurança WS - Linguagem de política de segurança de serviços da Web	Esta especificação indica as asserções de política que se aplicam ao Web Services Security: SOAP Message Security, WS-Trust e WS-Secure Conversation.	https://specs.xmlsoap.org/ws/2005/07/securitypolicy/ws-securitypolicy.pdf
		Linguagem de confiança de serviços da Web WS-Trust	Usa os mecanismos de mensagens seguras do WS-Security para definir primitivas e extensões adicionais para troca de tokens de segurança para permitir a emissão e disseminação de credenciais dentro de diferentes domínios de confiança.	https://specs.xmlsoap.org/ws/2005/02/trust/ws-trust.pdf
		WS- Secon - Linguagem de conversação segura de serviços da Web	A Web Services Secure Conversation Language (WS-SecureConversation) é construída sobre os modelos WS-Security e WS-Policy para fornecer comunicação segura entre serviços.	https://www.ibm.com/docs/en/was/9.0.5?topic=conversation-web-services-secure
		SAML v1.1 - Linguagem	Estrutura segura de mensagens e	http://docs.oasis-open.org/imi/identity/cs/imi-saml1.1-profile-cs-01.html

		de marcação de declaração de segurança versão 1.0	token de segurança. Consulte Camada de acesso e apresentação. OpenSAML é uma implementação de SAML.	
		SAML v2.0 - Linguagem de marcação de declaração de segurança versão 2.0	Estrutura segura de mensagens e token de segurança. Um subconjunto do SAML 1.1, os elementos estão em desenvolvimento como parte do projeto de autenticação para todo o governo.	http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html
		XACML v2.0 - Linguagem de marcação de controlo de acesso eXtensible versão 2.0	Esquema XML para criar políticas e automatizar seu uso para controlar o acesso a dispositivos e aplicativos diferentes em uma rede.	https://www.oasis-open.org/standard/xacmlv2-0/
		Liberty ID-WSF v2.0	Para consideração onde a identidade federada de aplicativo para aplicativo é necessária e os perfis SAML V2.0 não são suficientes.	https://saml.xml.org/liberty-alliance-id-ff-and-id-wsf
		XML - Sintaxe e processamento de criptografia Enc XML	Este documento especifica um processo para criptografar dados e representar o resultado em	https://www.w3.org/TR/xmlenc-core1/

			XML. Os dados podem estar em vários formatos, incluindo fluxos de octetos e outros dados não estruturados, ou formatos de dados estruturados, como documentos XML, um elemento XML ou conteúdo de elemento XML.	
	Protocolos de rede	HTTPS - Protocolo de transferência de hipertexto executado em SSL	HTTPS (Hypertext Transfer Protocol over SSL) é uma extensão do protocolo HTTP que suporta criptografia para maior segurança. HTTPS não é um protocolo independente. É HTTP simples, executado em protocolos criptográficos SSL ou TLS.	http://www.ietf.org/rfc/rfc2818.txt
		SSL v3.0 - Camada de soquetes seguros versão 3	Use para transmissão criptografada de qualquer quantidade de dados entre o navegador da web e o servidor da web por TCP/IP. Usado para HTTPS (HTTP em um fluxo	https://datatracker.ietf.org/doc/html/rfc6101

			SSL/TLS) para abrir uma sessão segura na porta 443. Também pode ser usado para transporte TCP seguro (por exemplo, VPN). Nota: TLS v1.0 é SSL v3.1	
		IPsec - Segurança de Protocolo de Internet	IPSec é um conjunto de regras ou protocolos de comunicação para configurar conexões seguras em uma rede. O Protocolo da Internet (IP) é o padrão comum que determina como os dados trafegam pela Internet. O IPSec adiciona criptografia e autenticação para tornar o protocolo mais seguro.	http://www.ietf.org/rfc/rfc2402.txt
		ESP IP - Protocolo de segurança de encapsulamento para VPN	Encapsulating Security Payload (ESP) é um membro do conjunto de protocolos Internet Protocol Security (IPsec) que criptografa e autentica os pacotes de dados entre computadores usando uma Rede Privada Virtual (VPN).	http://www.ietf.org/rfc/rfc2406.txt
		S-HTTP - Hipertexto	Também conhecido	https://archive.unescwa.org/secure-hypertext-transfer-protocol

		Seguro Protocolo de transferência	como HTTPS, é uma extensão do Hypertext Transport Protocol (HTTP) que fornece serviços de segurança para confidencialidade, autenticidade e integridade de transações entre servidores e clientes HTTP. Para fins de navegadores de Internet, o S-HTTP é uma alternativa competitiva ao padrão Secure Sockets Layer (SSL), mais amplamente utilizado.	
		TLS v1.0 - Segurança da camada de transporte	Mecanismo de atualização RFC 2616 em HTTP 1.1; iniciar o Transport Layer Security através de uma conexão TCP existente. Ainda não interage com SSL v3.	http://www.ietf.org/rfc/rfc2246.txt
	Transferência de correio	S/MIME v3 0 - Extensões seguras de correio da Internet multiuso versão 3	Use MIME quando a segurança não for uma preocupação. Use a criptografia S/MIME quando não estiver usando os protocolos de transporte de mensagens.	http://www.ietf.org/rfc/rfc2633.txt

	Infraestrutura de chave pública (PKI)	RFC2527 Internet X.509 - Política de certificados de infraestrutura de chave pública e estrutura de práticas de certificação	Produzido pelo grupo Public-Key Infrastructure X.509, ou PKIX, um grupo de trabalho da Internet Engineering Task Force dedicado à criação de RFCs e outras documentaçõe s de padrões sobre questões relacionadas à infraestrutura de chave pública (PKI) baseada em certificados X.509. Nota: As agências que pretendam implementar qualquer novo sistema PKI devem contactar a Secção de TIC da Comissão de Serviços do Estado para obter aconselhament o.	http://www.ietf.org/rfc/rfc2633.txt
	Cartões inteligente s	ISO/IEC 7816	ISO/IEC 7816 é uma norma internacional relacionada a cartões de identificação eletrónica, especialmente cartões inteligentes, gerida conjuntamente pela Organização Internacional de Padronização (ISO) e pela	https://www.iso.org/obp/ui/en/#!iso:std:77181:en

			Comissão Eletrotécnica Internacional (IEC). É uma extensão da ISO/IEC 7810. É editado pelo Comitê Técnico Conjunto (JTC) 1 / Subcomitê (SC) 17. ISO 7816-1 Características físicas ISO 7816-2 Dimensões e localização dos contatos ISO 7816-3 Sinais eletrónicos e protocolos de transmissão Comandos industriais ISO 7816-4 para intercâmbio Sistema numérico ISO 7816-5 e procedimento de registo para identificadores de aplicativos Elementos de dados intersetoriais ISO 7816-6	

Apêndice 6 - Standards de serviços Web

Categoria	Domínio	Nome	Comentários	URL
Serviço de internet	Serviços de registo	ebXML RIM e RS v2.1 - Linguagem de marcação extensível de e-business , modelo de informações de registo e serviços de registo versão 2.1	Aplicação padrão aberta para Serviços de Informações e Registos Cadastrais em contexto de e-business, como alternativa aos Web Services.	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=regrep
		ebXML RIM e RS v3.0 - Linguagem de marcação extensível de e-business, modelo de informações de registo e serviços de registo versão 3.0	Aplicação padrão aberta para Serviços de Informações e Registos Cadastrais em contexto de e-business, como alternativa aos Web Services.	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=regrep
		UDDI v3 - Descrição Universal, Descoberta e Integração Versão 3	Um padrão aberto para descrever, publicar e descobrir componentes de software baseados em rede.	http://www.uddi.org/
	Descrição	Linguagem de descrição de serviços da Web WSDL v1.1 versão 1.1	Especifica o local do serviço e as operações ou métodos que o serviço expõe.	https://www.w3.org/TR/2001/NOTE-wsdl-20010315
		Linguagem de descrição de serviços da Web WSDL v2.0 versão 2.0	Esta especificação define uma linguagem para descrever a funcionalidade abstrata de um serviço, bem como uma estrutura para descrever os detalhes concretos de	https://www.w3.org/TR/2007/REC-wsdl20-20070626/

			uma descrição de serviço.	
		WSBPEL - Linguagem de execução de processos de negócio de serviços da Web	BPEL é uma linguagem baseada em XML usada para conectar e partilhar dados entre serviços em um fluxo de trabalho comercial.	http://docs.oasis-open.org/wsbpel/2.0/OS/wsbpel-v2.0-OS.html
		FWSI - Estrutura para Implementação de Serviços Web	Define métodos e componentes funcionais para implementação de serviços da Web ampla, multiplataforma e independente de fornecedor em todos os setores.	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=fwsi
		CPPA - Perfil e Acordo do Protocolo de Colaboração ebXML	Descrever como os parceiros comerciais se envolvem em colaborações comerciais eletrónicas por meio da troca de mensagens eletrónicas	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ebxml-cppa
		EBXML - Processo de negócios ebXML da BP	Fornece uma base de processos de negócios baseada em padrões que promove a automação e a troca previsível de definições de colaboração de negócios usando XML.	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ebxml-bp
		BPEL4WS - Linguagem de Execução de Processos de Negócios para Serviços Web	BPEL (Business Process Execution Language for Web Services,	http://www-128.ibm.com/developerworks/library/specification/ws-bpel/

			também WS-BPEL, BPEL4WS) é uma linguagem usada para composição, orquestração e coordenação de serviços web.	
	Acesso	SOAP v1.1 - Protocolo Simples de Acesso a Objetos Versão 1.1	SOAP é um protocolo leve para troca de informações em um ambiente distribuído e descentralizado. É um protocolo baseado em XML que consiste em três partes: um envelope que define uma estrutura para descrever o que está em uma mensagem e como processá-la, um conjunto de regras de codificação para expressar instâncias de tipos de dados definidos pela aplicação e uma convenção para representar chamadas e respostas de procedimentos remotos.	http://www.w3.org/TR/2000/NOTE-SOAP-20000508/
		SOAP v1.2 - Protocolo Simples de Acesso a Objetos Versão 1.2	A versão 1.2 do SOAP fornece um mecanismo simples e leve para troca de informações estruturadas e	http://www.w3.org/TR/2001/WD-soap12-20010709/

			digitadas entre pares em um ambiente distribuído e descentralizado usando XML. SOAP v1.2 é recomendado.	
	Mensagens	ebXML MSG - Serviços de mensagens em linguagem de marcação extensível para e-business	O objetivo principal do serviço de mensagens ebXML (ebMS) é facilitar a troca de mensagens comerciais eletrónicas dentro de uma estrutura XML que aproveite padrões comuns da Internet, sem fazer qualquer suposição sobre o modelo de integração e consumo que essas mensagens seguirão no back-end.	http://docs.oasis-open.org/ebxml-msg/ebms/v3.0/core/cs02/ebms_core-3.0-spec-cs-02.html
		Mensagens confiáveis de serviços da Web WSRM	O WS-Reliability 1.1 fornece uma maneira padrão e interoperável de garantir a entrega de mensagens para aplicativos ou serviços da Web.	http://docs.oasis-open.org/ws-rx/wsrm/200702
	Serviços geográficos	WFS - Serviço de recursos da Web	Consórcio Geoespacial Aberto Internacional.	http://www.opengeospatial.org/standards/wfs
		WMS - Serviço de Mapas Web	Consórcio Geoespacial Aberto Internacional	http://www.opengeospatial.org/standards/wms

		WCS - Serviço de Cobertura Web 1.1.0	Consórcio Geoespacial Aberto (OGC)	http://www.opengeospatial.org/standards/wcs
		NZGMS - Padrão de metadados geoespaciais do governo da Nova Zelândia	Land Information A Nova Zelândia lidera esse padrão.	http://www.e.govt.nz/standards/e-gif/geospatial-information
		ESA - Especificação de Dados Básicos de Serviços de Emergência e Administração Governamental	Land Information A Nova Zelândia lidera esse padrão. A versão mais atual é V1.9.7 publicada em 2004.	http://www.e.govt.nz/standards/e-gif/geospatial-information
	Conformidade	WS-I Basic Profile v1.2 Web Services – Perfil Básico da Organização de Interoperabilidade	Os perfis fornecem diretrizes de implementação sobre como as especificações de serviços da Web relacionadas devem ser usadas em conjunto para melhor interoperabilidade. Até o momento, o WS-i finalizou o Perfil Básico, o Perfil de Anexos e o Perfil de Ligação Simples SOAP. O Grupo de Trabalho de Mensagens Seguras de Padrões de Autenticação desenvolverá um perfil de 'mensagens seguras através de serviços web' a partir dos perfis WS-i durante 2008.	http://www.ws-i.org/profiles/BasicProfile-1.2.html

		Perfil Básico WSS-I v1.1 Segurança de Serviços da Web – Organização de Interoperabilidade Básica	Rascunho 1.1 Perfil Básico de Segurança aceito pelo OASIS.	http://www.ws-i.org/Profiles/BasicSecurityProfile-1.1.html

Apêndice 7 - Integração de dados, metadados, acesso à informação e apresentação

Categoria	Domínio	Nome	Comentários	URL
Integração de dados	Conjunto de caracteres primários	ASCII - Código Padrão Americano para Intercâmbio de Informações	Conjunto mínimo de caracteres para intercâmbio de dados.	http://www.columbia.edu/kermit/ascii.html
		UTF-8 - Formato de transformação UCS (codificação de 8 bits)	UTF-8 é uma codificação de caracteres de comprimento variável para Unicode. Ele pode representar qualquer caractere do conjunto de caracteres Unicode, mas é compatível com versões anteriores de ASCII.	http://www.ietf.org/rfc/rfc2279.txt
		UTF-16 - Formato de transformação UCS (codificação de 16 bits)	UTF-16 é uma codificação de caracteres de comprimento variável para Unicode. Ele pode representar qualquer caractere no conjunto de caracteres Unicode, mas é compatível com versões	http://www.ietf.org/rfc/rfc2781.txt

			anteriores de ASCII.	
	Dados estruturados	XML v1.0 - Linguagem de marcação extensível versão 1.0	Opção preferida para transporte estruturado de dados.	http://www.w3.org/TR/REC-xml
	Dados em lote/em massa	XML - Linguagem de Marcação Extensível	XML 1.0 é preferido para transporte de dados estruturados. As partes devem concordar com os registos do cabeçalho do arquivo antes da troca.	https://www.w3.org/XML/
		CSV - Valores Separados por Vírgula	Certas implementaçõ es de XML podem falhar no modo em massa/lote; nesse caso, as agências podem usar o padrão obsoleto de CSV. As partes devem concordar com os registos do cabeçalho do arquivo antes da troca.	https://www.gov.uk/guidance/using-csv-file-format
	Processamento de dados	API simples SAX para XML	Analisador para trocas transacionais. SAX é uma API Java para navegar em documentos XML.	https://learn.microsoft.com/en-us/archive/msdn-magazine/2000/november/the-xml-files-sax-the-simple-api-for-xml
		Modelo de objeto de documento DOM	O Document Object Model (DOM) é uma interface de programação para documentos da web. Ele	http://www.w3.org/DOM/

			representa a página para que os programas possam alterar a estrutura, o estilo e o conteúdo do documento.	
		XSLT - Transformações de linguagem de folha de estilo eXtensible	Uma linguagem usada pelo XSL para transformar documentos XML em outros documentos XML.	http://www.w3.org/TR/xslt
		Transformações de linguagem de folha de estilo eXtensible XPath	XPath é uma linguagem para endereçar partes de um documento XML, projetada para ser usada tanto por XSLT quanto por XPointer.	http://www.w3.org/TR/xpath
		XQuery 1.0 - Linguagem de consulta XML	Uma linguagem de consulta que pode expressar consultas em diversas fontes de dados, incluindo documentos estruturados e semiestruturados, bancos de dados relacionais e repositórios de objetos, armazenados fisicamente em XML ou visualizados como XML por meio de middleware.	http://www.w3.org/TR/xquery/

		XLink 1.0 - Linguagem de vinculação XML	Uma linguagem de ligação que permite a inserção de elementos em documentos XML para criar e descrever links entre recursos.	http://www.w3.org/TR/xlink/
		SQL – Linguagem de Consulta Estruturada	SQL é uma linguagem de computador de banco de dados projetada para a recuperação e gestão de dados em sistemas de gestão de banco de dados relacional (RDBMS), criação e modificação de esquema de banco de dados e gestão de controlo de acesso a objetos de banco de dados.	https://pubmed.ncbi.nlm.nih.gov/18428713/
		SPARQL - Linguagem de Consulta para RDF	Esta especificação define a sintaxe e a semântica da linguagem de consulta SPARQL para RDF. SPARQL pode ser usado para expressar consultas em diversas fontes de dados, sejam os dados armazenados	http://www.w3.org/TR/rdf-sparql-query/

			nativamente como RDF ou visualizados como RDF por meio de middleware.	
	Distribuição de conteúdo e feeds de canal	RSS 1.0 Distribuição realmente simples	RSS é um formato de distribuição e descrição de metadados extensível, leve e multifuncional. RSS é um aplicativo XML, está em conformidade com a especificação RDF do W3C e é extensível via namespace XML e/ou modularização baseada em RDF.	http://web.resource.org/rss/1.0/
		RSS 2.0 Distribuição realmente simples	Uma alternativa ao RSS 1.0 que também conta com amplo apoio da comunidade.	http://www.rssboard.org/rss-specification
		Formato de distribuição ATOM 1.0	Formato de distribuição baseado em XML. O desenvolvimento foi motivado pela existência de muitas versões incompatíveis do formato de distribuição RSS.	http://www.ietf.org/rfc/rfc4287
		Serviço de distribuição de recursos geoespaciais GeoRSS	Objetos codificados geograficamente para feeds RSS .	http://www.georss.org/gml

	Transações comerciais	UBL - Linguagem Universal de Negócios	Definir uma biblioteca XML comum de documentos comerciais (pedidos de compra, faturas, etc.)	http://www.oasis-open.org/committees/ubl/
	Setor de saude	HL7 - Nível de Saúde 7	Um padrão internacional adotado pelo setor saúde. Está convergindo para HL7 Versão 2.4 para resultados laboratoriais e Índice Nacional de Saúde (NHI).	http://www.hl7.org/
Metadados	Modelagem de dados	UML - Linguagem de Modelagem Unificada	UML é a especificação da OMG e a maneira como o mundo modela não apenas a estrutura, o comportamento e a arquitetura do aplicativo, mas também os processos de negócios e a estrutura de dados.	http://www.uml.org/
		ER - Modelo de Relacionamento entre Entidades	A modelagem entidade-relacionamento é um método de modelagem de banco de dados de esquema relacional, usado para produzir um tipo de esquema conceitual ou	https://medium.com/@GeneHFang/the-entity-relationship-model-edd123e71434

			modelo de dados semânticos de um sistema, geralmente um banco de dados relacional, e seus requisitos de cima para baixo.	
		RDF - Estrutura de descrição de recursos	Um formato de arquivo XML para descrever metadados. RDF é usado pelo RSS1.0.	http://www.w3.org/RDF/
		OWL - Linguagem de Ontologia da Web	Um formato de arquivo XML para descrever metadados.	http://www.w3.org/TR/owl-features/
		SKOS - Sistema Simples de Organização do Conhecimento	Um modelo de dados comum para partilhar e vincular sistemas de organização do conhecimento através da Web.	http://www.w3.org/TR/skos-reference/
		SAWSDL - Anotações Semânticas para Esquema WSDL e XML	Interface comum entre descrições semânticas e descrições não semânticas (por exemplo, WSDL).	http://www.w3.org/TR/sawsdl/
		XMI - Intercâmbio de Metadados XML	Permite fácil intercâmbio de metadados entre ferramentas de modelagem, como UML e repositórios remotos de metadados.	https://link.springer.com/referenceworkentry/10.1007/978-1-4899-7993-3_902-2
		XML v1.0 - Linguagem	Metalinguagem para criar	http://www.w3.org/TR/REC-xml/

		de marcação extensível versão 1.0	tags para definir, transitar, validar e interpretar dados.	
		XML v1.1 - Linguagem de marcação extensível versão 1.1	A distinção entre documentos XML 1.0 e XML 1.1 será indicada pelas informações do número de versão na declaração XML no início de cada documento.	http://www.w3.org/TR/2002/WD-xml11-20020425/
		GML - Linguagem de Marcação Geográfica	GML é uma gramática XML para expressar características geográficas. GML serve como linguagem de modelagem para sistemas geográficos, bem como como formato de intercâmbio aberto para transações geográficas na Internet.	http://www.opengeospatial.org/standards/gml
		Definições de esquema W3C - Definições de esquema do World Wide Web Consortium	Use quando outros esquemas customizados para uso por agências governamentais não forem especificamente identificados.	http://www.w3.org/TR/xmlschema-1/
		DTD - Definição de Tipo de Documento	Descreve vários elementos e atributos para XML.	http://www.w3.org/TR/REC-html40/intro/sgmltut.html

		UBL - Linguagem Universal de Negócios	Regras de nomenclatura e design para design de esquema.	http://www.oasis-open.org/committees/sc_home.php?wg_abbrev=ubl-ndrsc
		UMCLVV (para CVLs) - Metodologia UBL para Lista de Códigos e Validação de Valores	Usado para validação contextual em instâncias XML de conjuntos de valores codificados expressos fora das instâncias.	http://www.oasis-open.org/committees/document.php?document_id=23703
		UN/EDIFACT - Diretórios das Nações Unidas para Intercâmbio Eletrónico de Dados para Administração, Comércio e Transporte	O padrão EDIFACT fornece: (i) um conjunto de regras de sintaxe para estruturar dados, (ii) um protocolo de intercâmbio interativo (I-EDI), (iii) mensagens padrão que permitem a troca entre vários países e vários setores.	http://www.unece.org/trade/untdid/welcome.htm
	Nome e endereço	xNAL v2 - Linguagem extensível de nomes e endereços versão 2	xNAL (OASIS) v3 como parte do OASIS CIQ v3 sendo elaborado; será incorporado ao e-GIF após um piloto bem-sucedido.	http://www.oasis-open.org/committees/ciq/ciq.html#4
	Relacionamento com o cliente	xCIL - Linguagem Extensível de Informações do Cliente	O superconjunto de xNAL que especifica formatos para elementos de informações do cliente, como número de telefone e fax, endereço	http://www.oasis-open.org/committees/ciq/ciq.html#7

			de e-mail, data de nascimento, sexo, etc. xCIL já está sendo considerado por várias agências e está sendo testado na mudança de endereço baseada na web Projeto de notificação.	
		xCRL - Linguagem Extensível de Relacionamento com o Cliente	Parte da família de padrões xCIL e xNAL que especifica formatos para relacionamentos entre clientes.	http://www.oasis-open.org/committees/ciq/ciq.html#8
		CIQ - Qualidade da Informação do Cliente	Especificações XML para definir e gerir informações/ perfil do Cliente (também chamado de "Parte") (incluindo relacionamentos cliente/parte).	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=ciq
	Relatórios de negócios	xBRL - Linguagem Extensível de Relatórios de Negócios	Grupo de Trabalho em andamento, liderado pela Receita Federal.	http://www.xbrl.org/Home/
	Dados estatísticos e metadados	SDMX - Troca de dados estatísticos e metadados	As Diretrizes Orientadas a Conteúdo SDMX recomendam práticas para a criação de dados interoperáveis e conjuntos de metadados usando os	http://www.sdmx.org/

			padrões técnicos SDMX. Prevê-se que sejam aplicáveis genericamente em domínios estatísticos.	
	Espaço para nome	OIDS - Identificadores de Objeto de Esquema	A Seção de TIC da Comissão de Serviços do Estado mantém 2.16.544.101 como o Arco OID do Governo.	https://www.itu.int/pub/T-HDB-LNG.4-2010
		URN - Nome Uniforme do Recurso	Uma forma de definir inequivocamente cada tipo de elemento e nome de atributo em um documento XML.	https://datatracker.ietf.org/doc/html/rfc8141
Acesso e apresentação de informações	Formatos de documento	DOC/DOCX	DOC/DOCX é um formato para documentos de processamento de texto; mais comumente para Microsoft Word.	https://www.leadtools.com/help/sdk/v21/main/api/file-formats-microsoft-office-word-format-doc-docx.html
		RTF – Formato Rich Text	RTF é um formato de arquivo de documento para intercâmbio de documentos entre plataformas.	https://docs.fileformat.com/word-processing/rtf/
		ODFOA v1 - Formato de documento	Vários candidatos a agências para salvar	http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=office

		aberto para aplicativos de escritório versão 1 DocBook	documentos em formato XML aberto.	
		TXT – Arquivo de Texto	TXT é um formato para arquivos que consistem em texto e geralmente contém muito pouca formatação (por exemplo, sem negrito ou itálico). A definição precisa do formato .txt não é especificada, mas normalmente corresponde ao formato aceito pelo terminal do sistema ou editor de texto simples.	https://docs.fileformat.com/word-processing/txt/
		PPT- Microsoft Power Point	PPT é um formato para apresentações.	https://www.microsoft.com/en-us/microsoft-365/powerpoint
		PDF – Formato de Documento Portátil	PDF é um formato de arquivo para troca de documentos.	https://www.adobe.com/ng/acrobat/about-adobe-pdf.html
	Formatos de imagem	GIF – O formato de intercâmbio gráfico	GIF é um formato de imagem bitmap que suporta até 8 bits por pixel, permitindo que uma única imagem faça referência a uma paleta de até 256 cores distintas escolhidas no espaço de cores RGB de	https://www.w3.org/Graphics/GIF/spec-gif89a.txt

			24 bits. Também suporta animações e permite uma paleta separada de 256 cores para cada quadro.	
		PNG – Gráficos de rede portáteis	PNG é um formato de arquivo extensível para armazenamento sem perdas, portátil e bem compactado de imagens raster.	http://www.w3.org/TR/2003/REC-PNG-20031110/
		TIFF – arquivo de imagem marcada	TIFF é um formato de arquivo flexível e adaptável para lidar com imagens e dados em um único arquivo, incluindo tags de cabeçalho (tamanho, definição, organização de dados de imagem, compactação de imagem aplicada) que definem a geometria da imagem.	https://docs.fileformat.com/image/tiff/
		JPEG – Grupo Conjunto de Especialistas em Fotografia	JPEG é um método de compactação de imagens fotográficas. O padrão JPEG especifica o codec, que define como uma imagem é compactada em um fluxo	https://www.w3.org/Graphics/JPEG/itu-t81.pdf

			de bytes e descompactada novamente em uma imagem, e o formato de arquivo usado para conter esse fluxo.	
		BMP - Mapa de bits	BMP é um formato de arquivo de imagem usado para armazenar imagens digitais bitmap.	http://atlc.sourceforge.net/bmp.html#_toc381201084
	Formatos de áudio	WAV – Formato de áudio em forma de onda	WAV é um padrão de formato de arquivo de áudio da Microsoft e IBM para armazenar um fluxo de bits de áudio em PCs.	https://docs.fileformat.com/audio/wav/
		MP3 – Mpeg 1 Camada de Áudio 3	MP3 é um formato de codificação de áudio digital que usa uma forma de compactação de dados com perdas .	https://www.thefreedictionary.com/MPEG-1+Audio+Layer+3
	Formatos de vídeo	DMF - Formato de mídia DivX	DMF inclui um codec, um player e um formato de contêiner de mídia.	https://acronyms.thefreedictionary.com/DivX+Media+Format
		MPEG - Grupo de Especialistas em Imagens em Movimento	MPEG é uma família de padrões usados para codificar informações audiovisuais (por exemplo, filmes, vídeos, músicas) em formato	https://www.mpeg.org/

			digital compactado.	
		AVI – Intercalação de Áudio e Vídeo	AVI é um arquivo contentor de multimídia da Microsoft.	https://docs.fileformat.com/video/avi/
		Tempo rápido	QuickTime é um arquivo contêiner multimídia que contém uma ou mais faixas, cada uma armazenando um tipo específico de dados: áudio, vídeo, efeitos ou texto.	https://support.apple.com/en-ng/guide/quicktime-player/welcome/mac
	Formatos de conteúdo da web	HTML v4.01 - Hipertexto Linguagem de marcação versão 4.01	HTML 4 é um aplicativo SGML em conformidade com o Padrão Internacional ISO 8879 – Standard Generalized Markup Language [ISO8879].	https://www.w3.org/TR/html401/
		XHTML - extensível Hipertexto Linguagem de marcação	XHTML é uma linguagem de marcação que possui a mesma profundidade de expressão que HTML, mas também está em conformidade com a sintaxe XML.	https://www.w3.org/TR/2001/REC-xhtml11-20010531/
	Compactação de arquivo	fecho eclair	O formato de arquivo ZIP é um formato de compactação e arquivo de dados.	https://www.nh.gov/file-format/zip

		GZIP	GZIP é um utilitário de compactação GNU ZIP. gzip (GNU zip) é um utilitário de compactação projetado para substituir o compress.	https://www.gnu.org/software/gzip/
		RAR- Roshal Arquivo	RAR é um formato de arquivo proprietário que suporta compactação de dados, recuperação de erros e extensão de arquivos.	https://www.rarlab.com/

Apêndice 8 - Protocolos/Portas protegidos

Porta insegura	Descrição	Protocolo	Porta alternativa segura	Protocolo
21 - FTP	Porta 21, o Protocolo de Transferência de Ficheiros (FTP) envia o nome de utilizador e a palavra-passe em texto simples do cliente para o servidor. Isto pode ser intercetado por um atacante e mais tarde utilizado para recuperar informações confidenciais do servidor. A alternativa segura, SFTP, na porta 22, utiliza encriptação para proteger as credenciais do utilizador e os pacotes de dados transferidos.	Protocolo de transferência de ficheiros	22* - SFTP	Protocolo de transferência segura de ficheiros
23 - Telnet	A porta 23, telnet, é utilizada por muitos sistemas Linux e quaisquer outros sistemas como um terminal básico baseado em texto. Toda a informação de e para o anfitrião numa ligação telnet é enviada em texto simples e pode ser intercetada por um atacante. Isto inclui o nome de utilizador e a palavra-passe, bem como toda a informação que está a ser apresentada no ecrã, uma vez que esta interface é toda em texto. O Secure Shell (SSH) na porta 22 utiliza encriptação para garantir que o tráfego entre o anfitrião e o terminal não é enviado em formato de texto simples.	Telnet	22* - SSH	Shell seguro
25 - SMTP	A porta 25, Simple Mail Transfer Protocol (SMTP), é a porta não encriptada	Protocolo simples de	587 - SMTP	SMTP com TLS

	predefinida para o envio de mensagens de correio eletrónico. Uma vez que não está encriptada, os dados contidos nas mensagens de correio eletrónico podem ser descobertos por sniffing de rede. A alternativa segura é utilizar a porta 587 para SMTP, utilizando o protocolo Transport Layer Security (TLS), que encripta os dados entre o cliente de correio eletrónico e o servidor de correio eletrónico.	transferência de correio		
37 - Tempo	A porta 37, Protocolo de Tempo, pode estar a ser utilizada por equipamento antigo e foi maioritariamente substituída pela utilização da porta 123 para o Protocolo de Tempo de Rede (NTP). O NTP na porta 123 oferece melhores capacidades de tratamento de erros, o que reduz a probabilidade de erros inesperados.	Protocolo de tempo	123 - NTP	Protocolo de Tempo de Rede
53 - DNS	O porto 53, Serviço de Nomes de Domínio (DNS), continua a ser amplamente utilizado. No entanto, a utilização do DNS sobre TLS (DoT) na porta 853 protege as informações do DNS de serem modificadas em trânsito.	Serviço de nomes de domínio	853 - DoT	DNS sobre TLS (DoT)
80 - HTTP	A porta 80, HyperText Transfer Protocol (HTTP), é a base de quase todo o tráfego dos navegadores Web na Internet. As informações enviadas por HTTP não são encriptadas e são suscetíveis de ataques de sniffing. É preferível utilizar HTTPS com encriptação TLS, uma vez que protege os dados em trânsito entre o servidor e o browser. Note que isto é frequentemente designado por SSL/TLS. A Secure Sockets Layer (SSL) foi comprometida e já não é considerada segura. Recomenda-se agora que os servidores e clientes Web utilizem Transport Layer Security (TLS) 1.3 ou superior para obter a melhor proteção.	Protocolo de transferência de hipertexto	443 - HTTPS	Protocolo de transferência de hipertexto (SSL/TLS)
143 - IMAP	A porta 143, Internet Message Access Protocol (IMAP), é um protocolo utilizado para recuperar mensagens de correio eletrónico. O tráfego IMAP na porta 143 não é encriptado e é suscetível de ser detetado pela rede. A alternativa segura é utilizar a porta 993 para IMAP, que adiciona segurança SSL/TLS para encriptar os dados entre o cliente de correio eletrónico e o servidor de correio eletrónico.	Protocolo de acesso a mensagens da Internet	993 - IMAP	IMAP para SSL/TLS
161/162 - SNMP	As portas 161 e 162, Simple Network Management Protocol, são normalmente utilizadas para enviar e receber dados utilizados para gerir dispositivos de infraestruturas. Dado que estas mensagens	Protocolo de gestão de rede simples	161/162 - SNMP	SNMPv3

	contêm frequentemente informações sensíveis, recomenda-se a utilização da versão 2 ou 3 do SNMP (abreviado SNMPv2 ou SNMPv3) para incluir encriptação e funcionalidades de segurança adicionais. Ao contrário de muitas outras abordadas aqui, todas as versões do SNMP utilizam as mesmas portas, pelo que não existe um emparelhamento seguro e inseguro definitivo. Será necessário um contexto adicional para determinar se as informações nas portas 161 e 162 são seguras ou não.			
445 - PME	A porta 445, Server Message Block (SMB), é utilizada por muitas versões do Windows para aceder a ficheiros através da rede. Os ficheiros são transmitidos sem encriptação e muitas vulnerabilidades são bem conhecidas. Por conseguinte, recomenda-se que o tráfego na porta 445 não seja autorizado a passar por uma firewall no perímetro da rede. Uma alternativa mais segura é a porta 2049, Network File System (NFS). Embora o NFS possa usar criptografia, recomenda-se que o NFS também não seja permitido através de firewalls.	Bloco de mensagens do servidor	2049 - NFS	Sistema de ficheiros de rede
389 - LDAP	A porta 389, Lightweight Directory Access Protocol (LDAP), é utilizada para comunicar informações de diretório dos servidores para os clientes. Pode ser um livro de endereços para correio eletrónico ou nomes de utilizador para início de sessão. O protocolo LDAP também permite que os registos no diretório sejam atualizados, introduzindo um risco adicional. Uma vez que o LDAP não é encriptado, é suscetível a ataques de sniffing e de manipulação. O Lightweight Directory Access Protocol Secure (LDAPS) adiciona segurança SSL/TLS para proteger as informações enquanto estão em trânsito.	Protocolo leve de acesso a diretórios	636 - LDAPS	Protocolo leve de acesso a diretórios seguros