

DESENHO DA ESTRATÉGIA E DA POLÍTICA DE GOVERNANÇA DE DADOS

Política de Governança de Dados

Versão 1

Novembro de 2024

Consultora: Marisa Balas

Contrato: 12/C/DSTP/2023 - Assistência técnica para o desenvolvimento de política, estratégia e plano de ação de Governança de Dados

Conteúdo

PARTE 1: Identificação da Política	3
PARTE 2: Conceitos de Governança de Dados	7
1 Introdução	8
2 O que é a Governança de Dados	9
3 Visão, Missão e Resultados da Governança de Dados	13
PARTE 3: Política de Governança de Dados	17
1 Disposições Iniciais	18
2 Âmbito da Política	18
3 Elementos da Política	19
4 Princípios da Política	20
5 Quadro de Governança de Dados	23
5.1 Modelo Operacional	24
5.2 Estrutura Organizacional	27
5.2.1 Comité Executivo de Governança de Dados	27
5.2.2 Núcleo de Governança de Dados	27
5.2.3 Escritório de Governança de Dados	28
5.2.4 Equipas de Dados	29
5.2.5 Fórum de Governança de Dados	29
5.3 Papeis e Responsabilidades dos Membros da Estrutura de Governança de Dados	32
5.3.1 Proprietário de Dados (Data Owners)	32
5.3.2 Curadores de Dados (Data Stewards)	33
5.3.3 Guardiões de Dados (<i>Data Guardians</i>)	35
5.3.4 Utilizadores de Dados (<i>Data Users</i>)	36
5.3.5 Analistas de Dados (<i>Data Analysts</i>)	37
5.3.6 Encarregados de Proteção de Dados (<i>Data Protection Officer</i>)	38
5.4 Avaliação e Monitoria Contínuas	41
5.4.1 Indicadores e Métricas	41
5.4.2 Avaliação Regular dos Elementos Facilitadores	44
5.4.3 Avaliação da Evolução da Maturidade da Gestão e Governança de Dados	45

PARTE 1: Identificação da Política

Política de Governança de Dados

Autoridade de aprovação: ÓRGÃO QUE APROVA A POLÍTICA, no uso das atribuições que lhe confere o art. XXXXX da LEI OU INSTRUMENTO QUE ATRIBUI OS PODERES, e tendo em vista o disposto na Lei XXXXX (acesso à informação), Lei Geral de Proteção de Dados Pessoais que estabelece os princípios de proteção de dados pessoais, na Lei XXXX, que dispõe estabelece a partilha de dados e infraestrutura no âmbito da administração pública de São Tomé e Príncipe, na Lei XXX que dispõe sobre requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem, QUE OUTROS INSTRUMENTOS DEVEMOS UTILIZAR? , resolve aprovar esta Política de Governança de Dados.

Categoria de política: Governança

Assunto: Governança de Dados

Responsável pela política: XXXX

Prestação de contas:

Entidade Responsável: XXXX

Oficial de Contacto: XXXX

Auditorias: As auditorias e avaliações regulares serão conduzidas para identificar áreas de melhoria.

Políticas, Normas e Procedimentos Relacionados: Nada nesta política impede quaisquer medidas que precisem ser tomadas para cumprir a lei para divulgar informações a organizações externas ou agências governamentais.

- Lei nº 3/2016 - **Lei de Garantia e Protecção dos Dados Pessoais das Pessoas Singulares** que dispõe sobre princípios, regras e instrumentos que visam a proteção e privacidade de dados pessoais.
- Lei nº 7/2017 que cria a **Agência Nacional de Protecção de Dados Pessoais**.
- Lei nº 15/2017 - **Lei sobre Cibercrime**, que aborda aspectos e conceitos da internet e também das ameaças surgidas com a chamada Revolução Tecnológica, estabelecendo as disposições penais materiais e processuais, bem como as disposições relativas à cooperação internacional em matéria penal, relativas ao domínio do cibercrime e da recolha de prova em suporte electrónico, relativa a ataques contra sistemas de informação, e adaptando o direito interno às convenções internacionais sobre o Cibercrime, vindo introduzir no ordenamento jurídico-penal os crimes de falsidade informática, dano relativo a programas ou outros dados informáticos, sabotagem informática, acesso ilegítimo,

intercepção ilegítima, reprodução ilegítima de programa protegido e inserção de dados falsos

- Lei nº XXX que estabelece o **Quadro Nacional de Interoperabilidade** que define um conjunto mínimo de premissas, políticas e especificações técnicas que regulamentam a utilização de Tecnologias de Informação e Comunicação (TIC) na interoperabilidade dos serviços de governo eletrónico.
- Lei nº XXX, de XXXXX - **Lei de Acesso à Informação** que se aplica aos órgãos públicos da administração direta e entes da administração indireta dos Poderes Executivo, legislativo, judiciário, incluindo ainda o tribunal de Contas, e o Ministério Público em todas as esferas. No que diz respeito à transparência ativa, esta lei traz consigo conceitos de dados abertos, quando trata que é dever dos órgãos e entidades públicas promoverem, independentemente de requerimentos, a divulgação em local de fácil acesso, no âmbito de suas competências, de informações de interesse coletivo ou geral por eles produzidas ou custodiadas, com exceção das protegidas por leis e normativos.
- Lei nº XXX, de XXXXX - Lei de partilha de dados e infraestrutura que dispõe sobre a governança na partilha de dados no âmbito da administração pública em São Tomé e Príncipe
- Política de Gestão Documental (existe?)
- Políticas e Procedimentos de Acesso e Proteção de Dados

Propriedade e gestão dos dados: Os dados institucionais são propriedade do Estado de São Tomé e Príncipe, não de quaisquer indivíduos. Os órgãos, suas direções ou departamentos podem ter a responsabilidade por alguns conjuntos de dados. Os administradores de dados órgãos, suas direções ou departamentos têm a responsabilidade final de gerir os dados sob sua autoridade em conformidade com a lei e as políticas do País.

Penalizações por não cumprimento: As penalidades por violação deliberada desta política serão determinadas de acordo com procedimentos disciplinares aplicáveis, descritos no manual ou código de conduta apropriado do funcionário público.

Histórico de Revisão e de aprovação:

- Outubro de 2024: Elaboração da linha de base da política
- Novembro de 2024: Validação dos elementos da política (em workshop)
- Novembro de 2024: Draft zero da política
- XXXX: Revisões de política. Aberto para comentários.
- XXXX: Revisão pela equipa de segurança cibernética: Política revista.
- XXXX: Revisão pelo escritório de consultoria jurídica. Política revista.
- XXXXX: Política aprovada e assinada.

Data de entrada em vigor: XXXX

Substitui: Não Aplicável

Próxima revisão: Esta Política será revista e atualizada a cada 3 (três) (OU CINCO?) anos a partir da data de aprovação, ou com mais frequência, se apropriado. Para a revisão, será realizada uma avaliação da evolução da maturidade da gestão de dados e do grau de preparação para as mudanças necessárias.

PARTE 2: Conceitos de Governança de Dados

1 Introdução

Os dados institucionais são um ativo estratégico para o Governo de São Tomé e Príncipe e desempenham um papel basilar na melhoria dos serviços e das políticas públicas, onde as organizações buscam extrair valor e evidências de seus ativos de dados.

Os crescentes volumes de dados provenientes de diversas fontes causam inconsistências de dados que precisam de ser identificadas e resolvidas antes de serem tomadas decisões com base em dados incorretos. A produção de relatórios e análises de dados cria maior necessidade de um entendimento comum dos dados em toda a organização. Adicionalmente, o impacto contínuo dos requisitos regulamentares, como a Lei de Garantia e Proteção dos Dados Pessoais das Pessoas Singulares, aumenta a pressão sobre as organizações para que tenham um forte controlo sobre quais os dados que estão armazenados, onde e como os dados estão a ser utilizados.

Torna-se necessário superar os seus desafios relativos a dados imprecisos e incompletos, arquitetura fragmentada e sistemas legados e questões de conformidade relacionadas com os regulamentos. Adicionalmente é importante garantir a conformidade e segurança, facilitar a tomada de decisões, promover a cultura de dados, e estabelecer responsabilidade e a prestação de contas.

O Governo de São Tomé e Príncipe identificou a necessidade de se definir e implementar uma política e estratégia de Governança de Dados que garanta que os dados da mais alta qualidade sejam recolhidos, protegidos, utilizados e disponibilizados às principais partes interessadas através de esforços coordenados dentro administração pública, com o objetivo de melhorar a eficiência e permitir uma melhor tomada de decisões por parte dos decisores políticos, e garantir a conformidade com as normas e princípios estabelecidos.

A elaboração e aplicação desta política de Governança de Dados é um esforço colaborativo entre os vários órgãos da administração pública, seus departamentos de TI, equipas de gestão de dados, equipas de segurança e proteção de dados, sector jurídico, e deve ser encarada como um esforço de melhoria contínua, onde a cada etapa se vislumbram novas melhorias a incorporar para etapas seguintes.

2 O que é a Governança de Dados

A Governança de Dados é definida como o exercício de autoridade e de controlo sobre a gestão de dados (DAMA International, 2017) que tem como objetivo implementar uma agenda de dados (Dyché & Levy, 2006), maximizando o valor dos ativos de dados (Carretero, Gualo, Caballero, & Piattini, 2017; Otto, 2011) e minimizando os riscos relacionados com os dados (DAMA International, 2017; Morabito, 2015).

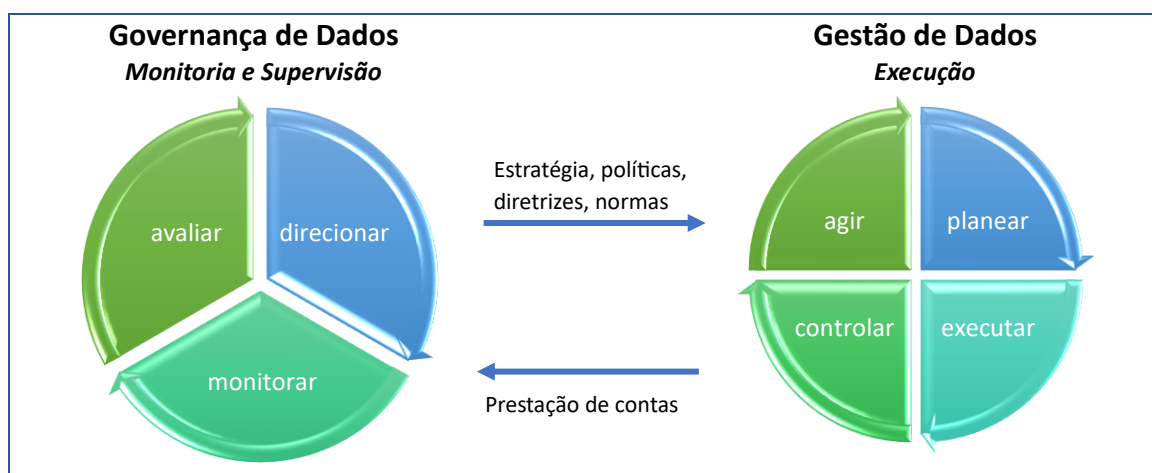
A Governança de Dados é essencial para garantir que a informação seja gerida de forma eficaz e estratégica, proporcionando a usabilidade dos dados, ou seja, sua fácil interpretação e aplicação em diferentes contextos. Além disso, assegura a disponibilidade dos dados, permitindo acesso contínuo e confiável às informações necessárias para as operações e decisões organizacionais. A qualidade dos dados é outro aspeto fundamental, garantindo que os dados sejam precisos, completos e relevantes para os objetivos propostos. A segurança de dados também é priorizada, protegendo as informações contra acessos não autorizados e possíveis violações. Por fim, a governança inclui a linhagem de dados, que rastreia a origem e as transformações que os dados sofrem ao longo do tempo, promovendo transparência e confiabilidade em todo o ciclo de vida dos dados (Figura 1).

Figura 1: Foco da Governança de Dados



É fundamental compreender a diferença entre a Governança de Dados e a Gestão de Dados. Enquanto a Governança de Dados provê o direcionamento, monitoramento, supervisão e avaliação da prática da Gestão de Dados, estabelecendo as diretrizes e as políticas a serem seguidas pela Gestão de Dados, com o foco em como as decisões sobre os dados são tomadas, como as pessoas e os processos devem comportar-se em relação aos dados, e como garantir a conformidade e prevenção de ocorrência de eventos de risco, a Gestão de Dados, por seu turno, garante que a organização obtém valor de seus dados, observando o que prescreve a Governança de Dados, fomentando uma maior eficiência organizacional (Figura 2).

Figura 2: Governança de Dados e Gestão de Dados



Fonte: Adaptado de DAMA International (2017)

Para que seja efetiva, a Governança de Dados abrange vários tópicos (Figura 3), tais como arquitetura de dados, modelação de dados, armazenamento e operações de dados, segurança de dados, interpretação e interoperabilidade de dados, documentos e conteúdos, dados de referência e mestres, armazenamento de dados e *business intelligence*, metadados e qualidade de dados (DAMA International, 2017).

Figura 3: As 11 Áreas de Conhecimento da Gestão e Governança de Dados



Fonte: Adaptado de DAMA International (2017)

O Ecossistema de Dados em São Tomé e Príncipe é composto por várias organizações, seus recursos, processos, procedimentos e tecnologias, que trabalham juntos para coletar, armazenar, processar, compartilhar e usar dados de forma eficiente. Este ecossistema é composto pela administração pública, cidadãos, instituições da sociedade civil organizada, academia, organizações internacionais, setor privado e demais interessados, que interagem e direta ou indiretamente consomem, produzem, fornecem dados e outros recursos relacionados (Figura 4).

Figura 4: O Ecossistema de Dados de São Tomé e Príncipe



- **Setor Público:** o Estado, em todas suas esferas e poderes, tem um papel fundamental na coleta e disponibilização de dados por meio dos órgãos públicos. As entidades governamentais são os principais produtores de dados públicos para consecução de políticas públicas. O governo também é responsável por estabelecer políticas e regulamentações para garantir a privacidade e segurança dos dados pessoais dos cidadãos, a eficiência na oferta de serviços públicos baseados em dados, a transparência dos dados públicos, e o direito de acesso à informação.
- **Setor Privado:** o setor privado é um importante contribuinte para a produção de dados no Ecossistema de Dados. As empresas coletam e processam dados de seus clientes e parceiros de negócios. Esses dados podem ser usados para impulsionar a inovação, criar produtos e serviços, e melhorar a eficiência dos negócios. Alguns desses dados são muito valiosos para desenvolvimento de políticas públicas.
- **Instituições académicas:** as universidades e outras instituições de pesquisa são importantes para o ecossistema de dados, desempenhando funções de pesquisa e

desenvolvimento do ecossistema de dados, desenvolvendo conhecimentos e tecnologias que podem ser usados para coletar, processar, analisar dados.

- **Sociedade civil:** diversas organizações sem fins lucrativos, cidadãos e os meios de comunicação, atuam no ecossistema de dados. Esses atores desempenham um papel crítico como produtores e usuários de dados que mantêm, e o seu valor aumenta por meio da reutilização por outros participantes do ecossistema.
- **Cidadão:** o cidadão participa no ecossistema a partir de seu empoderamento na tomada de decisão de como dá acesso e partilha os seus dados no dia a dia e de como monitora seus interesses, enquanto titular de direitos, seja nas relações de mercado com o Estado ou com outros cidadãos e entidades, por exemplo. Além do direito de participação em discussões públicas sobre políticas de dados, regulamentações e ética digital, fiscalização e denúncias de práticas inadequadas de coleta e uso de dados e incentivo à transparência e responsabilidade, exigindo políticas claras de privacidade, notificações adequadas sobre uso de dados e adoção de práticas éticas.
- **Organizações da sociedade civil:** compreendidas aqui como entidades privadas sem fins lucrativos que possuem um objeto social e que são importantes aliadas do Poder Público no desenvolvimento e implementação de políticas públicas que atendam às demandas sociais, inclusive com atuação já histórica e destacada na conquista e manutenção de direitos digitais.
- **Organizações Internacionais:** Esses grupos atuam no ecossistema de dados como definidores de padrões e melhor prática e métodos, atributos fundamentais para a comparabilidade internacional dos dados produzidos.
- **Mídias:** Os meios de comunicação de massa, ou seja, os jornais, revistas, rádio, televisão, sites de notícias e Mídias sociais, patrocinados ou independentes, públicos ou privados, desempenham por meio dos seus agentes um papel ativo do Ecossistema de Dados quando coletam, analisam e disseminam informações baseadas em dados. As informações geradas pelos meios de comunicação podem ser usadas para embasar a elaboração e o monitoramento de decisões, incluindo a concepção e ajustes em políticas públicas.

3 Visão, Missão e Resultados da Governança de Dados

Visão: O Governo de São Tomé e Príncipe pretende uma Governança de Dados que suporte o cumprimento dos objectivos estratégicos do Governo de São Tomé e Príncipe, promovendo um ambiente de dados confiável e transparente, onde os dados sejam geridos de forma ética, segura e responsável, assegurando a privacidade, a equidade e a criação de valor para todos os cidadãos, enquanto se viabiliza a interoperabilidade e a transformação digital.

A **Missão** da Governança de Dados é garantir que os dados da mais elevada qualidade são coletados, processados, protegidos, utilizados e disponibilizados às principais partes interessadas do ecossistema de dados, através de políticas, normas e mecanismos institucionais que garantem a gestão ética, segura e transparente dos dados, protegendo os direitos individuais, promovendo a interoperabilidade e fortalecendo a confiança pública no ecossistema digital

Os **Objectivos Estratégicos** da Governança de Dados são (**Figura 5**):

- Garantir conformidade com as leis, regulamentos, intercâmbios e normas aplicáveis
- Promover uma visão comum das práticas relacionadas com os dados, atuando como a única fonte de verdade sobre padrões e práticas que todos devem seguir
- Melhorar a acessibilidade e a qualidade e precisão dos dados
- Melhorar a comunicação e a colaboração entre todos os intervenientes do ecossistema de dados
- Promover a interoperabilidade e a partilha segura de dados entre órgãos públicos
- Proteger os dados contra ameaças internas e externas, garantindo a proteção de dados pessoais e a privacidade dos cidadãos
- Usar dados para orientar políticas públicas e decisões baseadas em evidências, melhorando o desempenho do Estado
- Estimular o uso de dados como motor de inovação e desenvolvimento económico.

Figura 5: A Missão e os Objetivos da Governança de Dados



Resultados: A Governança de Dados garante que os dados são consistentes, compreensíveis, corretos, completos, fiáveis, seguros e detetáveis pois estabelece os processos para padronizar, integrar, proteger e armazenar os dados. Pretende-se, com uma Governança de Dados efetiva, alcançar os seguintes resultados (Figura 6):

- **Alteração de comportamentos em relação aos dados.** A Governança de Dados promove literacia em matéria de dados, sedimentando uma cultura baseada em dados que cria ferramentas e competências, aumenta a confiança dos usuários nas condições e fontes de dados e aumenta as competências e a compreensão dos dados.
- **Democratização dos dados.** A Governança de Dados introduz procedimentos para democratizar os dados, ou seja, eliminar silos de dados permitindo a partilha e o uso de dados de forma cada vez mais ampla e por mais utilizadores. As equipas podem aceder de

forma rápida e independente os dados necessários para suas atividades, o que lhes permite agilizar a tomada de decisões.

Figura 6: Resultados da Governança de Dados em São Tomé e Príncipe



- **Segurança de dados** - A Governança de Dados cria regras e ferramentas que protegem os dados e amplia as práticas de segurança utilizadas pelos órgãos da Administração Pública.
- **Qualidade de Dados (Dados confiáveis)** - Com padrões claros para coleta, categorização e armazenamento de dados, a Governança de Dados evitará que dados de baixa qualidade influenciem decisões importantes.
- **Eficiência Operacional** - A Governança de Dados possibilita a construção de uma cultura de excelência operacional, com processos claramente definidos e estabelecidos, simplificados, o que reflete diretamente na melhoria da consistência dos dados. Equipas e processos mais eficientes proporcionam a redução de custos operacionais, podendo esses recursos serem redistribuídos para outras iniciativas.
- **Decisões Informadas** - Numa cultura orientada por dados, as decisões são tomadas com base em provas de dados e não em instintos. A Governança de Dados possibilitará aos gestores a visualização e até previsão dos problemas com alternativas de como tratá-los e, dessa forma tomarem as melhores decisões para solucioná-los.

- **Redução de Riscos** - O risco da não conformidade em relação aos dados organizacionais pode ser severo em setores regulados como saúde, educação, produção, seguros e finanças, incluindo aplicação de multas, perda de produtividade e de receita, bem como interrupção em operações. A Governança de Dados deve ser capaz de ajudar a conhecer e implementar métodos e técnicas no sentido de identificação, mitigação e contingência dos riscos.
- **Fomento da inovação** - A implementação de diretrizes de Governança de Dados, uma vez que essa promove o incentivo à democratização de dados, resulta no fomento à inovação na prestação de serviços públicos, de forma a alcançar resultados que não seriam alcançáveis sem o uso de dados.

PARTE 3: Política de Governança de Dados

1 Disposições Iniciais

2. Todo dado coletado, analisado, armazenado, produzido, disseminado e/ou enviado para um órgão da Administração Pública é considerado um ativo de informação.
3. Cabe a cada órgão da Administração Pública definir, no âmbito das suas competências, os seus ativos de informação estratégica, também denominados Elementos de Dados Críticos.
4. Todo ativo de informação estratégica da Administração Pública deve ser armazenado em servidores de bases de dados ou de arquivos, instalados nos centros de dados do Governo, centralizados ou não, onde os controlos de segurança da informação e comunicações definidos são implantados e mantidos pelas equipas dedicadas à Segurança de Dados.
5. Não devem ser utilizados equipamentos de armazenamento de dados e informações para guarda de ativos de informação estratégica que estejam fora dos centros de dados do Governo, podendo ser utilizado o ambiente de nuvem para armazenamento de ativos de informação estratégica, desde que de acordo com os controlos de segurança da informação e comunicações definidos.

2 Âmbito da Política

6. Esta política de Governança de Dados aplica-se a todos os participantes do ecossistema de dados, todos os processos para o acesso, transformação, armazenamento de dados, uso e transferência de dados, incluindo os dados sensíveis e sigilosos, entre entidades externas e o Governo de São Tomé e Príncipe em ambos os sentidos:
 - Todo e qualquer órgão ou Instituição da Administração Pública de São Tomé e Príncipe (ALINHAR com documento de eGOV – Verificar escrita com INIC);
 - Todos funcionários públicos em todas as suas Unidades Orgânicas e, particularmente, a todos os indivíduos que especificam processos de dados, que desenvolvem, gerem, administram ou dão suporte a sistemas e aplicativos de tecnologia da informação que geram, coletam, armazenam, mantêm, transmitem ou registam dados institucionais. Aplica-se igualmente a todos os indivíduos que fornecem dados externos ou informações especializadas, incluindo todos os contratantes e consultores do Governo de São Tomé e Príncipe;
 - Todos os dados e produtos de dados institucionais utilizados na administração pública incluindo, entre outros, dados financeiros, dados patrimoniais, dados organizacionais, bem como dados pessoais gerados ou geridos da administração pública;

- A política abrange, mas não se limita a dados institucionais em qualquer formato (papel, digital ou audiovisual), quer sejam dados impressos ou em formato eletrónico, documentos de trabalho, documentos eletrónicos, correio eletrónico institucional, transações online, informação geográfica como mapas, planos e fotografias, gravações de som e vídeo, dados biométricos, dados de backup e arquivados, independentemente de onde os dados sejam mantidos (em arquivo de papel, em bases de dados locais ou em dispositivos de armazenamento, ou na nuvem);
- Todos os processos de gestão de dados com enfoque para processos que definem o acesso aos dados, solicitação de dados, recolha de dados, validação de dados, e elaboração de informação com base em dados;
- Todos os sistemas e aplicativos de tecnologia da informação que geram, coletam, armazenam, mantêm, transmitem ou registam dados institucionais, independentemente de quem gere, possui ou administra o sistema e o aplicativo, ou de onde este se localiza.

3 Elementos da Política

7. A Política de Governança de Dados promove uma visão comum das práticas relacionadas com os dados e promove uma utilização mais eficaz dos dados, baseada em princípios inalienáveis. Melhora a compreensão dos dados recolhidos, reportados e utilizados. Como resultado, a política promove respostas mais consistentes, eficientes e coordenadas a questões de dados e melhora a comunicação e a colaboração entre todos os intervenientes
8. Esta política é composta pelos seguintes elementos:
 - **Princípios** de Governança de Dados a serem respeitados por todos os participantes do ecossistema de dados, estabelecendo as regras para controlar a *integridade, segurança, qualidade* e *uso* de dados ao longo de seu *ciclo de vida*;
 - **Quadro de governança de dados** que define os aspetos práticos operacionais para a gestão de dados que irão suportar e aplicar a política de governação de dados e os princípios definidos:

4 Princípios da Política

9. Esta política define os princípios integrados à Governança de Dados para reforçar a transparência governamental, apoiar a interoperabilidade, garantir proteção e privacidade de dados, promover inclusão, e fomentar decisões informadas baseadas em dados claros e precisos.
10. Os princípios da Governança de Dados estão alinhados com os princípios de dados definidos na Estratégia de Dados, tendo sido igualmente adotados os princípios estabelecidos na norma **ISO/IEC 38505**, intitulada *"Governance of Data – Application of ISO/IEC 38500 to the governance of data"*, que fornece diretrizes específicas para aplicar os princípios de governança de TI (estabelecidos na ISO/IEC 38500) ao contexto da Governança de Dados. São igualmente adotados e harmonizados os princípios sugeridos pela Organização para a Cooperação e Desenvolvimento Económico (**OCDE**) que destaca a necessidade para maximizar o valor dos dados como ativos económicos e sociais, e simultaneamente proteger os direitos individuais e promover confiança (Tabela 1).

Tabela 1: Os Princípios da Governança de Dados para São Tomé e Príncipe

Pilar	Princípio	Diretrizes
Organização da Governança de Dados Liderança engajada em promover um modelo claro e abrangente de tratamento de dados entre as principais agências proprietárias ou utilizadoras de dados críticos	Responsabilidade (Responsibility)	- A Governança de dados deve definir claramente os papéis e responsabilidades no uso e gestão de dados, para que os dados sejam tratados como ativos estratégicos da organização. - É essencial estabelecer normas e diretrizes consistentes para orientar todos os envolvidos, visando implementar e definir critérios para o uso de dados em toda a organização.
	Transparência e Prestação de Contas (Accountability)	- As políticas e práticas de Governança de Dados devem ser transparentes, permitindo que as partes interessadas compreendam como os dados são coletados, usados e protegidos. - Os órgãos da Administração Pública devem ser responsabilizados por práticas inadequadas ou violações de dados.
	Cooperação Internacional (International Cooperation)	- A Governança de Dados deve promover a colaboração entre países para alinhar práticas de Governança de Dados e criar um fluxo internacional seguro e confiável de dados. - Os princípios globais e regionais devem ser respeitados, equilibrando soberania digital e interconexão global.

Alinhamento entre a Governança de Dados e a Estratégia Organizacional Garantir que os dados estejam alinhados com as necessidades do negócio, o que inclui garantir que os dados atendam aos requisitos de qualidade necessários	Estratégia (Strategy)	• A Governança de Dados deve estar alinhada com os objetivos estratégicos da Administração Pública. • As decisões sobre dados devem contribuir para criar valor e apoiar o alcance das metas organizacionais.
	Aquisição (Acquisition)	• As decisões sobre a aquisição de dados (coleta, compra ou integração) devem ser justificadas e estar alinhadas com as necessidades estratégicas da Administração Pública. • Deve haver clareza sobre a origem, qualidade e finalidade dos dados adquiridos.
	Qualidade e Integridade dos Dados (Data Quality)	• A Governança de Dados deve garantir que as decisões sejam baseadas em dados, sendo para tal necessário definir padrões e procedimentos para garantir a precisão, relevância e atualidade dos dados. • Os dados necessitam ser precisos, completos, confiáveis e atualizados para atender às necessidades organizacionais e para evitar discriminações ou erros.
	Desempenho (Performance)	• A Governança de Dados deve garantir que os dados sejam geridos para fornecer resultados eficientes, eficazes e sustentáveis. • Os processos relacionados aos dados devem ser monitorados e otimizados para alcançar níveis de desempenho esperados.
	Disponibilidade e Acessibilidade de Dados (Availability)	• A Governança de Dados deve garantir a partilha atempada de um conjunto de dados entre diferentes funções da Administração Pública para a boa execução das suas funções. • Os dados devem ser disponibilizados de forma ampla e acessível para promover inovação, eficiência e criação de valor social e económico.
Conformidade Regulamentar Especialmente para setores fortemente regulamentados, como a proteção de	Ética no Uso de Dados (Data Ethics)	• A Governança de Dados deve estabelecer diretrizes para uso responsável e ético, respeitando os direitos dos indivíduos e evitando discriminações, viés algorítmico e violações de direitos fundamentais. • O uso de dados deve ser sempre alinhado com os valores democráticos e os direitos humanos.

DESENHO DA ESTRATÉGIA E DA POLÍTICA DE GOVERNANÇA DE DADOS

dados pessoais, serviços financeiros, de telecomunicações, e de cuidados de saúde	Proteção de Dados e Privacidade (Data protection and privacy)	• A Governança de Dados deve garantir a conformidade com leis, regulamentações, normas aplicáveis e padrões éticos, implementando mecanismos robustos de segurança e anonimização. • Políticas internas devem ser documentadas, comunicadas e aplicadas, balanceando o acesso aos dados com a necessidade de proteger informações sensíveis e pessoais.
	Gestão de Riscos e Segurança (Risk Management)	• A Governança de Dados deve identificar, avaliar e mitigar riscos associados ao uso de dados, como Cibersegurança, como violações de privacidade, segurança e má interpretação e uso indevido. • Políticas internas devem definir e implementar medidas preventivas para proteger sistemas e bases de dados contra ameaças externas.
Cultura de Dados e Entendimento comum Os esforços só poderão surtir efeitos se houver um entendimento sobre o que é comum, que padrões deverão ser respeitados, que dados serão partilhados e como serão partilhados, bem como uma gestão eficaz dos metadados	Comportamento Humano (Human Behaviour)	• A Governança de Dados deve considerar os fatores humanos, como cultura organizacional, ética e comportamentos e medir a capacidade da organização para mudar os comportamentos necessários para a adaptação aos princípios preconizados nesta política. • Deverá ser promovida uma cultura de decisões orientadas por dados confiáveis e bem geridos.
	Interoperabilidade e Portabilidade de Dados (Interoperability)	• A Governança de Dados deve promover padrões técnicos e organizacionais para facilitar a partilha segura e eficaz de dados entre sistemas e setores. • A Governança de Dados deve incentivar a portabilidade de dados para garantir flexibilidade e inovação.
	Inovação e Desenvolvimento Baseado em Dados (Innovation)	• A Governança de Dados deve criar um ambiente que incentive a inovação orientada por dados, especialmente para impulsionar serviços públicos e soluções tecnológicas. • A Governança de Dados deve facilitar parcerias público-privadas para maximizar o valor dos dados.
	Inclusividade e Equidade (Inclusivity and Equity)	• A Governança de Dados deve garantir que o acesso e os benefícios dos dados sejam distribuídos de forma equitativa, abordando desigualdades e promovendo inclusão social. • As políticas devem considerar as necessidades de grupos vulneráveis e populações marginalizadas.

5 Quadro de Governança de Dados

11. O Quadro de Governança de Dados procede à definição e aplicação sistemáticas de **princípios, papéis e responsabilidades, processos e procedimentos**, e **métricas**, organizados em um **modelo operacional** como forma de melhorar a supervisão, a orientação e a qualidade dos dados. Este quadro inclui um **ciclo de melhoria contínua**, usando para o efeito modelos de avaliação, onde cada etapa serve de aprendizagem e melhoria em novos ciclos de trabalho.
12. Os seguintes elementos constituem o quadro de governança de dados de STP para promover uma gestão e utilização dos dados mais eficaz evitando as ineficiências operacionais e a exposição do Governo a riscos indesejados (**Erro! A origem da referência não foi encontrada.**):
 - O **Modelo Operacional** que explicita como processos, funções e recursos são organizados e executados para alcançar os objetivos estratégicos, procurando eficiência, fluxos e entrega de valor para a organização. Dependendo da organização, a estrutura pode ser centralizada (uma autoridade central gere tudo), replicada (uma autoridade definida que é replicada em toda as instâncias ou localizações) ou federada (um grupo central que define as normas e políticas e múltiplos grupos que as implementam ao nível local).
 - A **Estrutura Organizacional** que define a hierarquia formal, os **papéis, responsabilidades e relações** de autoridade dentro da organização da Governança de Dados, representando quem faz o quê e como a autoridade e a comunicação fluem entre as diferentes partes da estrutura. Ela complementa o Modelo Operacional selecionado.
 - Os **Processos e Procedimentos** que estabelecem as formas de gerir os dados em todo o seu ciclo de vida, garantindo a uniformização das operações relacionadas com dados.
 - As **Métricas de Desempenho e de Conformidade** que permitem avaliar a eficiência, eficácia e a conformidade das operações de dados com o prescrito e descrito nos processos de gestão de dados.
 - O **Modelo de Avaliação da Maturidade e Melhoria Contínua** permite criar ciclos de avaliação da maturidade da Governança de Dados, avaliando o estágio de maturidade atual e pretendido, identificando as áreas que exigem melhorias. Exige atenção especial à **Gestão de Mudança**.

Figura 7: Quadro de Governança de Dados para São Tomé e Príncipe



Fonte: Baseado no Quadro de Governança e Gestão de Dados da Dama International (2017)

5.1 Modelo Operacional

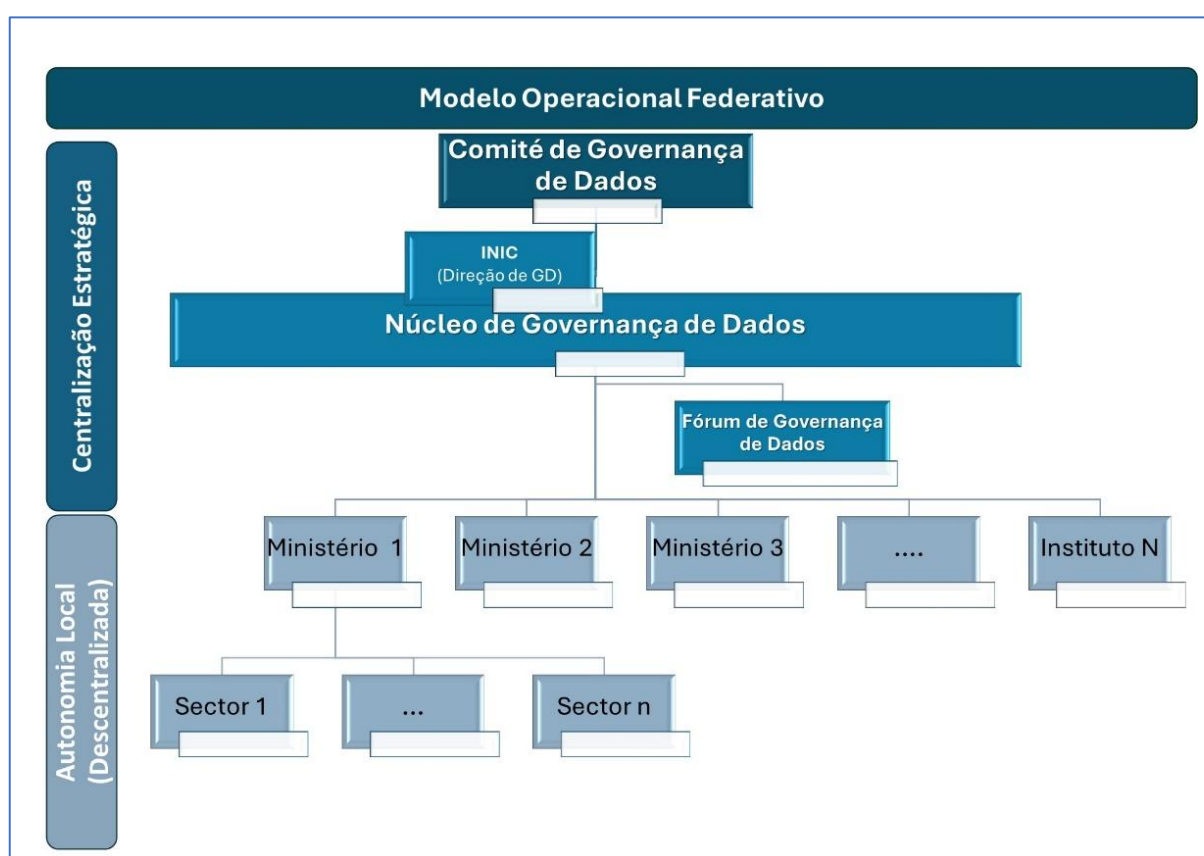
13. A Governança de Dados exige coordenação entre áreas funcionais pelo que é imperioso estabelecer um Modelo Operacional que defina as interações entre todos os intervenientes e uma Estrutura Organizacional que crie a base hierárquica das funções, papéis e responsabilidades.
14. Foi selecionado o **Modelo Operacional Federativo** para Governança de Dados em São Tomé e Príncipe. Este modelo é particularmente útil para o caso da Administração Pública uma vez que existem vários órgãos, várias direções e departamentos, cada um com suas próprias necessidades e responsabilidades, mas que precisam seguir diretrizes e objetivos comuns para a gestão de dados de forma integrada, respeitando as particularidades de cada unidade ou entidade.
15. O Modelo Operacional Federativo combina o equilíbrio entre a padronização e o controlo ao nível central e multifuncional com a flexibilidade e a autonomia operacional ao nível dos vários órgãos da Administração Pública, o que facilita a adaptação às mudanças de contexto ou às necessidades específicas e a escalabilidade. Para que o modelo resulte, é importante

DESENHO DA ESTRATÉGIA E DA POLÍTICA DE GOVERNANÇA DE DADOS

estabelecer uma forte colaboração e coordenação entre a componente centralizada do modelo e as unidades locais.

16. O Modelo Operacional Federativo é constituído por um nível central, composto por um Comité Executivo e por um núcleo multifuncional de Governança de Dados, que é coordenado pela Direção de Governança de Dados inserida no INIC (Centro de Inovação e Conhecimento), e por um nível local, composto por todos os órgãos que fazem parte da Administração Pública de São Tomé e Príncipe. É igualmente proposto que ao nível central seja estabelecido um Fórum de Governança de Dados, para fortalecer o conhecimento e a inovação, através da investigação de temas. O Modelo Operacional Federativo é ilustrado na Figura 8.

Figura 8: O Modelo Operacional Federativo da Governança de Dados em São Tomé e Príncipe



17. A **Centralização Estratégica** do Modelo Operacional Federativo é levada a cabo por uma entidade central e multifuncional que estabelece padrões, diretrizes, normas de qualidade, segurança e conformidade que são obrigatórios para toda a administração pública.
18. As seguintes funções são executadas ao **nível central**:

- Definir e aprovar a política de governança de dados e as políticas específicas para as áreas de Gestão de Dados

- Estabelecer padrões mínimos para qualidade, segurança, interoperabilidade e uso ético de dados
- Estabelecer uma plataforma central para armazenar metadados e garantir rastreabilidade.
- Garantir o alinhamento com regulamentações externas (como leis de proteção de dados pessoais).
- Coordenar a integração e cooperação entre unidades.
- Monitorar e auditar a conformidade regulatória.

19. A **Autonomia Local (Descentralização)** do Modelo Operacional Federativo é composta pelos órgãos, agências, direções ou departamentos locais que possuem liberdade para gerir e implementar os dados conforme suas necessidades específicas, desde que sigam as diretrizes definidas centralmente, adaptando as práticas de governança às suas operações sem comprometer os objetivos organizacionais.

20. As seguintes funções são executadas ao **nível local**:

- Desenhar os modelos de dados que suportam operações de negócio específicas.
- Gerir seus próprios dados conforme suas necessidades específicas.
- Implementar políticas locais desde que sigam os princípios gerais definidos pelo nível central.
- Adotar ferramentas e processos que melhor atendam aos seus contextos, respeitando os padrões definidos.

5.2 Estrutura Organizacional

21. Esta política estabelece igualmente a estrutura organizacional definindo a hierarquia de funções e respetivas responsabilidades necessários para uma Governança de Dados bem-sucedida, alinhada ao Modelo Operacional Federativo escolhido. As funções e responsabilidades de cada parte da estrutura organizacional estão ilustradas na Figura 9.

5.2.1 Comité Executivo de Governança de Dados

22. O Comité Executivo de Governança de Dados (CEGD) regula e fornece orientação estratégica para o cuidado geral dos dados e supervisiona o desenvolvimento do programa de governança de dados ao nível estratégico.

23. As principais responsabilidades incluem:

- Alinhar estratégias, projetos e recursos de Governança de Dados com a estratégia corporativa.
- Estabelecer objetivos para o programa de governança de dados, identificar iniciativas que necessitem de governança de dados, supervisionar o progresso da implementação do programa e atribuir funções aos administradores e proprietários de dados.
- Aprovar padrões de dados, políticas, regras comerciais e aquisição de ferramentas de apoio.
- Solucionar questões e problemas que tenham sido escalonados pelo Núcleo de Governança de Dados.
- Informar sobre o programa e promover a importância da governança dos dados.
- Resolver problemas escalados a partir do Comité de Governança de Dados.
- Aprovar políticas e processos de dados propostos para toda a agência.

5.2.2 Núcleo de Governança de Dados

24. O Núcleo de Governança de Dados (NGD) é responsável pela gestão geral da Governança de Dados da organização. É composto pelas principais partes interessadas nos dados, que prestará assistência na resolução de questões relacionadas com os dados que surjam e na orientação da estratégia e da política para os dados. Consiste de Proprietários de Dados, apoiados pelos Curadores de Dados, com conhecimento organizacional sobre os dados e representantes do Departamento de Tecnologia da Informação, e é orientado por um Coordenador de Governança de Dados.

25. O NGD reúne-se regularmente para resolver questões críticas em matéria de dados e desenvolver e recomendar políticas, regras e procedimentos de dados.

26. As principais responsabilidades incluem:

- Facilitar o diálogo entre diferentes *stakeholders* para alinhar interesses e prioridades em torno da governança de dados.
- Criar consensos sobre padrões e regulamentos que promovam o uso responsável e seguro dos dados.
- Estabelecer, documentar e aplicar padrões, políticas e processos de dados em toda a agência.
- Identificar, priorizar e apoiar a resolução de problemas críticos de dados que afetam a qualidade e o uso dos dados.
- Encaminhar as políticas de dados para o Comitê Executivo de Governança de Dados para aprovação e questões controversas, altamente visíveis ou de alto risco.
- Responsabilizar os Escritórios de Governança de Dados e todas as Equipes de Dados pela participação no programa de Governança de Dados e adesão à Política de Governança de Dados.
- Através do Fórum de Governança de Dados, reunir especialistas, acadêmicos, gestores, representantes governamentais e membros da sociedade civil para debater desafios e oportunidades em governança de dados.

5.2.3 Escritório de Governança de Dados

27. O Escritório de Governança de Dados (EGD) é responsável pela Governança de Dados dentro de cada um dos órgãos e trabalha para ajudar a modelar e reforçar que a Governança de Dados é uma iniciativa transversal a toda a Administração Pública e que todos os funcionários devem estar cientes e cumprir as políticas de dados estabelecidas ao nível central.

28. As principais responsabilidades incluem:

- Definir a visão e prioridades para o uso de dados na sua organização.
- Produzir relatórios e recomendações para apoiar a formulação e revisão de políticas de governança de dados.
- Defender a criação de marcos legais e institucionais que sejam inclusivos, éticos e alinhados com boas práticas internacionais.
- Responsabilizar toda a sua equipa pela adesão às políticas e processos de dados estabelecidos através da Governança de Dados.
- Identificar tendências tecnológicas e propor como podem ser usadas para melhorar a governança de dados.
- Explorar novas maneiras de usar dados de forma ética e eficiente em benefício da sociedade.

5.2.4 Equipas de Dados

29. As Equipas de Dados são constituídas por todos os técnicos e funcionários que no seu dia-a-dia lidam com as diferentes áreas de Gestão de Dados, desde arquitetos de dados, a modeladores e especialistas de segurança, a utilizadores de dados.

30. As principais responsabilidades incluem:

- Comunicar eficazmente informações complexas derivadas de dados, fundamentais para a transparência e responsabilidade na administração pública.
- Gerir de forma eficiente os dados abertos, fomentando a partilha de informação e promovendo utilização de dados no desenvolvimento de políticas públicas inclusivas e informadas.
- Manter a qualidade, acessibilidade e integridade dos dados.
- Analisar e interpretar dados, utilizando ferramentas e metodologias analíticas para fundamentar a tomada de decisões e políticas baseadas em evidências.
- Desenvolver estratégias informadas por dados, melhorando a capacidade de decisão estratégica e operacional na administração pública.
- Promover a integração e interoperabilidade de dados, essenciais para a eficiência dos sistemas de informação interdepartamentais e interagências.
- Aplicar os princípios de ética, privacidade e de segurança associadas à utilização de dados na administração pública, promovendo uma cultura de respeito pela confidencialidade e pelo direito à privacidade.

5.2.5 Fórum de Governança de Dados

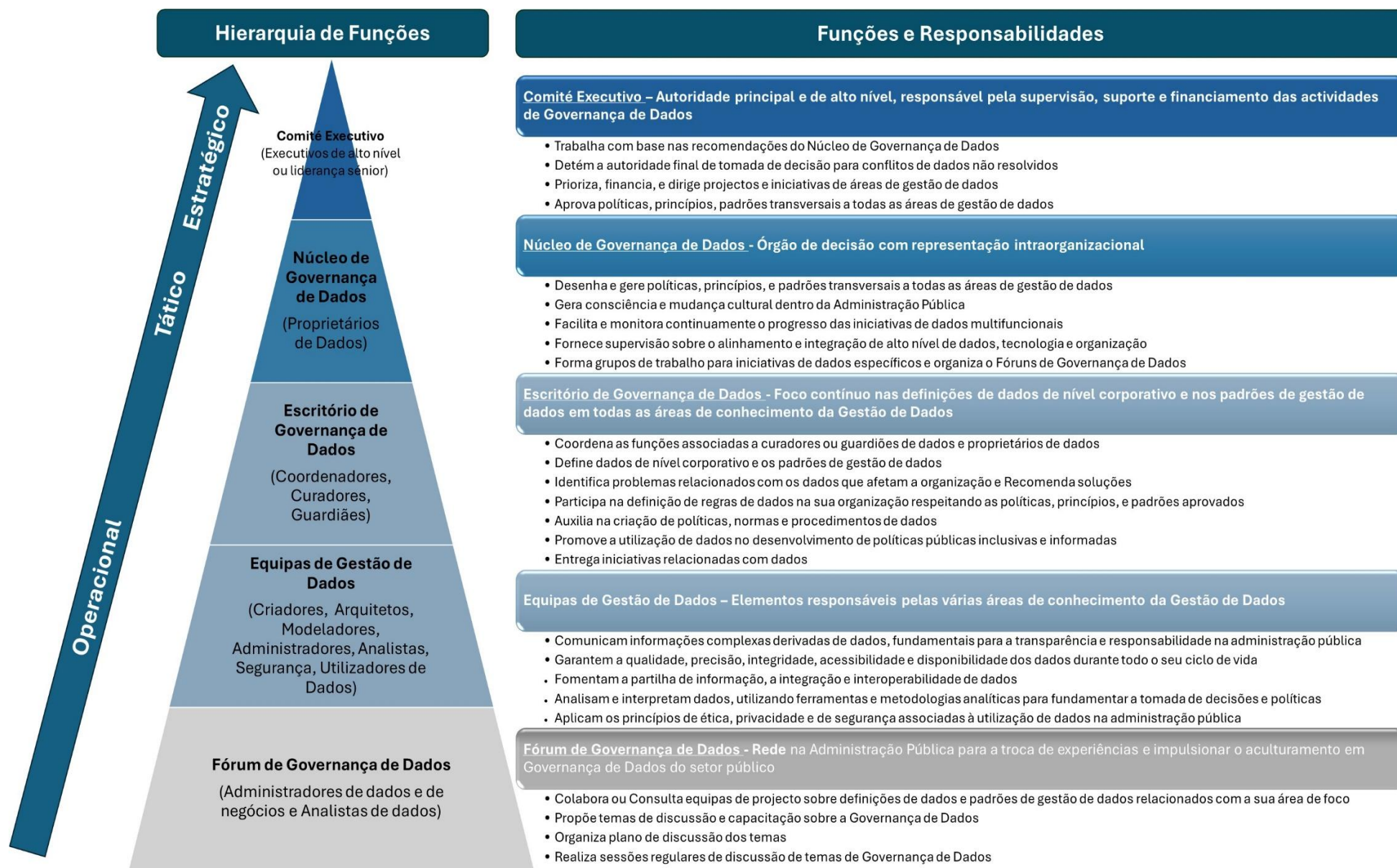
31. O Fórum de Governança de Dados é uma comunidade de interesse focadas em uma ou mais áreas temáticas ou projectos específicos. É um espaço para discussão, investigação e disseminação de ideias, em um ambiente colaborativo e interdisciplinar com foco em ampliar o conhecimento, alinhar interesses e propor soluções inovadoras sobre governança de dados.

32. As principais responsabilidades incluem:

- Abordar temas emergentes como inteligência artificial, ética no uso de dados, privacidade digital, e inclusão social.
- Compartilhar experiências bem-sucedidas de outros países, organizações ou setores sobre como implementar governança de dados.
- Organizar palestras, workshops e seminários para aumentar a consciência sobre a importância da governança de dados.
- Promover a alfabetização digital para que cidadãos e organizações compreendam como seus dados são usados e como podem protegê-los.

- Estimular a pesquisa sobre temas específicos como interoperabilidade, proteção de dados pessoais e governança ética da inteligência artificial.
- Incentivar estudos sobre o impacto da governança de dados na economia, na administração pública e na inclusão social.

Figura 9: Hierarquia de Funções e Respetivas Responsabilidades da Estrutura de Governança de Dados



5.3 Papeis e Responsabilidades dos Membros da Estrutura de Governança de Dados

33. Os responsáveis pela gestão de ativos de dados representam os interesses de todas as partes interessadas e devem adotar uma perspetiva organizacional para garantir a alta qualidade no uso dos dados. Os responsáveis pela gestão de dados podem ser diferenciados pelo seu lugar dentro da estrutura organizacional.

5.3.1 Proprietário de Dados (Data Owners)

34. O Proprietário de Dados é geralmente um administrador sénior da organização, como um ministro de tutela, diretor nacional ou chefe de departamento, responsável por criar e manter fontes confiáveis de dados para as principais operações da administração pública. Este papel é essencial para assegurar que os dados sejam geridos de forma estratégica, ética e conforme às normas legais e organizacionais.

35. Os Proprietários de Dados desempenham um papel indispensável na administração pública, promovendo decisões informadas, assegurando a conformidade regulatória e fortalecendo a confiança nos ativos de dados da organização. Os Proprietários de Dados possuem autoridade para gerir e proteger os ativos de dados institucionais. Eles são responsáveis por implementar protocolos locais eficazes que orientem o uso apropriado dos dados, garantindo a conformidade com requisitos legais e normativos e alinhando a gestão de dados ao ciclo de vida da gestão de dados.

36. Principais Responsabilidades:

- **Planeamento Estratégico e Políticas de Dados**
 - Formular estratégias e políticas para os domínios de dados sob sua responsabilidade.
 - Nomear curadores (stewards) de dados para domínios específicos, supervisionando suas atividades.
- **Compreensão e Valorização dos Dados**
 - Entender o valor, a finalidade e o uso dos ativos de dados.
 - Garantir que os dados atendam às necessidades organizacionais e regulamentares.
- **Conformidade e Classificação de Dados**
 - Garantir conformidade com políticas, normas e regulamentações legais e institucionais, incluindo a classificação de dados segundo padrões aplicáveis.
 - Implementar diretrizes operacionais, de intercâmbio e de segurança para o uso e compartilhamento de dados.

- **Gestão do Ciclo de Vida dos Dados**
 - Supervisionar o ciclo de vida completo dos dados, incluindo coleta, retenção, comunicação, acesso, permissões e descarte.
 - Garantir que os dados sejam utilizados de forma apropriada, alinhados às metas organizacionais e regulatórias.
- **Colaboração e Governança de Dados**
 - Facilitar a colaboração entre administradores e curadores de dados para promover a qualidade e integridade dos dados.
 - Participar ou nomear representantes para o Núcleo de Governança de Dados, priorizando questões críticas relacionadas a dados.
 - Trabalhar em conjunto com administradores de dados para resolver problemas e, quando necessário, informá-los ao sector de informática.
- **Promoção da Qualidade de Dados**
 - Liderar iniciativas que assegurem a integridade, confiabilidade e disponibilidade dos dados.
 - Monitorar e tratar questões de qualidade de dados, colaborando para implementar melhorias contínuas.
- **Autorização e Comunicação de Dados**
 - Garantir que a coleta e a comunicação de dados sejam devidamente autorizadas.
 - Tomar decisões estratégicas sobre acesso, permissões e compartilhamento de dados para promover o uso ético e eficiente.
- **Supervisão do Programa de Dados**
 - Assegurar a implementação e aplicação de políticas e diretrizes de Governança de Dados.
 - Orientar iniciativas de tomada de decisão baseadas em dados e promover a cultura de administração de dados.

5.3.2 Curadores de Dados (Data Stewards)

37. Os Curadores de Dados desempenham um papel fundamental na garantia de que os utilizadores possam aceder consistentemente a dados de alta qualidade e alinhados com as necessidades organizacionais e regulamentares. Eles atuam como a ponte entre as áreas de negócios e tecnologia (TI), promovendo a colaboração, a democratização e o uso responsável dos dados em toda a organização.

38. Os Curadores de Dados são indispensáveis para a gestão eficaz e ética de dados. Eles promovem uma cultura de integridade, asseguram a aplicação de políticas de Governança de Dados e facilitam a tomada de decisões baseadas em dados. Os Curadores de Dados

classificam e aprovam o acesso a dados sob delegação de um Proprietário de Dados. Eles possuem autoridade para tomar decisões sobre acesso, permissões, retenção e descarte de dados, sempre alinhados aos Padrões de Proteção de Dados. Seu papel é essencial para transformar os dados em ativos estratégicos, garantindo sua confiabilidade e alinhamento com os objetivos institucionais.

39. Principais Responsabilidades:

- **Criação de Ativos de Dados**
 - Supervisionar a criação de ativos de dados, garantindo que políticas e protocolos de segurança sejam seguidos.
 - Implementar práticas de documentação e registro para assegurar a rastreabilidade e o contexto dos dados.
- **Garantia de Qualidade dos Dados**
 - Padronizar definições, regras e descrições de dados para fornecer clareza e consistência organizacional.
 - Trabalhar com equipes de Governança de Dados para monitorar e melhorar continuamente a qualidade dos dados.
 - Garantir consistência, confiabilidade, precisão e pontualidade de acordo com os padrões estabelecidos.
- **Proteção de Dados e Segurança**
 - Estabelecer e implementar protocolos de segurança alinhados às metas e requisitos de conformidade da organização.
 - Identificar e mitigar ameaças potenciais em colaboração com equipes de TI.
 - Assegurar que políticas de segurança sejam aplicadas e decisões relacionadas a dados sejam devidamente documentadas para garantir integridade, transparência e confiança.
- **Definição e Gestão de Políticas de Acesso**
 - Proteger dados institucionais confidenciais, garantindo que sejam acessados apenas por pessoas autorizadas e dentro do escopo de suas funções.
 - Estabelecer políticas claras de acesso, assegurando que usuários autorizados tenham acesso apenas aos dados relevantes para suas funções.
 - Documentar, revisar e atualizar autorizações de acesso conforme necessário, garantindo transparência e rastreabilidade.
- **Facilitação de Colaboração e Otimização de Fluxos de Trabalho**
 - Auxiliar equipes técnicas e comerciais na descoberta e utilização confiável de dados.

- Atuar como um elo crítico na comunicação entre as áreas, promovendo a colaboração e o compartilhamento ético de dados.
- **Supervisão Tática da Governança de Dados**
 - Implementar políticas de Governança de Dados no nível operacional, garantindo que os padrões e diretrizes sejam seguidos em toda a organização.
 - Receber atribuições e prioridades do Núcleo de Governança de Dados (NGC) para orientar ações específicas.

5.3.3 Guardiões de Dados (*Data Guardians*)

40. Os Guardiões de Dados são responsáveis pela gestão técnica e operacional dos dados, assegurando que sejam armazenados, protegidos e disponibilizados de maneira eficiente e segura. Eles atuam como administradores dos sistemas que hospedam os dados, implementando políticas e procedimentos definidos por Curadores e Proprietários de Dados.

41. Os Guardiões de Dados garantem que as plataformas tecnológicas, ferramentas e processos atendam aos padrões estabelecidos de Governança de Dados, contribuindo para a integridade e segurança dos ativos de dados. Além disso, são responsáveis por garantir a conformidade com regulamentações em constante evolução, avaliando políticas de Governança de Dados, processos internos e sua implementação.

42. Principais Responsabilidades:

- **Gestão do Ativo de Dados**
 - Gerir o armazenamento, backup e recuperação dos dados.
 - Manter a infraestrutura técnica necessária para suportar a disponibilidade e o desempenho dos sistemas de dados.
- **Segurança de Dados**
 - Implementar controles de acesso, proteção contra ameaças cibernéticas e mecanismos de criptografia, conforme as políticas estabelecidas.
 - Monitorar e relatar violações de segurança, colaborando com a equipa de TI e com os Curadores de Dados para mitigar riscos.
 - Configurar políticas aprovadas que determinem quais usuários podem aceder ativos de dados específicos, garantindo o alinhamento com as funções organizacionais e o uso pretendido.
- **Conformidade com Políticas de Governança de Dados**
 - Aplicar as diretrizes e padrões definidos pelos Proprietários e Curadores de Dados.
 - Garantir que os sistemas estejam alinhados às regulamentações de proteção de dados e requisitos de auditoria.

- **Garantia da Qualidade Técnica**
 - Monitorar a integridade dos dados nos sistemas, identificando e corrigindo inconsistências ou erros.
 - Implementar rotinas de validação técnica para assegurar a consistência dos dados armazenados.
- **Suporte Técnico e Operacional**
 - Atuar como ponto de contato técnico para questões relacionadas ao armazenamento e acesso a dados.
 - Oferecer suporte às equipas de negócio e de TI na utilização das plataformas de dados.
 - Ajudar usuários a descobrir, entender e confiar nos dados necessários para suas operações.
- **Documentação e Auditoria**
 - Manter registos detalhados sobre configurações técnicas, mudanças no ambiente de dados e acessos realizados.
 - Facilitar auditorias internas e externas relacionadas ao uso e segurança dos dados.

5.3.4 Utilizadores de Dados (*Data Users*)

43. Os Utilizadores de Dados representam o destino final de qualquer sistema de Governança de Dados. Todas as demais funções da equipa de Governança — Administradores, Curadores e Guardiões — existem para fornecer suporte, segurança e acessibilidade aos Utilizadores.

44. Os Utilizadores de Dados incluem profissionais de diversas áreas dentro da organização, como marketing, pesquisa, gestão, executivos e equipas operacionais. A principal função dos Utilizadores de Dados é aplicar os ativos de dados em casos de uso específicos, promovendo uma cultura de tomada de decisões baseada em dados. Além disso, têm a responsabilidade de garantir a segurança, integridade e uso ético dos dados acedidos.

45. Principais Responsabilidades:

- **Aderência a Políticas e Normas de Governança de Dados**
 - Tratar os dados de acordo com os procedimentos de classificação da informação e as políticas aplicáveis.
 - Observar restrições éticas e legais associadas aos dados, incluindo leis de proteção de dados pessoais.
- **Garantia de Qualidade e Confiabilidade**

- Garantir que os dados utilizados, bem como os resultados de análises realizadas, sejam precisos, isentos de vieses e interpretados corretamente.
- Chamar a atenção da equipa de Governança de Dados para questões de qualidade ou credibilidade em conjuntos de dados.
- **Segurança e Privacidade**
 - Respeitar os direitos de privacidade individual e as garantias de confidencialidade, conforme leis e políticas aplicáveis.
 - Garantir o uso de controles de acesso adequados, relatando qualquer violação, especialmente no caso de compartilhamento inadequado de dados pessoais.
- **Uso Intencional e Controlado de Dados**
 - Aceder, usar e divulgar dados de maneira responsável, que garanta confidencialidade, precisão, e relevância para os stakeholders.
 - Usar os dados mais precisos e atualizados disponíveis para análises e relatórios.
- **Educação e Capacitação**
 - Participar de treinamentos e sessões educacionais relacionadas à Governança de Dados, segurança e boas práticas de uso.
 - Utilizar ferramentas como dicionários de dados, catálogos e bases de conhecimento para localizar e extrair valor de conjuntos de dados.
- **Colaboração com Outras Funções de Governança de Dados**
 - Interagir com Administradores, Curadores e Guardiões de Dados para entender, aceder e utilizar os dados de forma eficaz.
 - Contribuir para o aprimoramento dos processos de Governança de Dados, sugerindo melhorias ou apontando falhas.
- **Responsabilidade Ética e Social**
 - Garantir que os dados sejam utilizados de forma ética e em alinhamento com os objetivos organizacionais e sociais.
 - Evitar práticas que comprometam a segurança, a reputação ou a privacidade dos indivíduos.

5.3.5 Analistas de Dados (*Data Analysts*)

46. Os Analistas de Dados desempenham um papel crucial ao transformar dados em discernimentos que suportam a tomada de decisões organizacionais. São responsáveis por coletar, organizar e interpretar dados de maneira sistemática, traduzindo-os em relatórios, visualizações e recomendações estratégicas. É nesse processo que o valor real dos dados se revela, contribuindo diretamente para o sucesso empresarial.

47. O Analista de Dados conecta o mundo técnico e o operacional, sendo o responsável por transformar grandes volumes de dados em soluções tangíveis. Por meio de suas análises, organizações podem otimizar processos, explorar novos mercados e criar estratégias baseadas em evidências sólidas. Além disso, ao assegurar a qualidade e o uso ético dos dados, esse profissional contribui diretamente para a sustentabilidade e inovação empresarial.

48. Principais Responsabilidades:

- **Coleta e Limpeza de Dados**
 - Recolher dados de diversas fontes, internas e externas.
 - Realizar a limpeza e organização dos dados para garantir sua precisão e usabilidade em análises futuras.
- **Análise Exploratória**
 - Conduzir análises iniciais para entender o contexto, identificar padrões, tendências e anomalias.
 - Criar visualizações e resumos estatísticos que auxiliem na interpretação dos dados.
- **Modelagem e Análise**
 - Aplicar técnicas estatísticas e modelos matemáticos para extrair insights profundos.
 - Desenvolver e aplicar algoritmos avançados para modelos preditivos, sistemas de recomendação e detecção de padrões.
 - Utilizar ferramentas para automatizar e aprofundar análises complexas.
- **Visualização de Dados**
 - Criar relatórios e *painéis de dados* interativos que tornem os resultados acessíveis e compreensíveis para públicos não técnicos.
 - Utilizar ferramentas para gerar visualizações impactantes.
- **Apoiar a Tomada de Decisões Baseada em Dados**
 - Transformar análises em insights práticos que informem decisões operacionais e estratégicas.
 - Apoiar gestores em decisões orientadas por dados para otimizar resultados.

5.3.6 Encarregados de Proteção de Dados (*Data Protection Officer*)

49. O Encarregado de Proteção de Dados (EPD) é um profissional-chave para assegurar a conformidade de uma organização com a legislação de proteção de dados. O EPD desempenha um papel essencial na supervisão, implementação e monitoria de práticas de

proteção de dados, garantindo que os dados pessoais sejam usados de forma segura e em conformidade com as normas aplicáveis.

50. O EPD é o guardião da conformidade e da ética no tratamento de dados pessoais. Seu trabalho é fundamental para proteger a privacidade dos indivíduos, mitigar riscos legais e reputacionais e fomentar a confiança de clientes, parceiros e colaboradores.

51. Principais Responsabilidades

- **Conformidade Legal**

- Garantir que a organização esteja em conformidade com as leis de proteção de dados relevantes e outras normas locais.
- Monitorar e alertar sobre mudanças legais que possam impactar o tratamento de dados.

- **Educação e Sensibilização**

- Criar diretrizes e ministrar treinamentos para colaboradores, promovendo uma cultura de proteção de dados.
- Divulgar materiais de comunicação sobre boas práticas e obrigações legais.
- Fornecer orientação para gestores e equipes sobre práticas de proteção de dados.
- Sensibilizar e alertar os responsáveis pelo tratamento sobre riscos e não conformidades que possam impactar a organização.

- **Garantia de Conformidade Operacional**

- Supervisionar e realizar avaliações de impacto à privacidade (DPIA) para identificar e mitigar riscos associados ao tratamento de dados pessoais.
- Monitorar práticas organizacionais para garantir o cumprimento das políticas de proteção de dados.
- Monitorar e documentar os tratamentos de dados pessoais, assegurando que sejam realizados de acordo com as normas.
- Propor estudos de impacto e responder às solicitações de titulares de dados sobre seus direitos.
- Analisar incidentes de dados, conduzindo investigações independentes para determinar causas e implementar medidas corretivas.
- Validar e verificar procedimentos organizacionais relacionados à proteção de dados.

- **Auditorias e Controles**

- Realizar auditorias regulares para avaliar a segurança e a conformidade dos sistemas e processos de dados.

- Identificar e corrigir não conformidades relacionadas ao tratamento de dados pessoais.
- Garantir a existência e a atualização da documentação relacionada aos tratamentos de dados, incluindo registros e relatórios de auditorias.
- **Gestão de Dados e Políticas**
 - Elaborar e manter um inventário dos dados tratados pela organização, bem como os sistemas utilizados para melhor geri-los.
 - Definir políticas de tratamento de dados e criar mapas de riscos para orientar a tomada de decisões.

5.4 Avaliação e Monitoria Contínuas

52. No início deste processo de elaboração da estratégia e da política de governança de dados, foi realizada uma avaliação quer do grau de prontidão para esta jornada, quer do nível de maturidade da governança e gestão de dados.
53. A avaliação ajudou a identificar o que estava funcionando bem, ou menos bem, e as áreas onde existem lacunas. Através desses resultados, foi possível estabelecer prioridades e definir os objectivos, e desenvolver um roteiro de implementação de iniciativas prioritárias, entre elas a Governança de Dados.
54. A revisão e monitoria contínuas do roteiro de implementação, adotando uma cultura de melhoria contínua, é uma forma de garantir que a Estratégia de Dados se mantém relevante e flexível face às mudanças nos ambientes empresariais e aos avanços tecnológicos. Além disso, isto oferece a oportunidade de modificar o plano à luz das lições aprendidas, da monitoria dos principais indicadores, e do feedback das partes interessadas. Para além de avaliar o desenvolvimento do roteiro estabelecido, utilizando os indicadores e as métricas propostas, os processos de avaliação, quando realizados de forma participativa, permitem criar uma linguagem comum para descrever o progresso nas áreas de Gestão e Governança de Dados e têm um impacto positivo na cultura de dados, pois ajudam a:
- a) Educar as partes interessadas sobre conceitos, princípios e práticas de gestão de dados;
 - b) Clarificar os papéis e responsabilidades das partes interessadas em relação aos dados organizacionais;
 - c) Destacar a necessidade de gerir os dados como um ativo estratégico;
 - d) Ampliar o reconhecimento das actividades de gestão de dados em toda a organização;
 - e) Contribuir para melhorar a colaboração necessária para uma governação eficaz dos dados

5.4.1 Indicadores e Métricas

Para a Governança de Dados

55. As métricas de governança de dados concentram-se na avaliação das políticas, processos e estruturas que garantem que os dados sejam geridos de forma responsável e em conformidade com os padrões.
56. A Tabela 2 ilustra vários indicadores e métricas para a Governança de Dados. Caberá à instituição ou órgão responsável pela Governança de Dados decidir que indicadores são prioritários e estabelecer avaliações regulares para determinar o seu grau de realização.

DESENHO DA ESTRATÉGIA E DA POLÍTICA DE GOVERNANÇA DE DADOS

Tabela 2: Exemplo de Indicadores e Métricas para a Governança de Dados

Indicador	Métrica
Adoção e conformidade de políticas	• Percentagem de órgãos que aderem à política de dados estabelecidas. • Número de violações ou exceções às políticas de dados relatadas e resolvidas.
Clareza na propriedade e administração de dados	• Percentagem de domínios de dados com proprietários ou administradores de dados claramente atribuídos. • Percentagem de domínios de dados com elementos de dados críticos definidos. • Número de questões levantadas e resolvidas pelos administradores e curadores de dados.
Envolvimento das partes interessadas	• Taxa de participação em reuniões do Núcleo de Governança de Dados. • Taxa de participação em encontros do Fórum de Governança de Dados. • Número de iniciativas apoiadas por equipas multifuncionais de governança de dados.
Normas e processos aprovados e implementados	• Percentagem de processos padronizados em toda a organização. • Número de normas e políticas aprovadas. • Número de normas e políticas implementadas.
Gestão eficaz dos riscos	• Frequência dos riscos relacionados com os dados identificados e mitigados. • Redução nos resultados da auditoria de conformidade relacionados à governança de dados.
Eficiência na tomada de decisões	• Tempo médio para resolver litígios ou decisões relacionados com dados. • Número de problemas escalados resolvidos com êxito através de estruturas de governação.
Dados manuseados de forma ética	• Número de funcionários treinados • Incidentes de Conformidade/ Não Conformidade • Envolvimento Executivo Corporativo

Para a Gestão de Dados

57. As métricas de gestão de dados medem a eficácia de atividades de Gestão de Dados como qualidade, integração e arquitetura de dados. Cabe a cada um dos órgãos da Administração Pública definir quais as áreas de gestão de dados prioritárias e quais as métricas que fazem sentido avaliar. A Tabela 3 ilustra vários indicadores e métricas para as várias áreas de conhecimento.

Tabela 3: Exemplo de Indicadores e Métricas para a Gestão de Dados

Indicador	Métrica
Qualidade de Dados	• Precisão: Percentagem de registos de dados sem erros. • Exaustividade: Percentagem de campos de dados obrigatórios preenchidos. • Pontualidade: Tempo médio entre a criação dos dados e a disponibilidade para utilização. • Consistência: Percentagem de dados consistentes entre sistemas.
Acessibilidade dos dados armazenados	• Percentagem de órgãos com políticas de acesso aos dados estabelecidas. • Percentagem de dados facilmente acessíveis a utilizadores autorizados. • Tempo médio necessário para atender às solicitações de acesso aos dados.
Documentação e gestão de metadados	• Percentagem de conjuntos de dados com documentação de metadados abrangente. • Número de atualizações de metadados concluídas dentro de um determinado período.
Integração e partilha de dados	• Percentagem de conjuntos de dados integrados em diferentes sistemas. • Número de falhas de integração durante um período especificado
Dados seguros e protegidos	• Número de violações de dados ou incidentes de acesso não autorizado. • Percentagem de dados sensíveis encriptados ou protegidos. • Percentagem de implementação de políticas de segurança • Taxa de proliferação de dados confidenciais
Dados mestre e de referência documentados e geridos	• Percentagem de entidades de dados mestre sem duplicatas. • Número de discrepâncias de dados de referência resolvidas.
Validação do desenho e modelação de dados	• Número de sistemas com modelos de dados documentados. • Número de modelo de dados de sistemas considerados críticos validados.
Uso e análise de dados	• Número de unidades de negócios que usam ativamente ativos de dados geridos. • Frequência de insights ou relatórios gerados a partir de dados geridos.
Sistemas arquitetados de acordo com boas práticas	• Taxas de conformidade com padrões de arquitetura • Tendências na implementação de padrões de arquitetura de dados
Ciclo de vida dos dados gerido	• Percentagem de dados obsoletos ou redundantes arquivados ou eliminados. • Taxa de conformidade com as políticas de retenção e eliminação de dados.

5.4.2 Avaliação Regular dos Elementos Facilitadores

58. A gestão de mudança avalia a capacidade da organização para mudar os comportamentos necessários para a adaptação ao novo contexto de Governança de Dados, identificando potenciais pontos de resistência e oportunidades de melhoria. Relativamente à capacidade e preparação do Governo para empreender a jornada de implementação da Estratégia de Dados, é importante considerar três elementos facilitadores, nomeadamente: (i) o engajamento e apoio da liderança de topo para promover a mudança requerida; (ii) o quadro legal e regulamentar conducente à governança e transformação digital; e (iii) a estrutura de governança e a colaboração das várias agências e instituições da Administração Pública.
59. Envolvimento e Apoio da Gestão de Topo: É essencial para garantir a visibilidade da liderança política que deverá promover um modelo claro e abrangente tratamento de dados entre as principais agências proprietárias ou utilizadoras de dados críticos e garantir a implementação de actividades ou planos relevantes.
60. Quadro Legal e Regulamentar: É crítico definir, implementar e auditar a eficácia de um quadro legal conducente à transformação digital. Tal quadro deve auxiliar o papel de uma estrutura de governança de dados através de instrumentos legais e regulatórios conducentes à proteção de dados e proteção de infraestruturas críticas de dados; partilha de dados e infraestruturas críticas; qualidade de dados; abertura de dados; segurança, arquivo e preservação digital de dados; e direitos de acesso à informação.
61. Estruturas Institucionais, Papeis e Responsabilidades, e Procedimentos de Gestão: A Estratégia de Dados só poderá ser devidamente implementada se existirem os mecanismos interinstitucionais que coordenem as questões de dados. É importante institucionalizar esta estrutura de governança de dados e definir cargos oficiais permanentes dedicados à gestão de dados. É vital criação de competências em dados na administração pública, entre os líderes governamentais e funcionários públicos. Adicionalmente, é essencial definir processos para medir o desempenho relativo à qualidade da prestação de serviços de dados, o que requer procedimentos claros de partilha de dados e clareza sobre quais são os dados críticos necessários para uma boa governação do país.
62. Caberá à estrutura de governança de dados, em coordenação com todas as instituições públicas envolvidas neste processo, proceder à avaliação do grau de preparação e estágio de maturidade da administração pública, relativamente a estes elementos facilitadores. Para tal são utilizados quatro níveis de prontidão (Tabela 4), consoante as evidências que forem encontradas e validadas:

Tabela 4: Classificação do grau de prontidão para a Governança de Dados

	Existe evidência clara
	Existe alguma evidência, mas não é tão clara
	Não existe evidência alguma
	Não existe informação suficiente para avaliar

5.4.3 Avaliação da Evolução da Maturidade da Gestão e Governança de Dados

63. A Avaliação da Maturidade da Gestão de Dados é realizada através do modelo DMMA (do Inglês Data Management Maturity Assessment) proposto pela DAMA Internacional. A maturidade é medida recorrendo à Roda de Dama (Figura 3), avaliando-se estágio atual (e o desejado) das 11 áreas de conhecimento com recurso a uma tabela de níveis (Figura 10) que descrevem as características de maturidade no que diz respeito à Gestão de Dados.

Figura 10: Os 5 níveis de maturidade propostos pela DAMA-DMBOK2



Fonte: Adaptado de DAMABOK, versão de 2017