# Soberania Tecnológica e Cibernética na Informatização da Administração Pública

Visão 2016-2017

PROF. DOUTOR ENG. PEDRO S. TETA

## Desafios da soberania Tecnologica  versus Governação Electronica

Existe uma crescente preocupação com a dependência do Estado angolano nas empresas que prestam serviços de desenvolvimento e gestão de bases de dados sensíveis e de sistemas críticos e sobre a segurança da informação do Estado e dos cidadãos e empresas.

# Índice

**Sumário Executivo**

A. Desafios a Endereçar

B. Tendências e Casos Internacionais de Referência

C. Opções de Desenvolvimento

D. Formas Complementares de Garantir a Soberania Tecnológica

E. Recomendações

Anexo 1: Casos Internacionais de Referência

# Desafios

Existe uma crescente preocupação com a dependência do Estado angolano nas empresas que prestam serviços de desenvolvimento e gestão de bases de dados sensíveis e de sistemas críticos e sobre a segurança da informação do Estado e dos cidadãos e empresas.

A Governação Electrónica envolve dois aspectos novos para o Estado.

1. Em primeiro lugar, envolve sistemas e redes tecnológicas cada vez mais integradas - integrated network administration - para suportar processos mais transversais e colaborativos, implicando interligação de redes e dados.

2. Em segundo lugar, envolve uma elevada complexidade tecnológica cujo desenvolvimento advém essencialmente do sector privado. A crescente utilização da Internet e do alojamento de bases de dados em modelo cloud aumenta a preocupação com o acesso por terceiros a bases de dados confidenciais e com a dependência do Estado em empresas privadas para gestão de informação do Estado.

Os desafios de segurança e de controlo da dependência do Estado são maiores quando as Administrações Públicas estão pouco desenvolvidas tecnologicamente em termos das suas instituições, processos e recursos humanos e decisionais.

**¿Como deve  o Executivo abordar este desafio?**

# Soluções

## Soluções

A solução preconizada é a conjugação de dois tipos de ações. Por um lado, a criação de uma entidade, pública ou público-privada, especializada na gestão de sistemas tecnológicos críticos. Por outro lado, a adopção de um conjunto de medidas que reduzem a dependência do Estado e aumentam os níveis de segurança dos sistemas críticos.

### Entidade Dedicada

Definir com detalhe o perímetro dos sistemas tecnológicos críticos do Estado e os desafios a resolver

Criar entidade dedicada, pública ou pública-privada.

Definir com detalhe e rigor:

- Objectivos a atingir em termos de desempenho e segurança
- Atribuições, competências e orçamento
- Níveis de serviço a garantir, remunerações e penalizações
- Desenho organizacional e operacional e inter-relação com outras entidades do Estado
- Plano de transferência para esta entidade
- Plano de gestão de risco
- Suporte legal e Contratualização entre esta entidade e o Estado

### Medidas Transversais

Desenhar e montar Business Continuity Plans para os sistemas críticos, por forma a reduzir a dependência de terceiros

Criar o Enquadramento Regulatório e Penal que permita proteger melhor os dados do Estado e dos Cidadãos – com penalizações claras a pessoas e empresas por incumprimento da lei

Separar a “Administração dos Sistemas” e o “Acesso aos Dados” utilizando mecanismos de encriptação

Realizar auditorias externas regulares aos Prestadores de Serviços de TI para o Estado

Conceber e Aprovar o Quadro Comum de Interoperabilidade da Administração Pública Angolana

Definir a Política de Segurança de Informação da Administração Pública Angolana

Implementar um Programa Alargado de Capacitação dos Quadros Angolanos de TI

Definir Service Level Agreements

Reforçar os Contratos (motivos e penalizações em caso de incumprimento)

Gerir os incumprimentos contratuais.

# Os Próximos Passos

**Os Próximos Passos**

Os próximos passos devem responder de forma flexível às decisões e nova informação que for surgindo.

Neste fase, recomendam-se as seguintes acções por forma a garantir implementação em 2015-2016.

- Validar preliminarmente os cenários apresentados
- Aprofundar os cenários apresentados e o seu impacto – aprofundar o Memorando
- Definir os Sistemas Chave do Estado e recolher informação de base sobre a sua gestão e desenvolvimento
- Avaliar cada um dos cenários em termos legais, operacionais e financeiros
- Definir Objetivos Concretos, um Plano de Acção e um Orçamento para o desenvolvimento das Medidas Chave para Garantir a Soberania Tecnológica
- Obter aprovação política final
- Identificar as entidades envolvidas e iniciar um processo negocial
- Implementar a solução aprovada politicamente e negociada com os principais parceiros

# Índice


## Sumário Executivo

**A. Desafios a Endereçar**

B. Tendências e Casos Internacionais de Referência

C. Opções de Desenvolvimento

D. Formas Complementares de Garantir a Soberania Tecnológica

E. Recomendações

Anexo 1: Casos Internacionais de Referência

# A. Desafios a Endereçar

A Governação Electrónica é um processo de modernização da governação através da utilização das tecnologias de informação e comunicação e que tem como figura central os cidadãos e as empresas. É um processo inadiável e fundamental para a modernização das funções do Estado, para a competitividade da economia, para o desenvolvimento social e para o bem estar dos cidadãos.

A Governação Electrónica envolve dois aspectos novos para o Estado. Em primeiro lugar, envolve sistemas e redes tecnológicas cada vez mais integradas - integrated network administration - para suportar processos mais transversais e colaborativos, implicando interligação de redes e dados. Em segundo lugar, envolve uma elevada complexidade tecnológica cujo desenvolvimento advém essencialmente do sector privado.

Estes dois factos colocam desafios de segurança e de controlo da dependência do Estado, especialmente quando as Administrações Públicas estão pouco desenvolvidas tecnologicamente.

Visão Definida para a Governação Electrónica em Angola

Uma governação focada em tornar os serviços públicos mais orientados, relevantes e acessíveis ao cidadão comum e às empresas, em todo o território nacional, com particular atenção aos mais desfavorecidos e suportada pela modernização de processos, pela qualificação dos funcionários públicos e por sistemas interoperáveis e seguros.

(in Plano Estratégico para a Governação Electrónica 2013-2017)

A Governação Electrónica permite maior acesso e qualidade da informação pública, promove a melhoria da prestação e da acessibilidade aos serviços públicos, aumenta as oportunidades de participação cívica e democrática e contribui para tornar os agentes governativos e a governação em geral mais eficaz e eficiente, menos onerosa e mais responsável.

# A. Desafios a Endereçar

O desenvolvimento da Governação Electrónica e da solução de criação de uma empresa pública dedicada coloca a Angola 6 grandes desafios para garantir a Soberania Tecnológica do país.

**6 Desafios Chave para a Soberania Tecnológica**

| | |
|---|---|
| **Segurança dos Dados** | Garantia da segurança e inviolabilidade dos dados do Estado e da privacidade da informação pessoal dos cidadãos e empresas registada nos sistemas críticos do governo. |
| **Interopera-bilidade** | Garantia da interoperabilidade técnica e semântica das aplicações da Administração Pública Angolana e do Estado, como forma de evitar duplicações, reduzir custos, potenciar serviços integrados e aumentar o desempenho. |
| **Poder de Decisão** | Garantia do livre poder de decisão do Estado Angolano na promoção e defesa dos seus interesses, e da respetiva capacidade de implementação, dentro de custos e riscos aprovados e controlados pelo Estado. |
| **Níveis de Desempenho** | Reforço continuado do nível de desempenho das aplicações chave do Governo e controlo dos seus riscos operacionais, evitando quebras de consequências graves. |
| **Angolanização** | Desenvolvimento das competências tecnológicas dos cidadãos angolanos e maximização da presença de empresas angolanas na prestação de serviços de TI. |
| **Sector TIC Competitivo** | Desenvolvimento de um sector de tecnologias de informação e comunicações dinâmico, inovador e competitivo, essencial ao desenvolvimento económico do país. |

# A. Desafios a Endereçar

O perímetro da Soberania Tecnológica do Estado Angolano deve abranger os sistemas críticos ao funcionamento e segurança do Estado e ao bem-estar dos cidadãos.

**Perímetro da Soberania Tecnológica do Estado**

**Informação Crítica**

1. Informação de Segurança Nacional
2. Informação sobre as Finanças Públicas
3. Informação Confidencial dos Cidadãos e Empresas

Proposta de Sistemas a Englobar

| | | |
|---|---|---|
| Registo Civil (Bilhete de Identidade, Passaporte…) | Gestão Financeira do Estado (Orçamento, Impostos, etc.) | Segurança Social |
| Registo de Propriedades | Tribunais e Polícia (Processos Judiciais, Registo Criminal…) | Educação (Registo do Percurso Escolar dos Alunos) |
| Registo Eleitoral | Controlo de Migrações | Saúde (Registo Saúde dos Pacientes) |

# Índice

**Sumário Executivo**

A. Desafios a Endereçar

**B. Tendências e Casos Internacionais de Referência**

C. Opções de Desenvolvimento

D. Formas Complementares de Garantir a Soberania Tecnológica

E. Recomendações

Anexo 1: Casos Internacionais de Referência

# B. Tendências e Casos Internacionais de Referência

A protecção dos dados dos Estados e dos Cidadãos é um assunto que está na agenda de muitos governos a nível mundial, que têm apostado no reforço da legislação e da regulação, especialmente em resultado da utilização da internet e da "cloud", com sedeação em países diferentes do país originário dos dados.

## Conclusões da Análise de Casos e Tendências Internacionais (1/2)

- O ambiente regulatório tem evoluído ao longo dos últimos anos e a nível mundial os países têm procurado cada vez mais dar resposta aos desafios que se levantam, nomeadamente através de Leis de Protecção de Dados. Neste ponto destaca-se a directriz europeia para a protecção de dados que tem servido de referência para inúmeros países desenvolverem a sua Lei de Protecção de Dados;

- A segurança dos dados e da confidencialidade da informação tem sido garantida maioritariamente através de regulação, acordos de confidencialidade, mecanismos de segurança e controlo das actividades desenvolvidos pelo sector privado;

- O desenvolvimento dos sistemas de Governação Electrónica é maioritariamente realizado através de prestação de serviços por privados, contudo não existe um padrão comum a todos os países. As entidades públicas são normalmente responsáveis pela supervisão e acompanhamento dos desenvolvimentos;

- A Administração dos Sistemas Chave é normalmente garantida por entidades públicas o que salvaguarda a segurança e privacidade dos dados;

- Em todos os casos analisados existe uma entidade responsável por garantir uma visão comum e transversal para o desenvolvimento dos sistemas Chave de Governação Electrónica do país;

# B. Tendências e Casos Internacionais de Referência

A garantia de uma visão transversal para o Sistemas Chave de Governação Electrónica é essencial ao bom desenvolvimento da Sociedade da Informação e à correcta priorização do investimento.

## Conclusões da Análise de Casos e Tendências Internacionais (2/2)

- Em países como o Brasil ou Portugal existem entidades responsáveis pela avaliação e aprovação dos investimentos em SI/TI que garantem a arquitectura comum dos sistemas de Governação Electrónica (SLPI no Brasil e AMA em Portugal) e entidades responsáveis pelo acompanhamento do desenvolvimento e pela administração dos sistemas (Serpro no Brasil e eSPap em Portugal);

- No continente africano existem casos de empresas públicas de desenvolvimento de Sistemas de Informação (SIL nas Maurícias e NOSi em Cabo Verde) que se tornaram referências prestando serviços aos sectores público e privado, nacional e internacional. De referir contudo que estas empresas iniciaram a sua actividade nos anos 80 e 90 e beneficiam de condições estruturais extremamente favoráveis (mão-de-obra qualificada, dimensão da economia, etc);

# Índice

**Sumário Executivo**

A. Desafios a Endereçar

B. Tendências e Casos Internacionais de Referência

**C. Opções de Desenvolvimento**

D. Formas Complementares de Garantir a Soberania Tecnológica

E. Recomendações

Anexo 1: Casos Internacionais de Referência

# Opções de Desenvolvimento

**Cenário 1: Empresa Pública**

**Criação de uma empresa de capitais públicos para gerir o desenvolvimento de Novos Sistemas e administrar os Sistemas Chave de Governação Electrónica existentes.**

# Avaliação das Opções

## Cenário 1: Empresa Pública | Vantagens e Desvantagens

### Vantagens

- Reforço do papel e da capacidade do Estado na gestão dos sistemas e da informação crítica
- Criação de know-how técnico no Estado e capacitação dos quadros angolanos criando maior autonomia futura
- Reforço da comunicação e criação de uma visão comum para a interligação dos sistemas chave de governação que promove a interoperabilidade
- Maior garantia de independência tecnológica
- Garantia da continuidade do negócio das empresas privadas na componente de desenvolvimento de software
- Promoção da inovação pelo Estado

### Desvantagens

- Escassez de recursos técnicos capacitados, com experiência no sector privado e domínio das principais tecnologias pode limitar o calendário de implementação
- Limitada cultura de gestão e orientação a resultados por parte das entidades do Estado pode limitar a eficiência e eficácia deste modelo
- Dependência direita do Estado e resposta direita a objectivos políticos poderão ter uma lógica de curto prazo e prejudicar o desempenho desta entidade
- A clarificação do papel desta entidade perante as outras entidades da Administração Pública é fundamental para evitar conflitos e disfuncionalidades

# Avaliação das Opções

## Cenário 1: Empresa Pública | Riscos e Factores Críticos de Sucesso

**Riscos**

- Incapacidade de atrair e treinar os recursos com o perfil desejado em tempo útil, pode enfraquecer e inviabilizar esta entidade
- Gestão da nova empresa poderá passar a reger-se por princípios políticos e administrativos e por princípios financeiros e de eficiência operacional, criando uma entidade menos capaz de modernizar a máquina do Estado
- Se a nova entidade abarcar demasiados sistemas do Estado, pode matar o dinamismo do sector privado, pelo que é necessário delimitar bem as suas competências e atribuições.
- Diferença de know-how técnico entre os colaboradores da nova empresa e os colaboradores das empresas externas de prestação de serviços pode manter a dependência do Estado, mas agora de forma centralizada
- Falta ou atrasos nos pagamento dos serviços prestados às demais entidades públicas podem limitar a capacidade desta nova entidade

**Factores Críticos de Sucesso**

- Equipa de Gestão Profissional e Competente composta por quadros de elevado perfil e com provas dadas
- Definição de objectivos concretos para a nova empresa e estabelecimento de *Service Level Agreements* exigentes e tangíveis, com calendário
- Obrigatoriedade de autossuficiência da nova empresa e estabelecimento de preços de mercado para os serviços prestados a serem pagos pelos demais organismos da administração pública (preços reais ou de transferência)
- Gestão do talento, com vista à retenção e formação de quadros especializados
- Envolvimento das empresas privadas atualmente com o desenvolvimento e gestão dos sistemas críticos do Estado por forma a não gerar roturas
- Estabelecimento de parcerias com os grandes players internacionais para garantir a absorção de conhecimento e inovação contínua

# Anexo 2: Avaliação das Opções

O Ultimo cenário em análise passa pelo reforço da situação actual, reforçando as competências das instituições existentes no âmbito da regulação, incluindo a aplicação das medidas transversais .

**Cenário 3: Reforço da Situação Actual**

**Passos para o Reforço da Situação Actual:**

1. Reforço das atribuições e competências das entidades públicas que actuam no sector das TI, nomeadamente o CNTI, para que possam efectivamente zelar pela criação de um visão comum para os Serviços Chave de Governação electrónica do Estado Angolano, bem como pelo cumprimento das normas de privacidade e segurança de informação e pelo cumprimentos dos contratos estabelecidos com prestadores de serviços privados;

2. Recrutamento gradual de especialistas com experiência em arquitectura, gestão e desenvolvimento de sistemas de informação e capacitação dos técnicos existentes;

3. Passagem de uma mensagem política clara que reforce o papel das instituições existentes e lhes permita posicionarem-se como entidades transversais para os assuntos relacionados com os Sistemas Chave de Governação Electrónica;

4. Aplicação das medias transversais..

# Índice

**Sumário Executivo**

A. Desafios a Endereçar

B. Tendências e Casos Internacionais de Referência

C. Opções de Desenvolvimento

**D. Formas Complementares de Garantir a Soberania Tecnológica**

E. Recomendações

Anexo 1: Casos Internacionais de Referência

# D. Formas Complementares de Garantir a Soberania Tecnológica

A garantia da soberania tecnológica passam não só pelo modelo de governação das TI do Estado, mas sobretudo pelo desenvolvimento de legislação, políticas e medidas concretas de regulação.

## Medidas Chave para Garantir a Soberania Tecnológica

1.- Criar o Enquadramento Regulatório e Penal que permita proteger os dados do Estado e dos Cidadãos

2.- Desenhar e implementar Business Continuity Plans que reduzem a dependência nos privados

3.- Conceber e Aprovar o Quadro Comum de Interoperabilidade da Administração Pública Angolana

4.- Definir a Política de Segurança de Informação da Administração Pública Angolana

5.- Separar a "Administração dos Sistemas" do "Acesso aos Dados" utilizando mecanismos de encriptação

6.- Implementar um Programa Alargado de Capacitação dos Quadros Angolanos de TI

7.- Realizar auditorias externas aos Prestadores de Serviços de TI ao Estado

8.- Definir Service Level Agreements

9.- Reforçar os Contratos (motivos e penalizações em caso de incumprimento)

10.- Gerir os incumprimentos contratuais

# Índice

**Sumário Executivo**

A. Desafios a Endereçar

B. Tendências e Casos Internacionais de Referência

C. Opções de Desenvolvimento

D. Formas Complementares de Garantir a Soberania Tecnológica

**E. Recomendações**

Anexo 1: Casos Internacionais de Referência

# E. Recomendações

É importante avaliar o impacto e os custos subjacentes a cada opção de desenvolvimento, bem como criar as condições para a implementação das medidas tendentes a garantirem a soberania tecnológica.

1.- Validar preliminarmente os cenários apresentados

2.- Aprofundar os cenários apresentados e o seu impacto – aprofundar o Memorando

3.- Definir os Sistemas Chave do Estado e recolher informação de base sobre a sua gestão e desenvolvimento

4.- Avaliar cada um dos cenários em termos legais, operacionais e financeiros

5.- Definir Objetivos Concretos, um Plano de Acção e um Orçamento para o desenvolvimento das Medidas Chave para Garantir a Soberania Tecnológica

6.- Obter aprovação política final

7.- Identificar as entidades privadas envolvidas e iniciar um processo negocial

8.- Implementar a solução aprovada politicamente e negociada com os principais parceiros

# Índice

**Sumário Executivo**

A. Desafios a Endereçar

B. Tendências e Casos Internacionais de Referência

C. Opções de Desenvolvimento

D. Formas Complementares de Garantir a Soberania Tecnológica

E. Recomendações

**Anexo 1: Casos Internacionais de Referência**

# Anexo 1: Casos Internacionais de Referência

A análise dos casos e tendências internacionais compreende três grandes grupos: Enquadramento Regulatório, análise de Países de Referência e Estudo de uma Parceria Público-Privada Angolana.

**Áreas de Estudo**

Enquadramento Regulatório

Casos da EU e dos EUA

Análise de Casos Internacionais de Referência

Brasil, Cabo Verde, Maurícias, Portugal

Um caso Angolano de cooperação público-privada

Angola Cables

# Anexo 1: Casos Internacionais de Referência

A União Europeia é considerada uma das entidades mais avançadas na protecção e privacidade de dados, colocando restrições à transferência de dados para países fora da União.

**Directriz Europeia para a Protecção de Dados**

A directriz europeia para a protecção de dados indica que cada Estado-Membro deve criar uma autoridade de supervisão, um órgão independente que monitoriza o nível de protecção de dados nesse Estado-Membro, dá conselhos ao governo sobre as medidas e regulamentos administrativos, e inicia os processo judiciais quando a regulação da protecção de dados foi violada. Os cidadãos podem apresentar queixas sobre violações de privacidade quer a esta entidade de supervisão.

As leis europeias obrigam as entidades a garantir a segurança de um conjunto de dados e apenas permite a transferência desses dados para outros países fora da União Europeia (UE) caso a UE considere que esse país possui leis de protecção de dados satisfatórias ou que a entidade em questão se comprometam a actuar segundo a lei em vigor na UE.

Consequentemente, não é possível transferir informação protegida dos cidadãos da União Europeia para servidores localizados em países fora da União que não satisfaçam os requisitos de protecção de dados definidos pela EU.

# Anexo 1: Casos Internacionais de Referência

Os Estados Unidos da América (EUA) não possuem à data nenhuma lei única de protecção de dados. A protecção de dados é baseada em três vectores de actuação: legislação, regulação e auto-regulação.

## A Protecção de Dados nos EUA

Os Estados Unidos da América não possuem actualmente nenhuma lei nacional de protecção de dados apesar de regularem a divulgação de informação pessoal a terceiros através de diversas leis.

Uma das grandes questões de privacidade que se levantam nos EUA prende-se com as empresas de alojamento de informação estrangeiras mas com servidores nos Estados Unidos. Estas poderão ser obrigadas a divulgar informação confidencial caso o Governo dos EUA considere essa informação crucial. Ou seja, a informação que se encontra alojada nos EUA poderá ser sempre visualizado por entidades americanas caso seja considerada de elevada importância nacional. Nesse caso, a empresa estará a cumprir com uma lei americana ao mesmo tempo que poderá estar a incorrer em incumprimento com uma lei do seu país de origem.

De realçar que de forma a harmonizar as diferenças de legislação foi desenvolvido em conjunto entre os EUA e a EU uma framework denominada “Porto Seguro”. Esta framework identifica e apoia as entidades americanas a cumprir com as normas de protecção de dados da EU. A participação neste framework é totalmente voluntária, ainda que depois da subscrição da mesma as entidades adquiram um conjunto de deveres e obrigações.

Também entre os EUA e a Suiça foi desenvolvida uma framework semelhante.

# Anexo 1: Casos Internacionais de Referência

A análise dos casos e tendências internacionais compreende três grandes grupos: Enquadramento Regulatório, análise de Países de Referência e Estudo de uma Parceria Público-Privada Angolana.

**Áreas de Estudo**

Enquadramento Regulatório

A União Europeia e os Estados Unidos da América

Análise de Casos Internacionais de Referência

Brasil, Maurícias, Portugal, Cabo Verde

Um caso Angolano de cooperação público-privada

Angola Cables

# Anexo 1: Casos Internacionais de Referência

O Brasil tem no Serviço Federal de Processamento de Dados (Serpro) um das maiores empresas públicas TIC a nível mundial, que actua apenas para o sector público.

## Brasil

| | |
|---|---|
| Conselho Nacional de Protecção de Dados | Entidade que será criada brevemente e que terá autonomia administrativa, orçamentária e financeira e a atribuição de actuar como Autoridade de Garantia quanto à protecção de dados pessoais. |
| Secretaria de Logística e Tecnologia da Informação<br>Ministério do Planejamento | A SLTI tem como missão propor políticas, planear, coordenar, supervisionar e orientar normativamente as actividades de governação electrónica, relacionadas com a padronização e a disponibilização de serviços electrónicos interoperáveis, ou a gestão dos recursos de tecnologias de informação, entre outros. |
| SERPRO | Empresa pública vinculada ao Ministério da Fazenda. A empresa, cujo negócio é a prestação de serviços em Tecnologia da Informação e Comunicações para o sector público, tem como objectivo modernizar e dar agilidade a sectores estratégicos da Administração Pública brasileira. |

# Anexo 1: Casos Internacionais de Referência

O Governo Brasileiro encontra-se actualmente a preparar um Anteprojecto da Lei de Protecção de Dados que será fortemente inspirado pela legislação da União Europeia, à semelhança do que acontece com outros países da América do Sul como a Argentina e o Uruguai.

**Brasil – Ambiente Regulatório**

A Lei de Protecção de Dados do Brasil, cuja elaboração começou já a ser preparada em 2010, prevê-se que será publicada num futuro próximo.

Simultaneamente, será criado o Conselho Nacional de Protecção de Dados do Brasil. Caberá a esse conselho zelar pela segurança no tratamento de dados e receber denúncias, além de punir quem usar indevidamente informações de terceiros.

A Lei de Protecção de Dados do Brasil será fortemente inspirada na legislação da União Europeia. Do grupo do G-20 apenas o Brasil não possui actualmente leis sobre dados pessoais.


Fonte: netquest.com.br

# Anexo 1: Casos Internacionais de Referência

O Anteprojecto da Lei de Protecção de Dados está a ser preparado pelo Ministério da Justiça Brasileiro e regulará a protecção de dados dos cidadãos brasileiros.

**Brasil – Tópicos Abordados pela Lei de Protecção de Dados Pessoais**

1. Dados pessoais só poderão ser manipulados para fins comerciais com aval do titular;
2. As pessoas devem ser informadas, no momento da colecta dos seus dados, como estes serão utilizados, quem fará o tratamento e quais as suas informações que poderão ser compartilhadas;
3. Se o uso dos dados for prolongado, o titular deverá ser questionado periodicamente se quer renovar o seu consentimento;
4. É proibido formar bancos de dados para fins comerciais com informações que possam levar à discriminação do usuário, como as que revelam raça ou etnia, religião, orientação sexual, filiação sindical ou partidária, bem como os dados genéticos e biométricos;
5. Para utilização das informações pessoais, os bancos de dados podem ser transmitidos a outra entidade, desde que exerçam actividade análoga e peçam autorização dos titulares dos dados;
6. O titular pode fazer pedido de “habeas data”, ou seja pedir para aceder às suas informações arquivadas;
7. Os dados de cidadãos brasileiros serão transferidos apenas para países que tiverem políticas de protecção de dados ou para locais que forem autorizados pelo conselho de protecção de dados.

Fonte: netquest.com.br

# Anexo 1: Casos Internacionais de Referência

A Serpro, criada em 1964 e cujo negócio é a prestação de serviços em TIC para o sector público brasileiro é considerada uma das maiores organizações públicas de TI no mundo.

**Brasil - Serviço Federal de Processamento de Dados (Serpro)**

| | |
|---|---|
| **Criação** | 1964 |
| **Estatuto** | Empresa Pública |
| **Constituição** | Empresa 100% Estatal vinculada ao Ministério da Fazenda |
| **Clientes** | Sector Público Brasileiro |
| **Produtos/Serviços** | • Sistemas de informação;<br>• Serviços de tecnologia da informação e integração de soluções;<br>• Consultoria e informações;<br>• Gestão de TIC dos sistemas estruturantes do governo federal. |

# Anexo 1: Casos Internacionais de Referência

**Anexo 1: Casos Internacionais de Referência**

A Serpro desenvolve e gere um conjunto vastíssimo de sistemas de informação da Administração Pública Brasileira.

**Brasil - Serviço Federal de Processamento de Dados (Serpro)**

| | |
|---|---|
| Missão | Prover e integrar soluções em tecnologia da informação e comunicação para o êxito da gestão e da governança do Estado, em benefício da sociedade. |
| Parcerias | O Serpro aposta em parcerias com instituições públicas de ensino superior espalhadas pelo país para desenvolver pesquisas, focadas em governo eletrônico, que possibilitem maior autonomia tecnológica, garantindo inovação e melhoria dos processos da empresa. |
| Sistemas Desenvolvidos e/ou Geridos | • SAJ - Sistema de Acompanhamento Judicial<br>• Página Sida - Sistema Integrado da Dívida Activa<br>• SIEF - Sistema Integrado de Informações Econômico Fiscais<br>• Sistema Integrado de Administração Financeira do Governo Federal – Siafi<br>• Entre Outros |

# Anexo 1: Casos Internacionais de Referência

O caso das Maurícias destaca-se pela existência de uma empresa pública TIC considerada de referência internacionalmente e que actua quer no sector público quer no sector privado.

## Maurícias

Data Protection Office

O Data Protection Office é a autoridade responsável por garantir a protecção e privacidade dos dados dos cidadãos. A lei de protecção de dados das Marurícias (Data Protection Act) remonta já a 2004.

SIL
State Informatics Ltd

A State Informatics Lds (SIL), fundada em 1989, tornou-se numa empresa de referência de serviços TIC quer nas Maurícias, sector público e privado, quer na região africana.
O facto de actuar livremente no mercado permite à empresa ter competências de topo para o desenvolvimento e gestão dos serviços de TI para a AP das Maurícias.

Central Information Systems Division
(under the aegis of The Ministry of Information and Communication Technology)

A *Central Information Systems Division* tem como missão disponibilizar serviços de suporte TIC de qualidade às instituições públicas.
Os seus serviços são sobretudo de manutenção e suporte técnico dos sistemas e equipamentos existentes mas são também responsáveis, por exemplo, pela administração do correio electrónico governamental.

# Anexo 1: Casos Internacionais de Referência

A empresa pública SIL destaca-se por ser considerada uma empresa de referência a nível do continente africano, exportando para diversos países no continente.

**Maurícias – State Informatics Ltd (SIL)**

| | |
|---|---|
| Criação | 1989 |
| Estatuto | Empresa Pública |
| Constituição | 100% Estatal |
| Clientes | Sector Privado e Público do Continente Africano |
| Produtos/Serviços | • Soluções de referência ao nível da Governação Electrónica;<br>• Serviços em diversas áreas como Project Management, Desenvolvimento Aplicacional, Disaster Recovery, Segurança e Privacidade, entre outros. |

# Anexo 1: Casos Internacionais de Referência

A SIL, como empresa global e de referência, destaca-se por uma maior "produtização" das suas soluções para Governo e empresas.

**Maurícias – State Informatics Ltd (SIL)**

| | |
|---|---|
| Missão | Tornar-se num player de referência no sector das TIC nas Maurícias e no Continente Africano, servindo quer os Governos quer as empresas da região. |
| Parcerias | • Oracle<br>• SAP<br>• Microsoft<br>• IBM<br>• CISCO<br>• Symantec |
| Sistemas Desenvolvidos e/ou Geridos | Sistemas Desenvolvidos pela SIL:<br>• Sistema Integrado de Registo de Empresas<br>• Solução Integrada para Gestão de Impostos<br>• Sistema de Monitorização de Ocorrência de Crimes<br>• Sistema Integrado de Gestão Financeira, entre outros. |

# Anexo 1: Casos Internacionais de Referência

A *Central Information Systems Division* tem como missão fornecer serviços de apoio TIC fiáveis, oportunos e rentável às Instituições Governamentais.

**Maurícias – Central Information Systems Division**

Serviços Disponibilizados:

- Manutenção do Sistema de Pagamentos do Governo
- Desenvolvimento e Manutenção de Websites do Governo
- Administração do Serviço de Correio Electrónico Governamental
- Assistência Técnica na escolha de hardware, software e serviços relacionados
- Desenvolvimento e Implementação aplicacional
- Administração de Base de Dados, Sistemas e Redes
- Manutenção de Software
- Comissionamento de equipamentos de informática
- Suporte técnico em hardware e software PC
- Prestação de serviço de backup Central de dados de Ministérios e Departamentos
- Captura de Dados

# Anexo 1: Casos Internacionais de Referência

Em Portugal, a ESPAP é a entidade responsável pelo desenvolvimento dos Sistemas de Informação para a Administração Pública Portuguesa. A AMA é responsável por gerir a estratégia das TI e dos SI na Administração Pública.

**Portugal**

COMISSÃO NACIONAL DE PROTECÇÃO DE DADOS

A Comissão Nacional de Protecção de Dados é a entidade portuguesa responsável por controlar e fiscalizar o processamento de dados pessoais, em rigoroso respeito pelos direitos e garantias consagradas na Constituição e na lei.

ama AGÊNCIA PARA A MODERNIZAÇÃO ADMINISTRATIVA

A AMA tem por missão identificar, desenvolver e avaliar programas, projectos e acções de modernização e de simplificação administrativa, nomeadamente no ambiente da Governação Electrónica e dos Sistemas e Tecnologias de Informação.

eSPAP Entidade de Serviços Partilhados da Administração Pública, I.P.

A eSPap assegura a prestação de um conjunto de serviços nas áreas do desenvolvimento e manutenção de software aplicacional e da gestão de infraestruturas de tecnologias de informação e comunicação, principalmente ao Ministério das Finanças, mas também a toda a Administração Pública em geral.

# Anexo 1: Casos Internacionais de Referência

A Comissão Nacional de Protecção de Dados (CNPD) é uma entidade administrativa independente com poderes de autoridade, que funciona junto da Assembleia da República.

**Portugal – Comissão Nacional de Protecção de Dados**

A CNPD tem como atribuição genérica controlar e fiscalizar o processamento de dados pessoais, em respeito pelos direitos, liberdades e garantias consagradas na Constituição e na lei. A CNPD tem ainda como atribuições:

- Controlar e fiscalizar o cumprimento das disposições legais e regulamentares em matéria de proteção de dados pessoais.
- Emitir parecer prévio sobre quaisquer disposições legais, bem como sobre instrumentos jurídicos comunitários ou internacionais relativos ao tratamento de dados pessoais.
- Exercer poderes de investigação e inquérito, podendo para tal aceder aos dados objeto de tratamento.
- Exercer poderes de autoridade, designadamente o de ordenar o bloqueio, apagamento ou destruição dos dados, assim como o de proibir temporária ou definitivamente o tratamento de dados pessoais.
- Advertir ou censurar publicamente o responsável do tratamento dos dados, pelo não cumprimento das disposições legais nesta matéria.
- Intervir em processos judiciais no caso de violação da lei de proteção de dados.
- Denunciar ao Ministério Público as infrações penais nesta matéria, bem como praticar os atos cautelares necessários e urgentes para assegurar os meios de provas.

# Anexo 1: Casos Internacionais de Referência

A AMA, instituto público responsável por promover e desenvolver a modernização administrativa em Portugal, organiza a sua actuação sobre três eixos fundamentais: Atendimento, Simplificação e Governo Electrónico.

**Portugal – Agência para a Modernização Administrativa (AMA)**

A AMA além do desenvolvimento e promoção da temática da identificação electrónica em Portugal, através de um projecto referência a nível mundial – o Cartão de Cidadão -, e de um trabalho profundo na área da Interoperabilidade a nível da AP, a AMA também é responsável pela operacionalização do ambicioso Plano global estratégico de racionalização e redução de custos nas TIC, na Administração Pública (PGERRCTIC), que prevê uma redução potencial de até 500 milhões de euro / ano em gastos TIC na Administração Central.

Este plano também dá à AMA várias competências na definição estratégica de políticas TIC e aprovação de gastos em toda a Administração Pública.

Os projectos TIC da Administração Pública têm legalmente de ser previamente aprovados pela AMA que verifica a existência de sistemas semelhantes, a interoperabilidade, as incompatibilidades, o alinhamento da tecnologia, etc.

# Anexo 1: Casos Internacionais de Referência

A unidade de Serviços Partilhados TIC de Portugal gere um conjunto de plataformas fulcrais e desenvolve novas soluções numa abordagem "chave na mão" para a Administração Pública.

**Portugal – Entidade de Serviços Partilhados da Administração Pública (ESPAP)**

| | |
|---|---|
| **Criação** | 2012 (Anteriormente Instituto de Informática, criado em 1977) |
| **Estatuto** | Entidade Pública |
| **Constituição** | 100% Estatal |
| **Clientes** | Principalmente o Ministério das Finanças, mas também a toda a Administração Pública |
| **Produtos/Serviços** | • Desenvolvimento aplicacional, sendo assegurada a manutenção e evolução de aplicações, desenvolvidas à medida ou suportadas em produtos de mercado (packages), bem como as alterações que decorram de alterações legislativas;<br>• Infra-estruturas TIC, em que o Centro de Processamento de Dados da eSPap assegura as condições logísticas e técnicas necessárias ao alojamento, operação e administração das aplicações desenvolvidas pela eSPap ou pelo cliente. |

# Anexo 1: Casos Internacionais de Referência

A unidade de Serviços Partilhados TIC gere mais de 600 servidores, explora mais de 35 sistemas de informação e conta com mais de 150 Tb de armazenamento disponível.

**Portugal – Entidade de Serviços Partilhados da Administração Pública (ESPAP)**

| | |
|---|---|
| **Missão** | Assegurar a obtenção de ganhos de eficácia e eficiência, através da utilização racional de recursos públicos comuns e da prestação de serviços partilhados, contribuindo para um Estado mais ágil e direccionado para o desenvolvimento sustentável do país. |
| **Parcerias** | |
| **Sistemas Desenvolvidos e/ou Geridos** | • Gestão das plataformas que suportam a prestação de serviços da eSPap onde se incluem o GeRFiP, GeRHuP, GeADAP, Catálogo Nacional de Compras Públicas, Sistema de Gestão do Parque de Veículos do Estado, entre outros;<br>• Bolsa de Emprego Público (BEP), Programa de Estágios Profissionais da Administração Central (PEPAC), Sistema de Informação de Gestão Orçamental (SIGO), Sistema de Orçamento de Estado (SOE), Sistema de Gestão da Receita (SGR), Sistema de Gestão de Contas do Tesouro (SGT), Sistema de Produtos de Aforro (SPA), Sistema de Mobilidade Especial (sigaME) |

# Anexo 1: Casos Internacionais de Referência

O NOSi passou recentemente a ter estatuto de Entidade Pública Empresarial (E.P.E.) focando a sua actividade no desenvolvimento e gestão de Sistemas de Informação.

**Cabo Verde**

NOSi
Núcleo Operacional para a Sociedade de Informação
Chefia do Governo

O NOSi até final de 2013 congregava as funções de entidade responsável pelo desenvolvimento e gestão dos Sistemas de Informação para a Administração Pública como era também responsável pela estratégia dos Sistemas de Informação na AP.

Recentemente foi decretado que o NOSi focaria a sua actividade apenas como empresa pública de prestação de serviços TIC, sendo um dos principais clientes a Administração Pública Cabo Verdiana, e que seria criada uma nova entidade que terá a seu cargo a estratégia da Sociedade de Informação e dos Sistemas de Informação no Governo Cabo-Verdiano.

Cabo Verde não apresenta à data nenhuma lei nacional de protecção de dados.

# Anexo 1: Casos Internacionais de Referência

O NOSi passou recentemente de uma entidade pública para uma entidade pública empresarial, com autonomia administrativa, financeira e patrimonial.

**Cabo Verde – Núcleo Operacional Sociedade de Informação (NOSi)**

| | |
|---|---|
| **Criação** | 1998 |
| **Estatuto** | Entidade Pública Empresarial (E.P.E.) |
| **Constituição** | 100% Pública – Sujeita à tutela das áreas das Finanças, das Tecnologias de Informação e Comunicação e da Reforma do Estado |
| **Clientes** | Administração Pública – Nacional e Internacionalmente |
| **Produtos/Serviços** | • O NOSi disponibiliza soluções num conjunto diversificado de áreas como a Educação, Infra-estrutura, Saúde e Segurança Social, Gestão do Território, Web, Identificação, Ambiente de Negócios, Poder Local, Finanças, entre outras; |

# Anexo 1: Casos Internacionais de Referência

O NOSi foi responsável pelo desenvolvimento e gestão da maioria dos sistemas de informação desenvolvidos para a AP Cabo Verdiana ao longo dos últimos anos.

**Cabo Verde – Núcleo Operacional Sociedade de Informação (NOSi)**

| | |
|---|---|
| **Missão** | Propor e executar as medidas de política nas áreas da inovação, da sociedade de informação e da governação eletrónica |
| **Parcerias** | • Huawei<br>• Microsoft<br>• Oracle<br>• Entre outras |
| **Sistemas Desenvolvidos e/ou Geridos** | Sistemas Geridos pelo NOSi<br>• Sistema Integrado de Previdência Social<br>• Sistema de Informação para a Saúde<br>• Sistema de Informação Geográfica<br>• Sistema Nacional de Identificação e Autenticação Civil<br>• Sistema Integrado de Gestão Orçamental e Financeira |

# Anexo 1: Casos Internacionais de Referência

A análise dos casos e tendências internacionais compreende três grandes grupos: Enquadramento Regulatório, análise de Países de Referência e Estudo de uma Parceria Público-Privada Angolana.

**Áreas de Estudo**

Enquadramento Regulatório

Casos da EU e dos EUA

Análise de Casos Internacionais de Referência

Brasil, Cabo Verde, Maurícias, Portugal

Um caso Angolano de cooperação público-privada

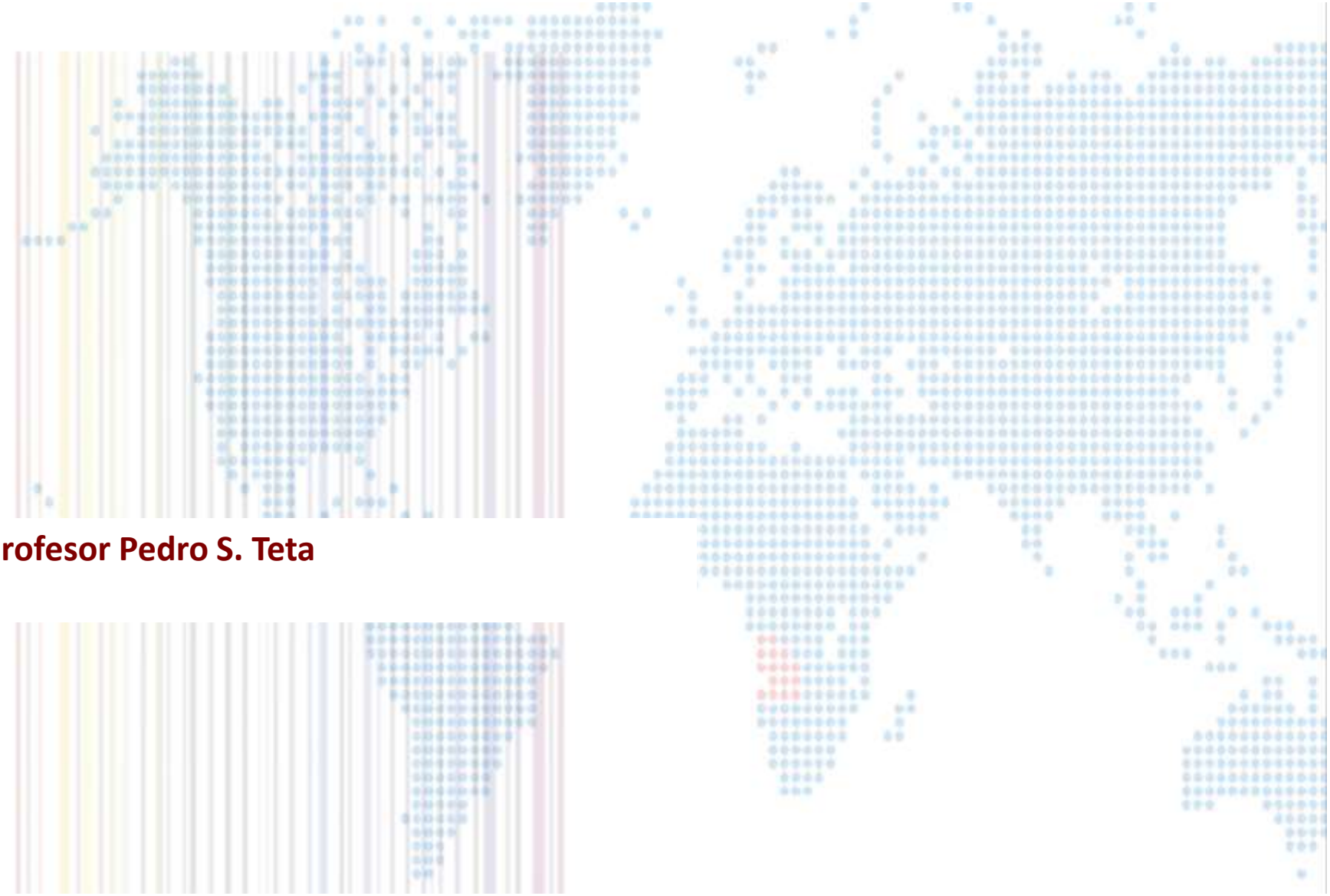
Angola Cables

# Anexo 1: Casos Internacionais de Referência

A Angola Cables é constituída pelos 5 principais operadores de telecomunicações em Angola, estando 51% do capital da empresa junto da Angola Telecom, empresa pública.

**Angola – Angola Cables**

| | |
|---|---|
| **Criação** | 2009 |
| **Estatuto** | Empresa Pública |
| **Constituição** | 51%-Angola Telecom; 31%-Unitel; 9%-MSTelecom; 6%-Movicel; 3%-Startel |
| **Clientes** | Operadores de Telecomunicações Angolanos |
| **Produtos/Serviços** | • Mercado de “wholesale” (venda a grosso): comercialização de capacidade em circuitos internacionais de voz e dados por cabo submarino de fibra óptica a operadores de telecomunicações |



**Profesor Pedro S. Teta**