QUADRO DE PESSOAL DAS AGÊNCIAS DE CIBERSEGURANÇA E PROTEÇÃO DE DADOS

Estudo de viabilidade sobre
cibersegurança e proteção de dados
Modelos de governança da proteção, funcionamento
Capacidade manual e de cibercriminalidade
Reforçar o apoio na Guiné-Bissau

Para
Programa Regional de
Integração Digital da África Ocidental

BS Innovations

GoSecure

Criado por : BS Innovations & GoSecure
07/2024

Índice de conteúdo

Lista de figuras

Definição de acrónimos

AfDB	Banco Africano de Desenvolvimento
ANP / NPA	Assembleia Nacional Popular
ARN	Autoridade Reguladora Nacional
AU	União Africana
CERTs	Equipas de resposta a emergências informáticas
CSIRTs	Equipas de resposta a incidentes de segurança informática
DGP	Governança e privacidade dos dados
DGTED	Direção Geral das Telecomunicações e Economia Digital
DPAs	Autoridades de Proteção de Dados
DPC	Comissão de Proteção de Dados
DPOs	Responsáveis pela proteção de dados
ECOWAS	Comunidade Económica dos Estados da África Ocidental
EU	União Europeia
GDPR	Regulamento Geral sobre a Proteção de Dados
GPA	Assembleia Global da Privacidade
IAPP	Associação Internacional de Profissionais de Privacidade
ICDPPC	Conferência Internacional sobre Privacidade e Dados Comissários responsáveis pela proteção
ICO	Gabinete do Comissário da Informação
ICT	Tecnologias da Informação e da Comunicação
IGF	Fórum de Governança da Internet
IT	Tecnologias da informação
ITMA	Instituto Tecnológico de Administração Modernização
ITU	União Internacional das Telecomunicações
KPIs	Indicadores-chave de desempenho
NDPA	Agência Nacional de Proteção de Dados
NGOs	Organizações Não-Governamentais
OCWAR-C	Resposta da África Ocidental em matéria de Cibersegurança e Luta Contra a Cibercriminalidade
ODPC	Gabinete do Comissário para a Proteção de Dados
OECD	Organização para a Cooperação e Desenvolvimento Económico Desenvolvimento
PMO	Gabinete do Primeiro-Ministro
PR	Presidente da República
SOC	Centro de Operações de Segurança
SOPs	Procedimentos Operacionais Normalizados
WARDIP	Programa Regional de Integração Digital da África Ocidental
WB	Banco Mundial
UNCTAD	Comércio e Desenvolvimento das Nações Unidas

I. Contexto

Em reconhecimento à necessidade da Guiné-Bissau de desenvolver uma economia digital, ao mesmo tempo em que se alinha e integra ao mercado digital regional da África Ocidental e ao mercado internacional, o Banco Mundial (BM) está financiando a preparação do Programa Regional de Integração Digital da África Ocidental (WARDIP) – Guiné-Bissau.

O objetivo do programa WARDIP – Guiné-Bissau é liderar a transformação digital em todo o país. Apoiará o desenvolvimento de modelos de governança, políticas e regulamentos nacionais, bem como a implementação de programas estratégicos que devem ser melhorados para eliminar os obstáculos à conetividade transfronteiriça dos fluxos e serviços de dados digitais. Deste modo, permitirá a emergência de um sistema nacional e regional integrado e competitivo, posicionando o país de forma competitiva na região africana e a nível mundial, promovendo simultaneamente a inovação e a prosperidade.

Nos últimos anos, a Guiné-Bissau registou um rápido progresso tecnológico e uma maior penetração da Internet. Com a crescente dependência das tecnologias de informação e comunicação (TIC), o país enfrenta um risco acrescido de ameaças e vulnerabilidades cibernéticas. Reconhecendo a importância da cibersegurança e da proteção de dados para garantir a segurança dos cidadãos, das empresas e das infraestruturas críticas, foi criado o projeto WARDIP.
Estes desafios exigem respostas múltiplas, reunindo o governo, o sector privado e a sociedade civil para enfrentar os desafios da cibersegurança e da governança da privacidade.

A tónica é colocada no alinhamento com as realidades políticas nacionais e no cumprimento dos requisitos regulamentares africanos e nacionais. No centro da iniciativa está a facilitação das ligações transfronteiriças e o fluxo contínuo de dados entre as economias digitais regionais africanas e os mercados internacionais no ecossistema digital.O estabelecimento de um modelo de governança robusto, que englobe elementos essenciais como a estrutura, os mecanismos de supervisão, as políticas e os processos, é fundamental para alcançar estes objetivos. Prevê-se que esta base estimule a criação de emprego e atraia investimentos para o país.

A fase inicial do projeto, Etapa 1, consistiu na realização de um estudo de viabilidade dos modelos de governança da cibersegurança e da proteção de dados.

A segunda fase do projeto, Etapa 2, consiste em apoiar o Governo da Guiné-Bissau na conceção das agências de proteção de dados e de cibersegurança, fornecendo aconselhamento e conhecimentos especializados. Começaremos por definir os principais objectivos de cada agência e, no contexto da Guiné-Bissau, delinear as estruturas das agências e a sua cooperação com outras entidades. Iremos também propor as diferentes fases de criação das agências.

II. Definição dos objectivos da Agência de Cibersegurança e Proteção de Dados

1. O que define uma agência

Uma agência é uma organização governamental ou semi-governamental estruturada e especializada, normalmente estabelecida por instrumentos legais como leis, decretos, ordens executivas ou tratados internacionais para tratar de questões específicas, gerir recursos públicos, aplicar leis ou prestar serviços públicos. Uma agência define-se pela sua autonomia e pela sua "responsabilidade estruturante" na implementação de políticas públicas. É única no seu domínio de intervenção e está sujeita às instruções e ao controlo financeiro do Estado.

2. Definição da Agência Nacional de Proteção de Dados

À medida que as atividades sociais e económicas em linha continuam a expandir-se, a importância da privacidade e da proteção de dados está a ser amplamente reconhecida.

Uma questão importante é a recolha, utilização e partilha de informações pessoais com terceiros sem a notificação ou o consentimento do consumidor.

Em 2021, de acordo com a análise da organização UNCTAD, 137 dos 194 países promulgaram leis para garantir a proteção dos dados e da privacidade. As taxas de adoção variam consoante as regiões, com 61% dos países em África e 57% na Ásia a terem estabelecido tais leis. Nos países menos desenvolvidos, apenas 48% têm regulamentos semelhantes em vigor[1].

Uma Agência/Autoridade Nacional de Proteção de Dados (ANPD) é normalmente a autoridade central a nível nacional que supervisiona a aplicação e o cumprimento das leis de proteção de dados.
Esta entidade supervisiona, através de poderes de investigação e correção, a aplicação da lei da proteção de dados. Presta aconselhamento especializado sobre questões de proteção de dados e trata as queixas apresentadas contra violações do Regulamento Geral sobre a Proteção de Dados e das leis nacionais pertinentes.

3. Definição de agência de cibersegurança

Uma agência de cibersegurança é uma entidade governamental ou semi-governamental encarregada de proteger os sistemas de informação, as redes e os dados contra ciberameaças e ataques. Desempenha um papel proactivo na informação do sector privado sobre potenciais ameaças, na segurança de infraestruturas críticas, na salvaguarda de dados sensíveis e na prevenção de cibercrimes. As principais responsabilidades da agência incluem a monitorização e deteção de atividades suspeitas, a coordenação de respostas a incidentes, a implementação de medidas de segurança preventivas, a educação e formação das partes interessadas sobre as melhores práticas de cibersegurança e a colaboração com outras agências governamentais, entidades do sector privado e parceiros internacionais. Além disso, a agência está envolvida no desenvolvimento e aplicação de políticas de cibersegurança e na promoção da investigação e inovação em tecnologias e soluções de cibersegurança.

A criação de uma agência deste tipo é crucial para estabelecer relações de confiança com outras agências de cibersegurança à escala internacional.

4. Objectivos da agência para a cibersegurança e a proteção de dados

Uma agência de cibersegurança ou de proteção de dados tratará de questões de cibersegurança ou de proteção de dados. Estas duas agências têm as suas próprias preocupações específicas, mas também têm vários objectivos comuns.

A. Objetivos comuns

Tanto uma autoridade/agência nacional de proteção de dados como uma agência nacional de cibersegurança partilham vários objectivos comuns que são cruciais para garantir a segurança e a privacidade dos dados, bem como para proteger as infraestruturas críticas das ciberameaças.

- **Proteção de dados sensíveis**
  Um dos objetivos comuns é garantir a proteção dos dados sensíveis contra o acesso não autorizado, às violações e os ciberataques.
  Ambas as agências trabalham para proteger os dados sensíveis, quer se trate de dados pessoais ou de informações críticas para a segurança nacional. Aplicam medidas de segurança para evitar violações de dados e ciberataques.

- **Conformidade regulamentar**
  Assegurar que as organizações cumprem as leis e regulamentos em matéria de cibersegurança e proteção de dados.
  Ambas as agências são responsáveis pela

1 https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

aplicação de leis e regulamentos, realizando auditorias e inspeções para garantir que as organizações cumprem os requisitos legais.

- **Sensibilização e educação**
  Educar o público e as empresas sobre as melhores práticas em matéria de cibersegurança e proteção de dados.
  Ambas as agências organizam campanhas de sensibilização e programas de formação para informar os cidadãos e as empresas sobre os riscos e as medidas de proteção.

- **Gestão de incidentes**
  Coordenar a resposta a incidentes de segurança e de proteção de dados.
  Ambas as agências estão envolvidas na gestão de incidentes, quer se trate de ciberataques ou de violações de dados. Coordenam os esforços de resposta e de atenuação para minimizar o impacto dos incidentes.

- **Colaboração internacional**
  Trabalhar com parceiros internacionais para reforçar a cibersegurança e a proteção de dados a nível mundial.
  Ambas as agências participam em fóruns internacionais, partilham informações e colaboram com homólogos estrangeiros para melhorar a segurança e a proteção de dados à escala mundial.

- **Desenvolvimento de políticas e normas**
  Desenvolver e promover políticas e normas de segurança e proteção de dados.
  Ambas as agências estão envolvidas no desenvolvimento de políticas e normas destinadas a melhorar a cibersegurança e a proteção de dados. Trabalham na criação de quadros regulamentares e de melhores práticas.

B. Pontos distintivos de cada agência

Embora tanto uma agência nacional de proteção de dados como uma agência nacional de cibersegurança partilham objetivos comuns em matéria de proteção de dados e de garantia do cumprimento da regulamentação, cada agência tem também os seus próprios objetivos distintivos que refletem o seu mandato específico e as suas áreas de incidência.

Estes objetivos distintos realçam os papéis únicos que cada agência desempenha no panorama mais vasto da segurança nacional e da proteção de dados.

Agência Nacional de Cibersegurança

- **Foco na segurança nacional**
  A agência é a principal responsável pela proteção dos interesses de segurança nacional, incluindo as infraestruturas críticas e as redes governamentais, contra as ciberameaças.

  Os governos devem adotar abordagens sofisticadas em matéria de cibersegurança, incluindo agências civis de cibersegurança centradas na proteção das redes e não no seu ataque. Isto promove relações de confiança com outras agências de cibersegurança a nível mundial. Além disso, o estabelecimento de limites mínimos de cibersegurança entre governos pode facilitar o livre fluxo de dados, sendo crucial a inclusão de cláusulas anti-espionagem nos acordos de partilha de dados transfronteiriços.

- **Coordenação da resposta a incidentes :**
  Lidera os esforços nacionais de resposta e atenuação de incidentes cibernéticos, incluindo a coordenação com múltiplas partes interessadas durante eventos cibernéticos de grande escala.

  A coordenação da resposta a incidentes é essencial para abordar e atenuar os ciber incidentes à escala nacional, trabalhando em colaboração com várias partes interessadas durante ciber incidentes de grande escala.

- **Informações sobre ameaças cibernéticas**
  Recolhe, analisa e divulga informações sobre ciberameaças às partes interessadas relevantes, incluindo outras agências governamentais

e parceiros do sector privado.
A informação sobre ciberameaças envolve a recolha, análise e divulgação de informações sobre ciberameaças às partes interessadas relevantes, incluindo outras agências governamentais e parceiros do sector privado.

- **Capacidades de ciberdefesa**
  Desenvolve e implementa ferramentas e tecnologias avançadas de ciberdefesa para detetar, prevenir e responder a ciberameaças.

- **Proteção de redes governamentais**
  A Agência trabalhará em estreita colaboração com as agências militares e de informação para garantir a segurança das redes de defesa nacional e dos sistemas de comunicação críticos do Governo.

  Esta colaboração visa detetar e compreender as ciberameaças de actores estatais e não estatais, fornecendo informações sobre as ciber operações dos adversários, incluindo as suas intenções, capacidades e atividades.

- **Proteger as infraestruturas críticas**
  Protege os serviços essenciais, como os sistemas de energia, transportes e comunicações, contra as ciberameaças, garantindo a sua resiliência e disponibilidade.

  Agência Nacional de Proteção de Dados

- **Foco na privacidade e nos dados pessoais**
  A agência é a principal responsável por garantir a privacidade e a proteção dos dados pessoais e das informações sensíveis dos cidadãos.

  Tal como definido nas "Perspectivas Europeias de Cibersegurança 2018", a agência pode conceber estratégias de privacidade que incluam a separação, a abstração, a ocultação, a informação, o controlo, a aplicação, a demonstração e a minimização dos dados pessoais.

- **Controlo da aplicação da regulamentação :**
  A Agência aplicará as leis e regulamentos relativos à proteção de dados, realizará auditorias e inspecções e imporá sanções em caso de incumprimento.

- **Gestão da violação de dados:**
  A Agência irá gerir e supervisionar as respostas às violações de dados, incluindo os requisitos de notificação e as medidas de atenuação. Uma proteção da identidade das vítimas de violações de dados pode reduzir as taxas de rotatividade dos clientes, reduzindo assim os custos relacionados com as violações.

- **Educação pública e empresarial:**
  A Agência educará o público e as empresas sobre os direitos e responsabilidades em matéria de proteção de dados e promoverá as melhores práticas de gestão dos dados e da privacidade.

  Para sensibilizar as partes interessadas para a proteção de dados, recomenda-se a organização de workshops de formação e sensibilização sobre proteção de dados, bem como sessões de jogos, estudos de casos e sessões de trabalho.

- **Orientação jurídica e de conformidade**
  A Agência fornecerá orientação e apoio às organizações no que respeita ao cumprimento das leis de proteção de dados e à garantia do tratamento legal dos dados pessoais.

  A responsabilidade pela conformidade é agora partilhada de forma mais equilibrada entre os responsáveis pelo tratamento e os subcontratantes.

- **Tratamento e processamento de dados**
  A Agência assegurará que os dados pessoais sejam recolhidos, armazenados, tratados e partilhados de forma a respeitar a legislação em matéria de privacidade e a proteger os direitos individuais.

III

Definição das etapas de criação e operacionalização da Agência

A conceção e criação de uma agência de cibersegurança e de uma autoridade de proteção de dados é um processo moroso que exige o envolvimento do Governo e uma estratégia clara. Através do projeto WARDIP, para o qual fomos mandatados, definimos esta estratégia e ajudamos na conceção de uma agência de cibersegurança e de uma agência de proteção de dados, tendo em conta os nossos vários estudos e análises no terreno.

No atual contexto da Guiné-Bissau, caracterizado pela frequente instabilidade política e pela falta de recursos qualificados, propomos a criação de duas entidades separadas: uma agência dedicada à cibersegurança e uma agência distinta de proteção de dados. Esta abordagem garante que cada domínio recebe atenção e conhecimentos especializados, abordando eficazmente os seus desafios únicos e requisitos regulamentares.

Apesar da dificuldade de encontrar recursos qualificados, não recomendamos que haja apenas uma agência a tratar da proteção de dados e da cibersegurança. Isto pode levar a um risco elevado de um ponto único de falha, a uma falta de foco na visão e a um problema de imparcialidade. Por exemplo, a agência de proteção de dados deve garantir que a agência de cibersegurança também cumpra as regras de proteção de dados e vice-versa.

Esta estratégia de dupla agência visa fornecer quadros robustos tanto para a cibersegurança como para a proteção de dados pessoais, promovendo um ambiente digital mais seguro e resiliente na Guiné-Bissau. À medida que a situação se estabiliza e os recursos se tornam mais disponíveis, estas entidades podem expandir as suas capacidades e aumentar ainda mais a sua eficácia.

Vários elementos motivaram esta escolha, nomeadamente:

- **Maior especialização e eficiência:**
  Com a criação de duas agências distintas, a Guiné-Bissau pode atingir um elevado nível de especialização e perícia tanto na cibersegurança como na proteção de dados. Cada agência pode concentrar-se no seu mandato específico, permitindo uma gestão mais direcionada e eficaz. A divisão de responsabilidades garante que ambos os domínios recebam a atenção e os recursos necessários.

  A existência de duas agências permite uma clara delimitação de funções, reduzindo o risco de conflito de prioridades e permitindo que cada agência desenvolva e aplique estratégias adaptadas ao seu domínio específico. Esta separação aumenta a responsabilidade e garante que as políticas de cibersegurança e de proteção de dados são sólidas e abrangentes.

  Além disso, ao ter agências especializadas, a Guiné-Bissau pode atrair e reter profissionais com experiência em cibersegurança ou proteção de dados, promovendo assim uma força de trabalho altamente qualificada em ambas as áreas. Esforços de recrutamento direcionados podem garantir que cada agência crie uma equipa de especialistas mais adequada aos seus respectivos desafios.

- **Melhoria da focalização e da afetação de** recursos:
  Duas agências distintas permitem uma melhor afetação de recursos, uma vez que cada agência pode concentrar-se nas suas necessidades e prioridades específicas. Isto garante que as áreas críticas da cibersegurança e da proteção de dados recebam financiamento, ferramentas e pessoal adequados, sem a concorrência por recursos que podem ocorrer numa estrutura de agência única. Ao dispor de recursos dedicados, cada agência pode responder mais eficazmente a incidentes e desafios no seu domínio, conduzindo a uma melhor segurança global e proteção de dados.

- **Formação e desenvolvimento profissional à medida :**
  Com duas agências especializadas, a Guiné-Bissau pode desenvolver programas de formação e desenvolvimento profissional

especificamente adaptados às necessidades específicas da cibersegurança e da proteção de dados. Esta abordagem específica garante que o pessoal esteja equipado com as mais recentes competências e conhecimentos pertinentes à sua área. A colaboração inter-agências através de workshops e seminários conjuntos pode ainda ser facilitada, promovendo a partilha de conhecimentos ao mesmo tempo que se mantém o foco especializado de cada agência.

- **Cooperação internacional reforçada:** Duas agências distintas podem promover uma melhor cooperação internacional, permitindo que cada agência se envolva com contrapartes globais na sua área específica de especialização. Isto permite uma participação mais eficaz em fóruns internacionais, partilha de informações e iniciativas de colaboração, reforçando a presença e a influência da Guiné-Bissau nas comunidades globais de cibersegurança e proteção de dados.

- **Responsabilidade e governança claras:** A criação de duas agências cria uma estrutura clara de responsabilização e governança, com responsabilidades definidas e mecanismos de supervisão para cada domínio. Esta clareza ajuda no desenvolvimento e aplicação de políticas, procedimentos e normas específicas para a cibersegurança e a proteção de dados. Simplifica também os processos de monitorização e avaliação, permitindo uma melhor avaliação do desempenho e a identificação de áreas a melhorar. Estruturas de responsabilização claras contribuem para uma gestão e governança mais eficazes, garantindo que os objectivos de cibersegurança e de proteção de dados são cumpridos de forma eficiente e eficaz.

Ao adotar esta abordagem abrangente, a Guiné-Bissau pode criar agências robustas e adaptáveis que respondam aos desafios imediatos colocados pela instabilidade política e pelos recursos limitados. Este quadro estratégico fornecerá uma base sólida para o futuro desenvolvimento de agências dedicadas à cibersegurança e à proteção de dados. De acordo com a nossa abordagem, definimos cinco etapas principais para a sua criação.

1. Planeamento e avaliação

A. Avaliação e análise das necessidades

- Realizar uma avaliação exaustiva do atual panorama da cibersegurança e da proteção de dados na Guiné-Bissau. Uma parte significativa desta análise já foi concluída no Entregável 1. No entanto, esta avaliação deve também avaliar a eficácia das políticas e regulamentos existentes e analisar o estado atual da infraestrutura das TIC.
- Avaliar as infraestruturas existentes, os quadros jurídicos e os recursos humanos disponíveis.
- Identificar as lacunas, os riscos e as necessidades para definir claramente o âmbito e os objetivos das agências.
- Envolver as partes interessadas do governo, do sector privado e da sociedade civil para recolher contributos e apoio.

B. Envolvimento das partes interessadas

- Envolver as principais partes interessadas, incluindo funcionários públicos, representantes do sector privado e da sociedade civil, a fim de recolher opiniões diversas e garantir um apoio alargado.
- Criar um comité diretor para orientar o processo de planeamento e execução de ambas as agências.

C. Definição da visão e da missão

- Definir a visão, a missão, os objectivos estratégicos e os indicadores-chave de desempenho (KPI) da agência, alinhando-os com as prioridades nacionais e as normas internacionais.
- Definir um roteiro para a implementação, incluindo cronogramas, marcos e requisitos de recursos.

2. Quadro jurídico e regulamentar

A. Redação de legislação

- Elaborar e adotar legislação que defina as funções, as responsabilidades e as compe-

tências das agências.
- Assegurar que a legislação prevê um quadro sólido para a aplicação de medidas de cibersegurança e de proteção de dados.

B. Desenvolvimento de políticas
- Formular políticas que apoiem a implementação de medidas de cibersegurança e de proteção de dados, com base no contexto da Guiné-Bissau.
- Alinhar estas políticas com as normas regionais e mundiais para garantir a conformidade e a interoperabilidade (directivas da CEDEAO, Convenção de Malabo, Convenção de Budapeste).

3. Estrutura organizacional

A. Estabelecer uma estrutura de governança
- Formar um comité de direção composto por representantes das instituições relevantes da Guiné-Bissau (Ministério dos Transportes e das Telecomunicações, Primeiro-Ministro, Assembleia Nacional), agências e principais interessados para supervisionar o processo de estabelecimento.
- Definir a estrutura organizacional, incluindo a hierarquia, os departamentos e as funções.

B. Recrutamento e reforço das capacidades
- Desenvolver um plano de recrutamento para atrair profissionais qualificados em matéria de cibersegurança, proteção de dados, direito e gestão.
- Implementar programas de reforço das capacidades para formar e melhorar as competências do pessoal existente e dos novos funcionários, tirando partido das parcerias com organizações internacionais e universidades.

C. Aquisição de infra-estruturas
- Assegurar o espaço de escritórios, as infraestruturas informáticas e as ferramentas de cibersegurança necessárias para as operações da agência.
- Implementar sistemas de comunicação seguros e soluções de armazenamento de dados para proteger informações sensíveis.

D. Nomeação de líderes
- Nomear profissionais experientes para dirigir as agências, assegurando um equilíbrio entre conhecimentos técnicos e capacidade administrativa.

4. Desenvolvimento de políticas e procedimentos

A. Definir políticas
- Elaborar políticas e procedimentos para as operações da agência, incluindo resposta a incidentes, proteção de dados, conformidade e processos de auditoria.
- Desenvolver orientações para a colaboração com outras agências governamentais, o sector privado e os parceiros internacionais.

B. Procedimentos Operacionais Normalizados (SOPs)
- Criar SOPs para operações diárias, gestão de incidentes, partilha de informações sobre ameaças e campanhas de sensibilização do público.
- Assegurar que os SOP's estão alinhados com o modelo de governança.

5. Mobilização de recursos e reforço de capacidades

A. Recursos Humanos
- Lançar ações de recrutamento para atrair e reter pessoal qualificado, oferecendo uma remuneração competitiva e um desenvolvimento profissional contínuo.
- Colaborar com as instituições de ensino para desenvolver uma reserva de profissionais formados.

B. Programas de formação
- Estabelecer parcerias com organizações internacionais para fornecer programas de formação e certificação para profissionais da cibersegurança e da proteção de dados.
- Desenvolver programas de formação interna para melhorar as competências do pessoal existente.

C. Aquisição de tecnologia

- Investir em ferramentas e infraestruturas tecnológicas avançadas para apoiar as necessidades operacionais da agência.
- Assegurar que a tecnologia é escalável e adaptável a requisitos futuros.

6. Sensibilização do público

A. Sensibilização do público e divulgação

- Realizar campanhas de sensibilização para informar o público e as empresas sobre o papel da agência e a importância da cibersegurança e da proteção de dados.
- Fornecer recursos e materiais de formação para ajudar as partes interessadas a compreender e a cumprir os novos regulamentos e as melhores

7. Implementação em grande escala e sua melhoria contínua

A. Expandir as operações

- Alargar gradualmente as operações da agência de modo a abranger todos os sectores e regiões, assegurando a aplicação efectiva do modelo de governança híbrido.
- Criar gabinetes regionais ou unidades de ligação para facilitar a aplicação e o apoio a nível local.

B. Controlo e avaliação

- Implementar mecanismos de controle e avaliação para acompanhar o desempenho da agência em relação aos seus indicadores-chave de desempenho.
- Efetuar auditorias e avaliações regulares para identificar áreas a melhorar e garantir o cumprimento das políticas e regulamentos.

C. Melhoria contínua

- Fomentar uma cultura de melhoria contínua, atualizando regularmente as políticas, os procedimentos e os programas de formação com base nas ameaças emergentes e nos avanços tecnológicos.
- Incentivar a inovação e a investigação para estar à frente dos desafios da cibersegurança e da proteção de dados.

8. Sustentabilidade e sua melhoria contínua

A. Mecanismos de financiamento

- Garantir fontes de financiamento sustentáveis, incluindo orçamentos governamentais, ajuda internacional e contribuições do sector privado, para assegurar a viabilidade da agência a longo prazo.
- Elaborar um plano financeiro que define as necessidades de financiamento e as prioridades de despesa.

B. Melhoria contínua

- Estabelecer uma cultura de melhoria contínua através de auditorias regulares, mecanismos de feedback e adoção das melhores práticas e tecnologias emergentes.
- Incentivar a inovação e a adaptabilidade no seio das agências para responder à evolução dos desafios em matéria de cibersegurança e de proteção de dados.

IV

Panorama das principais instituições nacionais da Guiné-Bissau e da sua interoperabilidade e impactos mútuos

As principais instituições nacionais da Guiné-Bissau são designadas como órgãos de soberania. Existem quatro órgãos de soberania:

- Presidente da República,
- Assembleia Nacional Popular,
- O Governo e
- Judiciário

O Presidente da República é o Chefe de Estado (art. 62º) e o Primeiro-Ministro é o Chefe de Governo (art. 97º) da Constituição da Guiné-Bissau. O poder executivo é detido pelo Governo, enquanto o poder legislativo é detido pela Assembleia Nacional Popular. O poder judicial é independente dos poderes executivo e legislativo.

A Guiné-Bissau é um Estado democrático com um sistema semi-presidencial.

A Guiné-Bissau, desde a sua independência, tem sido marcada por acontecimentos que têm provocado instabilidade política no país.

- **O Presidente da República (PR)** tem o poder de nomear e demitir o Primeiro-Ministro, o Presidente do Tribunal de Contas, o Procurador-Geral da República, o Chefe das Forças Armadas, promulgar ou vetar leis, dissolver o Parlamento, etc.

  O Presidente da República é eleito por sufrágio direto (art. 63º) para um mandato, renovável uma vez, de cinco anos (art. 66º), o PR tem sempre, na Guiné-Bissau, uma legitimidade democrática indiscutível.

- **O Governo** é chefiado pelo Primeiro-Ministro. O PR tem o poder de nomear e demitir o Primeiro-Ministro, tendo em conta os resultados das eleições, após ouvir as opiniões das forças políticas representadas na Assembleia Nacional Popular.

  Os restantes membros do Governo são nomeados ou exonerados pelo PR sob proposta do Primeiro-Ministro (art. 68.º).

- **A Assembleia Nacional** Popular é o órgão supremo de legislação e de controlo político que representa todos os cidadãos guineenses. Decide sobre todas as questões fundamentais da política interna e externa do Estado. (Ref. artigo 76.ºda Constituição).

Como mencionado no artigo 85.º,a Assembleia Nacional Popular tem o poder de aprovar moções de confiança ou de censura ao Governo. A não aprovação de uma moção de confiança ou a aprovação de uma moção de censura, por maioria absoluta, implica a demissão do Governo.

De acordo com o artigo 81.ºda Constituição, um deputado tem o direito de apresentar inquéritos ao Governo, oralmente ou por escrito, e deve receber uma resposta em sessão ou no prazo de 15 dias, por escrito, se forem necessárias mais investigações.

De acordo com o artigo 94.ºda Constituição, a Assembleia Nacional Popular não pode ser dissolvida nos doze meses seguintes ao ato eleitoral, nos últimos seis meses do mandato do PR, nem durante o estado de sítio ou o estado de emergência. A dissolução da Assembleia Nacional Popular não impede os deputados de continuarem o seu mandato até à abertura da legislatura após as novas eleições.

O artigo 95ºestabelece que: "Entre legislaturas e durante o período de dissolução da Assembleia Nacional Popular, funcionará uma Comissão Permanente da Assembleia Nacional Popular. A Comissão Permanente é presidida pelo Presidente da Assembleia Nacional Popular e composta pelo Vice-Presidentes e pelos representantes dos partidos políticos com assento na Assembleia Nacional Popular, de acordo com a sua representação.

A Comissão Permanente é competente para:

- Acompanhar todas as atividades do Governo e da Administração.
- Exercer os poderes da Assembleia Nacional Popular em relação ao mandato dos

deputados.

- Convocar a Assembleia Nacional Popular sempre que necessário.
- Preparar a abertura das sessões parlamentares.
- Comentar qualquer imposição de lei marcial ou declaração de estado de emergência.

A Comissão Permanente é responsável e responde por todas as suas actividades perante a Assembleia Nacional Popular.

- **O Poder Judiciário** é o órgão central responsável pela aplicação das leis que regem o comportamento da sociedade. Esse poder é essencial em qualquer Estado democrático e de direito. O Poder Judiciário é um poder que desempenha o papel fundamental de mediador entre os que governam (o governante) e os que legislam (a assembléia).

Tal como consta no artigo 59ºda Constituição da Guiné-Bissau, a organização do poder político assenta na separação e interdependência dos órgãos de soberania e na subordinação de todos à Constituição. Tendo em conta esta interdependência, verifica-se que a Assembleia Nacional Popular é o órgão que pode demonstrar a melhor estabilidade quando consideramos o aspecto da continuidade.

V

Definição do quadro regulamentar

1. Regulamento relativo à cibersegurança e à proteção de dados

A. Estatuto do regulamento

A Constituição da Guiné-Bissau protege o direito à informação e à proteção jurídica (artigo 34.º). Este artigo não menciona a privacidade, mas é bastante genérico. Atualmente, a Guiné-Bissau não dispõe de legislação sobre proteção de dados no seu direito interno, nem de legislação conexa, como a legislação sobre cibercriminalidade ou sobre transacções electrónicas. Existe um projeto em curso para propor o projeto de lei a ser votado e adotado. O projeto de lei está relacionado com o cibercrime.

Para além da Constituição, existe na Guiné-Bissau uma lei penal que data de 1993. Abrange uma vasta gama de actos criminosos, mas não está totalmente adaptada à cibercriminalidade ou às infrações relacionadas com as transacções electrónicas. Contém apenas disposições gerais relativas às atividades fraudulentas e à falsificação[2].

Apesar das leis nacionais em vigor, não existe atualmente qualquer regulamentação que regule a criação de agências de cibersegurança ou de proteção de dados. No entanto, enquanto membro da CEDEAO, a Guiné-Bissau está disposta a seguir as directivas desta instituição regional. A CEDEAO tem orientações claras em termos de cibersegurança e proteção de dados. A diretiva da CEDEAO abrange muitos aspectos, incluindo orientações sobre a organização da instituição, o seu mandato e os regulamentos a serem implementados e aplicados. O nome da diretiva é : ***"Diretiva C/DIR. 1/08/11 relativa à luta contra a cibercriminalidade na Comunidade Económica dos Estados da África Ocidental (CEDEAO)"*** [3]. Esta directiva:

- Indica as infrações especificamente relacionadas com as tecnologias da informação e da comunicação, incluindo o acesso fraudulento, a interferência, a interceção de dados e a modificação de dados;
- Incorpora as infracções tradicionais nas infracções às tecnologias da informação e da comunicação;
- Incentiva a cooperação entre as autoridades nacionais competentes e as autoridades estrangeiras competentes para efeitos de investigações ou processos relativos a infracções que envolvam sistemas ou dados informáticos, bem como para efeitos de recolha de provas, sob forma eletrónica, de uma infração. Esta comunicação deve ser efectuada em conformidade com as regras de transferência de dados pessoais previstas.

Além disso, a Guiné-Bissau assinou a Convenção de Malabo **"Convenção da União Africana sobre Cibersegurança e Proteção de Dados Pessoais"** em 31 de janeiro de 2015[4]. A Convenção de Malabo :

- visa criar um quadro legislativo para a cibersegurança e a proteção dos dados pessoais;
- *exige que os Estados-Membros desenvolvam uma política nacional de cibersegurança e um mecanismo institucional adequado para a governança; legislação e instituições contra a cibercriminalidade; garantia de monitorização e resposta a incidentes e alertas, coordenação nacional e transfronteiriça e cooperação global.*

Existem também algumas convenções mundiais, como a **Convenção de Budapeste,** que estão abertas a todos os países do mundo. A Convenção de Budapeste proporciona um quadro jurídico para a cooperação internacional não só no que diz respeito à cibercriminalidade (crimes contra e através de computadores), mas também no que diz respeito a qualquer crime que envolva provas electrónicas. É mais do que um documento jurídico; ***é um quadro que permite a centenas de profissionais das Partes partilhar experiências e criar relações que facilitam a cooperação*** em casos específicos, incluindo em situações de emergência, para além das disposições específicas previstas na presente Convenção. Qualquer país pode utilizar a Convenção de Budapeste **como diretriz, lista de controlo ou lei-modelo.** Além disso, o facto de se tornar Parte neste Tratado implica vantagens adicionais. Trata-se do acordo internacional mais completo e coerente sobre cibercriminalidade e provas electrónicas até à data. Serve de orientação para qualquer país que desenvolva legislação nacional em matéria de cibercriminalidade e de quadro para a cooperação

2 https://ihl-databases.icrc.org/en/national-practice/penal-code-and-code-criminal-procedure-1993
3 https://www.ecowas.int/member-states/
4 https://au.int/sites/default/files/treaties/29560-sl-AFRICAN_UNION_CONVENTION_ON_CYBER_SECURITY_AND_PERSONAL_DATA_PROTECTION_0.pdf

internacional entre os Estados Partes nesse tratado[5].

B. Conformidade com a legislação nacional e internacional

Atualmente, a Guiné-Bissau não cumpre qualquer legislação nacional ou internacional em matéria de cibersegurança e de proteção de dados. O projeto de lei está em curso.

Existem algumas instituições que tentam assumir as responsabilidades relacionadas com a cibersegurança e a proteção de dados, mas é necessário que sejam mais poderosas e tenham um mandato claro para que o país cumpra ou esteja em vias de cumprir a legislação nacional e internacional.

Na lista das instituições atuais , podemos identificar :

- **Autoridade Reguladora Nacional (ARN-TIC)[6],** uma instituição reguladora independente, que tem como funções colaborar com o Governo na definição das linhas estratégicas das políticas gerais de tecnologias de informação e comunicação, na coordenação da atividade dos operadores de comunicações, incluindo a emissão de pareceres, a elaboração de projectos de legislação e a regulação do sector das tecnologias de informação e comunicação;
- **ITMA** para a digitalização dos serviços do Governo. É uma pessoa colectiva de direito público, criada para operacionalizar a rede privada do Governo e as iniciativas de modernização tecnológica na administração central e local do Estado, reforçando a participação e o envolvimento de diferentes actores e instituições na prestação de serviços públicos. O ITMA é dotado de personalidade jurídica e goza de autonomia administrativa, financeira e patrimonial. O ITMA também trabalha na implementação de políticas de digitalização nos sectores públicos. Aquando da sua criação, o ITMA estava na dependência direta do Primeiro-Ministro. Mas não foi um êxito devido à falta de empenhamento.
- **A Direção Geral de Telecomunicações e Economia Digital (DGTED),** tal como mencionado no entregável 1 deste projeto, é responsável por propor directivas ao ministério que podem ser apresentadas ao conselho de ministros e seguidas até à assembleia nacional para serem votadas como lei. Para conhecer as directrizes correctas a propor ao ministério, a DGTED participa em conferências, debates com países terceiros e outras instituições. A DGTED também recebe directivas do seu ministério de tutela para os aspectos políticos relacionados com o programa de governo. Assegura-se de partilhar-las com as organizações operacionais, como a ITMA, a ARN e outras entidades que não interessam a este estudo. Na ausência de um modelo de governança estruturado, a DGTED cobre parcialmente alguns aspectos da cibersegurança. Mas não abrange todos os aspectos da governança de cibersegurança e de proteção de dados.

C. Integração das disposições legais de acordo com o contexto da Guiné-Bissau

O projeto de lei está em vias de ser apresentado à ANP. De acordo com a Constituição da Guiné-Bissau, para que uma lei seja posta em prática, como mencionado no mandato da Assembleia Nacional Popular no artigo 85 da Constituição da Guiné-Bissau, um projeto de lei deve ser submetido à Assembleia Nacional Popular para votação dos deputados.

D. Definição dos tipos de colaborações internacionais

A Guiné-Bissau participa em alguns fóruns sobre cibersegurança. Mas como as entidades de cibersegurança e de proteção de dados não estão criadas, a participação da Guiné-Bissau em alguns debates ou a partilha de informações entre países ou partes interessadas não estão estruturadas. As convenções ou diretivas regionais ou internacionais explicam as regras de colaboração entre os seus membros. As agências que serão criadas a partir deste relatório devem tirar partido disso.

E. Definição dos processos de controlo das leis e políticas

A polícia judiciária está habilitada a receber quei-

5 https://rm.coe.int/cyber-buda-benefits-2024-july-2789-5929-5498-v-1/1680b0d659
6 https://arn.gw/activeapp/wp-content/uploads/2015/03/3.-%c2%a6SUP.-B.-O.-N.-%c2%a6-21-2010.pdf

xas e a efetuar investigações. Uma vez provada a existência de uma infração, o caso é remetido aos tribunais, que podem aplicar a lei e aplicar as medidas punitivas previstas na lei. Tal como previsto no CAPÍTULO VII da Constituição da Guiné-Bissau, enquanto um dos quatro órgãos de soberania, o poder judicial é responsável pela aplicação da lei quando necessário.

F. Quadro regulamentar para a criação de agências

Para que uma agência seja criada, é obrigatório que exista uma lei que imponha a criação da agência e o seu mandato. Esta lei identificará claramente o âmbito da agência e as obrigações das entidades públicas e privadas. A lei explicará como será aplicada a autonomia da agência.

VI

Definição do organograma e da arquitetura da Agência

O organigrama e a arquitetura da Agência Nacional de Cibersegurança e Proteção de Dados são cruciais para estabelecer um quadro claro e eficaz que delineia as funções, responsabilidades e relações hierárquicas dentro da agência. Ao ilustrar a cadeia de comando, os processos de tomada de decisão e a distribuição de tarefas, o organigrama facilita a transparência e a responsabilização.

No primeiro entregável deste projeto, recomendamos à Guiné-Bissau o modelo híbrido de governança da cibersegurança e da proteção de dados. O objetivo é ter uma estrutura que possa permitir a continuidade mesmo em caso de grande mudança na visão política do país. Este modelo, mesmo que seja a melhor abordagem com base na nossa análise do contexto da Guiné-Bissau, tem os seus desafios. Os desafios incluem a falta de recursos e a complexidade da estrutura se esta não for implementada de acordo com o nível de maturidade do país em matéria de cibersegurança e proteção de dados. A maturidade aqui pode ser vista como o número de recursos técnicos disponíveis para cumprir o mandato das agências, o nível de consciencialização das partes interessadas públicas e privadas, o número de infra-estruturas críticas e a sua dimensão, a flexibilidade do orçamento, entre outros.

Conscientes dos desafios, propomos a implementação de um modelo híbrido sob a forma de um roteiro.

- Nos primeiros dois anos, recomendamos a implementação de duas agências principais:
  - → Uma agência/autoridade para a proteção de dados
  - → Uma agência para a cibersegurança

- Durante os primeiros dois anos, deve ser concluída a avaliação de todos os ativos críticos da Guiné-Bissau. Todos os ativos serão categorizados com base na sua criticidade e domínio de atividade.
- Todas as organizações públicas e privadas devem receber formação para reconhecer os riscos e as suas responsabilidades em matéria de cibersegurança e proteção de dados.
- No terceiro ano, devem ser criadas mais duas agências especializadas para cobrir as recomendações sobre cibersegurança e proteção de dados dirigidas às agências superiores. Com base nesta estrutura, os mandatos das ARN devem ser revistos para abranger também as realidades da cibersegurança e da proteção de dados no seu domínio (serviços de telecomunicações e TIC). Uma vez concluída a avaliação dos ativos críticos, outros domínios podem ser acrescentados às responsabilidades das ARN, como a energia, os transportes, etc. Para além desta nova visão da ARN, pode ser criada outra agência para as finanças, os seguros, a banca, a saúde, etc. Estas agências terão um mandato semelhante ao da ARN, mas serão especializadas de acordo com as realidades do seu domínio. Em função da avaliação, do carácter crítico e do número de domínios, o número de agências satélite pode ser revisto.

Uma vez que a proposta das agências especializadas dependerá da avaliação e de outros contributos que ainda não foram efectuados e que não fazem parte do presente mandato, na secção seguinte serão apresentadas em pormenor as duas primeiras agências principais que constituirão o núcleo de toda a estratégia:

- A Agência Nacional de Proteção de Dados
- A Agência Nacional de Cibersegurança

1. Agência Nacional de Proteção de Dados

O comprometimento de dados pessoais pode levar a perturbações significativas tanto para os indivíduos como para as empresas envolvidas. Com a migração de quantidades crescentes de dados para sistemas informáticos e dispositivos electrónicos, é necessário proteger estes sistemas e salvaguardar os dados dos indivíduos contra roubo e utilização indevida. A confiança é essencial para uma economia e sociedade baseadas em dados. Para construir um ecossistema de dados de confiança, as nossas organizações têm de passar da conformidade para a responsabilidade. Os dados pessoais dos cidadãos devem ser mantidos com precisão e protegidos por uma agência executiva.

No entanto, até agora, na Guiné-Bissau, não existe uma autoridade de proteção de dados, um órgão regulador ou uma organização responsável pela proteção das informações pessoais e por garantir que as entidades governamentais e as empresas cumpram as leis de proteção de dados.

A. Responsabilidades da agência de proteção de dados

A futura autoridade de proteção de dados a criar será :

- **Trabalhar com as organizações para que adotem a proteção de dados como parte da sua cultura empresarial :**

  Um ecossistema de dados fiável e sólido promove a confiança e a inovação. Para ajudar as organizações a promover a confiança e a adotar uma mentalidade de responsabilidade, a Agência de Proteção de Dados desenvolverá um Programa de Gestão da Proteção de Dados para ajudar as organizações a adotar a proteção de dados como parte da sua cultura empresarial. São necessários processos sólidos de proteção de dados para que as organizações possam utilizar melhor os dados. Para tal, as organizações devem adotar uma abordagem de "proteção de dados desde a conceção", que considera a proteção de dados como uma consideração fundamental nas fases iniciais do desenvolvimento de qualquer produto ou serviço.
  O rigor deste quadro também exigirá que as empresas realizem uma avaliação do impacto da proteção de dados como parte da conceção, implementação e revisão de sistemas, aplicações e processos empresariais.

- **Trabalhar para implementar programas personalizados de sensibilização para a proteção de dados:**

  Um dos objectivos de uma agência de proteção de dados é implementar programas personalizados de sensibilização para a proteção de dados. Estes programas educam e capacitam vários intervenientes, garantindo que compreendem e cumprem os regulamentos de proteção de dados. A importância destes programas reside na sua capacidade de reduzir o risco de violações de dados e melhorar a postura geral de segurança, abordando lacunas de conhecimento específicas e vulnerabilidades exclusivas de diferentes segmentos de público. Para tal, a agência efectua avaliações exaustivas das necessidades, concebe conteúdos adaptados e utiliza diversos métodos de ensino, como o e-learning, workshops e campanhas públicas. A agência atualizará continuamente os programas com base no feedback e nas ameaças emergentes e, em seguida, garantirá que todos os participantes estejam equipados com os conhecimentos mais recentes e as melhores práticas em matéria de proteção de dados.

- **Trabalhar num processo de autorização de tratamento de dados :**

  A Agência Nacional de Proteção de Dados será responsável pela emissão, controlo e revogação das autorizações para a recolha de dados pessoais por entidades públicas ou privadas. Em caso de incumprimento, serão tomadas medidas, incluindo a eventual revogação da autorização.

- **Profissionalizar os responsáveis pela proteção de dados para apoiar a aplicação eficaz das medidas de proteção de dados :**

  A Agência desenvolverá um quadro de competências em matéria de proteção de dados para desenvolver os Responsáveis pela Proteção de Dados (RPD) como uma carreira profissional dedicada a supervisionar os requisitos de proteção de dados das organizações. Este quadro garantirá que os responsáveis pela proteção de dados disponham das aptidões, competências e certificações necessárias para o desempenho das suas funções.

Reforçar a posição da Guiné-Bissau como centro de dados fiável, introduzindo marcas de confiança para a proteção de dados e trabalhando com as autoridades estrangeiras de proteção de dados para facilitar os fluxos de dados transfronteiriços:

A agência irá desenvolver um quadro de referência, um sistema de marcas de confiança de proteção de dados para certificar os processos de proteção de dados das organizações. As marcas de confiança irão aumentar a conformidade e reforçar a posição da Guiné-Bissau como um centro de dados de confiança. Assim, o país obterá vantagens significativas, incluindo o crescimento económico através do aumento do investimento estrangeiro, da criação de emprego e da inovação tecnológica. Este estatuto reforçará também uma reputação global, atraindo empresas multinacionais e promovendo a confiança do público. Irá, sem dúvida, impulsionar o crescimento sustentável da economia digital.

Para garantir uma proteção de dados sólida, é essencial ter uma estrutura de agência bem organizada e eficiente. A seguir, apresentamos uma visão geral da futura agência com base na nossa análise.

B. Estrutura da agência e vantagens da nossa escolha

Num contexto bissau-guineense de Estado democrático com um regime semipresidencial caracterizado por uma instabilidade política frequente e recursos limitados, propomos uma estrutura supervisionada pela Assembleia Nacional Popular que assegura uma supervisão estratégica global. O Conselho de Administração, composto por representantes do Governo, um perito independente e membros do sector privado, supervisionará as atividades da agência.

O diretor-geral dirigirá a ANPD. Será apoiado pelos directores de Regulação e Conformidade, Operações e Execução, e Formação e Sensibilização. Cada um dos diretores terá a sua força de trabalho composta por peritos técnicos, especialistas e técnicos.

A colocação da Assembleia Nacional Popular (ANP) como autoridade supervisora da Agência Nacional de Proteção de Dados (ANPD) garante uma maior responsabilização e transparência através de relatórios e auditorias regulares, protege a ANPD de influências políticas e fornece apoio legislativo e financeiro. Esta estrutura promove a eficiência operacional com linhas claras de autoridade e unidades especializadas, e assegura a melhoria contínua através de iniciativas de reforço de capacidades e formação. De um modo geral, permite que a ANPD. funcione de forma eficaz, transparente e independente, o que é crucial num ambiente politicamente instável.

O organograma abaixo descreve a estrutura da Agência Nacional de Proteção de Dados, criada para salvaguardar a privacidade dos dados em todo o país.

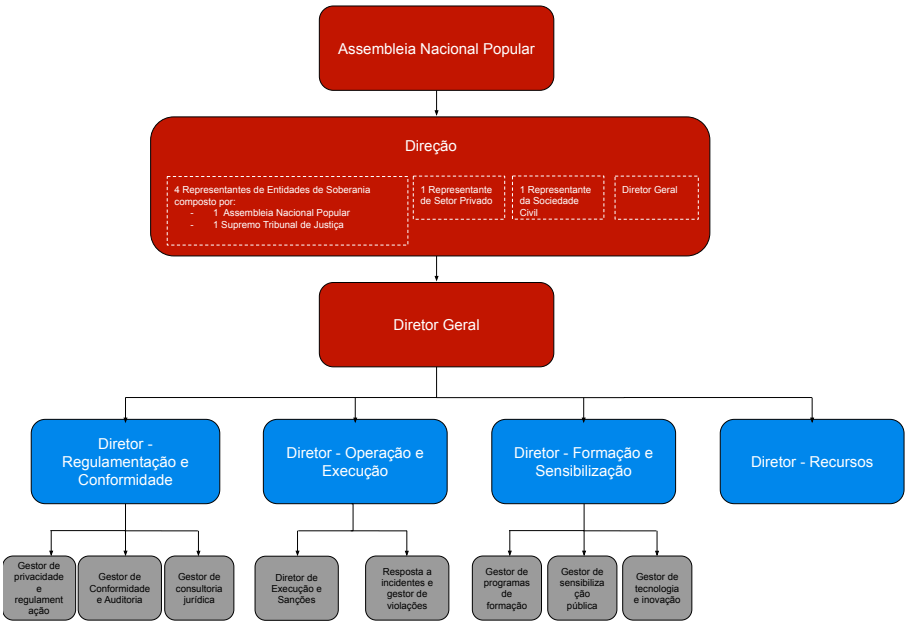

Figura 01: Organograma da agência de proteção de dados

C. Definir os principais departamentos e as suas funções e práticas operacionais

A agência é dirigida por um Diretor-Geral, que é apoiado por três Directores de Departamento Técnico, cada um responsável por áreas operacionais específicas: Regulamentação e Conformidade, Operações e Execução, e Formação e Sensibilização.

- **A Assembleia Popular Nacional:** A ANP assegura o alinhamento com as políticas nacionais e as normas internacionais. As responsabilidades da ANP incluem a supervisão estratégica, a proteção da ANPD contra influências políticas e a garantia de transparência através de relatórios e auditorias regulares. Desempenha um papel crucial no apoio legislativo, desenvolvendo e alterando leis de proteção de dados e aprovando o orçamento da ANPD. para garantir que a agência dispõe de recursos adequados. A ANPD também assegura a eficiência e a eficácia operacionais, mantendo linhas de autoridade claras e apoiando iniciativas de reforço de capacidades para promover a melhoria contínua das práticas de proteção de dados.

- **O Conselho de Administração**

  O Conselho de Administração é composto por 5 membros, incluindo o Diretor-Geral, que é nomeado por defeito. Os outros 4 membros são :

  - 1 membro do sector judiciário
  - 1 membro da Assembleia Nacional Popular
  - 1 representante do sector privado (Câmara de Comércio, instituições financeiras, instituições de TIC, instituições de saúde, etc.);
  - 1 representante da sociedade civil.

  O Conselho de Administração é composto por :

  - Um Presidente
  - Um vice-presidente
  - Um secretário
  - Um Tesoureiro

  O Conselho de Administração é composto por vários comités cujo papel consiste em realizar tarefas específicas ou fazer recomendações ao Conselho de Administração para aprovação. Estes comités incluem :

  - Um Comité Executivo
  - Um Comité de Auditoria e Finanças
  - Um Comité de Recursos Humanos

  As decisões do conselho de administração serão validadas por um quórum. O requisito de quórum promove uma governança inclusiva e transparente, assegurando que as decisões reflectem os interesses e as competências de todos os sectores envolvidos. Para aprovar uma decisão, deve ser convocada uma assembleia ordinária ou extraordinária. Para que a assembleia seja válida, o quórum deve ser respeitado. Para ter quórum, devemos ter pelo menos 3 pessoas do conselho de administração presentes e prontas para votar. Estas 3 pessoas devem conter pelo menos :

  - 1 dos dois órgãos de soberania membros E
  - 2 dos 3 membros não pertencem a órgãos de soberania

  O Conselho de Administração é responsável pelo planeamento estratégico, definindo objetivos e estratégias a longo prazo para a agência. Monitoriza o desempenho da agência através de análises regulares, assegurando que são feitos os ajustamentos necessários para atingir os objectivos. Assegura que a agência funciona de forma aberta e responsável, mantendo a confiança do público e das partes interessadas. O conselho de administração é responsável pela coordenação do processo de contratação do diretor-geral. Para o efeito, recorrerá aos serviços de uma empresa de recrutamento independente.

- **Diretor Geral:**

  O diretor-geral é responsável pela tomada de decisões de alto nível, pelo envolvimento das partes interessadas e pela colaboração internacional.

  O diretor-geral é responsável pela tomada de decisões de alto nível, pelo envolvimento das partes interessadas e pela colaboração internacional. O diretor-geral é responsável pela liderança estratégica e pela direção geral da agência, assegurando a aplicação da legislação e das políticas em matéria de proteção de dados. O

diretor-geral é responsável pela não realização dos objectivos em matéria de cibersegurança. Apresenta relatórios regulares ao Conselho de Administração para o manter informado sobre as atividades da agência, os progressos e os desafios enfrentados, assegurando o alinhamento com os objetivos estratégicos.

- **Diretor - Regulamentação e Conformidade**
  A principal função do Diretor de Regulamentação e Conformidade é gerir o desenvolvimento de políticas de proteção de dados, quadros de conformidade e atividades de consultoria jurídica. Esta função implica liderar a criação e a revisão de políticas e regulamentos de proteção de dados, prestar aconselhamento jurídico sobre questões de proteção de dados e controlar a conformidade com as leis e os regulamentos em matéria de proteção de dados:

  → **Divisão de Política e Regulamentação:** esta divisão desenvolve e atualiza leis, regulamentos e orientações em matéria de proteção de dados. Redige legislação, colabora com as partes interessadas para recolher contributos e garante que as leis nacionais estão em conformidade com as normas internacionais (por exemplo, Regulamento Geral sobre a Proteção de Dados (RGPD), Quadro de Privacidade da OCDE, Convenção 108+ - Conselho da Europa, etc.). Esta unidade efectua revisões regulares das políticas para manter as leis actualizadas em relação às tendências e ameaças emergentes.

  → **Divisão de Conformidade e Auditoria:** esta divisão controla e reforça o cumprimento da legislação em matéria de proteção de dados e realiza auditorias regulares. Realiza auditorias, analisa relatórios de conformidade e oferece orientação às organizações para as ajudar a cumprir as leis de proteção de dados.

  → **Consultoria jurídica:** esta divisão presta apoio e aconselhamento jurídico em questões de proteção de dados, trata de litígios jurídicos e garante que as ações da agência são juridicamente sólidas e coerentes. Esta divisão também apoia a aplicação da legislação em matéria de proteção de dados.

- **Diretor - Funcionamento e Execução**
  O Diretor de Funcionamento e Execução irá gerir as atividades de execução e a resposta operacional às violações de dados. Assegurará que as violações da legislação em matéria de proteção de dados sejam tratadas de forma eficaz; coordenará a resposta da agência a incidentes de violação de dados e assegurará uma gestão operacional eficaz e eficiente:

  → **Divisão de Aplicação e Sanções:** Esta divisão aplica a legislação em matéria de proteção de dados e impõe sanções em caso de incumprimento. Esta unidade conduzirá investigações sobre potenciais violações da legislação em matéria de proteção de dados. Haverá dois tipos de sanções em caso de violação da regulamentação em matéria de proteção de dados, nomeadamente sanções administrativas e sanções penais.

  As sanções administrativas podem incluir :

  - **Coimas:** podem ser impostas sanções pecuniárias às organizações que violem os regulamentos relativos à proteção de dados. Estas coimas podem ser substanciais, dependendo da gravidade e da natureza da violação. Podem representar uma percentagem das vendas ou ser determinadas de outra forma.
  - **Advertência:** podem ser emitidas advertências ou repreensões oficiais a organizações ou indivíduos por incumprimento ou infracções menores, como a não comunicação de incidentes relacionados com dados privados ou outros.
  - **Suspensão temporária das actividades:** suspender temporariamente certas actividades de tratamento de dados até que a conformidade seja alcançada
  - **Ordens de correção:** ordens para tomar medidas específicas para remediar violações, tais como melhorar as medidas de segurança dos dados ou

retificar atividades de tratamento de dados impróprias.

- **Revogação de licenças ou certificações:** para as organizações que necessitam de licenças ou certificações específicas para funcionar, estas podem ser revogadas em caso de incumprimento grave.
- **Publicidade da sanção:** a publicidade das sanções pode ter um efeito dissuasor e pode prejudicar a reputação da organização infratora.

As sanções penais podem incluir :

- **Ações judiciais:** podem ser instauradas ações judiciais contra pessoas ou organizações por infracções graves, que podem dar origem a registos criminais.
- **Prisão:** em casos graves, as pessoas responsáveis por violações graves da legislação em matéria de proteção de dados podem ser condenadas a pena de prisão.

→ **Resposta a incidentes e gestão de violações :** A unidade de resposta a incidentes e gestão de violações será responsável pela gestão das violações de dados que envolvam informações pessoais. Esta unidade assegura que as violações são tratadas de forma rápida e eficaz para proteger a privacidade dos indivíduos, cumprir os requisitos legais e mitigar quaisquer danos causados pela violação. Esta divisão assegura que os incidentes são tratados rapidamente para minimizar os danos, restabelecer as operações normais e prevenir futuras ocorrências. A unidade colabora com os departamentos internos (jurídico, comunicações...) e entidades externas (reguladores, Polícia Judiciária, peritos de terceiros) para assegurar uma resposta coordenada. Será composta por equipas especializadas, tais como equipas de deteção de violações, equipas de resposta a incidentes, equipas forenses, equipas de notificação e de remediação.

- **Diretor - Formação e Sensibilização**

O Diretor de Formação e Sensibilização é responsável pelo desenvolvimento e apresentação de programas de formação abrangentes sobre proteção de dados. Estes programas incluem workshops, seminários e campanhas de sensibilização do público concebidos de acordo com o contexto da Guiné-Bissau para educar várias partes interessadas sobre as melhores práticas em matéria de proteção de dados.
O papel também envolve a promoção da inovação tecnológica através da investigação e implementação de novas tecnologias para melhorar as capacidades da agência.
Esta melhoria contínua ajuda a agência a manter-se à frente das ameaças emergentes e a manter normas sólidas de proteção de dados.

→ **Divisão de programas de formação:** esta divisão é responsável pelo desenvolvimento, implementação e manutenção de programas de formação abrangentes destinados a melhorar as práticas de proteção de dados entre as várias partes interessadas.
Esta unidade garante que os funcionários, as organizações e os grupos profissionais específicos estão bem informados sobre os regulamentos de proteção de dados, as melhores práticas e as últimas tendências neste domínio. Serão realizados programas de formação actualizados regularmente para refletir os últimos desenvolvimentos em matéria de proteção de dados e cibersegurança
Esta unidade também desenvolverá um quadro de competências em matéria de proteção de dados para desenvolver os Responsáveis pela Proteção de Dados (RPD) como uma carreira profissional dedicada a supervisionar os requisitos de proteção de dados das organizações. Este será um programa de formação avançada para os profissionais aprofundarem os seus conhecimentos em matéria de proteção de dados.

Seguem-se algumas práticas operacionais para o funcionamento eficaz da divisão:

- Lacuna de competências e análise das partes interessadas: Identificar os diferentes grupos que necessitam de formação e determinar a lacuna de conhecimentos.
- Criação e personalização de conteúdos :

Desenvolver materiais de formação, incluindo apresentações, manuais, módulos de e-learning e vídeos, adaptados a diferentes públicos. Adaptar os conteúdos de formação a sectores e funções específicas para garantir a sua relevância e eficácia.

→ Prestação de formação :

- Implementar plataformas de e-learning para oferecer programas de formação flexíveis e acessíveis.
- Organizar workshops e seminários presenciais ou virtuais para experiências de aprendizagem interactivas.
- Formar indivíduos seleccionados para se tornarem formadores nas suas organizações ou comunidades para expandir o alcance dos programas de formação.

→ Desenvolver um quadro de competências em matéria de proteção de dados

- Divisão de Sensibilização do Público: esta divisão é responsável pela sensibilização do público para as questões da proteção de dados e da privacidade.

Esta unidade assegura que o público em geral seja informado dos seus direitos em matéria de privacidade dos dados e da importância da proteção dos dados através de várias campanhas de sensibilização e iniciativas educativas. Esta unidade trabalhará com várias partes interessadas centradas em diferentes aspectos da sensibilização do público. Por exemplo, os meios de comunicação social, as escolas e a sociedade civil. Seguem-se algumas práticas operacionais para o funcionamento eficaz da divisão:

→ Criação e personalização de conteúdos :

- Desenvolver conteúdos educativos, tais como brochuras, infografias, vídeos e publicações nas redes sociais.
- Adaptar as mensagens a diferentes grupos demográficos e regiões para garantir a sua relevância e eficácia.

→ Envolvimento da comunidade :

- Envolver-se com as comunidades locais através de reuniões de câmara, workshops e programas escolares.
- Organizar eventos como o Dia da Proteção de Dados, webinars e fóruns públicos para aumentar a sensibilização.
- Colaborar com organizações comunitárias, organizações não governamentais (ONG) e empresas locais para ampliar os esforços de sensibilização.

→ Colaboração e parcerias: trabalhar com outras agências governamentais, o sector privado e organizações internacionais para promover a sensibilização para a proteção de dados e adotar as melhores práticas mundiais em iniciativas de sensibilização do público.

- Divisão de Tecnologia e Inovação: a Divisão de Tecnologia e Inovação é responsável por supervisionar a adoção e implementação de novas tecnologias e soluções inovadoras para melhorar as práticas de proteção de dados na agência e em todo o país. Esta divisão assegura que a agência se mantenha à frente dos desafios emergentes em matéria de proteção de dados, tirando partido das tecnologias de ponta e promovendo uma cultura de inovação contínua. A Divisão implementará tecnologias de ponta para melhorar as capacidades de proteção de dados, tendo em conta o panorama tecnológico e as infra-estruturas específicas da Guiné-Bissau.

Melhorará a capacidade da agência para proteger os dados pessoais e garantir a conformidade com os regulamentos de proteção de dados. A colaboração e a investigação serão também um objetivo fundamental. A Divisão irá estabelecer boas parcerias com os líderes da indústria local e internacional, instituições académicas e organismos internacionais para se manter na vanguarda dos avanços tecnológicos em matéria de proteção de dados.

Abaixo algumas práticas operacionais para o funcionamento eficaz da Divisão:

→ Realizar soluções de prova de conceito para avaliar a viabilidade e a eficácia das novas tecnologias.

→ Realizar investigação contínua para identificar tecnologias e tendências emergentes em matéria de proteção de dados.

- Definição e implementação de iniciativas inovadoras.

- **Direção dos recursos**

  O Departamento de Recursos gere os recursos administrativos, financeiros, humanos e materiais da agência. Assegura que as operações cumprem a legislação e os regulamentos relevantes, apoiando as metas e os objectivos estratégicos globais da agência.

  Para cumprir eficazmente o seu papel multifacetado, o Departamento de Recursos emprega uma série de práticas operacionais concebidas para garantir uma gestão eficiente e a conformidade em todas as áreas de atividade da agência:

  - **Gestão administrativa:** Trata das operações administrativas da agência.
  - **Recursos humanos:** Recrutamento, formação e atividades sociais no estrangeiro. Desenvolve e implementa políticas de recursos humanos para melhorar o desenvolvimento e o bem-estar dos funcionários.
  - **Bens e aquisições:** Gere os ativos e as aquisições da agência, assegurando o acompanhamento e a manutenção adequados. Coordena os projectos logísticos e imobiliários em função dos objectivos estratégicos.
  - **Operações financeiras:** Dirige as atividades financeiras da agência, incluindo a elaboração do orçamento, as operações fiscais e o planeamento financeiro. Assegura o cumprimento dos regulamentos financeiros e prepara as demonstrações financeiras.
  - **Actividades contabilísticas:** Planeia e desenvolve os processos financeiros e contabilísticos da agência em colaboração com a Direção-Geral. Prepara as demonstrações financeiras e gere os orçamentos.
  - **Planeamento de recursos:** Coordena o planeamento e a execução das atividades relacionadas com os recursos financeiros, humanos, materiais e imobiliários. Assegura a utilização eficaz dos recursos em todos os departamentos.
  - **Apoio à governança:** Ajuda na governança, permitindo que a administração geral avalie, dirija e controle os recursos de forma eficaz. Propõe políticas para otimizar a gestão dos recursos.
  - **Conformidade regulamentar:** Assegura que todas as operações cumprem as leis e regulamentos atuais. Gere os assuntos jurídicos, assegura as atividades e prepara os documentos legislativos necessários.
  - **Gestão de documentos e de stocks:** Arquiva documentos administrativos e gere o armazenamento de documentos e materiais, assegurando que os registos estão bem organizados e acessíveis.

D. Definição das fontes de financiamento da Agência

A Agência Nacional de Proteção de Dados (ANPD) recebe normalmente financiamento das dotações orçamentais do Governo. Isto assegura uma fonte de financiamento estável e previsível, permitindo à agência planear e executar projectos a longo prazo.[7]

No entanto, também beneficia de vários outros tipos de financiamento que complementam o seu orçamento e melhoram as suas capacidades operacionais.[8]

Com base no contexto da Guiné-Bissau, eis uma lista das potenciais fontes de financiamento:

- **Coimas e sanções:** Receitas geradas pelas multas e sanções impostas às organizações que violam as leis de proteção de dados. Note-se que o facto de a agência ter o poder de cobrar sanções que se enquadram no seu próprio orçamento pode causar um enviesamento. Mas esta decisão foi tomada porque foi necessário escolher entre este risco e o risco de controlo político. Dado que a autonomia financeira deve ser um dos indicadores-chave de desempenho da agência, aceitamos este risco. No entanto, a aplicação de sanções deve ser controlada e contestada pelos tribunais competentes.
- **Subsídios e donativos:** Apoio financeiro de organizações internacionais, organizações sem fins lucrativos e parceiros do sector privado.
- **Ajuda internacional e assistência ao desenvol-**

7 https://www.dataguidance.com/notes/canada-data-protection-overview
8 https://ico.org.uk/about-the-ico/who-we-are/how-we-are-funded/

vimento: Financiamento de agências de ajuda internacional e programas de desenvolvimento destinados a reforçar a infraestrutura e as capacidades de proteção de dados.

- **Taxas regulamentares e de serviço:** Taxas cobradas às organizações por atividades regulamentares, tais como registo, avaliações de impacto da proteção de dados, licenças e certificações. Também taxas por serviços prestados pela agência, tais como programas de formação, serviços de consultoria e auditorias de proteção de dados.

E. Definir as relações com a entidade de controlo

Com base nos nossos estudos e na análise do contexto guineense, propomos a Assembleia Nacional Popular (ANP) como entidade de referência da Agência Nacional de Proteção de Dados (ANPD). A ANP supervisionará a agência.

A nossa escolha foi guiada pela estrutura organizacional do Estado explicada acima.

É evidente que a Assembleia Nacional Popular terá numerosas responsabilidades em relação ao ANPD. De seguida, apresentamos as principais responsabilidades a considerar e as funções e práticas:

- **Supervisão e orientação estratégica:**

  Responsabilidades da ANP: A ANP fornecerá uma orientação estratégica de alto nível para ajudar a ANPD a enfrentar desafios complexos em matéria de proteção de dados e assegurará que as atividades da ANPD estejam em conformidade com as políticas nacionais de proteção de dados e as melhores práticas internacionais.

  Principais tarefas e práticas :

  - Revisões regulares: Programar revisões semestrais das atividades, estratégias e políticas da ANPD. Compare-as com as políticas nacionais e as normas internacionais, como o RGPD.
  - Avaliação comparativa: Utilizar os quadros internacionais de proteção de dados como referência. Efetuar estudos comparativos para garantir que as políticas da ANPD estão em conformidade com as melhores práticas mundiais.
  - Mecanismo de feedback: Desenvolver um mecanismo de feedback estruturado em que a **ANPD** apresente relatórios pormenorizados sobre os seus esforços de alinhamento. A **ANPD** pode dar feedback e diretivas com base nestes relatórios.
  - Criação de comités consultivos: Formação de um comité consultivo composto por peritos em proteção de dados para fornecer conhecimentos e orientações sobre questões estratégicas.

- **Responsabilidade :**

  Responsabilidades da ANP: A ANP assegura que a ANPD funciona de forma transparente, com relatórios e auditorias regulares. Promove a confiança do público na ANPD, assegurando que esta funciona de forma independente de influências políticas.

  Principais tarefas e práticas :

  - Relatórios anuais: Obrigar a ANPD a apresentar relatórios anuais que detalham as suas atividades, situação financeira e indicadores de desempenho. Estes relatórios devem ser acessíveis ao público.
  - Auditorias públicas: Efetuar auditorias regulares às operações e finanças da ANPD. Publicar os resultados das auditorias para manter a transparência e a confiança do público.
  - Envolvimento do público: Realizar fóruns e consultas públicas para envolver os cidadãos e as empresas nas preocupações com a proteção de dados e no papel da ANPD.

- **Apoio legislativo :**

  Responsabilidades da ANP: Apoiar o desenvolvimento e a alteração das leis de proteção de dados para acompanhar os avanços tecnológicos e as ameaças emergentes Aprovar o orçamento da ANP, assegurando que esta dispõe dos recursos necessários para cumprir o seu mandato.

  Principais tarefas e práticas :

  - **Desenvolvimento legislativo:** Trabalhar com a ANPD para elaborar e atualizar leis de proteção de dados. Isto inclui a realização de avaliações de impacto e a consulta das partes interessadas para garantir que as leis

são relevantes e eficazes.

→ Supervisão financeira: Criar um subcomité de supervisão financeira para controlar as despesas da ANPD e garantir que os fundos são utilizados de forma eficaz e eficiente.

O facto de a Assembleia Nacional supervisionar a Agência de Proteção de Dados ajuda a garantir uma governança sólida em matéria de proteção de dados, que é simultaneamente responsável e fiável. Eis alguns exemplos em que este modelo de governança funciona muito bem:

- No Quénia, o Gabinete do Comissário para a Proteção de Dados (ODPC) responde perante a Assembleia Nacional, o que reforça a transparência e a responsabilidade nas suas operações.
- No Gana, a Comissão de Proteção de Dados (CPD) funciona de forma independente, mas responde perante o Parlamento, garantindo que as suas decisões não sofrem interferências executivas.
- Na Maurícia, o Gabinete de Proteção de Dados (RPD) responde perante a Assembleia Nacional, garantindo que as suas actividades estão em conformidade com as políticas nacionais de proteção de dados.
- No Reino Unido, o Information Commissioner's Office (ICO), o Comissário Federal para a Proteção de Dados e a Liberdade de Informação da Alemanha e muitas outras agências nacionais de proteção de dados respondem perante os respectivos parlamentos.

F. Definir tipos de colaboração multissectorial: com o sector privado e outras agências/entidades governamentais

Para melhorar eficazmente as capacidades de proteção de dados e de cibersegurança, é crucial participar em várias formas de colaboração que potenciem os pontos fortes dos sectores público e privado. Abaixo, exploramos os diferentes tipos de colaborações multi-sectoriais que podem desempenhar um papel vital na consecução deste objetivo.

- **Parcerias Público-Privadas[9]:** Temos de estabelecer uma colaboração para potenciar as competências, a tecnologia e os recursos e criar um canal de comunicação. Por exemplo:
  → Definir acordos que descrevam a forma como os dados podem ser partilhados e protegidos nos diferentes sectores.

G.Definir tipos de cooperações internacionais, programas de intercâmbio

Uma proteção de dados eficaz exige também a cooperação entre as autoridades de proteção de dados a nível internacional e o desenvolvimento de normas transfronteiriças. Deve ser possível dar respostas coordenadas em caso de tratamento transnacional de dados, que se tornou uma realidade omnipresente, e garantir os mesmos direitos a todas as pessoas cujos dados são tratados (as pessoas em causa), independentemente do seu local de residência. A ANPD deve cooperar com organizações internacionais e com as autoridades de controlo de outros países no exterior, a fim de apoiar a aplicação efectiva da lei e partilhar as melhores práticas. Isto será possível trabalhando no âmbito de vários quadros internacionais e promovendo programas e intercâmbios de pessoal.

São possíveis muitos tipos de colaboração internacional:

- **Acordos bilaterais entre países para colaborar em questões de proteção de dados e privacidade.**
  Eis alguns exemplos de colaborações bilaterais:
  → **A República Democrática do Congo (RDC)[10]** e o Ruanda assinaram vários acordos bilaterais, incluindo os que incidem sobre o comércio e a proteção de dados. Estes acordos facilitam a cooperação na partilha de dados, reforçam o apoio mútuo em iniciativas de cibersegurança e promovem normas para a proteção de informações pessoais.
  → **África do Sul e Nigéria[11]:** O acordo abrange elementos de proteção de dados, assegurando que ambos os países colaboram na proteção de dados sensíveis relacionados com investimentos e actividades económicas.
  → **Escudo de proteção da privacidade EUA-UE[12]:** Um acordo entre os Estados Unidos e a União Europeia para facilitar o intercâmbio transatlântico de dados

9 https://www.nationalisacs.org/
10 https://www.trade.gov/
11 https://investmentpolicy.unctad.org/
12 https://ec.europa.eu/info/law/law-topic/data-protection_en

pessoais para fins comerciais

- **Acordos de cooperação entre vários países ou regiões (por exemplo, países da África Ocidental) para estabelecer normas e práticas comuns em matéria de proteção de dados**
  - **Lei Complementar da CEDEAO sobre a Proteção de Dados Pessoais[13]:** A lei exige que os Estados membros da CEDEAO estabeleçam quadros jurídicos nacionais para a proteção de dados pessoais, incluindo a criação de autoridades nacionais de proteção de dados. Define as obrigações dos responsáveis pelo tratamento de dados para garantir a confidencialidade e a segurança dos dados pessoais.
  - **Iniciativa de cibersegurança G7-CEDEAO[14]:** Lançada durante a Presidência alemã do G7 em 2022, esta iniciativa visa reforçar a cibersegurança e a proteção de dados em toda a África Ocidental. O Plano de Ação da CEDEAO (2022-2025) inclui várias medidas para aumentar a ciber-resiliência regional, centrando-se no desenvolvimento de medidas regionais de criação de confiança, no reforço da cooperação e das capacidades cibernéticas e na melhoria do desenvolvimento de competências. Esta iniciativa envolve a colaboração entre os Estados membros da CEDEAO e parceiros internacionais, como o Departamento de Estado dos EUA e o Ministério Federal dos Negócios Estrangeiros alemão.
  - **Convenção da União Africana sobre Cibersegurança e Proteção de Dados Pessoais (Convenção de Malabo):** Embora mais abrangente do que apenas a África Ocidental, a Convenção de Malabo, adoptada pela União Africana em 2014, procura harmonizar as leis de proteção de dados e cibersegurança em todo o continente africano. A convenção estabelece princípios e medidas para a proteção de dados pessoais, a segurança das transacções electrónicas e o combate à cibercriminalidade. Incentiva os Estados membros a estabelecer quadros jurídicos e a cooperar em questões de cibersegurança. Ao tirar partido destas parcerias internacionais, a Guiné-Bissau pode criar quadros de proteção de dados mais fortes que se alinham com as melhores práticas globais, garantindo a segurança e a privacidade dos dados pessoais além-fronteiras.
- Participação em organizações e conferências internacionais: O envolvimento com organizações internacionais e a participação em conferências importantes melhorará significativamente as capacidades de proteção de dados da Guiné-Bissau. Estas plataformas fornecem acesso às melhores práticas globais, facilitam a cooperação internacional e ajudam a alinhar os quadros nacionais de proteção de dados com as normas internacionais. Eis uma lista não exaustiva de quadros de cooperação internacional que trabalham em questões de privacidade e proteção de dados, com os quais a APDN da Guiné-Bissau poderia trabalhar:
  - **Assembleia Mundial da Proteção da Vida Privada[15] (também conhecida por Assemblée mondiale pour la protection de la vie privée) :** A Assembleia Mundial para a Proteção da Vida Privada (Global Privacy Assembly - GPA), anteriormente conhecida como Conferência Internacional dos Comissários para a Proteção da Vida Privada e dos Dados (ICDPPC), é um fórum anual onde as autoridades de proteção de dados e da vida privada de todo o mundo se reúnem para debater questões emergentes, partilhar boas práticas e colaborar em iniciativas de proteção de dados.
  - **Convenção do Conselho da Europa para a Proteção das Pessoas relativamente ao Tratamento Automatizado de Dados de Carácter Pessoal (Convenção 108):** A Convenção 108 é um tratado internacional de referência que estabelece um quadro para a proteção de dados e da privacidade.

    Está aberta à adesão de países europeus e não europeus.

    A adesão à Convenção 108 ajudará a Guiné-Bissau a alinhar as suas leis de proteção de dados com as normas internacionais e facilitará os fluxos de dados transfronteiriços.
  - **Grupo de Trabalho da OCDE sobre**

13 https://dig.watch/resource/suplementary-act-personal-data-protection-within-ecowas#:~:text=The%20act%20asks%20ECOWAS%20member,and%20use%20of%20personal%20data & https://ictpolicyafrica.org/es/document/z69cbq7b51?page=10
14 https://www.ecowas.int/
15 https://globalprivacyassembly.org/ & https://www.edpb.europa.eu/our-work-tools/support-cooperation-and-enforcement/international-cooperation-cooperation-other_en

Governança de Dados e Privacidade (DGP) : O DGP da OCDE desenvolve políticas e orientações sobre governança de dados e privacidade. Constitui um fórum de diálogo e cooperação internacional sobre questões de proteção de dados. Ao participar no fórum, o país beneficiará de debates políticos de alto nível e terá acesso a recursos para melhorar os seus quadros de proteção de dados.

- **Cimeira Africana de Proteção de Dados[16]:** A participação proporcionará uma plataforma para a Guiné-Bissau partilhar experiências, aprender as melhores práticas e colaborar em iniciativas regionais de proteção de dados.
- **Cimeira Global sobre a Privacidade da Associação Internacional de Profissionais da Privacidade (IAPP):** Estes eventos ajudarão os profissionais da proteção de dados a manterem-se actualizados sobre os desenvolvimentos globais e a estabelecerem contactos com peritos internacionais.
- **Fórum sobre a Governança da Internet (IGF):** A Agência Nacional de Proteção de Dados da Guiné-Bissau pode contribuir para os debates mundiais sobre a governança da Internet e a proteção de dados e aprender com eles.

2. Agência Nacional de Cibersegurança

A criação de uma Agência Nacional de Cibersegurança reflete o compromisso estratégico de salvaguardar as infra-estruturas digitais e críticas do país. Esta agência desempenhará um papel crucial no desenvolvimento e na aplicação de políticas abrangentes de cibersegurança, na resposta a ameaças e incidentes e na promoção de uma cultura de sensibilização e resiliência em matéria de cibersegurança em todos os sectores da sociedade. Implicará igualmente a regulamentação dos proprietários de infra-estruturas críticas de informação no que respeita às actividades de cibersegurança, bem como a supervisão dos prestadores e profissionais de serviços de cibersegurança. Além disso, estabelecerá plataformas de participação intersectorial para facilitar a coordenação e a cooperação eficazes entre as principais instituições públicas e o sector privado.

Dada a nossa decisão de implementar um modelo híbrido de governança da cibersegurança na Guiné-Bissau, é importante delinear como a Agência Nacional de Cibersegurança funcionará dentro deste modelo; combinando a coordenação centralizada com a execução descentralizada.

- **Coordenação centralizada:** A agência coordenará de forma centralizada as políticas, estratégias e planos de resposta a incidentes de cibersegurança através da Direção-Geral e do Departamento de Estratégia e Política. Isto garante a coerência e o alinhamento com os objectivos nacionais.
- **Implementação descentralizada:** Os departamentos operacionais e as unidades especializadas implementarão estas políticas e responderão a incidentes em diferentes regiões e sectores. Isto permite respostas adaptadas às ameaças locais e o aproveitamento das competências locais.

Esta abordagem dupla garante flexibilidade, resiliência e uma cobertura abrangente do panorama da cibersegurança do país, respondendo eficazmente às ciberameaças nacionais e localizadas.

A. Estrutura da agência e vantagens da nossa escolha

A Agência Nacional de Cibersegurança foi concebida para funcionar eficazmente no quadro de um regime semi-presidencial, sob a supervisão do Gabinete do Primeiro-Ministro. A agência será dirigida por um diretor-geral, que responde perante um conselho de administração composto por representantes do governo, do sector privado e da sociedade civil.

O Conselho de Administração assegura que as estratégias e ações da agência estão alinhadas com as prioridades e interesses nacionais.

A agência será composta por vários departamentos operacionais e unidades especializadas, cada um com funções específicas essenciais para a cibersegurança nacional.

O organograma abaixo descreve a estrutura da Agência Nacional de Cibersegurança, criada para garantir um ecossistema digital seguro e resiliente.

16 https://dataprotectionafrica.org/

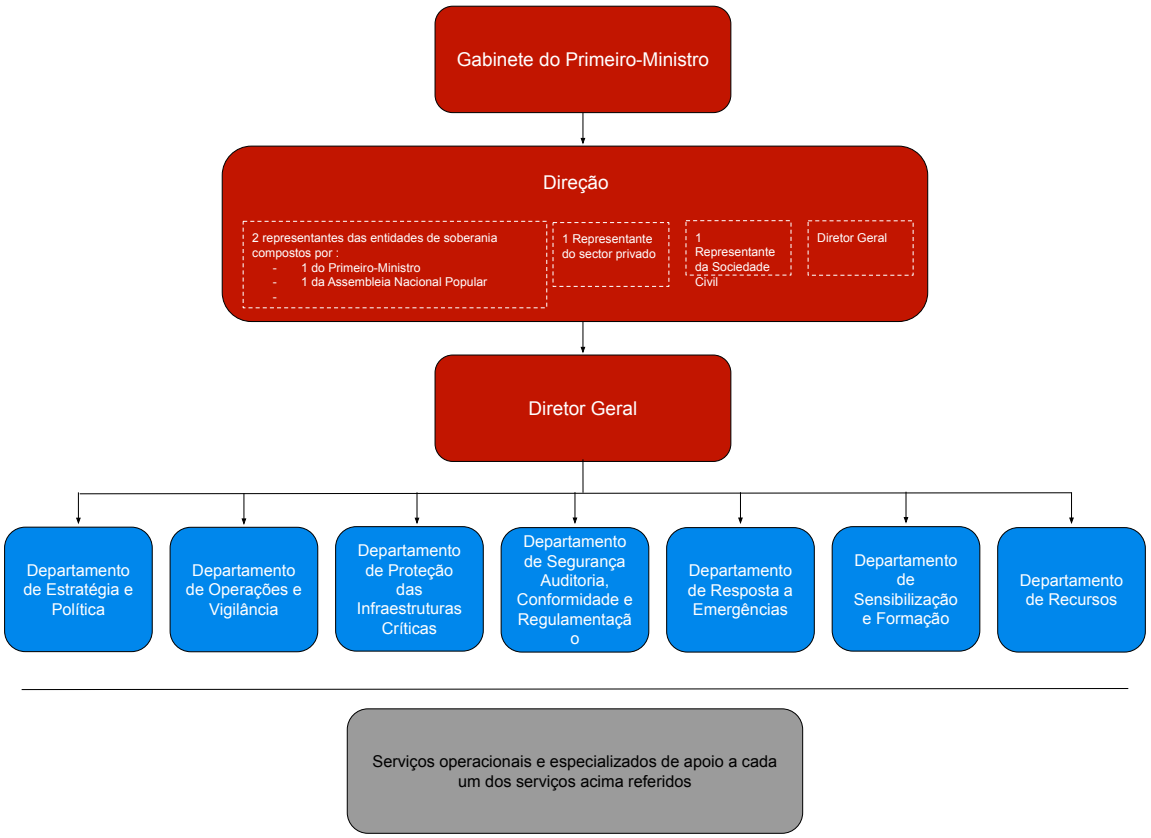

Figura 02 : Organograma da agência de cibersegurança

B. Definir os principais departamentos e as suas funções e práticas operacionais

A agência é dirigida por um diretor-geral, que é apoiado por sete diretores de departamento, cada um responsável por áreas operacionais específicas.

- **O Gabinete do Primeiro-Ministro :**

O Gabinete do Primeiro-Ministro (PMO) é o órgão **executivo** central do regime semi-presidencial da Guiné-Bissau, com responsabilidades que incluem o apoio ao Primeiro-Ministro na coordenação das políticas e ações do Governo. O PMO assegura que as estratégias e decisões de vários ministérios e agências governamentais estão em conformidade com a visão do Primeiro-Ministro e as prioridades nacionais. Especialmente no contexto da cibersegurança, desempenhará um papel crucial de supervisão, fornecendo direção estratégica, orientação política e supervisão de alto nível para garantir que as atividades da agência estão alinhadas com as prioridades de segurança nacional. O PMO também aprova o orçamento da agência, mobiliza recursos adicionais e avalia o desempenho da agência, garantindo a responsabilização e a transparência. Este envolvimento de alto nível garante que a Agência Nacional de Cibersegurança funcione com a autoridade e o apoio político necessários

- **O Conselho de Administração**

O Conselho de Administração é composto por 5 membros, incluindo o Diretor-Geral, que é nomeado por defeito. Os outros 4 membros são :

- 1 membro do Primeiro-Ministro
- 1 membro da Assembleia Nacional Popular
- 1 representante do sector privado (Câmara de Comércio, instituições financeiras, instituições de TIC, instituições de saúde, etc.);
- 1 representante da sociedade civil.

O Conselho de Administração é composto por :

- Um Presidente
- Um vice-presidente
- Um secretário

→ Um Tesoureiro

O Conselho de Administração é composto por vários comités cujo papel consiste em realizar tarefas específicas ou fazer recomendações ao Conselho de Administração para aprovação. Estes comités incluem :

→ Um Comité Executivo
→ Um Comité de Auditoria e Finanças
→ Um Comité de Recursos Humanos

As decisões do conselho de administração serão validadas por um quórum. O requisito de quórum promove uma governança inclusiva e transparente, assegurando que as decisões reflectem os interesses e as competências de todos os sectores envolvidos. Para aprovar uma decisão, deve ser convocada uma assembleia ordinária ou extraordinária. Para que a assembleia seja válida, o quórum deve ser respeitado. Para ter quórum, devemos ter pelo menos 3 pessoas do conselho de administração presentes e prontas para votar. Estas 3 pessoas devem conter pelo menos :

- 1 dos dois órgãos de soberania membros
- 2 dos 3 membros não pertencem a órgãos de soberania

O Conselho de Administração é responsável pelo planeamento estratégico, definindo objetivos e estratégias a longo prazo para a agência. Monitoriza o desempenho da agência através de análises regulares, assegurando que são feitos os ajustes necessários para atingir os objetivos. Assegura que a agência funciona de forma aberta e responsável, mantendo a confiança do público e das partes interessadas. O conselho de administração é responsável pela coordenação do processo de contratação do diretor-geral. Para o efeito, recorrerá aos serviços de uma empresa de recrutamento independente.

- **Diretor-geral:** liderada por um diretor-geral, é o órgão central de coordenação da Agência Nacional de Cibersegurança, responsável pela estratégia global, pela direção política e pela administração. Desenvolve e supervisiona a implementação de estratégias e políticas nacionais abrangentes em matéria de cibersegurança, assegurando o alinhamento com as prioridades nacionais. Atuando como o principal centro de tomada de decisões, a Direção-Geral fornece orientação estratégica e define a direção para os vários departamentos operacionais e unidades especializadas da agência, assegurando uma abordagem coesa e unificada da cibersegurança. Além disso, gere o orçamento, os recursos e o capital humano da agência, assegurando uma afectação óptima para cumprir a missão da agência. Isto inclui um planeamento meticuloso, a monitorização e o ajustamento dos recursos para satisfazer as exigências dinâmicas da cibersegurança. A Direção-Geral desempenha também um papel crucial no envolvimento das partes interessadas, representando a agência em reuniões governamentais de alto nível e em fóruns internacionais, promovendo a colaboração e melhorando as capacidades e a eficácia da agência. A Direção-Geral coordena a resposta da agência durante incidentes cibernéticos significativos ou emergências nacionais, assegurando uma mitigação rápida e eficaz e a colaboração com as entidades relevantes. Avaliando regularmente o desempenho, assegura o cumprimento dos objectivos e prepara relatórios exaustivos para o Conselho de Administração e para o Gabinete do Primeiro-Ministro

- **Departamento de Estratégia e Política**
  O Departamento de Estratégia e Política é essencial no desenvolvimento e implementação de políticas e estratégias abrangentes de cibersegurança para proteger a infraestrutura digital da Guiné-Bissau. Este departamento é responsável por contribuir para a formulação e execução de políticas públicas de segurança digital, comunicando eficazmente essas políticas a todas as partes interessadas e promovendo uma rede de parceiros-chave. Tirando partido do seu conhecimento profundo dos desafios da cibersegurança e da experiência técnica e operacional de outros departamentos, o departamento conduz o pensamento estratégico da agência para identificar e

compreender as questões de cibersegurança decorrentes da transformação digital global. Orienta as ações da agência, estabelecendo um quadro regulamentar sólido, ajudando os beneficiários a compreender as questões de segurança digital e conduzindo o trabalho doutrinário interministerial.

O departamento também assegura a coerência setorial e territorial das práticas de cibersegurança, tirando partido das potenciais entidades descentralizadas de cibersegurança e promovendo a consideração das questões de cibersegurança a nível nacional e continental, em colaboração com os seus parceiros.

Eis as principais práticas operacionais:

- **Formular políticas e quadros nacionais de cibersegurança:** O departamento formula políticas e quadros nacionais detalhados de cibersegurança, elaborando regulamentos e diretrizes que regem as práticas de cibersegurança em diferentes sectores. Isto assegura uma abordagem normalizada da cibersegurança a nível nacional.
- **Efetuar avaliações de risco e identificar prioridades estratégicas:** São efectuadas avaliações de risco regulares para identificar potenciais ameaças e vulnerabilidades na infraestrutura digital nacional. Estas avaliações servem de base à definição de prioridades das ações estratégicas e à afetação eficaz de recursos para atenuar os riscos identificados.
- **Coordenar com outras agências governamentais para garantir a integração das políticas:** O departamento colabora estreitamente com outras agências governamentais para integrar as políticas de cibersegurança em todos os sectores, criando uma abordagem unificada e abrangente da cibersegurança nacional.
- **Desenvolvimento e implementação de políticas públicas:** Contribui para o desenvolvimento e implementação da política pública de segurança digital, comunicando essas políticas a todas as partes interessadas e promovendo a colaboração com os principais parceiros. Isto inclui campanhas de sensibilização do público e atividades de envolvimento das partes interessadas. Reflexão estratégica e orientação da agência: Facilita a reflexão estratégica dentro da agência para identificar e compreender os desafios de segurança trazidos pela transformação digital. Utiliza os conhecimentos técnicos e operacionais de outras subdivisões para informar e orientar a direção estratégica da agência.
- **Quadro regulamentar e apoio às partes interessadas:** Orienta as ações da agência através da criação de um quadro regulamentar abrangente e da assistência aos beneficiários na compreensão e cumprimento dos requisitos de segurança digital. Realiza trabalhos doutrinários interministeriais para garantir a coerência das políticas nos diferentes sectores da administração pública.
- **Coerência Sectorial e Territorial:** Garante a coerência das práticas de cibersegurança nos vários sectores e regiões, mantendo uma postura de cibersegurança consistente e eficaz em todo o país.
- **Promoção das questões de cibersegurança a nível nacional e continental:** Promove a importância de abordar as questões de cibersegurança tanto a nível nacional como continental. Colabora com parceiros internacionais para partilhar as melhores práticas e defender medidas de cibersegurança mais fortes nos debates políticos.

- **Departamento de Operações e Vigilância**

O Departamento de Operações e Vigilância é um pilar fundamental da Agência Nacional de Cibersegurança, incumbido das responsabilidades críticas de monitorizar as ciberameaças, gerir incidentes e coordenar os esforços de resposta para proteger a infraestrutura digital nacional. Este departamento opera o Centro de Operações de Segurança (COS) para monitorizar as ameaças em tempo real, assegurando que quaisquer sinais de comprometimento são detectados e tratados prontamente. Desenvolve e implementa protocolos abrangentes de resposta a incidentes para

tratar e atenuar eficazmente os impactos dos ciber incidentes. Além disso, o departamento colabora estreitamente com as autoridades policiais e outras agências relevantes durante incidentes cibernéticos, garantindo uma resposta coordenada e eficiente. Toma as medidas necessárias para proteger os sistemas de informação de empresas vitais, intervém durante tentativas de pirataria informática ou ataques na Web e presta assistência técnica essencial e gestão de incidentes.

O departamento apoia grandes projetos sensíveis com assistência técnica, acompanha a execução dos principais planos de ação em matéria de cibersegurança e avalia os projetos de aquisição de soluções informáticas e de segurança, fornecendo especificações técnicas. Por último, gere o equipamento informático, as redes locais, as bases de dados, os sistemas de informação e as aplicações da agência, garantindo a sua segurança.

Eis as principais práticas operacionais :

- **Operar o Centro de Operações de Segurança (COS):** O departamento gere o COS para fornecer monitorização em tempo real do tráfego de rede e das atividades do sistema, detectando quaisquer sinais de comprometimento e respondendo prontamente a incidentes de segurança.
- **Desenvolver e implementar protocolos de resposta a incidentes:** Cria e mantém protocolos abrangentes de resposta a incidentes para lidar com incidentes cibernéticos de forma eficiente, minimizando o seu impacto e garantindo uma recuperação rápida.
- **Colaborar com os serviços responsáveis pela aplicação da lei e outros organismos relevantes:** Trabalha em estreita colaboração com os organismos responsáveis pela aplicação da lei e outros organismos relevantes para garantir uma resposta coordenada e eficaz aos ciber incidentes, facilitando a partilha de informações e as acções conjuntas.
- **Garantir a segurança das empresas vitais:** Toma as medidas necessárias para garantir a segurança dos sistemas de informação das empresas de importância vital, intervindo em caso de tentativas de pirataria informática ou de ataques na Web e prestando a assistência técnica necessária.
- **Gestão de incidentes e assistência técnica:** Gere e responde a incidentes de cibersegurança, oferecendo apoio técnico e orientação às organizações afectadas e realizando análises e relatórios pós-incidentes.
- **Coordenar os esforços de cibersegurança:** Assegura a coordenação entre as várias partes interessadas na cibersegurança, promovendo a colaboração e uma abordagem unificada da cibersegurança nacional.
- **Correlacionar indicadores de segurança:** Analisa e correlaciona indicadores de segurança em sistemas e redes nacionais para identificar padrões, tendências e potenciais ameaças.
- **Avaliar os mecanismos de segurança:** Realiza auditorias técnicas e operações white-hat para avaliar a eficácia dos mecanismos de segurança em vigor, identificando lacunas e recomendando melhorias.
- **Apoiar projectos sensíveis:** Fornece assistência técnica a grandes projectos sensíveis, garantindo que as medidas de cibersegurança são integradas e eficazes ao longo dos ciclos de vida do projeto.
- **Monitorizar planos e programas de cibersegurança:** Acompanha a execução dos principais planos e programas de ação de cibersegurança, garantindo que os objectivos são atingidos e que são feitos os ajustes necessários.
- **Avaliar projectos de aquisição de TI e de segurança:** Analisa as especificações técnicas dos projectos de aquisição de TI e de segurança, garantindo que cumprem as normas de cibersegurança exigidas.
- **Estabelecer normas de segurança de TI:** Desenvolve normas de segurança de TI específicas e cria guias técnicos para ajudar as organizações a cumprir os requisitos de cibersegurança.

• Departamento de Proteção das Infraestruturas Críticas O Departamento de Proteção das

Infraestruturas Críticas tem por missão proteger as infra-estruturas críticas da nação contra as ciberameaças e garantir a sua resiliência. Este departamento lidera o esforço nacional para proteger as infraestruturas críticas de todos os perigos, gerindo os riscos e aumentando a resiliência através da colaboração com a comunidade das infra-estruturas críticas. Coordena e colabora entre o Governo e o sector privado para proteger os serviços e bens essenciais.

Eis as principais práticas operacionais:

- **Identificar e classificar as infra-estruturas críticas:** O departamento identifica e classifica as infra-estruturas críticas nacionais, incluindo serviços essenciais como a energia, a água, os transportes e as telecomunicações. Isto envolve a avaliação da criticalidade de várias infra-estruturas e a determinação da sua prioridade para medidas de proteção.
- **Desenvolver e aplicar normas e melhores práticas de cibersegurança:** Desenvolve e aplica normas e melhores práticas sólidas de cibersegurança adaptadas às necessidades específicas dos sectores críticos. Isto inclui a criação de directrizes e quadros para garantir que os proprietários e operadores de infra-estruturas críticas implementem medidas de segurança eficazes.
- **Efetuar regularmente auditorias de segurança e avaliações de vulnerabilidade:** Realiza auditorias de segurança e avaliações de vulnerabilidade regulares para identificar potenciais pontos fracos e ameaças às infraestruturas críticas. Estas avaliações ajudam a avaliar a postura de segurança e a implementar as melhorias necessárias para aumentar a resiliência.
- **Coordenar e colaborar entre o Governo e o sector privado:** Coordena esforços e colabora com várias entidades governamentais, partes interessadas do sector privado e parceiros internacionais. Isto assegura uma abordagem unificada para proteger as infra-estruturas críticas, facilitando a partilha de informações e potenciando os conhecimentos colectivos.
- **Conduzir e facilitar avaliações de vulnerabilidade e de consequências:** Facilita as avaliações de vulnerabilidade e de consequências para ajudar os proprietários e operadores de infra-estruturas críticas, bem como os parceiros estatais, locais, tribais e territoriais, a compreender e a enfrentar os riscos. Isto envolve a análise do impacto potencial de várias ameaças e o desenvolvimento de estratégias de atenuação.
- **Fornecer informações sobre ameaças e perigos emergentes:** Fornece informações atempadas sobre ameaças e perigos emergentes às partes interessadas das infra-estruturas críticas. Isto garante que podem ser tomadas medidas adequadas para proteger contra a evolução das ciberameaças e outros riscos.
- **Desenvolver ferramentas e formação para a gestão de riscos:** Desenvolve e oferece ferramentas e programas de formação para ajudar os parceiros do Governo e da indústria a gerir os riscos para os seus ativos, sistemas e redes. Isto inclui workshops, simulações e exercícios práticos para melhorar as capacidades de preparação e resposta das partes interessadas em infra-estruturas críticas.
- **Melhorar a resiliência através da colaboração:** Envolve-se numa colaboração contínua com a comunidade de infra-estruturas críticas para melhorar a resiliência global. Isto envolve planeamento conjunto, partilha de informações e esforços de resposta coordenados para garantir que as infra-estruturas críticas possam resistir e recuperar rapidamente de incidentes cibernéticos.
- **Apoio aos parceiros estatais, locais, tribais e territoriais:** Fornece apoio e orientação aos parceiros estatais, locais, tribais e territoriais nos seus esforços para proteger as infra-estruturas críticas. Isto inclui a oferta de conhecimentos especializados, recursos e assistência no desenvolvimento e implementação de iniciativas locais de cibersegurança.

- **Departamento de Auditoria de Segurança,** Conformidade e Regulamentação O Departamento de Auditoria de Segurança, Confor-

midade e Regulamentação é responsável por garantir a integridade, confidencialidade e disponibilidade dos sistemas de informação em todo o país através da realização de auditorias de segurança exaustivas. Desempenha um papel vital na preparação e execução de directivas estratégicas e nacionais para a auditoria da segurança dos sistemas de informação.
O departamento também monitorizará a conformidade com os regulamentos de cibersegurança, reforçará a adesão às normas de segurança e fornecerá orientações e recomendações para melhorar a postura de segurança das organizações. Assegurará que as organizações cumpram as políticas nacionais de cibersegurança, mantendo assim uma infraestrutura digital robusta e resistente.

Eis as principais práticas operacionais:

- **Preparar planos de ação para a execução de auditorias de segurança:** Desenvolve e implementa planos de ação para dar seguimento às orientações estratégicas e nacionais para as auditorias de segurança dos sistemas de informação. Isto garante que os processos de auditoria estão alinhados com os objectivos nacionais de cibersegurança.
- **Monitorizar o cumprimento das auditorias de segurança obrigatórias:** Supervisiona a conformidade das organizações com os regulamentos de auditoria de segurança obrigatórios, assegurando que as empresas cumprem as normas de segurança exigidas. Isto inclui auditorias periódicas e obrigatórias para garantir a conformidade contínua.
- **Incentivar as organizações a participarem em auditorias de segurança:** Promove a importância das auditorias de segurança junto das organizações, encorajando-as a submeterem-se voluntariamente a auditorias de segurança para melhorar a segurança dos seus sistemas de informação. Isto ajuda a criar uma cultura de segurança proactiva na indústria.
- **Acompanhamento da execução das missões de auditoria:** Acompanha a execução das missões de auditoria de segurança obrigatórias e periódicas aos sistemas e redes informáticos das organizações, assegurando a sua conformidade com a regulamentação existente. Isto inclui o acompanhamento do progresso e dos resultados destas auditorias.
- **Assistência na realização de auditorias de segurança:** Fornece assistência a instituições e organizações na realização de missões de auditoria de segurança. Isto inclui a oferta de conhecimentos técnicos e apoio para garantir auditorias abrangentes e eficazes.
- **Desenvolver e atualizar guias técnicos e especificações de auditoria:** Cria e atualiza regularmente guias técnicos e modelos para a realização de auditorias de segurança. Isto assegura que os auditores dispõem dos recursos necessários e dos procedimentos normalizados para realizarem as suas tarefas de forma eficaz.
- **Avaliar relatórios de auditoria e apresentar recomendações:** Analisa a qualidade dos relatórios de auditoria, identificando deficiências e propondo recomendações adequadas. Isto implica estudar os relatórios de auditoria recebidos, determinar as deficiências e sugerir medidas corretivas.
- **Desenvolver estruturas de auditoria de segurança:** Estabelece quadros de auditoria de segurança para apoiar tanto os auditores como as organizações auditadas. Estes quadros garantem a qualidade das auditorias efectuadas a nível nacional.
- **Melhorar os conhecimentos dos auditores e da segurança da informação:** Reforça as capacidades dos auditores de segurança e dos responsáveis pela segurança dos sistemas de informação, proporcionando oportunidades de formação e desenvolvimento. Isto garante que eles permaneçam proficientes nas mais recentes práticas e tecnologias de segurança.
- **Tratar dos pedidos de certificação dos auditores de segurança:** Gere os processos de certificação e renovação dos auditores de segurança, assegurando que cumprem as normas e critérios exigidos. Isto inclui a supervisão do desempenho e das atividades dos auditores certificados.

- **Garantir o reconhecimento dos programas de formação em segurança:** Verifica e assegura o reconhecimento dos programas de formação em segurança dos sistemas de informação. Isto ajuda a manter elevados padrões de educação e formação no domínio da cibersegurança.
- **Monitorizar o desempenho dos auditores:** Acompanha e avalia o desempenho dos auditores de segurança dos sistemas de informação para garantir que cumprem as normas profissionais e contribuem efetivamente para o processo de auditoria de segurança.
- **Atualizar as especificações e os critérios de certificação:** Actualiza regularmente as especificações e os critérios para a atribuição de certificações de auditoria de segurança. Isto assegura que as normas de certificação permanecem relevantes e rigorosas.
- **Participar no desenvolvimento de tecnologias e sistemas de segurança de ponta:** Contribui para o avanço das tecnologias e sistemas de segurança de ponta para permitir que o Estado cumpra eficazmente as suas missões de soberania.
- **Apoiar a conceção e a implementação de serviços digitais:** Assiste os serviços estatais como o ITMA e os operadores críticos na conceção e implementação dos seus serviços digitais, garantindo a sua segurança e resiliência.
- **Partilhar as melhores práticas através de guias técnicos:** Publica guias técnicos sobre as melhores práticas para os produtos mais utilizados, partilhando conhecimentos e experiência para melhorar as práticas gerais de cibersegurança.
- **Definir quadros de certificação técnica:** Define os quadros de certificação técnica, avalia as soluções de cibersegurança e promove soluções digitais fiáveis e de elevada qualidade. Isto inclui o estabelecimento de normas e padrões de referência para a certificação.
- **Aplicar regulamentos de cibersegurança:** Desenvolve e aplica requisitos de conformidade de cibersegurança, realizando auditorias e inspecções regulares de conformidade para garantir que as organizações cumprem as normas regulamentares.
- **Apoiar a conformidade regulamentar:** Fornece orientação e apoio às organizações para as ajudar a cumprir os regulamentos de cibersegurança, assegurando que compreendem e aderem às normas e práticas necessárias.

- **Departamento de Resposta a Emergências**

O Departamento de Resposta a Emergências dedica-se à gestão e resposta a incidentes de cibersegurança, garantindo uma recuperação rápida e um impacto mínimo na infraestrutura digital da nação. Este departamento desempenha um papel central na manutenção da ciber-resiliência nacional, supervisionando a coordenação dos esforços de resposta durante os principais incidentes de cibersegurança, fornecendo apoio técnico e orientações cruciais às organizações afectadas e compilando e divulgando análises e recomendações abrangentes após os incidentes. Assegura a monitorização contínua dos riscos cibernéticos, facilitando alertas rápidos e medidas proativas para mitigar potenciais ameaças. Ao colaborar com fornecedores de serviços de Internet, agências governamentais, entidades do sector privado e parceiros internacionais, o departamento promove uma abordagem abrangente e unificada da gestão de incidentes de cibersegurança.
O departamento mantém também canais de comunicação sólidos com os meios de comunicação social nacionais e as partes interessadas, aumentando a visibilidade e a eficácia dos esforços da agência tanto a nível nacional como internacional.

Para desempenhar eficazmente o seu papel crítico, o Departamento de Resposta a Emergências utiliza um conjunto abrangente de práticas operacionais fundamentais concebidas para garantir uma gestão rápida e eficiente dos incidentes de cibersegurança.
Aqui há :

- **Coordenar os esforços de resposta durante os principais incidentes de cibersegurança:** O departamento lidera a coordenação dos

esforços de resposta durante incidentes de cibersegurança significativos, assegurando uma reação rápida e eficaz para atenuar o impacto. Isto implica trabalhar em estreita colaboração com várias partes interessadas, incluindo agências governamentais, entidades do sector privado e parceiros internacionais, para orquestrar uma resposta abrangente.

- **Prestar apoio técnico e orientação às organizações afectadas:** Oferece assistência técnica e orientação às organizações afetadas por incidentes de cibersegurança. Este apoio inclui aconselhamento em tempo real sobre medidas de contenção, erradicação e recuperação para minimizar os danos e restaurar rapidamente as operações normais.
- **Compilar e divulgar relatórios e recomendações pós-incidente:** Após a resolução de um incidente, o departamento compila relatórios pormenorizados que analisam o incidente, identificam as causas principais e fornecem recomendações para evitar ocorrências futuras. Estes relatórios são partilhados com as partes interessadas relevantes para melhorar a resiliência geral da cibersegurança.
- **Monitorização dos riscos cibernéticos e coordenação de alertas rápidos:** Monitoriza continuamente os riscos cibernéticos e coordena alertas rápidos para ataques que ocorram no ciberespaço nacional. Isto implica colaborar com os fornecedores de serviços Internet e com várias partes interessadas para detetar e responder rapidamente às ameaças.
- **Preparar e divulgar alertas de ciber-riscos:** Desenvolve e envia mensagens electrónicas para informar os utilizadores da Internet sobre vulnerabilidades e riscos cibernéticos, fornecendo orientações sobre como se protegerem. Esta comunicação proactiva ajuda a aumentar a sensibilização e a prevenir potenciais ataques.
- **Coordenação internacional com centros semelhantes (CERT):** Coordena com homólogos internacionais, como outras equipas de resposta a emergências informáticas (CERT), para identificar e combater os riscos cibernéticos. Isto inclui a partilha de informações sobre a evolução da cibersegurança a nível mundial e a colaboração em ameaças transfronteiriças.
- **Facilitar a comunicação e a coordenação entre as partes interessadas na cibersegurança:** Assegura uma comunicação e coordenação eficazes entre as várias partes interessadas na cibersegurança, incluindo profissionais e peritos em segurança da informação. Isto implica a organização de workshops, eventos e a manutenção de canais de comunicação abertos entre a agência e as instituições relevantes.
- **Manter a comunicação com os meios de comunicação social nacionais:** Mantém os meios de comunicação social nacionais informados através de comunicados de imprensa, briefings e conferências. Isto ajuda a divulgar informações importantes sobre as atividades da agência e as ameaças à cibersegurança ao público em geral.
- **Promover as missões da Agência e reforçar a sua presença nacional e internacional:** Envolve-se em actividades mediáticas para sensibilizar para as missões da agência e aumentar a sua visibilidade e influência a nível nacional e internacional. Isto inclui a participação e a organização de eventos que realcem o papel e as realizações da agência.
- **Facilitar a comunicação entre profissionais e peritos:** Promove a comunicação entre profissionais e peritos em segurança da informação e outras partes interessadas na cibersegurança. Isto é conseguido através da organização de workshops e eventos que facilitam o intercâmbio de conhecimentos e a colaboração.
- **Prestar serviços de assistência em linha e de centro de atendimento telefónico:** Oferece serviços de assistência em linha e opera um centro de atendimento telefónico para fornecer apoio e orientação imediatos sobre questões de cibersegurança. Isto assegura que os indivíduos e as organizações têm acesso a aconselhamento especializado quando necessário.

- **Departamento de Sensibilização e Formação**
  O Departamento de Sensibilização, Formação e Investigação dedica-se a educar e formar as partes interessadas sobre as melhores práticas de cibersegurança, a promover uma cultura de sensibilização para a cibersegurança e a fomentar a inovação e a investigação neste domínio para se manter à frente das ameaças emergentes.
  Criará um quadro de cibersegurança resiliente através da integração de iniciativas educativas, da sensibilização do público e da investigação de ponta.

  As práticas operacionais que se seguem contribuirão para a realização dos objectivos do serviço:
  - **Desenvolver e ministrar programas de formação em cibersegurança:** Cria e implementa programas abrangentes de formação em cibersegurança adaptados a vários públicos, incluindo funcionários governamentais, funcionários do sector privado e o público em geral. Estes programas têm como objetivo melhorar a compreensão e as competências em matéria de práticas de cibersegurança.
  - **Criar uma força de trabalho profissional:** Incentivaremos os atuais profissionais da cibersegurança a desenvolverem as suas carreiras no sector, definindo percursos profissionais mais claros, promovendo certificações reconhecidas internacionalmente e criando fortes comunidades de prática. Para aumentar a mão de obra, atrairemos estudantes promissores através de bolsas de estudo e programas de patrocínio. Apoiaremos também os novos participantes na profissão através de um currículo orientado para a indústria para os estudantes, bem como de oportunidades de atualização e requalificação para profissionais a meio da carreira.
  - **Realizar campanhas de sensibilização do público:** Organiza e realiza campanhas de sensibilização do público para educar os cidadãos sobre questões de cibersegurança, destacando a importância da segurança online e das melhores práticas. Estas campanhas utilizam várias plataformas midiáticas para chegar a uma vasta audiência.
  - **Colaborar com instituições de ensino:** Trabalha em parceria com instituições de ensino para integrar a cibersegurança nos seus currículos, garantindo que os estudantes de todos os níveis estão equipados com os conhecimentos e as competências necessárias para navegar no mundo digital de forma segura.
  - **Facilitar as parcerias de investigação:** Estabelece e mantém parcerias com instituições académicas e organizações de investigação para promover a colaboração em projectos de investigação sobre cibersegurança. Estas parcerias têm como objetivo potenciar as competências e os recursos para enfrentar os desafios nacionais em matéria de cibersegurança.
  - **Financiar e realizar projectos de investigação sobre cibersegurança:** Atribui financiamento e recursos para apoiar e realizar projectos de investigação que promovam a compreensão das ameaças à cibersegurança e desenvolvam soluções inovadoras. A agência deve criar um consórcio. Este consórcio reunirá o Governo, a indústria e o meio académico para colaborar na investigação e procurar soluções viáveis e práticas com potencial de comercialização.
  - **Monitorizar os avanços tecnológicos:** Monitoriza continuamente os avanços tecnológicos globais e as tendências em matéria de cibersegurança. Integra inovações relevantes nas estratégias nacionais para garantir que o país se mantém na vanguarda das práticas de cibersegurança.
  - **Identificar e estudar projectos de investigação nacionais:** Identifica e estuda projectos de investigação de importância nacional, coordenando com as estruturas relevantes para ativar o papel dos laboratórios nacionais de investigação. Isto assegura que os esforços de investigação se alinham com as prioridades nacionais.

- **Contribuir para os planos de desenvolvimento:** Participa na preparação de planos de desenvolvimento nacionais e facilita as ligações com instituições científicas. Isto garante que as considerações de cibersegurança sejam integradas em iniciativas de desenvolvimento mais amplas.
- **Acompanhar os desenvolvimentos científicos a nível mundial:** Manter-se a par dos desenvolvimentos científicos e tecnológicos mundiais no domínio da cibersegurança. Isto implica a análise da investigação mais recente, a participação em conferências internacionais e a integração de novas descobertas nas políticas e práticas nacionais.

- **Direção dos recursos**

  O Departamento de Recursos gere os recursos administrativos, financeiros, humanos e materiais da agência. Assegura que as operações cumprem a legislação e os regulamentos relevantes, apoiando as metas e os objectivos estratégicos globais da agência.

  Para cumprir eficazmente o seu papel multifacetado, o Departamento de Recursos utiliza uma série de práticas operacionais concebidas para garantir uma gestão eficiente e o cumprimento de todas as áreas de atividade da agência:
  - **Gestão administrativa:** Trata das operações administrativas da agência, assegurando o cumprimento das leis e dos regulamentos. Isto inclui o arquivamento de documentos e a gestão do armazenamento.
  - **Recursos humanos:** Recrutamento, formação e atividades sociais no estrangeiro. Desenvolve e implementa políticas de recursos humanos para melhorar o desenvolvimento e o bem-estar dos funcionários.
  - **Bens e aquisições:** Gere os ativos e as aquisições da agência, assegurando o acompanhamento e a manutenção adequados. Coordena os projectos logísticos e imobiliários em função dos objectivos estratégicos.
  - **Operações financeiras:** Dirige as atividades financeiras da agência, incluindo a elaboração do orçamento, as operações fiscais e o planeamento financeiro. Assegura o cumprimento dos regulamentos financeiros e prepara as demonstrações financeiras.
  - **Atividades contabilísticas:** Planeia e desenvolve os processos financeiros e contabilísticos da agência em colaboração com a Direção-Geral. Prepara as demonstrações financeiras e gere os orçamentos.
  - **Planeamento de recursos:** Coordena o planeamento e a execução das atividades relacionadas com os recursos financeiros, humanos, materiais e imobiliários. Assegura a utilização eficaz dos recursos em todos os departamentos.
  - **Apoio à governança:** Ajuda na governança, permitindo que a direção geral avalie, dirija e controle os recursos de forma eficaz. Propõe políticas para otimizar a gestão dos recursos.
  - **Conformidade regulamentar:** Assegura que todas as operações cumprem as leis e regulamentos atuais. Gere os assuntos jurídicos, assegura as atividades e prepara os documentos legislativos necessários.
  - **Gestão de documentos e de stocks:** Arquiva documentos administrativos e gere o armazenamento de documentos e materiais, assegurando que os registos estão bem organizados e acessíveis.

C. Definição das fontes de financiamento da Agência

A Agência Nacional de Cibersegurança poderá ter várias fontes de financiamento para apoiar as suas operações e iniciativas. Estas fontes incluem fundos públicos, subvenções governamentais, parcerias com o sector privado, contribuições internacionais e receitas geradas por serviços especializados e sanções.

Estas fontes de financiamento são também essenciais para apoiar as operações da agência, desenvolver programas de sensibilização, investir na investigação e desenvolvimento de tecnologias de segurança e melhorar as capacidades de resposta a incidentes. Eis algumas das principais fontes potenciais de financiamento de uma agência nacional de cibersegurança para apoiar as suas operações e iniciativas.

- **Dotações orçamentais do Governo:**
  - **Orçamento nacional:** O gabinete do Primeiro-Ministro atribuirá fundos específicos do orçamento nacional para apoiar as iniciativas de cibersegurança. Esta dotação é crucial para manter a infraestrutura de cibersegurança, incluindo o desenvolvimento de políticas, a contratação de profissionais qualificados e a aquisição das tecnologias necessárias.
  - **Orçamentos suplementares:** Em caso de incidentes significativos, os governos podem conceder dotações orçamentais suplementares adicionais. Isto garantirá que a agência de cibersegurança possa responder eficazmente e aplicar medidas de segurança reforçadas.

- **Ajuda internacional e subvenções:**
  Outras fontes são os financiamentos de agências internacionais de ajuda e programas de desenvolvimento:
  - **União Europeia (UE):** A UE prestou apoio financeiro e técnico a projectos de cibersegurança em países em desenvolvimento como a Guiné-Bissau. Isto inclui financiamento para a criação e o reforço de equipas de resposta a incidentes de segurança informática (CSIRT) e outras capacidades de cibersegurança.
  - **Banco Mundial:** O Banco Mundial oferece subvenções e empréstimos destinados a melhorar a infraestrutura digital e a cibersegurança nos países em desenvolvimento. Estes fundos ajudam a aumentar a resiliência e as capacidades nacionais em matéria de cibersegurança.
  - **Banco Africano de Desenvolvimento (BAD):** Em 2021, o Banco Africano de Desenvolvimento concedeu uma subvenção de 2 milhões de dólares para reforçar a cibersegurança e impulsionar a inclusão financeira em África[17].
  - **Nações Unidas e a União Internacional das Telecomunicações (UIT)** e outros organismos da ONU podem fornecer assistência técnica e financiamento para projetos específicos de cibersegurança.

- **Parcerias Público-Privadas :**
  - **Colaborações com o sector privado:** As parcerias com empresas privadas locais e internacionais podem fornecer apoio financeiro e conhecimentos técnicos especializados. Estas parcerias são cruciais para potenciar a inovação e os recursos do sector privado.

- **Acordos bilaterais e multilaterais:**
  - **Cooperação internacional:** A Guiné-Bissau pode envolver-se em acordos bilaterais e multilaterais com outros países para reforçar a cibersegurança. Estes acordos podem incluir apoio financeiro, assistência técnica e iniciativas conjuntas para combater as ciberameaças.

- **Cooperação regional:**
  - **Comunidade Económica dos Estados da África Ocidental (CEDEAO):** A CEDEAO fornece financiamento e apoio a projectos de colaboração em matéria de cibersegurança aos seus membros. Estas iniciativas reforçam as medidas de segurança regional através da partilha de recursos e de esforços colectivos.
  - **União Africana (UA):** A UA apoia iniciativas de cibersegurança em todo o continente, oferecendo financiamento e assistência técnica aos estados membros para melhorar a sua postura de cibersegurança.

- **Donativos e patrocínios[18]:**
  - **Organizações filantrópicas:** Fundações como a Fundação Bill e Melinda Gates e outras podem conceder subsídios para projetos de cibersegurança no âmbito da sua missão mais vasta de apoio ao desenvolvimento digital e à governança.
  - **Patrocínios de empresas:** Os programas de formação, as conferências e os workshops sobre cibersegurança podem atrair o patrocínio de intervenientes do sector interessados em promover a sensibilização para a cibersegurança e a criação de capacidades.

17 https://www.afdb.org/en/news-and-events/press-releases/african-development-bank-extends-grant-2-million-strengthen-cybersecurity-and-boost-financial-inclusion-africa-42526
18 https://cybilportal.org/projects-by?page=region&_sft_region=western-africa & https://fintechnews.ae/5586/fintech/bill-and-melinda-gates-foundation-donates-us1-5-m-to-strengthen-cybersecurity-in-africa-and-asia/

D. Definir as relações com a entidade de controlo

Com base no nosso estudo, escolhemos o Gabinete do Primeiro-Ministro como entidade supervisora da Agência Nacional de Cibersegurança. Esta é uma decisão estratégica que se baseia na necessidade de uma liderança e coordenação fortes e centralizadas ao mais alto nível do governo. A cibersegurança é um aspecto crítico da segurança nacional, que afeta tudo, desde a estabilidade económica à segurança pública e às relações internacionais. Ao colocar a Agência Nacional de Cibersegurança sob a supervisão direta do Gabinete do Primeiro-Ministro, garantimos que as prioridades de cibersegurança estão alinhadas com os objectivos estratégicos globais da nação e que os esforços de resposta são coordenados em todos os setores e agências relevantes. Esta decisão tira partido da autoridade executiva e das capacidades abrangentes de supervisão do Gabinete do Primeiro-Ministro, facilitando uma ação rápida e decisiva face às ciberameaças e garantindo que as medidas de cibersegurança são integradas em todos os aspectos da política e da governança nacionais. O Gabinete do Primeiro-Ministro, com o seu amplo mandato e influência direta sobre todas as funções governamentais, está numa posição única para fornecer a liderança, os recursos e a orientação política necessários para salvaguardar eficazmente a nossa infraestrutura digital e melhorar a nossa postura nacional em matéria de cibersegurança.

E. Definir tipos de colaboração multissectorial: com o sector privado e outras agências/entidades governamentais

No contexto da Guiné-Bissau, as colaborações multissectoriais são essenciais para a construção de um quadro de cibersegurança resiliente.
São possíveis várias formas de colaboração com o sector privado, com outros organismos governamentais e com as forças da ordem, nomeadamente a polícia judiciária.

Impulsionada pelo modelo de governança híbrido da cibersegurança, a agência pode aproveitar os recursos, as competências e as tecnologias disponíveis em diferentes sectores para reforçar a resiliência nacional em matéria de cibersegurança.
A seguir, o principal tipo de colaboração a estabelecer:

- **Colaboração com o setor privadoColaboração público-privada:** Assinar acordos formais entre entidades públicas e empresas privadas para trabalharem em conjunto em projetos ou iniciativas específicas. Estes acordos servirão de base para o desenvolvimento de infra-estruturas de cibersegurança, programas conjuntos de formação em cibersegurança e plataformas partilhadas de informação sobre ameaças.

  Partilha de informações por sector específico e informações sobre ameaças:
  A agência deve ter centros setoriais específicos que facilitem a partilha de informações sobre ameaças à cibersegurança e de melhores práticas entre os sectores público e privado.

  → **Formação e desenvolvimento de capacidades:** Conceber programas para melhorar as competências e os conhecimentos em matéria de cibersegurança através da colaboração entre entidades públicas e empresas privadas. Desenvolver programas de certificação em colaboração com os líderes do sector.

  → **Campanha de sensibilização para a cibersegurança :** Colaborar com entidades do sector privado para sensibilizar o grande público e as empresas para as melhores práticas de cibersegurança. Lançar campanhas conjuntas de sensibilização para a cibersegurança. Desenvolver materiais e recursos educativos para distribuição pública.

  → **Colaboração na resposta a incidentes:** Esforços conjuntos entre os sectores público e privado para responder e atenuar o impacto dos incidentes de cibersegurança. Coordenar a resposta a ciberataques em grande escala, protocolos partilhados de resposta a incidentes

Realizar exercícios e simulações de resposta a incidentes

- **Colaboração com outras agências e entidades governamentais**
  - **Coordenação interagências:** Estabelecer protocolos para a partilha de informações sobre cibersegurança e de informações sobre ameaças entre a agência e outras entidades governamentais (ARN, DGTED, ITMA, Polícia Judiciária, ANPD, etc.) Criar grupos de trabalho conjuntos e grupos de trabalho interagências.
  - **Colaboração na resposta a incidentes:** coordenar os esforços de resposta a incidentes com outras agências governamentais. Colaborar com CERT e SOC de sectores específicos A Agência Nacional pode aproveitar as atividades CERT da ARN e a equipa SOC da Polícia Judiciária, por exemplo. Estas atividades garantirão uma resposta unificada e eficaz aos incidentes de cibersegurança.
  - **Colaboração com os organismos responsáveis pela aplicação da lei e pelos serviços de informação :** Estabelecer uma colaboração com os organismos responsáveis pela aplicação da lei e pelos serviços de informação para combater a cibercriminalidade e proteger a segurança nacional. (Criar um canal de comunicação seguro para a partilha de informações em tempo real. Formar grupos de trabalho conjuntos para investigar casos complexos de cibercriminalidade. Partilhar análises forenses e conhecimentos técnicos para apoiar as investigações. Realizar exercícios conjuntos de gestão de crises para melhorar a coordenação e as capacidades de resposta.

F. Definir tipos de cooperação internacional e programas de intercâmbio

A cooperação internacional envolve a ação coordenada voluntária de dois ou mais países que operam ao abrigo de um quadro jurídico para atingir um objetivo específico. No contexto da cibersegurança, este conceito engloba amplamente questões como a extradição e o auxílio judiciário mútuo, bem como medidas gerais para garantir a cooperação transfronteiriça em matéria de cibersegurança. Estas medidas incluem igualmente a partilha de informações e recursos, num quadro bilateral ou multilateral, com o objetivo de facilitar respostas eficientes às ciberameaças. Ao estabelecer cooperações internacionais, a agência reforçará as suas capacidades, manter-se-á actualizada sobre as tendências mundiais em matéria de cibersegurança e construirá uma infraestrutura resistente. Estas iniciativas não só protegerão as infra-estruturas críticas e os dados sensíveis, como também promoverão uma cultura sólida de cibersegurança, tanto a nível nacional como internacional.

São possíveis muitos tipos de colaboração internacional:

- **Acordos bilaterais entre países Eis alguns exemplos de colaborações bilaterais :**
  - **O Gana e o Reino Unido**[19] assinaram um acordo de parceria para reforçar as capacidades de cibersegurança do Gana. Este acordo visa a partilha de informações sobre ameaças, a realização de formação conjunta e o desenvolvimento de infra-estruturas de cibersegurança.
  - **África do Sul e Nigéria**[20]**:** O acordo engloba elementos de proteção de dados, garantindo que ambos os países

- **Acordos de cooperação entre vários países ou regiões**
  - **Resposta da África Ocidental em matéria de cibersegurança e de luta contra a cibercriminalidade (OCWAR-C)**[21] Este projeto visa melhorar a cibersegurança e combater a cibercriminalidade na África Ocidental através do reforço das capacidades e da cooperação regional.
  - **União Internacional das Telecomunicações (UIT) A UIT**[22] oferece programas de formação e recursos para melhorar as capacidades de cibersegurança nos países membros. Por exemplo, o projeto "Enhancing Cybersecurity in Least Developed Countries" (Melhorar a cibersegurança nos

19 https://www.csa.gov.gh/uk-and-ghana-forge-collaboration-path-in-cybersecurity.php#:~:text=UK%20AND%20GHANA%20FORGE%20COLLABORATION%20PATH%20IN%20CYBERSECURITY&text=Tim%20Galvin%2C%20outlined%20key%20focus,strengthening%20capabilities%20to%20combat%20cybercrime
20 https://investmentpolicy.unctad.org/
21 https://www.ocwarc.eu/
22 https://www.itu.int/en/ITU-D/Cybersecurity/Pages/CYBLDC.aspx

países menos desenvolvidos).

- **A Interpol[23]** coordena os esforços internacionais de combate à cibercriminalidade através da cooperação policial, do reforço das capacidades e do apoio operacional.
- **Conselho da Europa -** Convenção de Budapeste sobre o Cibercrime Proporciona um quadro para a cooperação internacional no combate ao cibercrime através da harmonização da legislação e do reforço das capacidades.
- **GLACY+ (Ação Global contra a Cibercriminalidade Alargada)[24]:** Um projeto conjunto da União Europeia e do Conselho da Europa para apoiar os países no reforço das suas capacidades de combate à cibercriminalidade.
- **A Diretiva da CEDEAO sobre a luta contra a cibercriminalidade** Em agosto de 2011, durante a sua Sexagésima Sexta Sessão Ordinária em Abuja, o Conselho de Ministros da CEDEAO adoptou a Diretiva C/DIR.1/08/11 sobre a luta contra a cibercriminalidade. Esta directiva obriga os Estados Membros a criminalizar a cibercriminalidade e estabelece um quadro para facilitar a cooperação internacional em matéria de cibersegurança. A este respeito, o n.º 1 do artigo 33.º da diretiva prevê que: "Sempre que os Estados-Membros sejam informados por outro Estado-Membro da alegada prática de uma infração, tal como definida na diretiva, esses Estados-Membros "cooperam na busca e no apuramento dessa infração, bem como na recolha de provas relativas à mesma".
- **Iniciativa de cibersegurança G7-CEDEAO[25]:** Lançada durante a Presidência alemã do G7 em 2022, esta iniciativa visa reforçar a cibersegurança e a proteção de dados em toda a África Ocidental. O Plano de Ação da CEDEAO (2022-2025) inclui várias medidas para aumentar a ciber-resiliência regional, centrando-se no desenvolvimento de medidas regionais de criação de confiança, no reforço da cooperação e das capacidades cibernéticas e na melhoria do desenvolvimento de competências. Esta iniciativa envolve a colaboração entre os Estados membros da CEDEAO e parceiros internacionais, como o Departamento de Estado dos EUA e o Ministério Federal dos Negócios Estrangeiros alemão.
- **Convenção da União Africana sobre Cibersegurança e Proteção de Dados Pessoais (Convenção de Malabo) :** Embora mais abrangente do que apenas a África Ocidental, a Convenção de Malabo, adoptada pela União Africana em 2014, procura harmonizar as leis de proteção de dados e cibersegurança em todo o continente africano. A convenção estabelece princípios e medidas para a proteção de dados pessoais, a segurança das transacções electrónicas e o combate ao cibercrime. Incentiva os Estados membros a estabelecer quadros jurídicos e a cooperar em questões de cibersegurança.

- **Participação em organizações e conferências internacionais:** No mundo interligado de hoje, a participação de uma agência nacional de cibersegurança em conferências internacionais sobre cibersegurança não é apenas benéfica, mas essencial. Estas conferências servem como uma plataforma global onde a agência pode interagir com os seus pares, partilhar conhecimentos e manter-se a par dos últimos desenvolvimentos neste domínio. Ao participar nestes eventos, a agência da Guiné-Bissau obterá informações sobre ameaças emergentes e mecanismos de defesa inovadores, que são cruciais para melhorar as medidas nacionais de cibersegurança.

  Além disso, as conferências internacionais constituem uma oportunidade única para estabelecer redes e alianças. O estabelecimento de relações com outras agências nacionais, líderes do sector privado e peritos académicos pode levar a esforços de colaboração na investigação, partilha de informações sobre ameaças e respostas coordenadas a incidentes cibernéticos. Estas parcerias são inestimáveis para criar uma frente unificada contra as ciberameaças que não conhecem

23 https://www.interpol.int/en/Crimes/Cybercrime
24 https://www.coe.int/en/web/cybercrime/glacyplus
25 https://www.ecowas.int/

fronteiras.
Além disso, a presença da agência nestas conferências sublinha o seu empenhamento nas normas e práticas mundiais de cibersegurança. Permite que a agência contribua para a formulação de políticas e quadros internacionais, assegurando que estes sejam abrangentes e incluam diversas perspectivas. Esta participação ativa ajuda a alinhar as estratégias nacionais com as melhores práticas mundiais, melhorando assim a postura geral de segurança.

VII

Definição do processo de recrutamento e manutenção de capacidades

1. Estratégia e processo de recrutamento

As agências de cibersegurança e de proteção de dados são fundamentais para o país. Por isso, o processo de recrutamento tem de ser bom para ter a pessoa competente no sítio certo.
Quando falamos de recrutamento, temos de fazer uma separação entre as categorias :

- **Conselho de Administração :**
  - Um conselho de administração é um grupo de pessoas que representa os interesses das partes interessadas de uma agência. Também fornece orientação e aconselhamento ao diretor-geral e à equipa executiva de uma organização.
  - Um conselho de administração proporciona uma supervisão geral das operações sem se envolver nas operações quotidianas. Os conselhos de administração podem ser mais orientados para o futuro, enquanto o diretor-geral e a equipa de gestão se concentram nos desafios do dia a dia.
  - O conselho de administração de uma agência define políticas e aconselha a equipa executiva sobre estratégia, remuneração dos executivos, gestão de recursos, responsabilidade social e outros assuntos. Espera-se que todos os membros do conselho de administração utilizem a sua posição e experiência para promover os melhores interesses da agência, mantendo-se objectivos e sem conflitos de interesses. Os membros do conselho de administração devem também respeitar o código de ética da agência.
  - O Conselho de Administração supervisiona as operações da agência, mas uma das suas funções é a contratação do diretor-geral. O conselho de administração também aprova a estratégia e assegura a sua execução.
  - Idealmente, um conselho de administração deve incluir representação pública e privada, cada uma eleita por um período específico. Muitas empresas procuram que os mandatos dos membros do conselho de administração comecem e terminem em alturas diferentes para evitar vagas e a necessidade de preencher vários cargos ao mesmo tempo.
  - Os membros do Conselho de Administração, conhecidos como diretores, são nomeados pela entidade que os tutela. As condições de nomeação podem variar consoante a entidade. No caso dos membros privados, estes podem ser nomeados pela câmara de comércio. O perito independente pode ser nomeado pelo conselho de administração após análise da candidatura. Muitas organizações escalonam os mandatos, o que ajuda a proporcionar uma mistura de continuidade e novas ideias.
  - O mandato dos membros do conselho de administração não deve exceder três no total, renovável uma vez.
  - Todos os membros do conselho de administração nomeados devem receber formação e passar um questionário relacionado com a formação com uma pontuação de 80% ou mais. Se falharem no teste mais de três vezes, a sua organização deve propor outra nomeação em substituição.

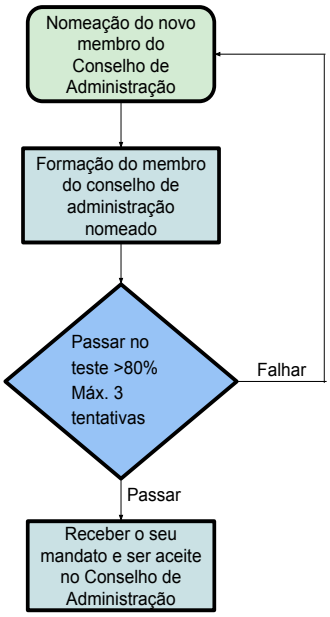

Figura 03: Gráfico de seleção dos membros do Conselho de Administração

- **A comissão executiva :**
  - Isto inclui a equipa de gestão, como o diretor-geral e o seu conselho de administração.
  - Para contratar um novo diretor-geral, o anúncio será feito ao público nos meios de comunicação social populares.
  - Os candidatos à posição de diretor-geral devem fazer um exame que avaliará as suas competências. O exame pode validar as competências técnicas, as competências sociais e os conhecimentos gerais. A preparação do exame e o processo de recrutamento devem ser confiados a uma empresa de recrutamento externa. Esta empresa pode ser nacional ou internacional. O critério importante é selecionar uma empresa que não tenha influência política. É da responsabilidade do conselho de administração selecionar a empresa responsável pela preparação do exame e pela conclusão do processo de recrutamento do diretor-geral.
  - O candidato a diretor-geral deve obter, pelo menos, 70% de aproveitamento na prova de concurso.
  - Os cinco melhores candidatos, no máximo, serão convocados para uma entrevista perante o Conselho de Administração ou a empresa de recrutamento selecionada. O candidato será classificado com base no seu desempenho na entrevista. O Conselho de Administração não deve ter conhecimento da sua classificação no concurso escrito.
  - A média das notas da prova escrita e da entrevista oral constituirá a nota final do candidato.
  - O primeiro candidato com a pontuação mais elevada, superior a 70%, será contactado para uma verificação do ecrã e validação das referências.
  - Se a verificação do ecrã for positiva, o contrato será negociado e enviado ao candidato.
  - Se o candidato aceitar a oferta, será identificada a data de início do mandato do diretor-geral.
  - O mandato do diretor-geral não deve exceder 2 anos.
  - O processo de recrutamento será iniciado pelo menos 6 meses antes do fim do atual mandato do diretor-geral. O atual Diretor-Geral pode participar no processo se tiver a intenção de ficar. Ser-lhe-á dada prioridade. É apenas necessária uma entrevista oral perante o Conselho de Administração. Cabe ao Conselho de Administração decidir se renova ou não o seu contrato. Se o contrato não for renovado, será iniciado o processo de contratação explicado acima. Este processo de renovação não deve exceder 30 dias.
  - A mesma pessoa não pode permanecer no cargo de diretor-geral da mesma agência por mais de quatro (4) anos consecutivos.

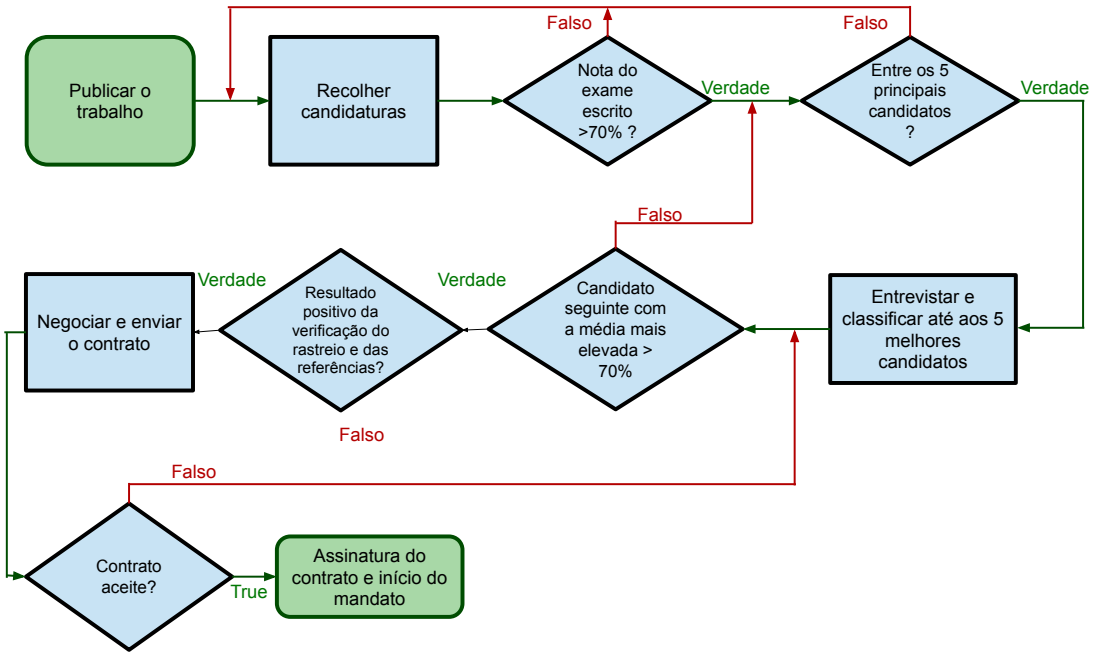

Figura 04: Gráfico do processo de contratação da direção executivat

- **A mão de obra :**
  - A seleção dos candidatos será feita com base no seu CV, na cópia dos certificados/ diplomas relevantes e, se possível, nos comprovativos de experiência e nas referências.
  - O diretor-geral pode solicitar o serviço de uma empresa externa para o ajudar no processo de recrutamento, mas continua a ser responsável.
  - Será necessário efetuar um teste técnico para validar as competências
  - A entrevista será efectuada, no máximo, para os 3 primeiros candidatos.
  - O candidato selecionado deve passar pela verificação do ecrã e pela validação das referências.
  - Em caso de resultado positivo da verificação do ecrã e das referências, o candidato será contratado. Caso contrário, será contactado o candidato seguinte. Se não houver nenhum candidato elegível, o processo de recrutamento será reiniciado.

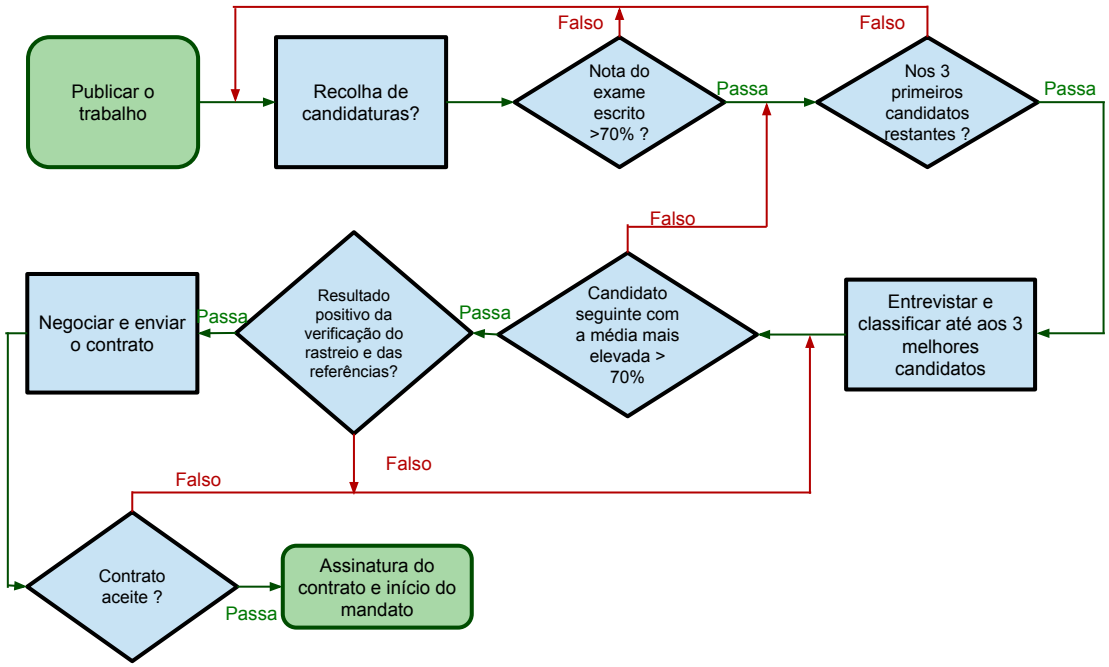

Figura 05 : Gráfico do processo de contratação de pessoal

2. Estratégia de formação e atualização de conhecimentos

O percurso de formação deve ser identificado para cada função. A auditoria da formação concluída será efectuada uma vez por ano.
Todos os trabalhadores e o conselho de administração devem seguir uma formação sobre :

- Como identificar o risco cibernético
- Como reagir no caso de pensarem que estão expostos a um incidente de segurança
- Como criar uma boa palavra-passe e as melhores práticas relacionadas com as palavras-passe

Estas sessões de formação devem ser seguidas do exercício de enviar alguns cenários de ataque controlados (phishing, teste da chave USB infetada no chão, etc.) aos empregados para ver as suas reações.
Dependendo do nível do funcionário, o percurso de formação será adaptado. O reforço das capacidades será abordado em pormenor no produto 4 do presente projeto.

VIII

Conclusão

No presente relatório, propusemos a conceção da Agência de Proteção de Dados e da Agência de Cibersegurança. Recomendamos que estas agências sejam resilientes em caso de mudança política. Para o efeito, propusemos um conselho de administração para cada uma delas. A estrutura do conselho de administração é tal que as mudanças políticas não devem influenciar as operações destas agências. O facto de o Diretor Geral não responder diretamente perante uma autoridade política, mas sim perante o seu Conselho de Administração, confere-lhe um certo grau de autonomia. Para cumprir a sua missão, o Diretor-Geral pode apoiar-se no seu gabinete de gestão e em peritos técnicos.

Estamos bem cientes da dificuldade de encontrar recursos qualificados. Mas este continua a ser um desafio permanente no domínio da cibersegurança, pelo que é essencial estabelecer planos de formação. No entanto, o processo de recrutamento garante que apenas os candidatos competentes são seleccionados. No caso de não ser possível preencher determinadas posições, as agências podem, em função do roteiro proposto, começar com equipas minimalistas, recorrendo ao auxílio de peritos estrangeiros para questões não secretas. Nos próximos resultados deste projeto, apresentaremos planos de reforço das capacidades. Isto deverá ajudar-nos a dispor de recursos mais qualificados ao longo do tempo.

RFP No: WARDIP – C – 15 - 2023

BS Innovations & GoSecure | Present in : Montreal, Canada & Cotonou, Benin
Tel : (+1) 514 652 7585 | E-mail : bkikisagbe@bs-innovations.com