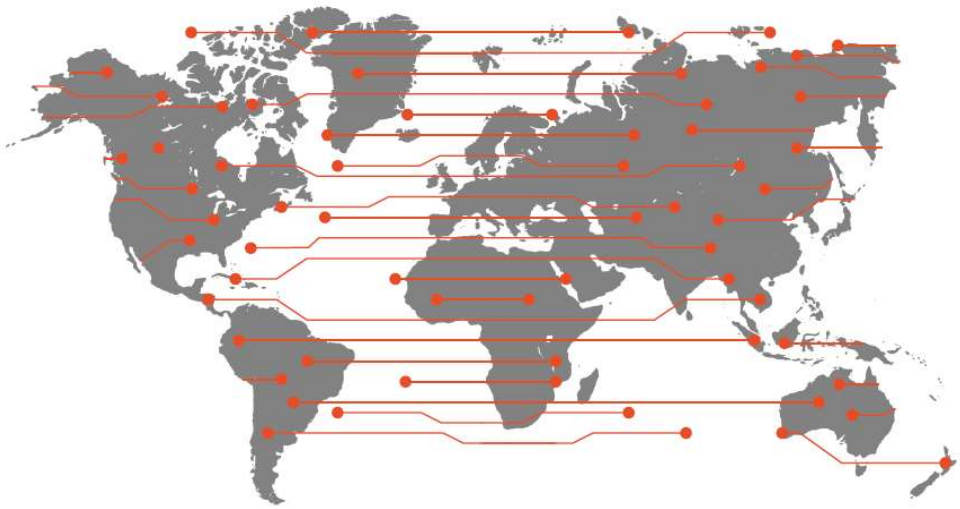

# D-05
# Plano de Ação da Estratégia Nacional de Cibersegurança da Guiné-Bissau

Setembro, 2024

## Informação do documento

| | | | |
|---|---|---|---|
| **Título do Projeto:** | Estudo de Viabilidade Sobre a Cibersegurança na Guiné-Bissau | | |
| **Título do relatório:** | D-05 Plano de Ação da Guiné-Bissau | | |
| **Versão:** | 1 | **Data da versão:** | 02-09-2024 |
| **Preparado por:** | Equipa de Cibersegurança da NRD | | |
| **Avaliado por:** | Salazar Cruz | | |
| **Aprovado por:** | Aníbal Baldé | | |

## Fluxo de informação

| Quem | Data | Contacto |
|---|---|---|
| NRD Cyber Security | 02-09-2024 | R. Jašinskienė |
| | | |
| | | |
| | | |

## Cronologia das versões:

| N.º da versão | Data | Observações |
|---|---|---|
| 0.1 | 02-09-2024 | Rascunho inicial |
| 1.0 | 12-09-2019 | Versão Final |
| | | |

# Índice

## Lista de acrónimos e Definições

Para efeitos da presente estratégia regional, serão aplicáveis as seguintes definições:

*Tabela 1 Termos e Abreviaturas*

| Termo/abreviatura | Significado/explicação |
|---|---|
| ARN | Autoridade Reguladora Nacional |
| AU | União Africana |
| CCIAS | Câmara de Comércio, Indústria, Agricultura e Serviços da Guiné-Bissau |
| CERT/CSIRT/CIRT/ | Equipa de Resposta a Emergências Informáticas<br>Equipa de Resposta a Incidentes de Segurança Informática<br>Equipa de Resposta a Incidentes Informáticos<br><br>Equipa responsável por alertar sobre ameaças, prevenir riscos e ameaças aos sistemas de informação, reagindo a incidentes de segurança e ajudando na resposta e recuperação. |
| Cibercrime | Atividades criminosas em que computadores e sistemas de informação estão envolvidos como ferramenta principal ou alvo primário. O cibercrime considera crimes tradicionais (e.g. fraude, falsificação e roubo de identidade), crimes relacionados com conteúdo (ex. distribuição online de pornografia infantil ou incitação ao ódio racial) e crimes únicos para computadores e sistemas de informação (e.g. ataques contra sistemas de informação, negação de serviço e malware). |
| Ciberespaço | A rede interdependente de infraestruturas de sistemas de informação, incluindo a Internet, redes de telecomunicações, sistemas de informação e Internet das coisas (IoT). |
| Cibersegurança | Conjunto de práticas destinadas a proteger o ciberespaço e os ciber-ativos das ameaças que estão associadas ou que podem prejudicar as suas redes e infraestruturas de informação. A cibersegurança procura preservar a disponibilidade e a integridade das redes e infraestruturas e a confidencialidade das informações nelas contidas. |
| Contrato/Projeto | N.º do contrato. WARDIP-C-10-2023 entre o Governo da Guiné-Bissau/ Programa Regional de Integração Digital da África Ocidental e a JSC NRD Cyber Security para a prestação de Serviços de Consultoria para a realização de Estudo de Viabilidade em Cibersegurança na Guiné-Bissau |
| Dados | Qualquer representação de factos, informações ou conceitos numa forma adequada para processamento num sistema digital. |
| DGTED | Direção-Geral das Telecomunicações e da Economia Digital |
| ECOWAS | Comunidade Económica dos Estados da África Ocidental |
| EMGFA | Estado-Maior General das Forças Armadas |
| ENISA | European Union Agency for Cybersecurity |
| Higiene de Segurança | As boas práticas que cada utilizador digital deve respeitar para preservar a segurança do sistema de informação que utiliza ou para o qual atua como administrador. |
| ICG | Índice Global de Cibersegurança |
| ICI | Infraestrutura Críticas de Informação |
| Infraestruturas Críticas | Infraestruturas públicas ou privadas, ou processos cuja destruição, paralisação, exploração ilegítima ou interrupção por um período definido de tempo causará perda de vidas ou perda significativa para a economia ou dano significativo à reputação da Guiné-Bissau ou aos seus símbolos de soberania. Nesta definição, infraestruturas incluem as redes, sistemas e os dados físicos ou digitais essenciais para fornecer este serviço. Este termo pode referir-se a um certo sistema ou processo cujo funcionamento é crítico dentro da organização. |
| Instituições beneficiárias | Ministério dos Transportes e Comunicações, Autoridade Reguladora Nacional, Instituto Tecnológico para a Modernização Administrativa |
| ITMA | Instituto Tecnológico para a Modernização da Administração |
| MTN | Operadora de telecomunicações |
| MTTED | Ministério dos Transportes, Telecomunicações e Economia Digital |
| NCCP | Plataforma Nacional de Cloud Computing |
| NCSS | Estratégia Nacional de Cibersegurança |
| NIC | Índice Nacional de Cibersegurança |
| NIST | Instituto Nacional de Padrões e Tecnologia |
| NRA | Autoridade reguladora nacional |
| NRD CS | JSC NRD Cyber Security |
| Operador de Infraestruturas Críticas | Operador público ou privado que opera uma infraestrutura crítica. |

| Termo/abreviatura | Significado/explicação |
|---|---|
| Operador de Serviço Essencial | Operador público ou privado que fornece um serviço essencial. |
| Países beneficiários | Guiné-Bissau |
| PICI | Proteção das Infraestruturas Críticas de Informação |
| PNUD | Programa das Nações Unidas para o Desenvolvimento |
| Proteção de Infraestruturas Críticas | Conjunto de práticas para proteger infraestruturas críticas de quaisquer riscos e ameaças que possam causar a interrupção total ou parcial dos serviços essenciais que fornecem. |
| Proteção de Serviços Essenciais | Conjunto de práticas para proteger serviços essenciais de quaisquer riscos e ameaças que possam causar a sua interrupção total ou parcial. |
| Redes | Conjunto de meios que asseguram o fornecimento de uma infraestrutura com produtos ou serviços necessários para o seu funcionamento (comunicações, energia, logística, etc.). |
| Serviço Essencial | Um serviço cuja interrupção total ou parcial pode ter um impacto sério no funcionamento da Guiné-Bissau, na economia do país ou na saúde, segurança e bem-estar dos cidadãos, ou qualquer combinação destes problemas que não se enquadram nos critérios de Infraestruturas Críticas. |
| SLAs | Service Level Agreement (Acordo de Nível de Serviço) |
| SIS | Serviços de Informação de Segurança |
| Sistema de Informação | Qualquer dispositivo isolado ou não isolado ou grupo de dispositivos interconectados que, total ou parcialmente, realiza o processamento automático de dados de acordo com um programa. |
| Centro de Operações de Segurança (SOC) | Unidade centralizada que monitora, deteta, investiga e responde a incidentes de cibersegurança em tempo real. |
| Tecnologias de informação e Comunicação (TIC) | Tecnologias utilizadas para reunir, armazenar, usar e enviar informações, incluindo tecnologias que envolvem o uso de computadores e qualquer sistema de comunicação, incluindo qualquer sistema de telecomunicações. |
| ToR | Termos de Referência |
| UIT | União Internacional das Telecomunicações |
| WARDIP | *Western Africa Regional Digital Integration Program* (Programa Regional de Integração Digital da África Ocidental) |
| WB | Banco Mundial |

# 1. Enquadramento

A implementação eficaz da Estratégia Nacional de Cibersegurança da Guiné-Bissau é sustentada por um Plano de Ação robusto, que serve como a espinha dorsal para a realização dos objetivos estratégicos do país. Este plano é concebido não apenas como uma lista de tarefas, mas como um mapa dinâmico que orienta a execução das políticas de cibersegurança, delineando os passos concretos a seguir.

Dentro do Plano de Ação, cada objetivo e subobjetivo é acompanhado por uma série de iniciativas específicas, claramente definidas, que detalham não só as responsabilidades, mas também os prazos para cada ação. Essa organização é vital para garantir que todos os envolvidos compreendam os seus papéis e contribuições esperadas.

Ao estabelecer uma ligação clara entre a visão estratégica e as ações práticas, o Plano de Ação garante que os esforços sejam sinérgicos e que os recursos sejam alocados de maneira a maximizar a eficiência. Este alinhamento estratégico é essencial para a construção de uma infraestrutura de cibersegurança resiliente.

Adicionalmente, o Plano não especifica apenas “o que” e “a quem” competem as iniciativas, mas também incorpora mecanismos de monitorização e revisão, permitindo que ajustes sejam feitos em resposta a novos desafios e oportunidades. Esta flexibilidade é fundamental para manter o plano relevante e eficaz num campo tão rapidamente evolutivo como o da cibersegurança.

## 2. Partes Interessadas Envolvidas na Cibersegurança da Guiné-Bissau

A implementação de uma Estratégia Nacional de Cibersegurança eficaz na Guiné-Bissau requer a colaboração e o empenho de uma ampla gama de partes interessadas. Este capítulo apresenta as diversas entidades que desempenham papéis cruciais no fortalecimento da cibersegurança nacional. Desde organismos governamentais a instituições privadas, cada um contribui com conhecimentos especializados, recursos e capacidades essenciais para a construção de um ambiente digital seguro e resiliente.

*Tabela 2 – Partes Interessadas Envolvidas na Cibersegurança da Guiné-Bissau*

| Partes Interessadas | Envolvimento Geral |
|---|---|
| **Autoridade Nacional de Cibersegurança** | A Autoridade Nacional de Cibersegurança será a principal entidade coordenadora central para todas as iniciativas de cibersegurança. As suas responsabilidades incluem o desenvolvimento e a implementação de políticas, a supervisão da criação e fortalecimento de unidades especializadas, a monitorização e avaliação contínua das atividades de cibersegurança, e a promoção da cooperação nacional e internacional. A Entidade também estará envolvida na formação de profissionais, na integração de cibersegurança nos currículos educativos e na promoção da inovação através de investigação e desenvolvimento. |
| **Ministro dos Transportes, Telecomunicações e Economia Digital /DGT** | Este Ministério será responsável pela coordenação geral das iniciativas de cibersegurança, supervisão da Entidade, desenvolvimento e implementação de políticas nacionais, e promoção da consciencialização pública. O Ministério também desempenhará um papel importante na captação de recursos, cooperação internacional, e na supervisão das campanhas de sensibilização e formação técnica. |
| **Ministério da Defesa Nacional** | O Ministério da Defesa será essencial na integração de medidas de cibersegurança nas infraestruturas críticas de defesa nacional. O Ministério colaborará na proteção de infraestruturas críticas e na resposta a incidentes relacionados à segurança nacional. Além disso, o Ministério participará da formação do pessoal e da implementação de políticas de segurança. |
| **Ministério da Administração Interna** | Este Ministério desempenhará um papel fundamental na implementação de medidas de cibersegurança para a proteção interna, identificação de infraestruturas críticas, e na colaboração com outras entidades governamentais e privadas. O Ministério também estará envolvido na resposta a incidentes e na coordenação de medidas de proteção. |
| **Ministério da Justiça** | O Ministério da Justiça será responsável pela criação e implementação de legislação específica para cibersegurança e cibercrime, desenvolvimento de procedimentos penais, e formação de autoridades judiciais. O Ministério também colaborará com a Entidade e outras entidades para assegurar a aplicação das leis pertinentes. |

| Partes Interessadas | Envolvimento Geral |
|---|---|
| **Ministério da Economia e Finanças** | Este Ministério desempenhará um papel fundamental na alocação de orçamento e recursos financeiros necessários para as iniciativas de cibersegurança. O Ministério também será responsável pela identificação de fontes de financiamento e pelo desenvolvimento de procedimentos financeiros. |
| **Ministério da Educação Nacional, Ensino Superior e Educação Científica; Universidades; e Centros de Investigação** | O Ministério da Educação Nacional, Ensino Superior e Educação Científica, as Universidades e os Centros de Investigação desempenharão um papel crucial na promoção da cibersegurança. O Ministério será responsável pelo desenvolvimento de currículos educativos, integrando a cibersegurança nos programas escolares, promovendo a formação técnica e profissional, e colaborando na sensibilização pública e na capacitação de professores. As universidades e centros de investigação contribuirão com a investigação avançada, a formação de profissionais qualificados e a promoção da inovação em cibersegurança. Além disso, estas entidades colaborarão com o governo e o setor privado em projetos de investigação, desenvolvimento de normas e padrões de segurança, reforçando a capacidade de resposta nacional. |
| **Autoridade Reguladora Nacional (ARN)** | As entidades reguladoras e autoridades supervisoras, como as de comunicações e privacidade de dados, desempenham um papel fundamental na implementação e supervisão da Estratégia Nacional de Cibersegurança da Guiné-Bissau. Estas entidades garantem que as políticas e práticas de cibersegurança sejam efetivamente aplicadas e conformes com as normas e regulamentos nacionais e internacionais. |
| **Fornecedores de Serviços de Internet (ISPs)** | Os ISPs colaborarão na implementação de medidas de segurança, resposta a incidentes, partilha de informações sobre ameaças e monitorização contínua das redes. Eles também participarão na formação técnica e na promoção de campanhas de consciencialização pública. |
| **Empresas de Tecnologia** | As empresas de tecnologia fornecerão conhecimento e competências técnicas, desenvolverão soluções inovadoras de cibersegurança, participarão em projetos de investigação e desenvolvimento, e colaborarão na formação de profissionais. Elas também estarão envolvidas na certificação de tecnologias e na implementação de sistemas avançados de segurança. |
| **Universidades e Centros de Investigação** | As universidades e centros de investigação contribuirão com a investigação avançada, desenvolvimento de currículos educativos, formação de profissionais qualificados e promoção da inovação em cibersegurança. Estas entidades colaborarão com o governo e o setor privado em projetos de investigação e desenvolvimento de normas e padrões de segurança. |
| **Organizações da Sociedade Civil** | As ONGs e associações de consumidores promoverão a consciencialização pública sobre cibersegurança, defenderão |

| Partes Interessadas | Envolvimento Geral |
|---|---|
| **(PNUD e outras)** | os direitos dos cidadãos no ambiente digital, e apoiarão a implementação de políticas de cibersegurança. Também participarão na monitorização da aplicação das leis e na promoção de campanhas de sensibilização. |
| **Organizações Internacionais (Regionais e Globais) de Cibersegurança** | Estas organizações fornecerão assistência técnica, recursos educacionais, padrões de certificação internacionais e apoio na organização de programas de capacitação. Elas também colaborarão na partilha de melhores práticas e na implementação de convenções internacionais. |
| **Países e Organizações Parceiras (Regionais e Globais)** | Os países e organizações parceiras cooperarão na troca de informações sobre ciberameaças, participação em exercícios conjuntos de resposta a incidentes, e na implementação de melhores práticas. Eles também participarão em programas de capacitação e desenvolvimento de projetos conjuntos de investigação e inovação em cibersegurança. |

## 3. Visão Detalhada das Iniciativas

Nesta secção serão detalhadas as várias iniciativas que serão implementadas como parte integrante da Estratégia Nacional de Cibersegurança da Guiné-Bissau. As 23 iniciativas foram agrupadas nos seguintes principais programas estratégicos:

- **P1. Programa de Governança, Política e Estratégia de Cibersegurança** - Este programa é destinado a estabelecer uma base sólida para a cibersegurança, este programa cria e implementa políticas, estratégias e estruturas de governança, definindo responsabilidades e coordenando ações entre várias entidades para uma abordagem integrada. **[4 Iniciativas]**
- **P2. Programa de Educação, Consciencialização e Capacitação em Cibersegurança** - Este programa tem como objetivo aumentar a literacia digital e a consciencialização sobre cibersegurança em todos os níveis da sociedade, através da implementação programas educacionais, campanhas de sensibilização e a capacitação contínua de profissionais e cidadãos. **[4 Iniciativas]**
- **P3. Programa de Desenvolvimento Legal e Regulamentar** - Este programa visa fortalecer o quadro legal e regulatório para enfrentar eficazmente os desafios da cibersegurança e cibercriminalidade e prevê a criação e atualização de legislações específicas e a padronização de procedimentos legais. **[3 Iniciativas]**
- **P4. Programa de Segurança e Gestão de Infraestruturas Críticas** - Focado na proteção das infraestruturas críticas do país, este programa pressupõe a identificação, avaliação e implementação de medidas de segurança específicas para assegurar a resiliência das infraestruturas contra ciberameaças. **[3 Iniciativas]**
- **P5. Programa de Gestão de Riscos e Resposta a Incidentes** - Este programa concentra-se na identificação, avaliação e mitigação de riscos, além de estabelecer capacidades robustas para a resposta a incidentes de cibersegurança. **[2 Iniciativas]**
- **P6. Programa de Cooperação Intersectorial e Parcerias Estratégicas** - Este programa pretende promover a colaboração entre diferentes setores, tanto públicos quanto privados, para fortalecer a cibersegurança através de parcerias estratégicas e a partilha de informações e recursos. **[2 Iniciativas]**
- **P7. Programa de Cooperação e Alinhamento Regional e Internacional** - Este programa intenta fortalecer a cibersegurança através da cooperação com outras nações e organizações internacionais e regionais, promovendo a troca de informações, melhores práticas e respostas coordenadas a ciberameaças. **[2 Iniciativas]**
- **P8. Programa de Inovação em Cibersegurança** - Centrado no fortalecimento da infraestrutura tecnológica e na promoção da inovação em cibersegurança, este programa pretende incentivar a investigação, o desenvolvimento de novas tecnologias e a certificação de soluções de segurança. **[2 Iniciativas]**
- **P9. Programa de Monitorização e Avaliação** - Este programa visa garantir a eficácia e a melhoria contínua das iniciativas de cibersegurança através de monitorização e avaliação sistemáticas. **[1 Iniciativa]**

Cada uma destas iniciativas está desenhada para responder a requisitos específicos dentro do âmbito abrangente da cibersegurança e são essenciais para a consecução dos objetivos estratégicos previamente estabelecidos na Estratégia Nacional de Cibersegurança da Guiné-Bissau.

Para cada iniciativa foi definido um nível de criticidade, o qual deverá ajudar a priorizar iniciativas e recursos, garantindo que as áreas mais críticas recebam a atenção necessária para fortalecer a segurança digital nacional.

- **Muito Alto**: Este nível de criticidade é atribuído a iniciativas que são essenciais para garantir a segurança e resiliência do ecossistema digital nacional. Qualquer falha ou atraso na implementação destas iniciativas pode ter consequências graves e imediatas para a segurança nacional e a continuidade dos serviços críticos.
- **Alto**: Iniciativas com este nível de criticidade são fundamentais para o fortalecimento e avanço significativo da cibersegurança nacional. São vitais para sustentar o progresso e alcançar um nível mais elevado de maturidade digital no país. A sua implementação é essencial para garantir uma proteção eficaz contra ciberameaças.
- **Médio**: Este nível de criticidade engloba iniciativas importantes para o desenvolvimento contínuo e preparação contra futuras ameaças. Estas medidas ajudam a construir uma base sólida e preparada para enfrentar desafios de cibersegurança de médio prazo, sem serem críticas no curto prazo.
- **Baixo**: Iniciativas como este nível de criticidade focam-se na otimização e inovação contínua, contribuindo para a evolução harmoniosa e eficiente da cibersegurança nacional. Embora não sejam urgentes, são importantes para garantir a sustentabilidade e adaptabilidade a longo prazo do ecossistema digital na Guiné-Bissau.

Adicionalmente, para cada iniciativa, desenvolveram-se projeções de investimento, refletindo os custos mínimos e máximos esperados. Estas projeções são baseadas nos valores padrão do mercado e incorporam uma análise cuidadosa dos recursos humanos e técnicos necessários. Existe também a oportunidade de criar sinergias entre as várias iniciativas, otimizando os recursos já existentes nas organizações envolvidas.

| ***P1. Programa de Governança, Política e Estratégia de Cibersegurança***<br>*Este programa é destinado a estabelecer uma base sólida para a cibersegurança, este programa cria e implementa políticas, estratégias e estruturas de governança, definindo responsabilidades e coordenando ações entre várias entidades para uma abordagem integrada.* | | | | | | |
|---|---|---|---|---|---|---|
| **Subobjetivos Relacionados**<br>**1.1; 1.2; 1.3; 1.4; 5.2; 6.2; 6.3; 7.1; 7.2** | **Objetivos**<br>• Desenvolver uma Política Nacional de Cibersegurança.<br>• Criar e atualizar periodicamente a Estratégia Nacional de Cibersegurança.<br>• Estabelecer um comitê interministerial para coordenar ações de cibersegurança.<br>• Promover a integração das políticas de cibersegurança na governança de TI das organizações.<br>• Garantir a implementação de processos e procedimentos consistentes. | | | | | |
| **Iniciativas** | **Atividades** | **Entidades Envolvidas** | **Criticidade** | **KPIs** | **Orçamento** | **Prazo** |
| **P1.1: Desenvolvimento e Implementação da Política Nacional de Cibersegurança** | **- Análise das Necessidades e Desafios**: Realizar uma análise detalhada do panorama atual da cibersegurança na Guiné-Bissau.<br>**- Consulta de Partes interessadas**: Envolver todas as partes interessadas relevantes, incluindo entidades governamentais, setor privado, academia e sociedade civil, para continuar a recolher contributos e feedback.<br>**- Redação da Política**: Desenvolver a Política Nacional de Cibersegurança, incorporando as melhores práticas internacionais.<br>**- Revisão e Aprovação**: Submeter o rascunho da política a uma revisão abrangente por peritos e partes interessadas e obter a aprovação formal das autoridades competentes.<br><br>**-Promulgação e Disseminação**: Publicar oficialmente a política, desenvolver materiais de comunicação e campanhas | *Entidades Governamentais:*<br>**Autoridade Nacional de Cibersegurança:** Coordenação e desenvolvimento da política.<br>**Ministério dos Transportes, Telecomunicações e Economia Digital /DGT:** Supervisão geral e apoio na elaboração da política.<br>**Ministério da Justiça**: Criação e alinhamento da política com a legislação nacional de cibersegurança.<br><br>*Setor Privado:*<br>**Empresas de Tecnologia da Informação**: Apoio técnico no desenvolvimento e implementação da política.<br>**Fornecedores de Serviços de Internet (ISPs)**: Implementação de medidas de segurança relacionadas à política. | Muito Alta | - Tempo Médio de Resposta a Incidentes de Cibersegurança.<br>- Número de Políticas e Regulamentos Desenvolvidos e Implementados.<br>- Taxa de Consciencialização em Cibersegurança entre as Partes Interessadas | 35.000 USD – 75.000 USD | Curto Prazo<br>(1-2 anos) |

| | | | | | | |
|---|---|---|---|---|---|---|
| | de sensibilização. *(nota: garantir alinhamento com o programa P2. Educação, Consciencialização e Capacitação em Cibersegurança)*<br>**- Monitorização e Avaliação**: Implementar mecanismos de monitorização contínua e realizar avaliações periódicas para assegurar a eficácia e atualização da política. *(nota: garantir alinhamento com a iniciativa P9.1 - Monitorização e Avaliação Integrada)* | *Parceiros Internacionais:*<br>**Organizações Internacionais de Cibersegurança**: Alinhamento da política com padrões e melhores práticas globais. | | | | |
| **P1.2: Criação e Fortalecimento da Autoridade Nacional de Cibersegurança** | **- Promulgação da Legislação Necessária**: Desenvolver e aprovar a legislação que estabelece e regulamenta a Autoridade Nacional de Cibersegurança (ANC).<br>**- Definição da Estrutura Organizacional**: Criar a estrutura organizacional da ANC, definindo as responsabilidades e funções de cada departamento.<br>**- Alocação de Orçamento e Recursos**: Assegurar financiamento adequado e recursos necessários para o funcionamento da ANC.<br>**- Recrutamento de Profissionais Qualificados**: Contratar e formar profissionais especializados em cibersegurança para integrar a ANC.<br>**- Implementação de Sistemas de Monitorização**: Desenvolver e implementar sistemas para monitorizar continuamente ciberameaças e responder de forma eficaz *(nota: garantir alinhamento com a iniciativa P9.1 - Monitorização e Avaliação Integrada).* | *Entidades Governamentais:*<br>**Entidade Responsável pela Coordenação da Implementação da Estratégia Nacional de Cibersegurança / ITMA**: Criação e fortalecimento da Autoridade Nacional de Cibersegurança (ANC).<br>**Ministério dos Transportes, Telecomunicações e Economia Digital /DGT:** Supervisão geral e coordenação da criação da ANC.<br>**Ministério da Justiça**: Desenvolvimento e promulgação de legislação e regulamentações necessárias para formalizar a ANC.<br>**Ministério da Economia e Finanças**: Alocação de orçamento e recursos financeiros necessários para o funcionamento da ANC.<br><br>*Setor Privado:*<br>**Empresas de Tecnologia**: Fornecimento de tecnologias | Muito Alta | - Número de Profissionais Qualificados Recrutados e Formados.<br>- Número de incidentes detetados e respondidos. | 30.000 USD – 60.000 USD | Curto Prazo<br>(1-2 anos) |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | avançadas e suporte técnico necessário para a ANC.<br>**Fornecedores de Serviços de Internet (ISPs)**: Colaboração na implementação de sistemas de monitorização e resposta a incidentes.<br><br>*Parceiros Internacionais:*<br>**Organizações Internacionais de Cibersegurança**: Alinhamento da ANC com padrões e melhores práticas globais.<br>**Países e Regiões Parceiras**: Cooperação e partilha de informações sobre ciberameaças e estratégias de resposta, ajudando no fortalecimento da ANC. | | | | |
| **P1.3: Desenvolvimento e Implementação de Políticas de Segurança e Quadro Nacional de Referência de Cibersegurança** | **- Criação de Políticas de Segurança**: Desenvolver políticas de segurança robustas que abranjam todos os aspetos críticos da cibersegurança.<br>**- Desenvolvimento do Quadro Nacional de Referência de Cibersegurança**: Estabelecer um referencial que forneça diretrizes claras e normas específicas para setores críticos.<br>**- Revisão e Aprovação das Políticas**: Submeter as políticas e o referencial a revisões por partes interessadas e obter aprovação formal.<br>**- Implementação das Políticas**: Promulgar e disseminar as políticas de segurança em todos os setores relevantes.<br>**- Sensibilização e Capacitação**: Realizar campanhas de sensibilização e programas de formação para garantir que todos as | *Entidades Governamentais:*<br>**Entidade Responsável pela Coordenação da Implementação da Estratégia Nacional de Cibersegurança / ITMA**: Coordenação do desenvolvimento e implementação das políticas e do quadro nacional de referência.<br>**Ministério dos Transportes, Telecomunicações e Economia Digital /DGT:** Supervisão geral da implementação das políticas e integração das normas de segurança no setor digital.<br>**Ministério da Justiça**: Colaboração na criação e revisão de normas legais e | Média | - Número de Políticas de Segurança Desenvolvidas e Implementadas.<br>- Taxa de Conformidade com o Quadro Nacional de Referência de Cibersegurança.<br>-Frequência e Eficácia das Revisões e Atualizações das Políticas. | 30.000 USD – 55.000 USD | Médio Prazo<br>(3-4 anos) |

| | | | | | | |
|---|---|---|---|---|---|---|
| | partes interessadas compreendem e aplicam as políticas de segurança. *(nota: garantir alinhamento com o programa P2. Educação, Consciencialização e Capacitação em Cibersegurança)*<br>**- Monitorização e Atualização Contínua**: Implementar um sistema de feedback contínuo e realizar revisões periódicas para atualizar as políticas conforme necessário *(nota: garantir alinhamento com a iniciativa P9.1 - Monitorização e Avaliação Integrada)* | regulamentares necessárias para a implementação das políticas de segurança.<br><br>*Setor Privado:*<br>**Empresas de Tecnologia**: Desenvolvimento e integração de soluções tecnológicas de segurança que estejam alinhadas com as novas políticas.<br>**Fornecedores de Serviços de Internet (ISPs)**: Implementação das normas de segurança estabelecidas nas políticas.<br><br>*Academia e Instituições de Investigação:*<br>**Universidades e centros de investigação**: Apoio no desenvolvimento de diretrizes e normas, além de realizar investigações para aperfeiçoar as políticas de segurança.<br><br>*Parceiros Internacionais:*<br>**Organizações Internacionais de Cibersegurança**: Alinhamento das políticas nacionais com as melhores práticas globais e padrões internacionais.<br>**Países e Regiões Parceiras**: Cooperação para partilha de experiências e melhores práticas na implementação das políticas de segurança. | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **P1.4: Desenvolvimento de Procedimentos para Identificação e Integração de Financiamentos** | **- Identificação de Fontes de Financiamento**: Pesquisar e identificar fontes de financiamento nacionais e internacionais que possam apoiar iniciativas de cibersegurança.<br>**- Desenvolvimento de Procedimentos de Captação de Recursos**: Criar procedimentos e estratégias para a captação eficaz de recursos financeiros.<br>**- Elaboração de Relatórios de Impacto**: Desenvolver relatórios periódicos que avaliem o impacto dos financiamentos na melhoria da cibersegurança, assegurando a prestação de contas e a justificação do uso dos fundos.<br>**- Estabelecimento de Sistema de Monitorização**: Implementar um sistema para monitorizar o uso dos recursos obtidos, garantindo transparência e eficiência na sua utilização *(nota: garantir alinhamento com a iniciativa P9.1 - Monitorização e Avaliação Integrada).* | *Entidades Governamentais:*<br>**Entidade Responsável pela Coordenação da Implementação da Estratégia Nacional de Cibersegurança / ITMA**: Coordenação da iniciativa e supervisão dos procedimentos de captação e uso dos recursos financeiros.<br>**Ministério da Economia e Finanças**: Responsável pela identificação de fontes de financiamento e pelo desenvolvimento de procedimentos financeiros necessários para a captação e gestão dos recursos.<br>**Ministério dos Negócios Estrangeiros**: Encarregado da identificação de oportunidades de financiamento internacional e da cooperação com doadores estrangeiros.<br><br>*Setor Privado:*<br>**Empresas de Consultoria Financeira**: Apoio na identificação de fontes de financiamento e na elaboração de propostas eficazes para a captação de recursos.<br><br>*Academia e Instituições de Investigação:*<br>**Universidades e centros de investigação**: Colaboração na elaboração de propostas para a | Baixa | - Número de Fontes de Financiamento Identificadas.<br>- Valor Total de Financiamento Captado<br>- Taxa de Utilização dos Recursos Obtidos.<br>- Frequência e Qualidade dos Relatórios de Impacto. | 15.000 USD – 25.000 USD | Médio Prazo<br>(3-4 anos) |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | obtenção de financiamento para projetos de investigação em cibersegurança.<br><br>*Parceiros Internacionais:*<br>**Organizações Internacionais de Cibersegurança**: Cooperação na obtenção de financiamentos e na partilha de melhores práticas globais.<br>**Instituições Financeiras Internacionais**: Fornecimento de recursos financeiros e apoio técnico para as iniciativas de cibersegurança. | | | | |

| ***P2. Programa de Educação, Conscienciali*zação e Capacitação em Cibersegurança**<br>*Este programa tem como objetivo aumentar a literacia digital e a consciencialização sobre cibersegurança em todos os níveis da sociedade, através da implementação programas educacionais, campanhas de sensibilização e a capacitação contínua de profissionais e cidadãos.* | | | | | | |
|---|---|---|---|---|---|---|
| **Subobjetivos Relacionados**<br>**1.3; 1.4; 1.5; 2.1; 2.2; 3.2; 3.3; 4.2; 5.1; 5.2; 6.1; 6.2; 6.3; 7.1; 7.2** | **Objetivos**<br>• Desenvolver currículos que integrem cibersegurança nos ensinos básico, secundário e superior.<br>• Realizar campanhas de sensibilização para aumentar a consciência pública sobre cibersegurança.<br>• Oferecer programas de formação contínua para profissionais de TI e segurança.<br>• Promover certificações profissionais reconhecidas internacionalmente em cibersegurança.<br>• Capacitar formadores e educadores em cibersegurança. | | | | | |
| **Iniciativas** | **Atividades** | **Entidades Envolvidas** | **Criticidade** | **KPIs** | **Orçamento** | **Prazo** |
| **P2.1: Desenvolvimento de Capacidades Técnicas e Humanas em Cibersegurança** | **- Desenvolvimento de Currículos Educativos em Cibersegurança**: Criar e implementar currículos específicos em cibersegurança para escolas e universidades.<br>**- Implementação de Programas de Formação Técnica**: Oferecer cursos de formação técnica em cibersegurança para profissionais do setor público e privado.<br>**- Promoção de Certificações Internacionalmente Reconhecidas**: Incentivar a obtenção de certificações reconhecidas globalmente em cibersegurança para padronizar e elevar a qualidade da força de trabalho.<br>**- Realização de Workshops e Seminários Regulares**: Organizar eventos educativos e de capacitação contínua para manter os profissionais atualizados sobre as últimas tendências e técnicas em cibersegurança. | *Entidades Governamentais:*<br>**Autoridade Nacional de Cibersegurança**: Coordenação geral da iniciativa e supervisão das atividades de capacitação. Supervisão e promoção de programas de formação técnica e certificações em cibersegurança.<br><br>**Ministério da Educação Nacional, Ensino Superior e Educação Científica**: Responsável pelo desenvolvimento de currículos educativos em cibersegurança e pela integração destes nos programas escolares e universitários.<br><br>*Setor Privado:*<br>**Empresas de Tecnologia**: Colaboração no | Muito Alta<br>Alta | - Número de Programas de Formação Implementados.<br>- Número de Profissionais Certificados em Cibersegurança.<br>- Taxa de Conclusão dos Cursos de Formação Técnica.<br>- Frequência e Participação em Workshops e Seminários. | 25.000 USD – 45.000 USD | Curto Prazo<br>(1-2 anos) |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | desenvolvimento de currículos educacionais e na oferta de workshops e seminários baseados nas necessidades do mercado.<br>**Fornecedores de Serviços de Internet (ISPs)**: Participação na formação técnica de profissionais para melhorar a segurança das redes.<br><br>*Academia e Instituições de Investigação:*<br>**Universidades e centros de investigação**: Desenvolvimento de programas de graduação e pós-graduação em cibersegurança, além de realizar investigações que inovem nas práticas de ensino.<br>**Instituições Educacionais Técnicas**: Implementação de programas de formação técnica e profissional em cibersegurança.<br><br>*Parceiros Internacionais:*<br>**Organizações Internacionais de Cibersegurança**: Fornecimento de recursos educacionais e apoio na certificação internacional.<br>**Países e Instituições Parceiras**: Cooperação para o desenvolvimento de programas de intercâmbio e capacitação técnica em cibersegurança. | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| **P2.2: Promoção e Disseminação de Cultura e Recursos de Cibersegurança** | **- Campanhas de Sensibilização Pública:** Desenvolver e implementar campanhas de sensibilização para aumentar a consciencialização sobre a importância da cibersegurança entre os cidadãos.<br>**- Desenvolvimento de Materiais Educativos:** Criar materiais educativos acessíveis e compreensíveis que ensinem práticas seguras no ambiente digital.<br>**- Integração da Cibersegurança nos Currículos Escolares:** Incorporar módulos de cibersegurança nos currículos das escolas primárias e secundárias.<br>**- Promoção de Eventos e Conferências:** Organizar eventos, workshops e conferências para discutir temas de cibersegurança e promover a troca de conhecimentos. | *Entidades Governamentais:*<br>**Autoridade Nacional de Cibersegurança**: Coordenação geral das campanhas de sensibilização e disseminação de recursos de cibersegurança.<br><br>**Ministério da Educação Nacional, Ensino Superior e Educação Científica**: Supervisão da integração de cibersegurança nos currículos escolares e no desenvolvimento de materiais educativos.<br><br>**Ministério dos Transportes, Telecomunicações e Economia Digital /DGT:** Coordenação das campanhas de sensibilização pública e promoção de eventos sobre cibersegurança.<br><br>*Setor Privado:*<br>**Empresas de Tecnologia**: Apoio no desenvolvimento de materiais educativos e recursos online, além de participação e patrocínio em eventos e conferências de cibersegurança.<br>**Fornecedores de Serviços de Internet (ISPs)**: Divulgação de campanhas de sensibilização através das suas plataformas e suporte técnico no desenvolvimento de recursos digitais. | Muito Alta | - Número de Campanhas de Sensibilização Realizadas<br>- Quantidade de Materiais Educativos Distribuídos.<br>- Número de Escolas com Currículos Integrados de Cibersegurança.<br>- Nível de Consciencialização Pública sobre Práticas de Cibersegurança. | 20.000 USD – 30.000 USD | Curto Prazo<br>(1-2 anos) |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | *Academia e Instituições de Investigação:*<br>**Universidades e centros de investigação**: Colaboração no desenvolvimento de currículos e materiais educativos, além de organização de conferências e workshops sobre cibersegurança.<br>**Escolas e Instituições Educacionais**: Implementação de programas educativos e participação ativa em campanhas de sensibilização.<br><br>*Organizações da Sociedade Civil:*<br>**ONGs**: Condução de campanhas de sensibilização e organização de eventos comunitários sobre cibersegurança.<br>**Associações de Consumidores**: Promoção da consciencialização pública sobre direitos e responsabilidades no ambiente digital.<br><br>*Parceiros Internacionais:*<br>**Organizações Internacionais de Cibersegurança**: Fornecimento de materiais educativos e apoio na organização de eventos e conferências.<br>**Países e Instituições Parceiras**: Cooperação para a partilha de melhores práticas e recursos educacionais, além de participação em eventos | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | internacionais sobre cibersegurança. | | | | |
| **P2.3: Capacitação de Profissionais e Decisores em Cibersegurança** | **- Programas de Formação Contínua**: Desenvolver e implementar programas de formação contínua em cibersegurança para profissionais de TI e decisores.<br>**- Workshops Especializados**: Organizar workshops especializados focados em temas avançados de cibersegurança e gestão de riscos.<br>**- Certificações Reconhecidas Internacionalmente**: Promover e facilitar a obtenção de certificações de cibersegurança reconhecidas internacionalmente para elevar os padrões de competência.<br>**- Desenvolvimento de Competências de Liderança**: Implementar programas de desenvolvimento de competências de liderança para decisores em cibersegurança, ajudando-os a tomar decisões estratégicas eficazes. | *Entidades Governamentais:*<br>**Autoridade Nacional de Cibersegurança**: Coordenação geral da iniciativa e supervisão dos programas de formação em cibersegurança.<br>**Ministério dos Transportes, Telecomunicações e Economia Digital /DGT:** Supervisão e coordenação dos programas de formação voltados para profissionais e decisores.<br>**Ministério da Administração Interna**: Foco na capacitação de decisores e profissionais ligados à segurança interna.<br>**Ministério da Educação Nacional, Ensino Superior e Educação Científica**: Colaboração na integração da cibersegurança nos programas de formação técnica e profissional.<br><br>*Setor Privado:*<br>**Empresas de Tecnologia**: Contribuição na oferta de workshops e cursos especializados, além de parcerias para certificações internacionais.<br>**Fornecedores de Serviços de Internet (ISPs)**: Participação na formação de seus profissionais e | Alta | - Número de Programas de Formação Contínua Implementados.<br>- Número de Workshops Especializados Realizados<br>- Número de Certificações Obtidas por Profissionais.<br>- Taxa de Participação em Programas de Desenvolvimento de Liderança. | 20.000 USD – 30.000 USD | Médio Prazo<br>(3-4 anos) |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | fornecimento de apoio técnico para iniciativas de capacitação.<br><br>*Academia e Instituições de Investigação:*<br>**Universidades e centros de investigação**: Desenvolvimento e oferta de programas de graduação e pós-graduação em cibersegurança, além de cursos de formação contínua para profissionais.<br>**Escolas Técnicas e Profissionais**: Implementação de programas de capacitação técnica focados em cibersegurança.<br><br>*Parceiros Internacionais:*<br>**Organizações Internacionais de Cibersegurança**: Fornecimento de recursos educacionais e apoio na organização de workshops e cursos especializados.<br>**Países e Instituições Parceiras**: Colaboração no desenvolvimento de programas de intercâmbio e capacitação técnica, bem como na participação em eventos internacionais. | | | | |
| **P2.4: Capacitação de Autoridades Judiciais e Policias em Cibersegurança e Cibercrime** | **- Desenvolvimento de Currículos de Formação Específicos**: Criar currículos de formação em cibersegurança e cibercrime adaptados às necessidades das autoridades judiciais e policiais.<br>**- Formações Regulares**: Implementar programas de treinamento contínuo para | *Entidades Governamentais:*<br>**Autoridade Nacional de Cibersegurança:** Coordenação geral da iniciativa.<br>**Ministério da Justiça**: Supervisão da formação das autoridades judiciais e | Alta | - Número de Currículos de Formação Desenvolvidos.<br>- Número de Formações e Workshops Realizados.<br>- Taxa de Participação em Formações e Workshops. | 20.000 USD – 35.000 USD | Médio Prazo<br>(3-4 anos) |

| | | | | | | |
|---|---|---|---|---|---|---|
| | manter as autoridades atualizadas sobre as últimas ameaças e técnicas de investigação.<br>**- Workshops Práticos**: Organizar workshops práticos que forneçam experiências práticas em investigação e resposta a cibercrimes.<br>**- Exercícios Simulados**: Realizar exercícios de simulação para testar e melhorar a capacidade de resposta a incidentes de cibercrime.<br>**- Promoção da Cooperação**: Incentivar a cooperação entre as autoridades judiciais e policiais para melhorar a coordenação e eficácia no combate ao cibercrime. | desenvolvimento de currículos específicos.<br>**Ministério da Administração Interna**: Supervisão da formação das forças policiais e implementação dos programas de treino.<br>**Procuradoria-Geral da República**: Colaboração no desenvolvimento de currículos e participação nos programas de capacitação.<br><br>*Setor Privado:*<br>**Empresas de Tecnologia**: Fornecimento de conhecimento técnico e participação na organização de workshops práticos e exercícios de simulação.<br><br>*Academia e Instituições de Investigação:*<br>**Universidades e centros de investigação**: Desenvolvimento de currículos de formação e oferta de cursos especializados em cibersegurança e cibercrime.<br>**Instituições Educacionais Técnicas**: Implementação de programas de formação técnica para autoridades judiciais e policiais.<br><br>*Parceiros Internacionais:*<br>**Organizações Internacionais de Cibersegurança**: Fornecimento | | - Melhoria Mensurável na Capacidade de Prevenção, Deteção, Investigação e Processamento de Cibercrimes. | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | de recursos educacionais e apoio na organização de programas de capacitação.<br>**Países e Instituições Parceiras**: Cooperação para o desenvolvimento de programas de intercâmbio e formação conjunta, além de participação em conferências e workshops internacionais sobre cibercrime. | | | | |

| ***P3. Programa de Desenvolvimento Legal e Regulamentar*** | | | | | | |
|---|---|---|---|---|---|---|
| *Este programa visa fortalecer o quadro legal e regulatório para enfrentar eficazmente os desafios da cibersegurança e cibercriminalidade e prevê a criação e atualização de legislações específicas e a padronização de procedimentos legais.* | | | | | | |
| **Subobjetivos Relacionados**<br>**1.1; 1.2; 5.1; 5.2; 6.1** | **Objetivos**<br>• Desenvolver e promulgar leis específicas para cibercrimes.<br>• Definir sanções apropriadas para diferentes tipos de cibercrimes.<br>• Padronizar procedimentos penais para investigação e julgamento de cibercrimes.<br>• Proporcionar formação contínua para autoridades judiciais e policiais sobre cibercriminalidade.<br>• Realizar campanhas de sensibilização sobre novas legislações de cibersegurança. | | | | | |
| **Iniciativas** | **Atividades** | **Entidades Envolvidas** | **Criticidade** | **KPIs** | **Orçamento** | **Prazo** |
| **P3.1:** Criação e Implementação da Estratégia Nacional de Combate à Cibercriminalidade Alinhada com Convenções Internacionais | **- Revisão de Convenções e Normas Internacionais**: Analisar e revisar as convenções e normas internacionais relevantes em cibercrime e cibersegurança.<br>**- Desenvolvimento da Estratégia Nacional**: Integrar os requisitos internacionais na elaboração da Estratégia Nacional de Combate ao Cibercrime .<br>**- Promoção da Ratificação de Convenções**: Promover a ratificação das convenções internacionais de cibercrime pela Guiné-Bissau.<br>**- Estabelecimento de Plano de Ação**: Criar um plano de ação detalhado para a implementação da Estratégia Nacional de Combate ao Cibercrime, incluindo cronogramas e responsabilidades.<br>**- Capacitação e Sensibilização**: Realizar campanhas de capacitação e sensibilização para garantir que todas as partes interessadas compreendem e | *Entidades Governamentais:*<br>**Autoridade Nacional de Cibersegurança:** Coordenação geral da iniciativa.<br>**Ministério da Justiça**: Supervisão da integração de requisitos internacionais na estratégia nacional.<br>**Ministério dos Negócios Estrangeiros**: Promoção da ratificação de convenções internacionais e facilitação da cooperação com parceiros internacionais.<br>**Procuradoria-Geral da República**: Participação no desenvolvimento e implementação da estratégia.<br><br>*Setor Privado:*<br>**Empresas de Tecnologia**: Fornecimento de conhecimento técnico e apoio na | Alta | - Número de Convenções Internacionais Revisadas e Integradas.<br>- Ratificação de Convenções Internacionais pela Guiné-Bissau.<br>- Implementação do Plano de Ação (percentagem dos objetivos alcançados). | 20.000 USD – 35.000 USD | Curto Prazo<br>(1-2 anos) |

| | | | | | | |
|---|---|---|---|---|---|---|
| | apoiam a Estratégia Nacional de Combate ao Cibercrime. *(nota: garantir alinhamento com o programa P2. Educação, Consciencialização e Capacitação em Cibersegurança)*<br>**- Monitorização e Avaliação:** Implementar mecanismos de monitorização contínua e avaliação da eficácia da estratégia *(nota: garantir alinhamento com a iniciativa P9.1 - Monitorização e Avaliação Integrada).* | implementação de melhores práticas internacionais.<br>**Fornecedores de Serviços de Internet (ISPs)**: Colaboração na implementação de medidas de segurança e integração de requisitos internacionais.<br><br>*Academia e Instituições de Investigação:*<br>**Universidades e centros de investigação**: Desenvolvimento de estudos para apoiar a estratégia e implementação de convenções internacionais.<br>**Instituições Educacionais Técnicas**: Capacitação de profissionais e desenvolvimento de currículos alinhados com normas internacionais.<br><br>*Parceiros Internacionais:*<br>**Organizações Internacionais de Cibersegurança**: Fornecimento de assistência técnica e apoio na implementação de convenções internacionais.<br>**Países e Instituições Parceiras**: Cooperação para o desenvolvimento e implementação da estratégia nacional e partilha de melhores práticas. | | | | |
| **P3.2:** Desenvolvimento e Padronização da Legislação e Procedimentos Penais para Cibercrimes | **- Redação e Promulgação de Leis Específicas**: Elaborar e aprovar legislação específica que aborde todos os aspetos dos cibercrimes, desde a definição de crimes até as penalidades. | *Entidades Governamentais:*<br>**Autoridade Nacional de Cibersegurança:** Coordenação da iniciativa. | Alta | - Número de Leis Específicas para Cibercrimes Redigidas e Promulgadas. | 15.000 USD – 30.000 USD | Médio Prazo<br>(3-4 anos) |

| | | | | | | |
|---|---|---|---|---|---|---|
| | **- Desenvolvimento de Procedimentos Penais Detalhados**: Criar procedimentos detalhados para a investigação, julgamento e punição de cibercrimes, assegurando clareza e consistência.<br>**- Consultas com Especialistas Jurídicos e Técnicos**: Envolver especialistas em direito e cibersegurança para garantir que as leis e procedimentos são eficazes e abrangentes.<br>**- Promoção de Programas de Capacitação**: Implementar programas contínuos de formação para autoridades judiciais e policiais, capacitando-os para lidar com cibercrimes de forma eficiente *(nota: garantir alinhamento com o programa P2. Educação, Consciencialização e Capacitação em Cibersegurança).*<br>**- Monitorização e Revisão das Leis e Procedimentos**: Estabelecer um sistema para monitorar a eficácia da legislação e dos procedimentos, e realizar revisões periódicas conforme necessário *(nota: garantir alinhamento com a iniciativa P9.1 - Monitorização e Avaliação Integrada).* | **Ministério da Justiça**: Liderança na redação e promulgação das leis, bem como no desenvolvimento de procedimentos penais.<br>**Procuradoria-Geral da República**: Participação na elaboração da legislação e supervisão dos processos judiciais.<br><br>*Setor Privado:*<br>**Empresas de Tecnologia**: Consultoria técnica e fornecimento de tecnologias de apoio à investigação.<br>**Fornecedores de Serviços de Internet (ISPs)**: Colaboração na aplicação das leis e fornecimento de dados para investigações.<br><br>*Parceiros Internacionais:*<br>**Organizações Internacionais de Cibersegurança**: Assistência técnica e partilha de melhores práticas na criação da legislação.<br>**Países e Instituições Parceiras**: Cooperação para troca de experiências e capacitação conjunta. | | - Desenvolvimento e Implementação de Procedimentos Penais.<br>- Frequência de Revisões e Atualizações da Legislação.<br>- Melhoria na Eficiência de Investigação e Julgamento de Cibercrimes. | | |
| **P3.3:** Criação e Implementação de Unidades Especializadas de Combate ao Cibercrime | **- Criação de Unidades Especializadas**: Criar unidades dedicadas ao combate ao cibercrime dentro das forças policiais.<br>**- Formação dos Membros das Unidades Especializadas**: Desenvolver e implementar programas de formação | *Entidades Governamentais:*<br>**Autoridade Nacional de Cibersegurança:** Coordenação geral da iniciativa.<br>**Ministério da Administração Interna**: Coordenação da | Baixa | - Número de Unidades Especializadas Criadas.<br>- Número de Profissionais Formados em Técnicas de Combate ao Cibercrime. | 30.000 USD – 45.000 USD | Longo Prazo<br>(5+ anos) |

| | | | | | | |
|---|---|---|---|---|---|---|
| | especializados em técnicas avançadas de combate ao cibercrime.<br>**- Capacitação das Unidades Especializadas com Ferramentas e Tecnologias Avançadas**: Equipar as unidades com as ferramentas e tecnologias necessárias para investigar, prevenir e responder eficazmente a cibercrimes.<br>**- Promoção da Cooperação e Partilha de Informações**: Incentivar a cooperação e a partilha de informações entre unidades nacionais e internacionais para fortalecer a capacidade de resposta a cibercrimes.<br>**- Monitorização e Avaliação Contínua**: Implementar sistemas de monitorização e avaliação contínua para medir a eficácia das unidades especializadas e ajustar as estratégias conforme necessário *(nota: garantir alinhamento com a iniciativa P9.1 - Monitorização e Avaliação Integrada).* | criação e implementação das unidades especializadas.<br>**Polícia Nacional**: Implementação direta das unidades e formação dos membros em técnicas de combate ao cibercrime.<br>**Ministério da Justiça**: Suporte legal e coordenação com a Procuradoria-Geral da República.<br><br>*Setor Privado:*<br>**Empresas de Tecnologia**: Fornecimento de ferramentas e tecnologias avançadas para equipar as unidades especializadas.<br>**Fornecedores de Serviços de Internet (ISPs)**: Colaboração na investigação de cibercrimes e partilha de dados relevantes.<br><br>*Parceiros Internacionais:*<br>**Organizações Internacionais de Cibersegurança**: Assistência técnica e recursos para a formação e equipagem das unidades.<br>**Forças Policiais de Outros Países**: Cooperação para partilha de informações e melhores práticas, além de participação em operações conjuntas e programas de capacitação. | | - Nível de Cooperação e Partilha de Informações com Unidades Internacionais. | | |

| ***P4. Programa de Segurança e Gestão de Infraestruturas Críticas***<br>*Focado na proteção das infraestruturas críticas do país, este programa pressupõe a identificação, avaliação e implementação de medidas de segurança específicas para assegurar a resiliência das infraestruturas contra ciberameaças.* | | | | | | |
|---|---|---|---|---|---|---|
| **Subobjetivos Relacionados**<br>**3.1; 3.2** | **Objetivos**<br>• Identificar e catalogar infraestruturas críticas.<br>• Realizar auditorias regulares de segurança.<br>• Desenvolver e implementar planos de proteção e resposta para infraestruturas críticas.<br>• Implementar políticas de notificação de incidentes.<br>• Capacitar e formar profissionais em cibersegurança para gestão de infraestruturas críticas. | | | | | |
| **Iniciativas** | **Atividades** | **Entidades Envolvidas** | **Criticidade** | **KPIs** | **Orçamento** | **Prazo** |
| **P4.1: Desenvolvimento e Implementação de Políticas e Planos de Proteção e Resposta para Infraestruturas Críticas** | **- Identificação de Infraestruturas Críticas**: Mapear e identificar infraestruturas críticas na Guiné-Bissau que necessitam de proteção especial.<br>**- Avaliação de Vulnerabilidades**: Realizar avaliações detalhadas para identificar vulnerabilidades e riscos associados a cada infraestrutura crítica.<br>**- Desenvolvimento de Políticas de Proteção**: Criar políticas de proteção específicas para cada infraestrutura crítica, alinhadas com as melhores práticas internacionais.<br>**- Implementação de Planos de Resposta a Incidentes**: Desenvolver e implementar planos eficazes de resposta a incidentes para minimizar o impacto de possíveis ataques ou falhas.<br>**- Realização de Exercícios de Simulação**: Realizar exercícios regulares de simulação de incidentes para testar e melhorar a preparação e resiliência das infraestruturas críticas. | *Entidades Governamentais:*<br>**Autoridade Nacional de Cibersegurança:** Coordenação geral da iniciativa. Desenvolvimento e monitorização das políticas de proteção e planos de resposta a incidentes.<br>**Ministério dos Transportes, Telecomunicações e Economia Digital /DGT:** Supervisão do desenvolvimento das políticas e planos de proteção.<br>**Ministério da Administração Interna**: Colaboração na identificação de infraestruturas críticas e avaliação de vulnerabilidades.<br>**Ministério da Defesa Nacional**: Implementação de medidas de proteção para infraestruturas críticas relacionadas à segurança nacional. | Alta | - Número de Infraestruturas Críticas Identificadas e Avaliadas.<br>- Desenvolvimento e Adoção de Políticas de Proteção para Infraestruturas Críticas.<br>- Implementação de Planos de Resposta a Incidentes.<br>- Frequência e Resultados dos Exercícios de Simulação de Incidentes.<br>- Redução de Vulnerabilidades e Riscos Identificados nas Avaliações. | 25.000 USD – 40.000 USD | Curto Prazo<br>(1-2 anos) |

| | | | | | | |
|---|---|---|---|---|---|---|
| | **- Monitorização e Atualização Contínua**: Estabelecer sistemas de monitorização contínua e atualização das políticas e planos para garantir sua eficácia e relevância diante de novas ameaças *(nota: garantir alinhamento com a iniciativa P9.1 - Monitorização e Avaliação Integrada).* | *Setor Privado:*<br>**Empresas de Energia e Telecomunicações**: Participação na identificação de infraestruturas críticas e desenvolvimento de políticas de proteção.<br>**Instituições Financeiras**: Implementação de planos de resposta a incidentes e colaboração em exercícios de simulação.<br>**Empresas de Tecnologia**: Fornecimento de soluções tecnológicas e expertise para a proteção e resposta a incidentes.<br><br>*Parceiros Internacionais:*<br>**Organizações Internacionais de Cibersegurança**: Assistência técnica e partilha de melhores práticas.<br>**Países e Instituições Parceiras**: Cooperação para exercícios conjuntos de simulação e troca de experiências sobre proteção de infraestruturas críticas. | | | | |
| **P4.2: Capacitação e Implementação de Sistemas Avançados em Infraestruturas Críticas** | **- Identificação das Necessidades de Segurança**: Avaliar e identificar as necessidades específicas de cibersegurança das infraestruturas críticas na Guiné-Bissau.<br>**- Implementação de Sistemas Avançados de Monitorização e Proteção**: Instalar e configurar sistemas avançados de cibersegurança que incluam | *Entidades Governamentais:*<br>**Autoridade Nacional de Cibersegurança:** Coordenação geral da iniciativa. Identificação das necessidades de segurança, implementação de sistemas avançados.<br>**Ministério dos Transportes, Telecomunicações e Economia** | Média | - Número de Infraestruturas Críticas Avaliadas e Necessidades Identificadas.<br>- Redução no Número de Incidentes de Cibersegurança em Infraestruturas Críticas. | 30.000 USD – 45.000 USD | Médio Prazo<br>(3-4 anos) |

| | | | | | | |
|---|---|---|---|---|---|---|
| | monitorização, deteção e resposta a ameaças.<br>**- Formação de Pessoal Qualificado**: Capacitar profissionais para operar, manter e atualizar os sistemas avançados de cibersegurança.<br>**- Realização de Auditorias Regulares**: Realizar auditorias periódicas para avaliar a eficácia dos sistemas implementados e garantir a conformidade com as melhores práticas de segurança.<br>**- Atualização e Manutenção Contínua**: Implementar um plano de manutenção contínua para garantir que os sistemas de cibersegurança permaneçam atualizados e eficazes contra novas ameaças. | **Digital /DGT:** Supervisão da implementação dos sistemas de cibersegurança.<br>**Ministério da Administração Interna**: Colaboração na identificação de infraestruturas críticas e apoio na implementação de medidas de segurança.<br>**Ministério da Defesa Nacional**: Proteção de infraestruturas críticas relacionadas à segurança nacional.<br><br>*Setor Privado:*<br>**Empresas de Tecnologia**: Fornecimento de sistemas avançados de monitorização e proteção, e formação de pessoal.<br>**Fornecedores de Serviços de Internet (ISPs)**: Colaboração na implementação de sistemas de monitorização e proteção de redes críticas.<br><br>*Parceiros Internacionais:*<br>**Organizações Internacionais de Cibersegurança**: Assistência técnica e partilha de melhores práticas.<br>**Países e Instituições Parceiras**: Cooperação na troca de conhecimentos e participação em formação conjunta. | | | | |
| **P4.3: Realização de Auditorias a Infraestruturas Críticas** | **- Auditorias de Segurança Periódicas:** Realizar auditorias de segurança regulares para avaliar a proteção das | *Entidades Governamentais:*<br>**Autoridade Nacional de Cibersegurança:** Coordenação | Baixa | - Frequência e Resultados das Auditorias de Segurança. | 20.000 USD – 30.000 USD | Longo Prazo<br>(5+ anos) |

| | | | | | | |
|---|---|---|---|---|---|---|
| | infraestruturas críticas e identificar áreas de melhoria.<br>**- Implementação de Recomendações de Auditoria:** Desenvolver e aplicar planos de ação baseados nas recomendações das auditorias para melhorar a segurança das infraestruturas.<br>**- Monitorização Contínua:** Implementar sistemas de monitorização contínua para detetar e responder a vulnerabilidades e incidentes em tempo real.<br>**- Revisão e Atualização das Medidas de Segurança:** Revisar e atualizar periodicamente as medidas de segurança para assegurar que permanecem eficazes diante de novas ameaças. | geral da iniciativa. Realização das auditorias de segurança, implementação das recomendações e monitorização contínua das infraestruturas críticas.<br>**Ministério dos Transportes, Telecomunicações e Economia Digital /DGT:** Supervisão da identificação e auditoria das infraestruturas críticas.<br><br>*Setor Privado:*<br>**Empresas de Energia e Telecomunicações**: Participação na auditoria e implementação das recomendações de segurança.<br>**Empresas de Tecnologia**: Fornecimento de ferramentas e soluções tecnológicas para auditorias de segurança.<br><br>*Parceiros Internacionais:*<br>**Organizações Internacionais de Cibersegurança**: Assistência técnica e partilha de melhores práticas para auditorias.<br>**Países e Instituições Parceiras**: Cooperação na realização de auditorias conjuntas e troca de experiências. | | - Taxa de Implementação das Recomendações de Auditoria.<br>- Tempo de Resposta a Vulnerabilidades e Incidentes.<br>- Melhoria na Classificação de Segurança das Infraestruturas Críticas após Auditorias.<br>- Redução no Número de Incidentes de Segurança Reportados. | | |

| ***P5. Programa de Gestão de Riscos e Resposta a Incidentes***<br>*Este programa concentra-se na identificação, avaliação e mitigação de riscos, além de estabelecer capacidades robustas para a resposta a incidentes de cibersegurança* | | | | | | |
|---|---|---|---|---|---|---|
| **Subobjetivos Relacionados**<br>**1.3; 1.4; 3.3; 4.2** | **Objetivos**<br>• Desenvolver uma política nacional de gestão de riscos.<br>• Desenvolver o Plano Nacional de Resposta a Incidentes.<br>• Implementar um sistema de gestão de incidentes de cibersegurança.<br>• Criar e fortalecer um centro de resposta a incidentes (CSIRT).<br>• Realizar avaliações regulares de riscos e desenvolver estratégias de mitigação.<br>• Promover a formação contínua dos profissionais responsáveis pela gestão de incidentes. | | | | | |
| **Iniciativas** | **Atividades** | **Entidades Envolvidas** | **Criticidade** | **KPIs** | **Orçamento** | **Prazo** |
| **P5.1: Criação, Operacionalização e Definição de Processos da CSIRT Nacional** | **- Criação da Estrutura Organizacional da CSIRT**: Estabelecer a estrutura organizacional, definir os papéis e responsabilidades dentro da CSIRT.<br>**- Desenvolvimento do Plano Nacional de Resposta a Incidentes**: Criar um plano abrangente que detalhe as estratégias para identificação, análise, resposta e recuperação de incidentes de cibersegurança. Este plano deverá integrar-se aos processos da CSIRT e alinhar-se com as políticas nacionais e internacionais de cibersegurança.<br>**- Desenvolvimento de Processos e Procedimentos de Resposta a Incidentes**: Criar e documentar processos e procedimentos detalhados para a deteção, análise e mitigação de incidentes de cibersegurança.<br>**- Formação da Equipa da CSIRT**: Recrutar e formar a equipa da CSIRT, garantindo | *Entidades Governamentais:*<br>**Autoridade Nacional de Cibersegurança:** Coordenação geral da iniciativa. Gestão diária da CSIRT, desenvolvimento de processos e procedimentos, e formação da equipa.<br><br>*Setor Privado:*<br>**Empresas de Tecnologia**: Fornecimento de tecnologias e ferramentas para monitorização e resposta a incidentes.<br>**Fornecedores de Serviços de Internet (ISPs)**: Colaboração na deteção de ameaças e monitorização de redes.<br><br>*Parceiros Internacionais:*<br>**Organizações Internacionais de Cibersegurança**: Assistência | Muito Alta | - Tempo de Resposta a Incidentes de Cibersegurança.<br>- Número de Incidentes Detetados e Mitigados.<br>- Nível de Conformidade com Procedimentos Documentados.<br>- Taxa de Cooperação e Partilha de Informações com Entidades Relevantes. | 25.000 USD – 40.000 USD | Curto Prazo<br>(1-2 anos) |

| | | | | | | |
|---|---|---|---|---|---|---|
| | que os membros possuam as competências necessárias para responder eficazmente a incidentes.<br>**- Implementação de Sistema de Monitorização e Alerta de Incidentes**: Desenvolver e implementar um sistema para monitorizar continuamente as ciberameaças e emitir alertas de incidentes.<br>**- Promoção da Cooperação e Partilha de Informações**: Incentivar a cooperação e a partilha de informações com outras entidades nacionais e internacionais relevantes. | técnica, fornecimento de melhores práticas e apoio na formação da equipa da CSIRT.<br>**Países e Instituições Parceiras**: Cooperação para troca de informações sobre ciberameaças e participação em exercícios de resposta a incidentes. | | | | |
| **P5.2: Desenvolvimento e Implementação de uma Política Nacional de Gestão de Riscos** | **- Revisão de Melhores Práticas Internacionais:** Analisar políticas de gestão de riscos bem-sucedidas e adaptá-las às necessidades da Guiné-Bissau.<br>**- Desenvolvimento da Política Nacional de Gestão de Riscos:** Criar uma política abrangente que inclua diretrizes para identificação, avaliação, mitigação e monitorização de ciber-riscos.<br>**- Identificação e Avaliação de Riscos em Setores Críticos:** Realizar avaliações de risco detalhadas para identificar ameaças e vulnerabilidades em infraestruturas e serviços essenciais.<br>**- Implementação de Medidas de Mitigação:** Desenvolver e implementar planos de mitigação de riscos baseados nos resultados das avaliações.<br>**- Formação e Capacitação:** Capacitar profissionais em setores críticos sobre a nova política e as melhores práticas de gestão de riscos. *(nota: garantir alinhamento com o programa P2.* | *Entidades Governamentais:*<br>**Autoridade Nacional de Cibersegurança:** Coordenação geral da iniciativa. Desenvolvimento da política, identificação e avaliação de riscos, e implementação de medidas de mitigação.<br><br>*Setor Privado:*<br>**Empresas de Tecnologia**: Fornecimento de ferramentas e conhecimento para a identificação e mitigação de ciber-riscos.<br>**Fornecedores de Serviços de Internet (ISPs)**: Colaboração na identificação de riscos em redes de comunicação e implementação de medidas de mitigação.<br><br>*Parceiros Internacionais:* | Alta | - Número de Avaliações de Riscos Conduzidas em Setores Críticos.<br>- Percentagem de medidas implementadas.<br>- Redução de Riscos Identificados nas Avaliações Periódicas. | 25.000 USD – 40.000 USD | Curto Prazo<br>(1-2 anos) |

| | | | | | | |
|---|---|---|---|---|---|---|
| | *Educação, Consciencialização e Capacitação em Cibersegurança)*<br>**- Monitorização Contínua e Revisão Regular:** Estabelecer sistemas para monitorizar continuamente os riscos e revisar a política regularmente para garantir melhorias contínuas *(nota: garantir alinhamento com a iniciativa P9.1 - Monitorização e Avaliação Integrada).* | **Organizações Internacionais de Cibersegurança**: Assistência técnica e partilha de melhores práticas para o desenvolvimento e implementação da política.<br>**Países e Instituições Parceiras**: Cooperação na troca de informações sobre ciber-riscos e participação em programas de capacitação e exercícios conjuntos. | | | | |

| ***P6. Programa de Cooperação Intersectorial e Parcerias Estratégicas***<br>*Este programa pretende promover a colaboração entre diferentes setores, tanto públicos quanto privados, para fortalecer a cibersegurança através de parcerias estratégicas e a partilha de informações e recursos.* | | | | | | |
|---|---|---|---|---|---|---|
| **Subobjetivos Relacionados**<br>**1.3; 1.5; 2.2; 3.2; 4.2; 5.2; 5.4** | **Objetivos**<br>• Estabelecer plataformas de diálogo e colaboração entre Governo, setor privado, academia e sociedade civil.<br>• Desenvolver parcerias estratégicas para iniciativas conjuntas de cibersegurança.<br>• Facilitar a partilha de informações e boas práticas entre os diferentes setores.<br>• Promover a criação de parcerias público-privadas.<br>• Realizar campanhas de sensibilização sobre a importância da coordenação intersectorial. | | | | | |
| **Iniciativas** | **Atividades** | **Entidades Envolvidas** | **Criticidade** | **KPIs** | **Orçamento** | **Prazo** |
| **P6.1: Coordenação Intersectorial e Partilha de Informação** | **- Estabelecimento de Plataformas de Diálogo:** Criar e implementar plataformas que facilitem a comunicação e a partilha de informações entre setores públicos e privados.<br>**- Desenvolvimento de Procedimentos para Partilha Segura de Informações:** Estabelecer normas e procedimentos para garantir a partilha segura de informações sensíveis entre as partes interessadas.<br>**- Promoção de Encontros Regulares entre Partes Interessadas:** Organizar reuniões e workshops regulares para fomentar a colaboração e a troca de conhecimentos entre os diferentes setores.<br>**- Facilitação da Comunicação Contínua:** Implementar sistemas de comunicação que permitam uma interação constante e eficaz entre os setores.<br>**- Monitorização e Avaliação da Coordenação e Partilha de Informação:** | *Entidades Governamentais:*<br>**Autoridade Nacional de Cibersegurança:** Liderança na coordenação da iniciativa e na facilitação da comunicação entre os setores governamentais. : Desenvolvimento de procedimentos de partilha segura de informações entre as instituições públicas e organização de encontros regulares.<br>**Ministério dos Transportes, Telecomunicações e Economia Digital /DGT:** Supervisão geral das plataformas de diálogo e da implementação das práticas de cibersegurança entre as entidades governamentais.<br>**Ministério da Defesa Nacional**: Partilha de informações sobre ameaças e vulnerabilidades que | Média | - Número de Procedimentos de Partilha Segura de Informações Desenvolvidos.<br>- Frequência e Participação em Encontros e Workshops Regulares.<br>- Nível de Satisfação das Partes Interessadas com a Coordenação e Partilha de Informação. | 20.000 USD – 30.000 USD | Curto Prazo<br>(1-2 anos) |

| | | | | | | |
|---|---|---|---|---|---|---|
| | Monitorar e avaliar continuamente a eficácia das atividades de coordenação e partilha de informação para realizar melhorias conforme necessário *(nota: garantir alinhamento com a iniciativa P9.1 - Monitorização e Avaliação Integrada).* | possam afetar infraestruturas críticas relacionadas à segurança nacional.<br>**Ministério da Administração Interna**: Coordenação e partilha de informações sobre incidentes de cibersegurança que impactem a segurança interna.<br>**Ministério da Justiça**: Garantia de que as informações compartilhadas respeitam as leis e regulamentos em vigor, além de colaborar na resposta a cibercrimes. | | | | |
| **P6.2: Desenvolvimento de Parcerias Público-Privadas** | **- Identificação e Envolvimento de Parceiros do Setor Privado*:*** Identificar empresas e organizações do setor privado que possam contribuir para a cibersegurança nacional e envolver esses parceiros em discussões iniciais.<br>**- Desenvolvimento de Acordos de Cooperação:** Estabelecer acordos formais de cooperação entre o setor público e privado, definindo responsabilidades, objetivos e benefícios mútuos.<br>**- Promoção de Projetos Conjuntos de Cibersegurança:** Planear e implementar projetos de cibersegurança em colaboração com parceiros privados, focando na inovação e na melhoria das defesas cibernéticas.<br>**- Monitorização Contínua da Eficácia das Parcerias:** Avaliar continuamente a eficácia das parcerias e dos projetos conjuntos, ajustando estratégias conforme necessário para maximizar os benefícios *(nota: garantir alinhamento* | *Entidades Governamentais:*<br>**Autoridade Nacional de Cibersegurança:** Liderança na coordenação e no desenvolvimento de parcerias entre o governo e o setor privado. Identificação de parceiros estratégicos, facilitação de projetos conjuntos e monitorização contínua da eficácia das parcerias público-privadas.<br>**Ministério dos Transportes, Telecomunicações e Economia Digital /DGT:** Supervisão geral da iniciativa e dos acordos de cooperação, assegurando a integração das parcerias nas políticas de cibersegurança nacionais.<br>**Ministério da Administração Interna**: Colaboração em iniciativas conjuntas que visam a | Média | - Número de Parceiros do Setor Privado Identificados e Envolvidos.<br>- Número de Projetos Conjuntos de Cibersegurança Iniciados e Concluídos.<br>- Nível de Satisfação dos Parceiros com a Colaboração. | 15.000 USD – 20.000 USD | Médio Prazo<br>(3-4 anos) |

| | | | | | | |
|---|---|---|---|---|---|---|
| | *com a iniciativa P9.1 - Monitorização e Avaliação Integrada).* | proteção das infraestruturas críticas e dos serviços essenciais.<br>**Ministério da Defesa Nacional**: Participação em projetos conjuntos que envolvem a segurança nacional, contribuindo com expertise e recursos.<br><br>*Setor Privado:*<br>**Empresas de Tecnologia**: Desenvolvimento de soluções inovadoras e participação ativa em projetos de cibersegurança, fornecendo tecnologia e conhecimento.<br>**Fornecedores de Serviços de Internet (ISPs)**: Colaboração em projetos de proteção de redes e partilha de informações sobre ciberameaças.<br>**Instituições Financeiras**: Participação em projetos de proteção de sistemas financeiros, assegurando a segurança das transações e a mitigação de riscos.<br><br>*Academia e Instituições de Investigação:*<br>**Universidades e Centros de Investigação**: Desenvolvimento de investigação e desenvolvimento de novas tecnologias de cibersegurança, além de participação em projetos conjuntos com o setor privado. | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | **Instituições Educacionais Técnicas**: Capacitação de profissionais em cibersegurança e colaboração com o setor privado em iniciativas de formação.<br><br>*Organizações da Sociedade Civil:* **ONGs**: Promoção da importância das parcerias público-privadas em cibersegurança, bem como apoio na implementação e monitorização de projetos conjuntos. | | | | |

| ***P7. Programa de Cooperação e Alinhamento Regional e Internacional***<br>*Este programa intenta fortalecer a cibersegurança através da cooperação com outras nações e organizações internacionais e regionais, promovendo a troca de informações, melhores práticas e respostas coordenadas a ciberameaças.* | | | | | | |
|---|---|---|---|---|---|---|
| **Subobjetivos Relacionados**<br>**4.2; 5.1; 5.2; 6.1; 6.3; 7.1; 7.2** | **Objetivos**<br>• Participar ativamente em fóruns e conferências internacionais de cibersegurança.<br>• Estabelecer acordos de cooperação com outros países e organizações internacionais.<br>• Alinhar as políticas nacionais de cibersegurança com as melhores práticas internacionais.<br>• Contribuir para respostas coletivas a ciber-incidentes a nível regional e internacional.<br>• Promover a participação em programas internacionais de capacitação e treino. | | | | | |
| **Iniciativas** | **Atividades** | **Entidades Envolvidas** | **Criticidade** | **KPIs** | **Orçamento** | **Prazo** |
| **P7.1: Participação Ativa em Programas e Iniciativas Regionais e Internacionais** | **- Participação em Fóruns e Conferências Internacionais:** Envolver-se em eventos internacionais de cibersegurança para trocar conhecimentos e experiências com outros países e organizações.<br>**- Estabelecimento de Parcerias com Organizações Internacionais:** Desenvolver parcerias estratégicas com entidades e organizações internacionais dedicadas à cibersegurança.<br>**- Contribuição para Iniciativas Regionais de Cibersegurança:** Participar e contribuir ativamente para programas e iniciativas de cibersegurança ao nível regional.<br>**- Alinhamento das Políticas Nacionais com Melhores Práticas Internacionais:** Ajustar e atualizar as políticas nacionais de cibersegurança para refletir as melhores práticas e normas internacionais.<br>**- Desenvolvimento de Projetos Conjuntos:** Colaborar em projetos de cibersegurança com outros países e | *Entidades Governamentais:*<br>**Autoridade Nacional de Cibersegurança:** Liderança e coordenação geral da participação em programas e iniciativas internacionais. Representação do país em fóruns internacionais, desenvolvimento de parcerias estratégicas e alinhamento das políticas nacionais com padrões globais.<br>**Ministério dos Negócios Estrangeiros**: Facilitação de relações internacionais e participação em programas de cibersegurança globais.<br><br>*Academia e Instituições de Investigação:*<br>**Universidades e Centros de Investigação**: Envolvimento em redes de investigação | Média | - Número de Fóruns e Conferências Internacionais Participados.<br>- Número de Parcerias com Organizações Internacionais Estabelecidas.<br>- Contribuições e Participações em Iniciativas Regionais de Cibersegurança. | 15.000 USD – 25.000 USD | Curto Prazo<br>(1-2 anos) |

| | | | | | | |
|---|---|---|---|---|---|---|
| | organizações para fortalecer as capacidades nacionais. | internacionais, colaboração em projetos globais, e promoção de intercâmbios académicos.<br>*Organizações da Sociedade Civil:*<br>**ONGs**: Sensibilização pública sobre cibersegurança e participação em iniciativas internacionais de educação e sensibilização.<br><br>*Parceiros Internacionais:*<br>**Organizações Internacionais de Cibersegurança**: Fornecimento de suporte técnico, recursos educacionais e colaboração em projetos globais.<br>**Países e Instituições Parceiras**: Cooperação na troca de informações sobre ciberameaças, participação em exercícios conjuntos e iniciativas regionais de cibersegurança. | | | | |
| **P7.2: Desenvolvimento de Procedimentos e Protocolos de Cooperação e Partilha de Informações** | **- Desenvolvimento de Protocolos de Partilha de Informações**: Criar protocolos específicos para a partilha de informações sobre ciberameaças e incidentes com parceiros internacionais.<br>**- Implementação de Procedimentos de Cooperação para Resposta a Incidentes**: Estabelecer procedimentos claros para a cooperação internacional na resposta a incidentes de cibersegurança.<br>**- Promoção da Troca Regular de Informações**: Facilitar a troca contínua de informações sobre ciberameaças e melhores práticas com parceiros regionais e internacionais.<br>**- Capacitação e Sensibilização das Partes Interessadas**: Formar e sensibilizar todas as | *Entidades Governamentais:*<br>**Autoridade Nacional de Cibersegurança:** Liderança na coordenação da iniciativa. Desenvolvimento dos protocolos de partilha de informações e implementação de procedimentos de cooperação.<br>**Ministério dos Negócios Estrangeiros:** Facilitação da cooperação internacional para a partilha de informações.<br><br>*Parceiros Internacionais:* | Média | - Número de Protocolos de Partilha de Informações Desenvolvidos e Implementados. | 15.000 USD – 20.000 USD | Médio Prazo<br>(3-4 anos) |

| | | | | | | |
|---|---|---|---|---|---|---|
| | partes interessadas relevantes sobre os novos procedimentos e protocolos para garantir a sua correta implementação e uso *(nota: garantir alinhamento com o programa P2. Educação, Consciencialização e Capacitação em Cibersegurança).*<br>**- Monitorização e Revisão dos Protocolos e Procedimentos**: Monitorizar a eficácia dos protocolos e procedimentos estabelecidos, e realizar revisões periódicas para garantir melhorias contínuas *(nota: garantir alinhamento com a iniciativa P9.1 - Monitorização e Avaliação Integrada).* | **Organizações Internacionais de Cibersegurança:** Assistência técnica no desenvolvimento dos protocolos.<br>**Países e Instituições Parceiras:** Cooperação na implementação de protocolos e partilha de informações. | | | | |

| ***P8. Programa de Inovação em Cibersegurança*** | | | | | | |
|---|---|---|---|---|---|---|
| *Centrado no fortalecimento da infraestrutura tecnológica e na promoção da inovação em cibersegurança, este programa pretende incentivar a investigação, o desenvolvimento de novas tecnologias e a certificação de soluções de segurança.* | | | | | | |
| **Subobjetivos Relacionados**<br>**1.5; 2.1; 4.2; 5.2; 5.3** | **Objetivos**<br>• Reforçar a infraestrutura tecnológica de cibersegurança.<br>• Promover a investigação e inovação em cibersegurança.<br>• Implementar programas de certificação para elevar o nível de segurança das soluções tecnológicas.<br>• Estabelecer centros de excelência em cibersegurança nas principais universidades e instituições de investigação.<br>• Fomentar a colaboração entre academia, Governo e setor privado para o desenvolvimento de tecnologias de cibersegurança. | | | | | |
| **Iniciativas** | **Atividades** | **Entidades Envolvidas** | **Criticidade** | **KPIs** | **Orçamento** | **Prazo** |
| **P8.1: Desenvolvimento e Certificação de Ferramentas de Cibersegurança** | **- Investimento em Investigação e Desenvolvimento (I&D)**: Alocar recursos para a investigação e desenvolvimento de novas tecnologias e ferramentas avançadas de cibersegurança.<br>**- Criação de Programas de Certificação**: Desenvolver programas de certificação para garantir que ferramentas e práticas de cibersegurança cumprem os padrões mais elevados.<br>**- Colaboração com Universidades e Centros de Investigação:** Estabelecer parcerias com instituições académicas e centros de investigação para fomentar a inovação em cibersegurança.<br>**- Promoção da Adoção de Tecnologias Certificadas:** Incentivar a implementação e uso de tecnologias de cibersegurança certificadas em setores públicos e privados.<br>**- Monitorização e Atualização Contínua:** Monitorar a eficácia das ferramentas desenvolvidas e realizar atualizações | *Entidades Governamentais:*<br>**Autoridade Nacional de Cibersegurança:** Liderança na coordenação da iniciativa. Implementação dos programas de certificação e promoção da adoção de tecnologias certificadas.<br><br>*Setor Privado:*<br>**Empresas de Tecnologia:** Desenvolvimento e certificação de novas ferramentas de cibersegurança.<br>**Fornecedores de Serviços de Internet (ISPs):** Colaboração na implementação e certificação de tecnologias de cibersegurança.<br><br>*Academia e Instituições de Investigação:* | Baixa | - Número de Tecnologias e Ferramentas de Cibersegurança Desenvolvidas.<br>- Quantidade de Programas de Certificação Criados e Implementados.<br>- Número de Parcerias com Universidades e Centros de Investigação. | 25.000 USD – 40.000 USD | Médio Prazo<br>(3-4 anos) |

| | | | | | | |
|---|---|---|---|---|---|---|
| | contínuas para manter a relevância e a segurança das tecnologias *(nota: garantir alinhamento com a iniciativa P9.1 - Monitorização e Avaliação Integrada).* | **Universidades e centros de investigação:** Desenvolvimento de ferramentas de cibersegurança e oferta de programas de certificação.<br>**Parceiros Internacionais:**<br>**Organizações Internacionais de Cibersegurança:** Fornecimento de padrões de certificação internacionais e assistência técnica. | | | | |
| **P8.2: Promoção de Investigação e Inovação em Cibersegurança** | **- Estabelecimento de Programas de Financiamento**: Criar e gerir programas de financiamento para apoiar investigações em cibersegurança na Guiné-Bissau.<br>**- Desenvolvimento da Infraestrutura do Centro de Excelência**: Planear e construir as instalações do centro de excelência e laboratórios de investigação.<br>**- Equipamento dos Laboratórios com Tecnologia de Ponta**: Adquirir e instalar equipamentos avançados e ferramentas de cibersegurança nos laboratórios.<br>**- Recrutamento e Formação de Investigadores Especializados**: Atrair e capacitar investigadores e especialistas em cibersegurança para trabalhar no centro.<br>**- Promoção da Colaboração Intersectorial**: Facilitar a colaboração entre universidades, setor privado e governo para promover a investigação e inovação em cibersegurança.<br>**- Promoção da Colaboração Nacional e Internacional**: Estabelecer parcerias com outras instituições e fomentar a | *Entidades Governamentais:*<br>**Autoridade Nacional de Cibersegurança:** Liderança na coordenação da iniciativa. Promoção da colaboração entre setores e disseminação de resultados de investigações.<br><br>*Setor Privado:*<br>**Empresas de Tecnologia:** Participação em programas de investigação e desenvolvimento de soluções inovadoras.<br><br>*Academia e Instituições de Investigação:*<br>**Universidades e centros de investigação:** Desenvolvimento de investigações em cibersegurança e organização de eventos académicos.<br><br>*Parceiros Internacionais:*<br>**Organizações Internacionais de Cibersegurança:** Assistência técnica e financiamento para programas de investigação. | Baixa | - Número de Programas de Financiamento Criados e Projetos Financiados.<br>- Quantidade de Parcerias e Colaborações Estabelecidas.<br>- Número de Publicações e Disseminações de Resultados de Investigação. | 75.000 USD – 100.000 USD | Longo Prazo<br>(5+ anos) |

| | | | | | | |
|---|---|---|---|---|---|---|
| | cooperação em projetos de investigação de cibersegurança.<br>**- Organização de Conferências e Workshops de Inovação**: Planear e realizar conferências e workshops para discutir inovações e tendências emergentes em cibersegurança.<br>**- Publicação e Disseminação de Resultados de Investigação**: Publicar e disseminar amplamente os resultados das investigações relevantes para promover o conhecimento e a aplicação prática das descobertas. | | | | | |

| ***P9. Programa de Monitorização e Avaliação*** | | | | | | |
|---|---|---|---|---|---|---|
| *Este programa visa garantir a eficácia e a melhoria contínua das iniciativas de cibersegurança através de monitorização e avaliação sistemáticas.* | | | | | | |
| **Subobjetivos Relacionados**<br>**1.1; 1.3; 1.4; 2.2; 5.1; 6.1; 6.2; 6.3; 7.1; 7.2** | **Objetivos**<br>• Desenvolver indicadores de desempenho para monitorizar as iniciativas de cibersegurança.<br>• Estabelecer mecanismos de avaliação contínua para medir a eficácia das políticas e ações.<br>• Criar relatórios regulares para documentar o progresso e identificar áreas de melhoria.<br>• Implementar sistemas de monitorização para garantir a conformidade com as normas e práticas de cibersegurança.<br>• Ajustar estratégias e ações com base nos resultados da monitorização e avaliação. | | | | | |
| **Iniciativas** | **Atividades** | **Entidades Envolvidas** | **Criticidade** | **KPIs** | **Orçamento** | **Prazo** |
| **P9.1: Monitorização e Avaliação Integrada** | **- Desenvolvimento de Indicadores de Desempenho**: Criar KPIs específicos para todas as iniciativas de cibersegurança, permitindo a medição precisa de seu progresso e impacto.<br>**- Implementação de um Sistema de Monitorização Contínua**: Estabelecer um sistema para monitorar continuamente a eficácia das políticas, estratégias e ações de cibersegurança.<br>**- Realização de Avaliações Periódicas**: Realizar avaliações regulares de todas as iniciativas de cibersegurança para determinar sua eficácia e identificar áreas de melhoria.<br>**- Publicação de Relatórios Regulares**: Desenvolver e publicar relatórios periódicos sobre o progresso e impacto das iniciativas de cibersegurança.<br>**- Ajuste de Estratégias e Ações**: Ajustar as estratégias e ações de cibersegurança com base nos resultados das avaliações | *Entidades Governamentais:*<br>**Autoridade Nacional de Cibersegurança:** Liderança na coordenação da iniciativa. Desenvolvimento de indicadores de desempenho, implementação do sistema de monitorização e condução de avaliações periódicas.<br><br>*Setor Privado:*<br>**Empresas de Tecnologia:** Fornecimento de tecnologias e ferramentas para a monitorização contínua e colaboração na definição de indicadores de desempenho.<br>**Fornecedores de Serviços de Internet (ISPs):** Participação na recolha de dados e na implementação do sistema de monitorização. | Baixa | - Número de Indicadores de Desempenho Desenvolvidos e Implementados.<br>- Frequência e Cobertura das Avaliações Periódicas Realizadas.<br>- Nível de Satisfação das Partes Interessadas com o Sistema de Monitorização e Avaliação. | 20.000 USD – 30.000 USD | Médio Prazo<br>(3-4 anos) |

| | | | | | | |
|---|---|---|---|---|---|---|
| | para garantir melhorias contínuas e eficácia. | *Academia e Instituições de Investigação:*<br>**Universidades e centros de investigação:** Desenvolvimento de metodologias para avaliação de políticas e ações de cibersegurança, e participação na análise de dados. | | | | |

# 4. Jornada Estratégica

A Jornada Estratégica da Guiné-Bissau em cibersegurança está estruturada em três horizontes de tempo de 2025 a 2030: curto, médio e longo prazo, com iniciativas distribuídas de acordo com a sua criticidade e impacto esperado.

*Tabela 3 Visão Geral da Jornada Estratégica*

| Criticidade | Horizonte 1 - Curto Prazo (1-2 anos) | Horizonte 2 - Médio Prazo (3-4 anos) | Horizonte 3 - Longo Prazo (5+ anos) |
|---|---|---|---|
| **Muito Alta** | P1.1 - Desenvolvimento e Implementação da Política Nacional de Cibersegurança<br>P1.2 - Criação e Fortalecimento da Autoridade Nacional de Cibersegurança<br>P2.1 - Desenvolvimento de Capacidades Técnicas e Humanas em Cibersegurança<br>P2.2 - Promoção e Disseminação de Cultura e Recursos de Cibersegurança<br>P5.1 - Criação, Operacionalização e Definição de Processos da CSIRT Nacional | | |
| **Alta** | P3.1: Criação e Implementação da Estratégia Nacional de Combate à Cibercriminalidade Alinhada com Convenções Internacionais<br>P4.1 - Desenvolvimento e Implementação de Políticas e Planos de Proteção e Resposta para Infraestruturas Críticas<br>P5.2: Desenvolvimento e Implementação de uma Política Nacional de Gestão de Riscos | P2.3: Capacitação de Profissionais e Decisores em Cibersegurança<br>P2.4: Capacitação de Autoridades Judiciais e Policias em Cibersegurança e Cibercrime<br>P3.2: Desenvolvimento e Padronização da Legislação e Procedimentos Penais para Cibercrimes | |
| **Média** | P6.1: Coordenação Intersectorial e Partilha de Informação<br>P7.1: Participação Ativa em Programas e Iniciativas Regionais e Internacionais | P1.3: Desenvolvimento e Implementação de Políticas de Segurança e Quadro Nacional de Referência de Cibersegurança<br>P4.2: Capacitação e Implementação de Sistemas Avançados em Infraestruturas Críticas<br>P6.2: Desenvolvimento de Parcerias Público-Privadas<br>P7.2: Desenvolvimento de Procedimentos e Protocolos de Cooperação e Partilha de Informações | |
| **Baixa** | | P1.4: Desenvolvimento de Procedimentos para Identificação e | P3.3: Criação e Implementação de Unidades |

| Criticidade | Horizonte 1 - Curto Prazo (1-2 anos) | Horizonte 2 - Médio Prazo (3-4 anos) | Horizonte 3 - Longo Prazo (5+ anos) |
|---|---|---|---|
| | | Integração de Financiamentos<br>P8.1: Desenvolvimento e Certificação de Ferramentas de Cibersegurança<br>P9.1: Monitorização e Avaliação Integrada | Especializadas de Combate ao Cibercrime<br>P4.3: Realização de Auditorias a Infraestruturas Críticas<br>P8.2: Promoção de Investigação e Inovação em Cibersegurança |

**Horizonte 1 - Curto Prazo (1-2 anos)**

No curto prazo, a Guiné-Bissau focar-se-á na construção das bases necessárias para uma estratégia nacional de cibersegurança robusta e eficaz. O ponto de partida será o **Desenvolvimento e Implementação da Política Nacional de Cibersegurança (P1.1),** que servirá como diretriz para todas as futuras iniciativas no domínio da cibersegurança. Em paralelo, a **Criação e Fortalecimento da Autoridade Nacional de Cibersegurança (P1.2)** será crucial para garantir a coordenação e supervisão adequadas das políticas e ações a nível nacional.

Outro passo essencial será a **Criação, Operacionalização e Definição de Processos da CSIRT Nacional (P5.1),** que permitirá ao país responder eficazmente a incidentes cibernéticos e mitigar potenciais riscos. Para assegurar que o país tem a capacidade de enfrentar os desafios cibernéticos, será promovido o **Desenvolvimento de Capacidades Técnicas e Humanas em Cibersegurança (P2.1)**, capacitando os recursos humanos nacionais.

A par deste desenvolvimento técnico, será fundamental a **Promoção e Disseminação de Cultura e Recursos de Cibersegurança (P2.2)**, sensibilizando a sociedade para a importância da segurança cibernética. No âmbito da proteção contra ameaças, a **Criação e Implementação da Estratégia Nacional de Combate à Cibercriminalidade Alinhada com Convenções Internacionais (P3.1)** permitirá um alinhamento com os padrões globais e a eficácia na luta contra a cibercriminalidade.

Adicionalmente, será desenvolvido e implementado um plano específico para a proteção das infraestruturas críticas, através do **Desenvolvimento e Implementação de Políticas e Planos de Proteção e Resposta para Infraestruturas Críticas (P4.1)**, garantindo a segurança dos setores mais sensíveis do país. A gestão de riscos será também uma prioridade, com o **Desenvolvimento e Implementação de uma Política Nacional de Gestão de Riscos (P5.2)**, que dotará o país de ferramentas para identificar e mitigar riscos de forma sistemática.

Para garantir uma abordagem integrada e alinhada com as melhores práticas internacionais, será promovida a **Coordenação Intersectorial e Partilha de Informação (P6.1)**, com a criação de plataformas de cooperação entre governo, setor privado e outras partes interessadas. Finalmente, a Guiné-Bissau participará ativamente em iniciativas regionais e internacionais, através da **Participação Ativa em Programas e**

**Iniciativas Regionais e Internacionais (P7.1)**, garantindo assim uma cooperação efetiva e o acesso a recursos e conhecimentos globais em cibersegurança.

**Horizonte 2 - Médio Prazo (3-4 anos)**

No médio prazo, a Guiné-Bissau focar-se-á na consolidação e expansão das iniciativas de cibersegurança, garantindo uma maior maturidade e resiliência no espaço cibernético nacional. Durante este período, será prioritário o **Desenvolvimento e Padronização da Legislação e Procedimentos Penais para Cibercrimes (P3.2)**, estabelecendo normas claras e consistentes para o combate à cibercriminalidade.

Além disso, o **Desenvolvimento e Implementação de Políticas de Segurança e do Quadro Nacional de Referência de Cibersegurança (P1.3)** permitirá a criação de um ambiente regulatório robusto que norteie as práticas de segurança em todo o país. A capacitação continuará a ser um foco central, com a **Capacitação de Profissionais e Decisores em Cibersegurança (P2.3)** e a **Capacitação de Autoridades Judiciais e Policiais em Cibersegurança e Cibercrime (P2.4)**, garantindo que todos os envolvidos possuam o conhecimento necessário para enfrentar os desafios cibernéticos.

Para fortalecer as infraestruturas críticas do país, será implementada a **Capacitação e Implementação de Sistemas Avançados em Infraestruturas Críticas (P4.2)**, assegurando que estas sejam protegidas contra ameaças sofisticadas. A coordenação entre diferentes setores e a partilha de informação serão otimizadas através do **Desenvolvimento de Parcerias Público-Privadas (P6.2)**, promovendo uma colaboração eficaz entre o governo e o setor privado.

No âmbito internacional, será reforçada a **Participação Ativa em Programas e Iniciativas Regionais e Internacionais (P7.2)**, estabelecendo procedimentos e protocolos claros para a cooperação e partilha de informações com outros países e organizações. A sustentabilidade financeira das iniciativas será garantida através do Desenvolvimento de **Procedimentos para Identificação e Integração de Financiamentos (P1.4)**, que permitirá aceder a recursos adicionais para suportar as ações em cibersegurança.

Finalmente, para assegurar a qualidade e eficácia das ferramentas utilizadas no país, será promovido o **Desenvolvimento e Certificação de Ferramentas de Cibersegurança (P8.1),** assim como a **Monitorização e Avaliação Integrada (P9.1)**, garantindo que todas as iniciativas sejam constantemente avaliadas e ajustadas conforme necessário para enfrentar os desafios emergentes.

**Horizonte 3 - Longo Prazo (5+ anos)**

No longo prazo, a Guiné-Bissau estará focada em consolidar e aprofundar as capacidades de cibersegurança, visando não apenas a manutenção da segurança, mas também o avanço contínuo nesta área crítica. Um dos principais objetivos será a **Criação e Implementação de Unidades Especializadas de Combate ao Cibercrime (P3.3)**, que permitirá ao país enfrentar de forma mais eficaz e proativa as ameaças cibernéticas, com equipas dedicadas e altamente especializadas.

A proteção das infraestruturas críticas continuará a ser uma prioridade, com a **Realização de Auditorias a Infraestruturas Críticas (P4.3)**, assegurando que estas estruturas essenciais estejam constantemente a ser avaliadas e melhoradas para resistir a potenciais ameaças.

Por fim, para promover a evolução contínua e a liderança no campo da cibersegurança, será incentivada a **Promoção de Investigação e Inovação em Cibersegurança (P8.2)**, apoiando o desenvolvimento de novas tecnologias, metodologias e soluções que possam antecipar e mitigar futuros desafios cibernéticos. Este enfoque na inovação posicionará a Guiné-Bissau como um país resiliente e preparado para enfrentar as dinâmicas do mundo digital em constante evolução.

A Jornada Estratégica da Guiné-Bissau para a cibersegurança é uma abordagem estruturada que visa construir uma base sólida a curto prazo, fortalecer capacidades a médio prazo e promover inovação e resiliência a longo prazo. Estes programas e iniciativas são essenciais para garantir a segurança digital e o desenvolvimento socioeconómico sustentável do país.