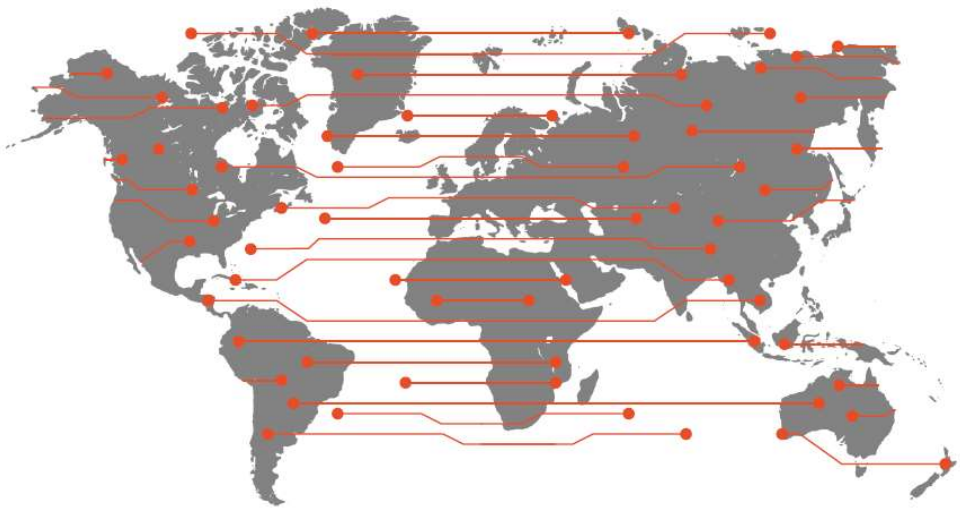

D-05
Estratégia Nacional de Cibersegurança da Guiné-Bissau

Setembro, 2024

Informação do documento

Título do Projeto:	Estudo de Viabilidade Sobre a Cibersegurança na Guiné-Bissau		
Título do relatório:	D-05 Estratégia Nacional de Cibersegurança 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

1. 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 Equipa de Resposta a Incidentes de Segurança Informática Equipa de Resposta a Incidentes Informáticos 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 Normas 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.
Operador de Serviço Essencial	Operador público ou privado que fornece um serviço essencial.
Países beneficiários	Guiné-Bissau

Termo/abreviatura	Significado/explicação
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. CAPÍTULO I – FUNDAMENTAÇÃO DA ESTRATÉGIA

1.1 INTRODUÇÃO

A Estratégia Nacional de Cibersegurança da Guiné-Bissau (2025 - 2030), doravante referida como "Estratégia Nacional", estabelece uma visão clara para fortalecer a segurança digital e aumentar a resiliência das infraestruturas críticas em resposta ao crescente panorama de ciberameaças. Esta Estratégia Nacional, concebida no contexto de uma África Ocidental em rápida digitalização, procura salvaguardar a integridade, a confidencialidade e a disponibilidade da Informação e Tecnologias que são vitais para a Guiné-Bissau.

Perante os riscos de ciberameaças, que podem comprometer a estabilidade económica e a segurança nacional, a Guiné-Bissau compromete-se a desenvolver capacidades robustas para prevenir, detetar e responder a incidentes no ciberespaço. A presente Estratégia alinha-se com as diretrizes regionais da CEDEAO e com os compromissos internacionais, nomeadamente com a Convenção de Budapeste e a Convenção de Malabo, assegurando uma abordagem coerente e efetiva à cibersegurança.

Adicionalmente, a Estratégia Nacional enfatiza a importância da cooperação entre os sectores público e privado e a sociedade civil para fomentar um ambiente de cibersegurança resiliente. Através desta colaboração, a Guiné-Bissau visa não apenas proteger os seus cidadãos e as suas infraestruturas críticas, mas também apoiar o desenvolvimento de uma economia digital inclusiva e segura.

Com uma visão clara para fortalecer a governança digital e a resiliência no ciberespaço, esta Estratégia estabelece as bases para uma Guiné-Bissau mais segura e próspera, onde o ciberespaço se afirma como um pilar de desenvolvimento socioeconómico e inovação.

1.2 ANÁLISE DO CONTEXTO ENVOLVENTE

A Guiné-Bissau faz fronteira com o Senegal a norte e com a Guiné a sul, e a sua costa no Oceano Atlântico é composta pelo arquipélago dos Bijagós, com mais de 100 ilhas. Apesar da sua dimensão, a Guiné-Bissau alberga uma grande variedade de grupos étnicos, línguas e religiões[1]. Desde a sua independência em 1974, a Guiné-Bissau tem sido palco de grandes convulsões políticas e militares. O historial de instabilidade política da Guiné-Bissau, uma guerra civil e vários golpes de Estado (o último em 2012) resultaram num Estado frágil, com uma economia débil, uma elevada taxa de desemprego, um nível significativo de corrupção e uma ampla pobreza[2], e também desafios significativos no desenvolvimento da sua economia digital.

Ambiente político e regulatório

Relativamente ao ambiente político e regulatório, a Guiné-Bissau carece de um quadro legal e regulamentar adequado para sustentar uma transformação digital, possui muitas leis ultrapassadas, algumas ainda datadas da época colonial. Embora existam alguns projetos de lei, muitos deles não avançam devido à significativa fragmentação e instabilidade política, que impedem a implementação de reformas necessárias, dificultando o compromisso político, a tomada de decisões eficazes e a coordenação institucional.

[1] https://www.worldbank.org/en/country/guineabissau/overview
[2] https://www.cia.gov/the-world-factbook/countries/guinea-bissau/summaries

Sistema Financeiro

Os serviços financeiros digitais cresceram significativamente devido ao crescimento da indústria do dinheiro móvel. Em 2020, a taxa de atividade da moeda móvel cresceu 77% e o valor das transações 235%, a taxa de crescimento mais elevada na região da UEMOA[5]. Contudo, cerca de 43% da população, especialmente mulheres e habitantes rurais, continua excluída do sistema financeiro formal. Apesar da adoção de uma estratégia nacional de inclusão financeira pelo Governo da Guiné-Bissau em 2023, a falta de programas robustos de educação financeira continua a limitar o crescimento da inclusão financeira digital[5].

Governança Digital

No que diz respeito à governança digital, a Guiné-Bissau está numa fase inicial de desenvolvimento. O Instituto Tecnológico para a Modernização da Administração (ITMA), criado em 2020, tem o mandato de liderar e coordenar a estratégia digital do Governo. No entanto, a falta de recursos financeiros e humanos tem dificultado o ITMA de cumprir plenamente com o seu papel. A ausência de uma estratégia de transformação digital a nível governamental também impede o desenvolvimento de serviços digitais integrados e eficientes[5]. O Índice de Desenvolvimento do Governo Eletrónico (EGDI) da ONU posicionou o país na 186ª posição entre 193 países em 2022[3]. As plataformas públicas digitais estão numa fase incipiente, mas iniciativas como o registo e pagamento automático de impostos e o registo de empresas demonstram potencial. No entanto, a falta de interoperabilidade entre sistemas críticos e a ausência de uma política abrangente de partilha e gestão de dados são barreiras significativas. A maioria das funções centrais do Governo é digitalizada, mas o sistema integrado de informação de gestão financeira (SIGFIP) não foi adotado uniformemente pelos ministérios[5].

Infraestrutura Digital

Relativamente ao desenvolvimento da infraestrutura digital na Guiné-Bissau este é, neste momento, limitado. Em 2024, apenas 31,6% da população utilizava a Internet, com 686,2 mil utilizadores[4]. A maioria das conexões são feitas através de dispositivos móveis, com 2,25 milhões de conexões móveis registadas em janeiro de 2024, representando 103,3% da população[4]. No entanto, a telefonia fixa é praticamente inexistente, seguindo um padrão comum em muitos países africanos. A conectividade internacional limitada resulta em preços elevados de acesso à Internet e baixa adoção da mesma. Para tentar ultrapassar esta situação, a ligação ao cabo submarino da Costa Africana à Europa (ACE) foi estabelecida, com a Guiné-Bissau conectada ao sistema em Novembro de 2022. Esta conexão visa melhorar a qualidade da conectividade no país e, consequentemente, reduzir os preços do acesso à internet e aumento na sua utilização[2], no entanto, neste momento encontra-se inoperacional, devido ao bloqueio na SCGB.

Competências Digitais

No que respeita às competências digitais e educacionais, o Governo da Guiné-Bissau está empenhado em aumentar as competências digitais, mas enfrenta limitações significativas. Em 2022, apenas 17% das escolas tinham acesso regular à eletricidade e muito menos à Internet. A aquisição de competências pelos estudantes é dificultada por professores sem formação adequada, greves frequentes e recursos escolares limitados. Existe também um fosso significativo em matéria de competências digitais[5].

[3] https://publicadministration.un.org/egovkb/en-us/Data/Country-Information/id/71-Guinea-Bissau
[4] https://datareportal.com/reports/digital-2024-guinea-bissau

E-Government

É ainda de grande importância referir a criação do "e-Government Interoperability Framework for Guiné-Bissau (eGIF-GB)", um passo essencial para alcançar plataformas públicas digitais e uma transformação digital governamental abrangente. O Governo da Guiné-Bissau recebeu apoio financeiro do Banco Mundial para implementar o Programa de Integração Digital Regional da África Ocidental (WARDIP). O objetivo do WARDIP é apoiar a Guiné-Bissau no desenvolvimento de uma economia digital e garantir um ambiente favorável à transformação digital, promovendo a inovação e a competitividade no mercado digital único regional. Um mercado online único permitirá que Governos, empresas e indivíduos acedam e ofereçam serviços públicos e privados online, bem como realizem vendas e compras online sem restrições em qualquer lugar da região. Os principais facilitadores para essa camada online são os serviços financeiros digitais (DFS), o quadro de interoperabilidade e a infraestrutura das chaves públicas digitais5.

Contexto legal e normativo

Perante o rápido crescimento da dependência das tecnologias de informação e da comunicação e dos riscos que lhe estão associados, o Governo da Guiné-Bissau tomou medidas para fazer face às ameaças e vulnerabilidades associadas, a fim de proteger os seus cidadãos, empresas e infraestruturas críticas. Em 22 de dezembro de 2020, foi celebrado um Acordo de Cooperação entre o Ministério da Justiça e dos Direitos Humanos e a Faculdade de Direito de Bissau. O acordo visa a elaboração de projetos legislativos relativos (i) à Lei da Cooperação Judiciária Internacional e (ii) à Lei do Cibercrime. Relativamente à Lei do Cibercrime, esta já se encontra na sua versão final, aguardando apenas a aprovação e publicação pelo Governo. No entanto, é importante salientar que esta lei abrange apenas os cibercrimes. Por outro lado, a Lei de Cibersegurança, que ainda está em fase de projeto, é igualmente importante. Esta lei visa estabelecer diretrizes e regulamentos para proteger as infraestruturas críticas de informação (ICI), garantir a segurança dos dados e fortalecer a resiliência do país contra ciberameaças.

Cenário de Ciberameaças

As ciberameaças são atividades maliciosas dirigidas contra sistemas informáticos e redes, com o objetivo de causar danos, roubar informações ou perturbar operações. Estas ameaças podem assumir várias formas e representam um desafio crescente para a segurança e integridade dos sistemas digitais em todo o mundo.

Para um país, a identificação e compreensão das ciberameaças são fundamentais para proteger a infraestrutura crítica, salvaguardar a privacidade dos cidadãos, manter a confiança nos sistemas digitais e garantir a resiliência nacional. A falha em identificar e mitigar ciberameaças pode resultar em danos financeiros significativos, perda de informações sensíveis e interrupção de serviços essenciais.

A Agência Europeia para a Segurança das Redes e da Informação (ENISA), no seu Relatório Anual sobre o Panorama de Ameaças de 2023[6], destacou a predominância de ameaças como o *ransomware*, o *malware*, a engenharia social, as ameaças contra dados, as ameaças contra a disponibilidade (*Denial of Service*), a manipulação de informação e os ataques à cadeia de

[5] Government of Guinea-Bissau under the West African Regional Digital Integration Program (WARDIP). (2023). *Consulting Services for Feasibility Study for the Development of an Interoperability Framework, Data Exchange Layer, and Services Platform and Action Plan for the Digitalization of the Main Public Services - Interoperability Framework, Interoperability Platform, and Enterprise Architecture.*

[6] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

suprimentos. Este relatório anual é essencial para compreender as tendências globais e para identificar as ameaças emergentes que podem afetar diferentes regiões do mundo.

As ciberameaças identificadas pela ENISA não são exclusivas da Europa. De acordo com o *African Cyberthreat Assessment Report de 2023*[7], o panorama das ciberameaças em África manteve-se altamente dinâmico, com ataques que evoluíram rapidamente em sofisticação e em escala. O relatório destaca o crescimento do *ransomware*, do comprometimento do e-mail empresarial, outras fraudes online e, especialmente, o *phishing*, como as ciberameaças que mais cresceram no continente. Este relatório alerta para o facto de, em 2023, ter sido estimado um aumento de 23% em comparação com o ano de 2022, no número médio de ciberataques semanais por organização em África, sendo esta média a mais alta do mundo. Além disso, o *African Cyberthreat Assessment Report* de 2023 sublinha a crescente exploração de diferentes canais de comunicação, incluindo redes sociais e aplicações de mensagens instantâneas, para realizar ataques de *phishing*, demonstrando que a cibersegurança continua a ser um desafio significativo tanto em contextos europeus quanto africanos.

No contexto específico da Guiné-Bissau, o panorama das ciberameaças é igualmente complexo e desafiante. A falta de infraestrutura básica de cibersegurança, como a ausência de certificados SSL/TLS, expõe ainda mais o país a riscos de ciberespionagem e cibersabotagem. A utilização de softwares não licenciados e sistemas operativos desatualizados facilita a proliferação de malware, ampliando as vulnerabilidades e aumentando a suscetibilidade a ataques que podem comprometer a confidencialidade e integridade das informações. Ameaças como interrupções no fornecimento de energia amplificam ainda mais os riscos, uma vez que falhas de energia podem resultar na perda de dados críticos e interromper serviços essenciais. A vulnerabilidade a ataques de negação de serviço (DDoS) e a corrupção de dados durante reinícios inesperados de sistemas são exemplos de como a disponibilidade e a segurança dos sistemas podem ser comprometidas.

Cibersegurança

Tendo em consideração o presente panorama, a cibersegurança é também uma área que necessita de atenção. A Guiné-Bissau está classificada na 161ª posição entre 175 países no Índice Global de Cibersegurança (GCI) da ITU[8]. A falta de uma legislação robusta e de capacidade técnica para lidar com incidentes de segurança digital são pontos fracos que precisam ser abordados.

Para construir um ambiente digital seguro e inclusivo, a Guiné-Bissau deve focar-se em reformas nos cinco pilares da economia digital: infraestrutura e telecomunicações, políticas e regulamentações, governança digital, serviços financeiros digitais e competências digitais. Reconhecendo as limitações impostas pela fragilidade do país, é essencial um esforço planeado e coordenado para criar um ambiente propício ao desenvolvimento digital.

O panorama digital na Guiné-Bissau reflete um compromisso crescente com a inovação e a inclusão digital, destacando-se como uma força motriz para o desenvolvimento nacional. A colaboração internacional, juntamente com a implementação de tecnologias emergentes, tem sido fundamental nesta caminhada, estabelecendo etapas vitais para a transformação digital do país. Continuar estes esforços de forma coordenada e sustentável é essencial para fomentar uma sociedade da informação segura e bem integrada.

[7] https://www.interpol.int/content/download/21048/file/24COM005030-AJFOC_Africa%20Cyberthreat%20Assessment%20Report_2024_complet.pdf
[8] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Diante dessas circunstâncias, é imperativo abordar prontamente as vulnerabilidades, cultivar uma cultura robusta de cibersegurança e investir significativamente em tecnologia e educação. A economia da Guiné-Bissau, embora enfrentando desafios, possui oportunidades únicas de crescimento através da digitalização, que podem revitalizar setores-chave do país. Assim, a Estratégia Nacional de Cibersegurança não apenas visa mitigar riscos, mas também alavancar o desenvolvimento económico, assegurando que a inovação digital contribui de forma sustentável para o progresso do país e para a segurança e prosperidade de todos os cidadãos.

1.3 PRINCÍPIOS ORIENTADORES

A Estratégia Nacional de Cibersegurança da Guiné-Bissau foi desenvolvida tendo por base um conjunto de princípios orientadores que se apresentam de seguida. Estes princípios foram desenvolvidos através de um processo colaborativo que considerou o enquadramento dos diplomas legais existentes no país, contribuições de diversas partes interessadas relevantes da Guiné-Bissau e as melhores práticas internacionais (ex. *International Telecommunication Union* (ITU) de 2021[9]).

Tabela 2 – Princípios Orientadores

Princípio	Descrição
1. Legalidade e Proteção dos Direitos Fundamentais	A presente Estratégia Nacional respeitará e promoverá a aderência às leis nacionais e internacionais, assegurando desta forma a proteção dos direitos fundamentais e das liberdades individuais no ciberespaço. Este princípio reforça o compromisso da Guiné-Bissau em manter um ambiente digital que respeite a privacidade e a integridade de cada cidadão.
2. Resiliência das Infraestruturas Críticas de Informação	É fundamental desenvolver e manter capacidades que permitam ao país identificar, detetar, responder e recuperar rapidamente de ameaças digitais, especialmente contra as Infraestruturas Críticas de Informação (ICI). A proteção das ICI é vital para a continuidade dos serviços essenciais e para a estabilidade nacional, dado o seu impacto direto na segurança, economia e bem-estar dos cidadãos. Desta forma, este princípio garante que a Guiné-Bissau possa sustentar um ambiente digital seguro e resiliente, apto a enfrentar desafios atuais e emergentes de forma eficaz.
3. Cooperação Intersectorial	Este princípio promove a colaboração entre diferentes sectores, tanto públicos quanto privados, para garantir uma abordagem integrada e abrangente à segurança digital. Reconhecendo que a segurança digital é uma responsabilidade partilhada, a Estratégia Nacional incentivará a troca de informações e melhores práticas entre todos os intervenientes relevantes.
4. Educação e Consciencialização em Cibersegurança	Um pilar fundamental da presente Estratégia é a promoção da literacia digital e da "Higiene de Segurança" em toda a população, com objetivo preparar os cidadãos para uma participação segura e informada no ciberespaço, enfatizando a importância da segurança pessoal e empresarial online.
5. Proporcionalidade dos Recursos	A alocação de recursos para a cibersegurança na Guiné-Bissau deve estar estritamente alinhada com a avaliação de riscos conduzida nacionalmente. Este princípio garante que os investimentos em tecnologias, infraestruturas e capacitação sejam diretamente proporcionais à gravidade e probabilidade das ameaças identificadas. Ao aplicar este princípio, o país assegura que os recursos limitados sejam utilizados de maneira mais estratégica e impactante, concentrando esforços e financiamentos nas áreas mais vulneráveis e críticas.

[9] https://ncsguide.org/wp-content/uploads/2024/05/508938E.pdf

2. CAPÍTULO II – VISÃO, MISSÃO E OBJETIVOS

Neste capítulo, apresentamos a visão, missão e objetivos estratégicos da Estratégia Nacional de Cibersegurança. Estes elementos fundamentais definem a direção e as aspirações do esforço coletivo para proteger o ciberespaço da Guiné-Bissau e fomentar um ambiente digital seguro, resiliente e inclusivo.

2.1 VISÃO

A Guiné-Bissau pretende fortalecer significativamente as suas capacidades de proteção das infraestruturas críticas e dos dados sensíveis, estabelecendo-se como um participante ativo e influente em cibersegurança na região.

2.2 MISSÃO

A missão da estratégia nacional de cibersegurança da Guiné-Bissau é proteger as infraestruturas críticas e os dados sensíveis, fortalecer a transição digital e melhorar a literacia sobre os riscos digitais. A estratégia promove a literacia e inclusão digital e a inovação, garantindo que todos beneficiem de um ecossistema digital mais seguro. Os objetivos serão alcançados através da colaboração estratégica entre o Governo, o setor privado e parceiros internacionais, assegurando recursos para proteger, detetar, responder e recuperar de ciberameaças, promovendo um uso ético e seguro da tecnologia e reforçando a segurança nacional e a estabilidade regional.

2.3 Objetivos Estratégicos e Subobjetivos

A elaboração da Estratégia Nacional de Cibersegurança da Guiné-Bissau foi fundamentada numa avaliação rigorosa da situação atual de cibersegurança do país[10]. Este processo envolveu a análise de informações fornecidas pelas partes interessadas e a revisão de documentos estratégicos. A avaliação foi feita a cinco dimensões estratégicas de cibersegurança alinhadas com os objetivos estratégicos da Estratégia Regional de Cibersegurança e de Luta Contra a Cibercriminalidade da CEDEAO, revelando que a Guiné-Bissau está num estágio inicial de desenvolvimento de práticas de cibersegurança, caracterizado por uma abordagem maioritariamente reativa e improvisada. Com base nesta avaliação, foi definido um objetivo de maturidade para os próximos cinco anos, que reflete onde a Guiné-Bissau pretende estar em termos de cibersegurança:

> *A Guiné começou a implementar práticas de cibersegurança e a reconhecer a importância de combater a cibercriminalidade, estando a trabalhar no alinhamento estratégico. Existem esforços para desenvolver políticas e participar em mecanismos regionais, embora estes ainda não sejam sistemáticos. A consciencialização sobre cibersegurança está a aumentar, mas ainda não está enraizada na cultura nacional.*

Consequentemente, foram definidos sete objetivos estratégicos, cada um com subobjetivos, que detalham as ações necessárias, garantindo um foco preciso e eficaz na implementação das iniciativas de cibersegurança na Guiné-Bissau:

Tabela 3 – Objetivos e subobjetivos Estratégicos

Objetivo	Subobjetivo
Objetivo Estratégico 1: *Desenvolver Estruturas de Governança, Políticas e Regulamentação de Cibersegurança*	• 1.1. Desenvolver a Política Nacional de Cibersegurança • 1.2. Implementar uma Autoridade Nacional de Cibersegurança • 1.3. Implementar um Quadro Nacional de Referência de Cibersegurança • 1.4. Adotar Políticas de Segurança da Informação e das Tecnologias e Atos Legais • 1.5. Garantir o Desenvolvimento do Ecossistema de Cibersegurança
Objetivo Estratégico 2: *Desenvolver capacidades e cultura em cibersegurança*	• 2.1. Garantir o Desenvolvimento de Competências em Cibersegurança • 2.2. Assegurar a Promoção da Cultura de Cibersegurança
Objetivo Estratégico 3: *Garantir a Cibersegurança das Infraestruturas Críticas de Informação*	• 3.1. Identificar as Infraestruturas Críticas de Informação do País • 3.2. Proteger e monitorizar as infraestruturas críticas de Informação e serviços essenciais • 3.3. Implementar uma Abordagem de Gestão de Risco

[10] Avaliação realizada com modelo adaptado do "Cybersecurity Capacity Maturity Model for Nations (CMM)"

Objetivo	Subobjetivo
Objetivo Estratégico 4: *Desenvolver as Capacidades e Competências de Resposta a Incidentes de Cibersegurança*	• 4.1. Desenvolver o Plano Nacional de Resposta a Incidentes • 4.2. Estabelecer e Operacionalizar o CSIRT Nacional (CSIRT)
Objetivo Estratégico 5: *Prevenir e Combater a Cibercriminalidade através de um Ambiente Adequado e da Capacidade de Apresentar os Infratores à Justiça*	• 5.1. Adotar Disposições Penais e Procedimentos Penais • 5.2. Implementar Capacidades de Luta Contra o Cibercrime
Objetivo Estratégico 6: *Assegurar a Coordenação e a Cooperação em Cibersegurança e Cibercriminalidade*	• 6.1. Promover a Ratificação das Convenções • 6.2. Assegurar a Coordenação Nacional • 6.3. Promover a Cooperação Internacional
Objetivo Estratégico 7: *Estabelecer Mecanismos Regionais de Cibersegurança*	• 7.1. Promover a Cooperação Regional • 7.2. Identificar e Procurar Financiamento para Dispositivos Nacionais e Regionais

Para alcançar estes objetivos a Guiné-Bissau irá implementar um conjunto de programas e iniciativas estratégias, as quais serão detalhadas no documento “Plano de Ação da Estratégia Nacional de Cibersegurança da Guiné-Bissau”.

OBJETIVO ESTRATÉGICO 1:
Desenvolver Estruturas de Governança, Políticas e Regulamentação de Cibersegurança

Este objetivo visa estabelecer um quadro regulatório e operacional robusto que fortaleça a segurança digital em Guiné-Bissau, alinhando-o com boas práticas internacionais e regionais. A criação de uma Política Nacional de Cibersegurança definirá diretrizes claras e responsabilidades para todas as partes envolvidas, garantindo que as práticas de segurança sejam padronizadas e consistentes em todo o país. Essa política será revista periodicamente para se adaptar às mudanças no panorama de ameaças e tecnologias, mantendo a sua eficácia e relevância.

A instauração de uma Autoridade Nacional de Cibersegurança centralizará a governança da cibersegurança, coordenando a implementação de políticas e a resposta a incidentes de segurança. Este órgão também promoverá a cultura de segurança, desenvolvendo competências através de programas contínuos de formação e sensibilização.

Complementarmente, será estabelecido um Quadro Nacional de Referência que defina as boas práticas mínimos para a segurança de informações e tecnologias. Este quadro incluirá medidas detalhadas para a proteção de infraestruturas críticas e gestão de dados, promovendo práticas seguras em todas as entidades nacionais.

A formulação de políticas específicas para a segurança da informação e a criação de legislação apropriada assegurarão a proteção eficaz contra ciberataques e outras ameaças digitais. Este enquadramento legal e regulatório garantirá que as medidas de segurança sejam aplicadas consistentemente, estabelecendo a Guiné-Bissau como um ambiente digital seguro e resiliente.

Subobjetivo 1.1 - Desenvolver a Política Nacional de Cibersegurança

Com a Estratégia Nacional de Cibersegurança em vigor, a Guiné-Bissau deve desenvolver uma Política Nacional de cibersegurança para garantir a proteção do ciberespaço e enfrentar os desafios relacionados à cibercriminalidade. A Política Nacional deve ser elaborada em alinhamento com a Estratégia regional da CEDEAO e revista periodicamente para assegurar sua relevância e eficácia. A Política Nacional de Cibersegurança deverá estabelecer diretrizes claras e responsabilidades para todas as partes interessadas, assegurando o alinhamento com as diretrizes e objetivos da Estratégia Regional e da Estratégia Regional da CEDEAO.

Além disso, deverá ser elaborada uma estratégia específica para combater a cibercriminalidade, incluindo objetivos, metas e ações concretas e garantindo mecanismos de coordenação entre as autoridades de aplicação da lei, o setor privado e outras partes interessadas. Para assegurar a atualização e relevância contínua, deverá ser definido um cronograma para a revisão e atualização periódica da Política Nacional de Cibersegurança, incorporando o feedback das partes interessadas e adaptando as políticas e estratégias às novas ameaças e tecnologias emergentes.

Para concretizar este objetivo, será essencial definir processos e procedimentos claros para a implementação das medidas de cibersegurança, assegurando a repetição e a consistência e garantir que esses processos sejam documentados e comunicados a todas as partes relevantes. A Política Nacional de Cibersegurança deve estar alinhada com os objetivos regionais e internacionais, promovendo a harmonização das práticas de cibersegurança e a participação ativa nas iniciativas e programas da CEDEAO e outras organizações internacionais.

Neste sentido, a promoção da consciência e a capacitação será alcançada através da realização de ações de sensibilização para aumentar a consciência sobre a importância da cibersegurança e da

luta contra a cibercriminalidade, bem como pela oferta de programas de formação e capacitação para profissionais de cibersegurança, autoridades de aplicação da lei e outras Partes Interessadas.

Subobjetivo 1.2 - Implementar uma Autoridade Nacional de Cibersegurança

Para fortalecer a cibersegurança e garantir um ciberespaço seguro e fiável, a Guiné-Bissau deve estabelecer uma Autoridade Nacional de Cibersegurança com responsabilidades claramente definidas. Esta autoridade será responsável pela governança global do sistema nacional de cibersegurança, incluindo a definição de políticas nacionais e setoriais, o desenvolvimento de estratégias, o acompanhamento de planos de ação e a preparação de textos legislativos e regulamentares. Além disso, esta Autoridade coordenará as respostas a incidentes de cibersegurança e facilitará a troca de informações entre as partes interessadas, tanto públicas quanto privadas.

A criação da Autoridade Nacional de Cibersegurança permitirá uma abordagem mais estruturada e proativa na proteção do ciberespaço nacional, assegurando a segurança das infraestruturas críticas e dos serviços essenciais. A autoridade terá um papel fundamental na promoção de uma cultura de cibersegurança, assegurando a formação contínua e o desenvolvimento de competências na área.

Para garantir o sucesso desta iniciativa, deverá ser estabelecido um quadro legal e regulatório que defina claramente as responsabilidades da Autoridade Nacional de Cibersegurança, alinhando as suas funções com as diretrizes da CEDEAO e outras convenções internacionais. Deverá existir um investimento na formação contínua de pessoal em cibersegurança, promovendo a contratação de especialistas qualificados e a criação de programas de formação e certificação na área. A coordenação intersectorial será facilitada para garantir uma resposta eficiente a incidentes de cibersegurança, estabelecendo mecanismos de comunicação e colaboração entre a autoridade e as infraestruturas críticas.

Além disso, as campanhas de sensibilização e educação sobre cibersegurança serão lançadas para o público em geral, incluindo módulos de cibersegurança nos currículos escolares e universitários.

Com essas iniciativas, a Guiné-Bissau estará mais bem preparada para enfrentar os desafios de cibersegurança, promovendo uma abordagem coordenada e eficaz que protege as suas infraestruturas críticas e serviços essenciais, enquanto desenvolve uma cultura de cibersegurança robusta e sustentável.

Subobjetivo 1.3 - Estabelecer um Quadro Nacional de Referência de Cibersegurança

Para garantir a proteção eficaz da Informação e Tecnologias, a Guiné-Bissau estabelecerá um referencial geral de segurança. Este referencial incluirá requisitos mínimos e boas práticas básicas para a segurança da Informação e Tecnologias, proporcionando uma base regulatória clara e consistente para todas as organizações relevantes. A implementação sistemática deste referencial promoverá a uniformidade nas práticas de segurança e ajudará a mitigar vulnerabilidades significativas.

Para atingir este objetivo, será criado um referencial de segurança abrangente que defina os requisitos mínimos e boas práticas básicas para a segurança da Informação e Tecnologias, alinhado com as melhores práticas internacionais e as diretrizes da CEDEAO. O referencial será formalizado através de legislação e regulamentação adequadas, garantindo que tenha um caráter jurídico vinculativo para todas as organizações relevantes. A implementação do referencial geral de

segurança será promovida em todas as entidades governamentais e infraestruturas críticas, estabelecendo mecanismos de auditoria e avaliação para monitorizar a conformidade com o referencial.

Subobjetivo 1.4 - Adotar Políticas de Segurança da Informação e Tecnologias e Atos Legais

Para garantir a proteção eficaz da Informação e Tecnologias na Guiné-Bissau, é decisivo adotar e implementar políticas de segurança claras e sistemáticas. Estas políticas deverão abranger todos os aspetos da segurança da Informação e Tecnologias, desde a gestão de acesso até à monitorização e resposta a incidentes. A formalização e aplicação consistente destas políticas são essenciais para proteger a integridade, confidencialidade e disponibilidade dos dados e sistemas de informação do país.

Para alcançar este objetivo, serão elaboradas políticas de segurança abrangentes para sistemas de informação que definam normas e procedimentos claros, assegurando que as políticas de segurança sejam alinhadas com as melhores práticas internacionais e diretrizes da CEDEAO. As políticas de segurança serão aplicadas de forma consistente em todas as entidades governamentais e infraestruturas críticas, estabelecendo mecanismos de monitorização e auditoria para garantir a conformidade com as políticas de segurança. Procedimentos detalhados para a proteção da Informação e Tecnologias serão criados, incluindo a gestão de acessos, monitorização de atividades e resposta a incidentes, além da implementação de tecnologias de segurança como *firewalls*, sistemas de deteção de intrusões (IDS) e soluções de gestão de incidentes.

As campanhas de sensibilização sobre a importância das políticas de segurança da Informação e Tecnologias serão realizadas para todos os funcionários, juntamente com programas de formação contínua em cibersegurança, focados na implementação e cumprimento das políticas de segurança. As políticas de segurança serão revistas e atualizadas regularmente para refletir as mudanças no panorama de ameaças e nas melhores práticas, incorporando feedback das auditorias de segurança e das avaliações de risco para melhorar continuamente as políticas de segurança.

As políticas de segurança da Informação e Tecnologias serão integradas na governança de TI das organizações, assegurando que a segurança da informação seja uma prioridade estratégica e operacional em todas as entidades.

Subobjetivo 1.5 - Garantir o Desenvolvimento do Ecossistema de Cibersegurança

Para melhorar a cibersegurança, a Guiné-Bissau promoverá o desenvolvimento de um ecossistema de cibersegurança robusto. Este ecossistema incluirá a criação de organizações dedicadas à cibersegurança, a promoção de parcerias entre o setor público e privado e a disponibilização de serviços especializados, como resposta a incidentes e consultoria de segurança. A implementação dessas políticas visa melhorar a qualidade e a acessibilidade dos serviços de cibersegurança na Guiné-Bissau.

Para atingir este objetivo, a criação de empresas e organizações dedicadas a oferecer serviços de cibersegurança será promovida, incentivando o empreendedorismo no setor de cibersegurança através de incentivos fiscais e programas de financiamento. Parcerias entre o setor público e privado serão desenvolvidas para fortalecer a capacidade de cibersegurança, facilitando a colaboração entre as entidades governamentais, empresas de tecnologia e instituições académicas. Serviços especializados de cibersegurança, como resposta a incidentes, auditorias de segurança e

consultoria, serão criados e promovidos, garantindo que esses serviços sejam acessíveis e de alta qualidade, atendendo às necessidades das infraestruturas críticas e serviços essenciais.

Normas de qualidade para os serviços de cibersegurança oferecidos no país serão implementados, assegurando que os operadores e organizações tenham fácil acesso a serviços de cibersegurança confiáveis e eficientes.

OBJETIVO ESTRATÉGICO 2:
Desenvolver capacidades e cultura em cibersegurança

A robustez de um ambiente digital não se mede apenas pela sua infraestrutura tecnológica, mas também pelo nível de competência e pela cultura de cibersegurança que permeia a sociedade. Com este objetivo, a Guiné-Bissau visa cultivar um ecossistema de cibersegurança sustentável que não só eduque, mas também envolva ativamente cidadãos, profissionais e instituições na proteção contra ciberameaças. Este objetivo estratégico engloba duas vertentes principais: o desenvolvimento de competências específicas na área de cibersegurança e a promoção de uma cultura de cibersegurança consciente e proativa.

O desenvolvimento de competências especializadas é vital para formar profissionais capazes de responder eficazmente aos desafios da cibersegurança. Para isso, serão criados programas estruturados de formação nas universidades e escolas técnicas, integrando a cibersegurança nos currículos de TI e promovendo a investigação e a inovação neste campo. Através da oferta de cursos de graduação e pós-graduação, bem como módulos específicos em cursos existentes, a Guiné-Bissau pretende preparar uma nova geração de profissionais qualificados. Estes esforços serão complementados por campanhas de sensibilização que aumentem a consciência sobre a importância da cibersegurança desde o ensino básico até ao secundário, incentivando uma abordagem integrada que abrange tanto os aspetos técnicos quanto os legais da cibersegurança.

Paralelamente, assegurar a promoção de uma cultura de cibersegurança robusta é essencial para que todos os segmentos da sociedade compreendam e implementem práticas seguras. Neste sentido, implementar-se-ão programas regulares de sensibilização através de campanhas de informação pública que utilizem diversos meios de comunicação, como televisão, rádio, internet e redes sociais. Esses programas serão desenhados não só para o público geral, mas também para funcionários públicos e empresas, reforçando a importância de práticas de segurança em todas as atividades diárias. Através de parcerias com organizações não-governamentais, o setor privado e instituições académicas, a Guiné-Bissau fomentará uma compreensão profunda e prática das boas práticas de cibersegurança, criando um ambiente digital mais seguro e confiável.

Este objetivo estratégico, ao focar tanto no desenvolvimento de competências quanto na promoção de uma cultura informada, estabelece uma base sólida para um futuro digital seguro na Guiné-Bissau, garantindo que a cibersegurança seja vista como uma responsabilidade partilhada por todos os cidadãos e instituições.

Subobjetivo 2.1 - Garantir o Desenvolvimento de Competências na Área de Cibersegurança

Para melhorar a cibersegurança na Guiné-Bissau, é fundamental garantir o desenvolvimento de competências na área. Isto inclui a criação de programas estruturados de formação em cibersegurança nas universidades e escolas técnicas, bem como a promoção da investigação e da inovação. Integrar a cibersegurança como um componente regular da formação profissional em TI é essencial para preparar a próxima geração de profissionais qualificados.

Para atingir este objetivo, serão estabelecidos cursos de graduação e pós-graduação em cibersegurança nas universidades e escolas técnicas, incluindo módulos específicos de cibersegurança nos cursos de TI existentes, abrangendo aspetos técnicos e legais. Programas de formação contínua serão implementados para profissionais de TI, focados em cibersegurança, promovendo certificações profissionais reconhecidas internacionalmente para aumentar a qualificação dos profissionais. Prevê—se ainda a realização de campanhas de sensibilização para

aumentar a consciência sobre a importância da cibersegurança entre estudantes, profissionais de TI e o público em geral, integrando a cibersegurança nos currículos escolares desde o ensino básico até o ensino secundário.

A investigação em cibersegurança será incentivada através de bolsas de estudo e financiamentos para projetos de inovação, estabelecendo parcerias entre universidades, Governo e setor privado para fomentar a investigação aplicada em cibersegurança. Os programas de formação em cibersegurança cobrirão tanto os aspetos técnicos quanto os legais da área, promovendo o desenvolvimento de competências em análise forense digital, gestão de incidentes e conformidade legal. A longo prazo, centros de excelência em cibersegurança deverão ser estabelecidos nas principais universidades e instituições de investigação, fomentando a colaboração entre os centros de excelência e outras instituições nacionais e internacionais.

A cibersegurança será incorporada como um componente essencial nos programas de formação profissional em TI, oferecendo workshops e cursos especializados para profissionais em exercício. Dever-se-ão realizar programas de capacitação para formadores e educadores na área de cibersegurança, assegurando que os educadores estejam atualizados com as últimas tendências e tecnologias em cibersegurança.

Subobjetivo 2.2 - Assegurar a Promoção da Cultura de Cibersegurança

A promoção de uma cultura de cibersegurança abrangente e contínua é fundamental para a Guiné-Bissau, tendo sempre em consideração a realidade do país. Para garantir o sucesso desta iniciativa, será essencial implementar programas regulares de sensibilização e campanhas públicas de informação que cheguem a todos os cidadãos, independentemente do seu nível de escolaridade. A cibersegurança será integrada na educação formal e, simultaneamente, dinamizados programas de formação contínua para cidadãos, funcionários públicos e empresas, recorrendo a uma variedade de meios de comunicação, como televisão, rádio, internet e redes sociais, de modo a alcançar diferentes públicos.

Serão criados materiais didáticos acessíveis e adaptados para professores e educadores, promovendo a compreensão das boas práticas de cibersegurança, de forma inclusiva e adequada aos diferentes níveis de literacia digital. Além disso, serão desenvolvidas parcerias com organizações não-governamentais, setor privado e instituições académicas para promover a cibersegurança através de eventos e campanhas educativas, assegurando que toda a população, independentemente do seu grau de instrução, esteja envolvida e informada.

OBJETIVO ESTRATÉGICO 3:
Garantir a Cibersegurança das Infraestruturas Críticas de Informação

Num mundo cada vez mais interconectado, a proteção das infraestruturas críticas de informação torna-se essencial para a segurança nacional da Guiné-Bissau. Este objetivo estratégico é dedicado à criação de um sistema robusto que não apenas identifica e protege estas infraestruturas essenciais, mas também promove uma gestão de riscos eficaz e uma cultura de segurança resiliente.

Em primeiro lugar é necessária uma identificação clara destas infraestruturas críticas que são vitais para o funcionamento do país, como redes de comunicação, sistemas financeiros e serviços governamentais. A identificação exata destes ativos críticos é essencial para a concentração de esforços de proteção e a alocação adequada de recursos. Posteriormente, a implementação de medidas de segurança robustas é fundamental. Estas medidas incluem a realização de auditorias de segurança regulares, a criação de políticas de segurança que abordem tanto a prevenção como a reação a incidentes e a implementação de sistemas de alerta precoce.

Além disso, a gestão de riscos desempenha um papel essencial, permitindo uma compreensão detalhada das potenciais vulnerabilidades e a elaboração de estratégias para mitigar os riscos identificados. Este processo envolve uma avaliação contínua, que garante que as medidas de proteção sejam sempre adequadas ao nível de ameaça atual e adaptáveis a mudanças no ambiente de segurança.

Este objetivo estratégico abarca ainda a formação e capacitação contínuas dos responsáveis pela gestão e operação das infraestruturas críticas, garantindo que as equipas estejam bem preparadas para responder de forma eficaz a ciberataques e otimizar os protocolos de segurança em uso. A integração destas práticas ao longo de todas as camadas da infraestrutura nacional não só fortalece as defesas contra ataques diretos, como também constrói uma base sólida para a resiliência a longo prazo.

Após a implementação deste objetivo, a Guiné-Bissau estabelece uma defesa sólida e proativa contra ameaças, protegendo os seus cidadãos e as funções críticas do estado, e contribuindo significativamente para a estabilidade e confiança no seu espaço digital.

Subobjetivo 3.1 - Identificar as Infraestruturas Críticas de Informação do País

Identificar de forma precisa e abrangente as infraestruturas críticas de informação do país é o primeiro passo no reforço da segurança das mesmas. Este processo envolve a catalogação das infraestruturas que são essenciais para o funcionamento do Estado e para a segurança dos cidadãos, incluindo redes de comunicações, sistemas de energia, serviços financeiros e infraestruturas de saúde, entre outros. A correta identificação destas infraestruturas permite não só uma alocação mais eficaz de recursos para a sua proteção, como também estabelece as bases para o desenvolvimento de estratégias de mitigação de riscos e resposta a incidentes. Através deste subobjetivo, a Guiné-Bissau assegura que todas as medidas subsequentes de proteção e gestão de riscos sejam direcionadas e eficientes, fundamentadas numa compreensão clara de quais são os ativos mais vitais que necessitam de proteção prioritária.

Subobjetivo 3.2 - Proteger e monitorizar as infraestruturas críticas de Informação e serviços essenciais

Para garantir um ciberespaço seguro e fiável, a Guiné-Bissau adotará uma abordagem sistemática para identificar, proteger e monitorizar infraestruturas críticas e serviços essenciais. A implementação de medidas robustas de cibersegurança para estas infraestruturas é fundamental para prevenir interrupções e assegurar a continuidade dos serviços vitais para o país. Os procedimentos incluirão a identificação consistente de redes e sistemas críticos, a realização de auditorias de segurança regulares e a implementação de políticas de notificação de incidentes de forma coordenada e eficiente.

Para atingir este objetivo, será estabelecido um processo formal para a identificação de infraestruturas críticas e serviços essenciais, desenvolvendo critérios claros e consistentes para classificar infraestruturas críticas com base na sua importância e potencial impacto. Implementar-se-á um programa de auditorias de segurança regulares para infraestruturas críticas e serviços essenciais, utilizando auditores qualificados e metodologias reconhecidas para avaliar a conformidade e identificar vulnerabilidades. Planos de proteção específicos serão criados e implementados para infraestruturas críticas, incluindo medidas preventivas e reativas, desenvolvendo planos de resposta a incidentes que sejam claros e acionáveis, assegurando a coordenação entre as partes envolvidas.

Serão estabelecidas políticas e procedimentos claros para a notificação de incidentes de cibersegurança, garantindo que as notificações de incidentes sejam sistemáticas e abrangentes, envolvendo todas as partes interessadas relevantes. Os programas de formação contínua em cibersegurança serão promovidos para operadores de infraestruturas críticas, incentivando a certificação profissional em cibersegurança para garantir que o pessoal envolvido esteja devidamente qualificado. A coordenação entre diferentes setores e entidades responsáveis pela segurança das infraestruturas críticas será facilitada, estabelecendo plataformas de colaboração e partilha de informações sobre ameaças e boas práticas.

Salienta-se ainda a importância do desenvolvimento e da implementação de políticas de segurança específicas para infraestruturas críticas, que abranjam a gestão de acesso, a monitorização e a resposta a incidentes, assegurando que todas as infraestruturas críticas tenham políticas de segurança documentadas e implementadas.

Subobjetivo 3.3 - Implementar uma Abordagem de Gestão de Risco

Para assegurar um nível adequado de cibersegurança, a Guiné-Bissau deve implementar uma abordagem sistemática de gestão de risco. Esta abordagem permitirá identificar, avaliar e mitigar os riscos associados às infraestruturas críticas e aos serviços essenciais, garantindo a continuidade e a segurança das operações. A gestão de riscos deve ser integrada em todas as camadas da administração pública e do setor privado, promovendo uma cultura de segurança e resiliência.

A adoção de uma abordagem de gestão de risco proporcionará uma visão clara das ameaças e vulnerabilidades, permitindo que os recursos sejam direcionados de forma eficiente para mitigar os riscos mais críticos. Esta prática é fundamental para fortalecer a cibersegurança nacional e proteger os ativos digitais da Guiné-Bissau contra ciberataques e outras ameaças.

Para alcançar este objetivo, será estabelecida uma política nacional que defina as diretrizes e responsabilidades para a gestão de riscos em cibersegurança, alinhada com as melhores práticas internacionais e as diretrizes da CEDEAO. Serão também implementados processos contínuos de

avaliação de riscos para identificar ameaças e vulnerabilidades, utilizando ferramentas e metodologias reconhecidas para a análise de riscos. Também serão desenvolvidos e implementados planos de mitigação de riscos para tratar as vulnerabilidades identificadas, priorizando as ações de mitigação com base no impacto e na probabilidade dos riscos. Neste sentido, programas de formação em gestão de riscos também serão promovidos para profissionais de cibersegurança, assegurando que todos os níveis da administração pública e do setor privado compreendam a importância da gestão de riscos.

Também serão estabelecidos processos de monitorização contínua dos riscos e das medidas de mitigação, realizando revisões periódicas para atualizar as avaliações de riscos e os planos de mitigação conforme necessário. A gestão de riscos será integrada nas operações diárias das infraestruturas críticas e dos serviços essenciais, garantindo que seja uma parte integral da tomada de decisões estratégicas e operacionais.

OBJETIVO ESTRATÉGICO 4
Desenvolver as Capacidades e Competências de Resposta a Incidentes de Cibersegurança

Para garantir um ciberespaço seguro e fiável na Guiné-Bissau, é essencial fortalecer as estruturas de resposta a incidentes de segurança. Este objetivo estratégico foca-se na implementação de um Plano Nacional de Resposta a Incidentes e na criação de um sistema de alerta e resposta em caso de incidente, através da criação e operacionalização da CSIRT. Estes esforços são fundamentais para estabelecer uma resposta imediata e eficaz contra as ameaças digitais. Com a criação do Plano Nacional de Resposta a Incidentes, o país definirá procedimentos claros e coordenará ações entre diversas entidades, garantindo uma gestão eficiente de incidentes. Paralelamente, a CSIRT servirá como um núcleo vital para a monitorização contínua e a análise de riscos, equipando a Guiné-Bissau com as ferramentas necessárias para uma resposta rápida e informada. Ao desenvolver estas capacidades, o país não só melhora a sua resiliência contra ataques digitais, mas também eleva a confiança na sua infraestrutura tecnológica, essencial para o avanço econômico e social.

Subobjetivo 4.1 - Desenvolver o Plano Nacional de Resposta a Incidentes

O desenvolvimento do Plano Nacional de Resposta a Incidentes constitui um pilar de extrema importância na estratégia de fortalecimento das capacidades de resposta a incidentes de cibersegurança da Guiné-Bissau. Este plano tem como propósito definir claramente os procedimentos, responsabilidades e recursos necessários para uma resposta rápida e eficaz aos a incidentes de cibersegurança, minimizando impactos e restaurando a normalidade operacional com celeridade. Enfatizando uma abordagem proativa e coordenada, o plano envolverá múltiplos partes interessadas, incluindo entidades governamentais, setor privado e comunidade académica, garantindo que todas as partes estejam preparadas e alinhadas com as melhores práticas internacionais de resposta a incidentes. A implementação deste plano será acompanhada de formações regulares e exercícios de simulação, reforçando as competências dos intervenientes e a resiliência do sistema de cibersegurança nacional.

Subobjetivo 4.2 - Estabelecer e Operacionalizar a CSIRT Nacional (CSIRT)

Para melhorar a cibersegurança e garantir um ciberespaço seguro e fiável, a Guiné-Bissau deverá estabelecer uma Equipa de Resposta a Incidentes de Segurança Informática (CSIRT) com responsabilidades bem definidas. A CSIRT terá como função principal a deteção, análise e resposta a incidentes de cibersegurança, promovendo uma abordagem estruturada e coordenada na gestão de incidentes.

A CSIRT nacional deverá coordenar com setores críticos e deverá também estabelecer uma rede com outras CSIRTs setoriais, facilitando a partilha de informações e a implementação de processos repetíveis para a deteção e resposta a incidentes. Esta estrutura permitirá uma resposta mais eficaz e eficiente a ciberameaças, garantindo a proteção das infraestruturas críticas e dos serviços essenciais do país.

A coordenação entre a CSIRT nacional e os setores críticos deverá também ser tida em conta, garantindo uma resposta integrada a incidentes de cibersegurança e estabelecendo canais de comunicação eficientes para a partilha de alertas e informações sobre ameaças entre a CSIRT e os setores críticos.

É ainda de extrema importância que se invista na formação e capacitação contínua dos membros da CSIRT em técnicas de deteção e resposta a incidentes, promovendo a certificação profissional em áreas relevantes de cibersegurança para os membros da CSIRT. Serão estabelecidas parcerias com

outras CSIRTs a nível regional e internacional para a partilha de informações e boas práticas, e a Guiné-Bissau participará em redes e fóruns de CSIRTs para fortalecer a capacidade de resposta a incidentes a nível nacional e internacional. Ferramentas avançadas de monitorização, deteção e resposta a incidentes serão adquiridas e implementadas, assegurando a integração de sistemas e tecnologias relevantes para a recolha e análise rápida de dados pertinentes durante um incidente.

OBJETIVO ESTRATÉGICO 5
Prevenir e Combater a Cibercriminalidade através de um Ambiente Adequado e da Capacidade de Apresentar os Infratores à Justiça

Para garantir uma redução efetiva da cibercriminalidade através de um ambiente de segurança adequado e a capacidade de apresentar os infratores à justiça, a Guiné-Bissau compromete-se a estabelecer um quadro legal e operacional robusto. Este objetivo estratégico visa assegurar que os cibercrimes sejam devidamente investigados, os infratores sejam responsabilizados e a justiça seja eficazmente administrada. A implementação deste objetivo será orientada pelos seguintes subobjetivos.

Subobjetivo 5.1 - Adotar Disposições Penais e Procedimentos Penais

Para alcançar este objetivo, é necessário criar e promulgar leis penais que abordem explicitamente os cibercrimes, alinhadas com as melhores práticas internacionais e diretrizes da CEDEAO, garantindo que a legislação cubra uma ampla gama de cibercrimes, incluindo acesso não autorizado, fraude eletrónica, ciberespionagem e ataques contra infraestruturas críticas. Sanções penais adequadas deverão ser estabelecidas para diferentes tipos de cibercrimes, com base na gravidade e impacto das infrações, incluindo disposições específicas para a proteção de infraestruturas críticas e serviços essenciais.

É ainda necessário que os procedimentos penais sejam padronizados para a investigação, acusação e julgamento de cibercrimes, assegurando que sejam claros, eficazes e proporcionem garantias processuais adequadas para os acusados. Devem também ser implementados programas de formação contínua para juízes, promotores e agentes da polícia sobre as especificidades dos cibercrimes e os procedimentos legais aplicáveis, promovendo a especialização de alguns membros do sistema judicial e das forças policiais em cibercriminalidade.

Além disso, deverão ser realizadas ações de sensibilização para informar o público e as partes interessadas sobre a nova legislação e as sanções associadas aos cibercrimes, assegurando que as autoridades de aplicação da lei estejam plenamente cientes das novas disposições legais e dos seus deveres no seu cumprimento. A cooperação com outras jurisdições e organizações internacionais na luta contra o cibercrime será fortalecida, participando ativamente em redes internacionais de combate ao cibercrime para troca de informações e boas práticas.

Deverá também ser estabelecido um mecanismo para monitorizar a implementação e a eficácia das leis penais e procedimentos penais relacionados com cibercrimes, revisando e atualizando periodicamente a legislação para refletir as mudanças no panorama das ciberameaças e as melhores práticas emergentes.

Subobjetivo 5.2 - Implementar Capacidades de Luta Contra o Cibercrime

Para reduzir eficazmente a cibercriminalidade e assegurar a capacidade de apresentar os infratores à justiça, a Guiné-Bissau necessita de desenvolver e fortalecer a sua capacidade de combate ao cibercrime, o que inclui a criação de uma autoridade coordenadora para unidades especializadas, a implementação de procedimentos padronizados de investigação e o estabelecimento de laboratórios de investigação e recursos de coleta de provas. Além disso, deverá haver um esforço contínuo para treinar oficiais de justiça e magistrados na gestão de casos de cibercrime.

Para assegurar o cumprimento deste objetivo, deverá ser estabelecida uma autoridade coordenadora responsável pela supervisão e coordenação das unidades de luta contra o cibercrime, garantindo que esta autoridade tenha os recursos e o apoio necessários para desempenhar

eficazmente as suas funções. Posteriormente, unidades especializadas de combate ao cibercrime deverão ser criadas dentro das forças policiais e do sistema judicial, garantindo que estas unidades tenham acesso a ferramentas e tecnologias avançadas para investigação de cibercrimes.

É igualmente importante assegurar que sejam criados laboratórios de investigação equipados com tecnologias avançadas para análise forense digital, garantindo que tenham capacidade para recolher, preservar e analisar provas digitais de maneira eficaz. Paralelamente devem ser estabelecidos recursos e procedimentos para a recolha, preservação e apresentação de provas digitais em tribunal, assegurando que os oficiais tenham acesso às ferramentas e conhecimentos necessários para coletar provas de maneira eficaz e legal. Complementarmente ao Subobjetivo anterior, programas de formação contínua devem ser implementados para oficiais de justiça, polícia e magistrados sobre cibercrime e cibersegurança, promovendo a especialização de alguns membros do sistema judicial e das forças policiais em investigações de cibercrime.

Além disso, deverão também ser lançadas campanhas de sensibilização para informar o público sobre o cibercrime e as medidas de prevenção, incluindo a inclusão de cibersegurança e cibercrime nos currículos de formação das forças policiais e dos cursos de direito.

A cooperação da Guiné-Bissau com outras jurisdições e organizações internacionais será fortalecida para troca de informações e boas práticas no combate ao cibercrime, levando a que participe ativamente em redes internacionais de combate ao cibercrime para melhorar a eficácia das investigações e a aplicação da lei nestas questões legais.

OBJETIVO ESTRATÉGICO 6
Assegurar a Coordenação e a Cooperação em Cibersegurança e Cibercriminalidade

Este objetivo visa fortalecer a cibersegurança na Guiné-Bissau através da coordenação eficaz tanto a nível nacional quanto internacional. A cooperação e alinhamento com normas e práticas globais são essenciais para enfrentar os desafios de cibersegurança de forma abrangente e integrada. Este objetivo é detalhado nos seguintes subobjetivos.

Subobjetivo 6.1 - Promover a Ratificação das Convenções

Para fortalecer a cibersegurança e garantir a capacidade de luta contra o cibercrime, a Guiné-Bissau promoverá a ratificação de convenções internacionais. A adesão a estas convenções permitirá ao país alinhar-se com as melhores práticas globais e fortalecer a cooperação internacional no combate ao cibercrime. Será estabelecido um processo formal para a ratificação dessas convenções, garantindo clareza e eficácia. Para aumentar a compreensão sobre a importância das convenções, serão realizadas campanhas de sensibilização que envolvem diversas partes interessadas. As políticas e práticas nacionais de cibersegurança serão alinhadas com as diretrizes internacionais, e a Guiné-Bissau participará ativamente em fóruns globais para compartilhar experiências e aprender com as melhores práticas. Um mecanismo de monitorização será implementado para garantir o cumprimento contínuo das convenções ratificadas. Além disso, será proporcionada formação contínua às autoridades para assegurar uma implementação eficaz.

Subobjetivo 6.2 - Assegurar a Coordenação Nacional

Para fortalecer a cibersegurança, é vital assegurar a coordenação eficaz entre todos os atores envolvidos. Neste sentido, é essencial que sejam criadas plataformas de diálogo e colaboração entre Governo, setor privado, academia e sociedade civil, bem como serem organizados encontros e workshops regulares para a troca de informações e boas práticas. Serão ainda desenvolvidos sistemas seguros para a partilha de informações sobre ameaças e incidentes, incentivando a confiança e a colaboração entre as partes interessadas. Deverão ser formadas parcerias estratégicas entre instituições de formação, fornecedores de cibersegurança e operadores de infraestruturas críticas e deverão também ser estabelecidos mecanismos formais de coordenação, como comitês interministeriais e grupos de trabalho, para gerirem todas estas iniciativas de cibersegurança.

Subobjetivo 6.3 - Promover a Cooperação Internacional

A promoção da cooperação internacional é essencial para fortalecer a cibersegurança e, neste sentido, deverão ser estabelecidas parcerias regulares com outros países e organizações internacionais para a troca de informações e melhores práticas. A Guiné-Bissau deverá participar ativamente em programas de cooperação internacional, como formações e exercícios de resposta a incidentes. Por outro lado, as políticas nacionais deverão ser alinhadas com as boas práticas internacionais, facilitando a cooperação e a resposta conjunta a ciber-incidentes. A Guiné-Bissau deverá contribuir para respostas coletivas a ciberameaças e promover a participação dos seus profissionais em programas internacionais de capacitação. A eficácia das iniciativas de cooperação deverá ser monitorizada, ajustando as estratégias para melhorar continuamente as relações internacionais em cibersegurança.

OBJETIVO ESTRATÉGICO 7
Estabelecer Mecanismos Regionais de Cibersegurança

Por fim, é essencial que a Guiné-Bissau se integre nos mecanismos regionais de cibersegurança e alinhe as ações nacionais com os objetivos e diretrizes da Comunidade Económica dos Estados da África Ocidental (CEDEAO). Neste sentido, este objetivo estratégico inclui os seguintes subobjetivos,

Subobjetivo 7.1 – Promover a Cooperação Regional

A Guiné-Bissau comprometer-se-á a intensificar a sua colaboração no âmbito da cibersegurança regional, adotando uma abordagem multifacetada conforme delineado nas iniciativas da CEDEAO. Inicialmente, a Guiné-Bissau irá colaborar com a CEDEAO para implementar o plano de assistência regional, beneficiando-se dos recursos e apoio oferecidos. Para isso, a Guiné-Bissau deverá criar e/ou eleger equipas dedicadas dentro dos órgãos que se ocuparão da questão da cibersegurança, garantindo que o país siga e contribua ativamente para as diretrizes da CEDEAO. De salientar ainda que as capacidades organizacionais e técnicas deverão ser desenvolvidas para implementar e gerir o plano, oferecendo formação e recursos adequados para as equipas envolvidas na implementação.

Adicionalmente, para assegurar a implementação eficaz da Estratégia Regional de Cibersegurança e de Luta Contra a Cibercriminalidade da CEDEAO, a Guiné-Bissau compromete-se a participar ativamente no Comité Técnico Regional (CTR), que poderá vir a ser criado pela CEDEAO para o Acompanhamento da Estratégia Regional. Isto incluirá a criação de procedimentos regulares para a participação nas reuniões do CTR, contribuindo para as discussões e implementando as recomendações do Comité. Deverão ser desenvolvidos procedimentos regulares para a participação ativa no CTR, designando um representante permanente e suplente. Consequentemente, um plano para implementar as recomendações do CTR a nível nacional deverá ser desenvolvido, monitorizando e relatando o progresso às partes interessadas. Toda a participação e as ações subsequentes da Guiné-Bissau deverá ser documentada em relatórios regulares, promovendo uma abordagem coordenada e eficaz.

Por fim, a Guiné-Bissau participará ativamente nas discussões e esforços preliminares para o estabelecimento de um Centro Regional de Coordenação em Cibersegurança. Este centro será fundamental para a coordenação de iniciativas de cibersegurança na região, permitindo a partilha de informações, a gestão de incidentes e a capacitação conjunta. A Guiné-Bissau envolver-se-á ativamente nas discussões e fases de planeamento para o estabelecimento do centro, contribuindo com ideias e propostas que reflitam as necessidades e capacidades do país. A infraestrutura de cibersegurança interna será desenvolvida e melhorada para se alinhar com os requisitos do centro de coordenação, investindo em tecnologia, equipamentos e recursos humanos. Programas de formação e capacitação deverão ser promovidos para preparar os profissionais de cibersegurança da Guiné-Bissau para participar nas atividades do centro. De forma a garantir a conformidade com as normas e boas práticas estabelecidas, protocolos e acordos de cooperação serão estabelecidos com o centro de coordenação e outros países membros.

Subobjetivo 7.2: Identificar e Procurar Financiamento para a Cibersegurança e Luta Contra o Cibercrime

Para fortalecer a cibersegurança e a luta contra o cibercrime, a Guiné-Bissau estabelecerá procedimentos regulares para identificar e procurar financiamentos disponíveis, tanto regionais quanto internacionais. A integração dessas fontes de financiamento no planeamento nacional de cibersegurança garantirá um esforço contínuo e coordenado para aceder aos recursos necessários

e implementar iniciativas eficazes. Serão estabelecidos procedimentos sistemáticos para monitorar e identificar oportunidades de financiamento em cibersegurança e cibercrime, criando uma base de dados centralizada. Deverá ser estabelecida uma equipa especializada responsável pela procura, elaboração de propostas e gestão de financiamentos. As fontes de financiamento identificadas serão integradas nos planos estratégicos e operacionais de cibersegurança, quer nacionais quer regionais. Paralelamente, serão implementados mecanismos de monitorização para acompanhar a eficácia das iniciativas de captação de recursos, avaliando o impacto dos financiamentos obtidos na melhoria da cibersegurança.

3. CAPÍTULO III - IMPLEMENTAÇÃO DA ESTRATÉGIA

3.1 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 4 – 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

Partes Interessadas	Envolvimento Geral
	colaborará com a Entidade e outras entidades para assegurar a aplicação das leis pertinentes.
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.

Partes Interessadas	Envolvimento Geral
Organizações da Sociedade Civil (PNUD e outras)	As ONGs e associações de consumidores promoverão a consciencialização pública sobre cibersegurança, defenderão 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 instituições 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.

3.2 Implementação da Estratégia Nacional de Cibersegurança

3.2.1 Enquadramento

A Autoridade Nacional de Cibersegurança será responsável pela liderança na implementação e coordenação da Estratégia Nacional de Cibersegurança e do Plano de Ação correspondente. Esta entidade apoiará o Governo nas decisões estratégicas relacionadas à cibersegurança. Detalhes sobre a composição e os membros da Autoridade Nacional de Cibersegurança serão formalizados através de uma Resolução do Conselho de Ministros que também contemplará a rotatividade na liderança para incentivar uma dinâmica renovada nas abordagens de cibersegurança.

A Autoridade Nacional de Cibersegurança terá autonomia para, por iniciativa própria ou a pedido de outros membros, convocar especialistas e representantes de setores públicos e privados para contribuir nas discussões, assegurando uma perspetiva abrangente sobre as questões de cibersegurança.

3.2.2 Objetivos e Responsabilidades

As responsabilidades da Autoridade Nacional de Cibersegurança âmbito da presente Estratégia incluirão:

- Avaliar e aconselhar o Governo sobre questões críticas para melhorar a cibersegurança;
- Desenvolver abordagens para criar estruturas e diretrizes eficazes no combate ao cibercrime, tanto a nível nacional quanto regional;
- Fomentar o desenvolvimento de capacidades institucionais robustas para a proteção contra cibercrimes;
- Estimular a colaboração e o alinhamento entre os diferentes níveis governamentais em assuntos de cibersegurança;
- Promover e fortalecer parcerias entre os setores público e privado para uma abordagem unificada da cibersegurança;
- Analisar continuamente o cenário de cibersegurança, identificando áreas prioritárias e garantindo abordagens específicas para cada desafio;
- Identificar as infraestruturas críticas de informação e implementar medidas de proteção;
- Detetar falhas na execução de projetos de cibersegurança e propor soluções;
- Garantir a implementação das ações e objetivos delineados na estratégia;
- Coordenar entre os diversos setores envolvidos para assegurar uma implementação eficaz e resultados consistentes;
- Explorar e propor opções de financiamento para a implementação da Estratégia;
- Supervisionar rigorosamente o cumprimento dos prazos e metas estabelecidos para cada ação.

3.3 Financiamento e Alocação de Recursos

A implementação eficaz da Estratégia Nacional de Cibersegurança da Guiné-Bissau requer a obtenção de recursos e financiamento apropriados. Para tal, o Plano de Ação delineia as potenciais fontes de financiamento e identifica as entidades responsáveis pelas diversas iniciativas previstas.

3.4 Monitorização e Avaliação da Estratégia

A Estratégia Nacional de Cibersegurança estará sob a supervisão da Autoridade Nacional de Cibersegurança, responsável pela avaliação anual focada na verificação do progresso em relação aos objetivos estratégicos e ao plano de ação.

Para garantir a eficácia desta estratégia, é fundamental estabelecer metas de desempenho anuais, que serão definidas para diversas instituições governamentais e partes interessadas, todas elas responsáveis pela implementação de ações específicas no contexto da cibersegurança. Toda esta informação será detalhada e incluída no plano de ação, garantindo uma visibilidade clara das expectativas e dos resultados esperados.

As metas de desempenho serão monitorizadas e avaliadas regularmente, permitindo ajustes conforme necessário, de acordo com a desenvolvimento dinâmico do ciberespaço. Este processo de monitorização contínua assegura que a estratégia mantenha a sua relevância e eficácia ao longo do tempo.