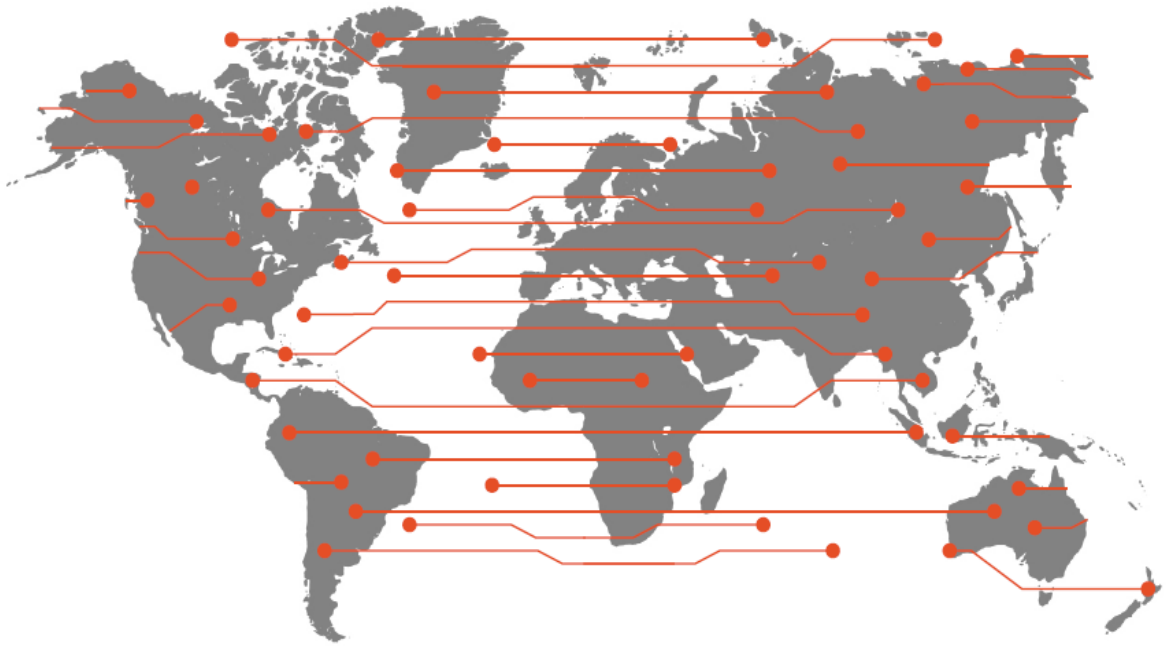
NRD Cyber Security

WORLD BANK GROUP

Projeto

"Desenvolvimento da Estratégia Nacional de Cibersegurança e Plano de Ação para São Tomé e Príncipe"



D-03

Estratégia Nacional de Cibersegurança de São Tomé e Príncipe

Versão 2

Informação do Documento

Título do Projeto:	Desenvolvimento da Estratégia Nacional de Cibersegurança e Plano de Ação para São Tomé e Príncipe		
Título do Relatório:	D-3 Estratégia Nacional de Cibersegurança de São Tomé e Príncipe		
Versão:	2	**Data da Versão:**	15-12-2023
Elaborado por:	Equipa da NRD Cyber Security		
Revisto por:			
Aprovado por:			

Fluxo de Informação

Quem	Data	Contacto
NRD Cyber Security para WB	31-10-2023	
WB para NRD Cyber Security	03-11-2023	
NRD Cyber Security para STP	17-11-2023	
NRD Cyber Security para WB	27-11-2023	
WB para NRD Cyber Security	30-11-2023	
NRD Cyber Security para STP	01-12-2023	
NRD Cyber Security para WB	18-12-2023	

Cronologia das Versões

Nº da Versão	Data	Comentários
1.0	27-10-2023	Versão Rascunho 1.0
1.1	20-11-2023	Versão Rascunho 1.1
2.0	15-12-2023	Versão final 2.0

Índice

1. Lista de Termos e Siglas

Tabela 1 Termos e abreviaturas

Termo / Sigla	Significado / Explicação
AGER	Entidade Reguladora do setor das TIC
ANPDP	Agência Nacional de Proteção de Dados Pessoais
CCTIC	Centro de Competências em TIC
CNPD	Comissão Nacional de Proteção de Dados
COSIC	Comissão para Sociedade de Informação e Comunicação
DITEI	Direção de Tecnologia da Informação
DGRN	Direção Geral de Registos e Notariado
INE	Instituto Nacional de Estatística
INIC	Instituto de Inovação e Conhecimento
MINR-STP	Ministério das Infraestruturas, Recursos Naturais e Meio Ambiente
SAFE	Sistema de Administração Financeira do Estado
STP	São Tomé e Príncipe
TI	Tecnologias de Informação
TIC	Tecnologias de Informação e Comunicação

1. CAPÍTULO I – FUNDAMENTAÇÃO DA ESTRATÉGIA

1.1 INTRODUÇÃO

A Estratégia Nacional de Cibersegurança de São Tomé e Príncipe (2024 - 2028), doravante designada por Estratégia Nacional, delineia uma abordagem multifacetada para salvaguardar a integridade, a confidencialidade e a disponibilidade das infraestruturas digitais do país. Esta estratégia, moldada pela visão de um ciberespaço seguro e resiliente, está alinhada com o compromisso do país em capitalizar os benefícios tecnológicos para promover o desenvolvimento socioeconómico e proteger os interesses nacionais no mundo digital.

São Tomé e Príncipe reconhece a importância do ciberespaço para o progresso social e económico, servindo como um catalisador para a inovação e inclusão. No entanto, tendo em consideração o atual panorama de crescentes ciberameaças, São Tomé e Príncipe reconhece que é imperativa uma resposta proativa e robusta, a fim de assegurar a continuidade dos serviços digitais e proteger os cidadãos contra possíveis ciberataques.

A presente Estratégia Nacional é guiada por um profundo respeito e promoção dos direitos humanos e liberdades fundamentais, assegurando a privacidade, a liberdade de expressão, e a proteção de dados pessoais, estando também em consonância com os princípios e valores consagrados na Constituição da República Democrática de São Tomé e Príncipe, refletindo o compromisso nacional com a ética, a integridade e a justiça.

A transparência e confiança são também elementos fundamentais desta Estratégia, estabelecendo um diálogo aberto e inclusivo entre cidadãos, empresas e instituições, e fomentando a participação ativa da sociedade no ciberespaço. Através da cooperação internacional e da inclusão digital, São Tomé e Príncipe reafirma o seu compromisso com a defesa da soberania no ciberespaço e com o fortalecimento dos laços internacionais.

Na confluência entre inovação e segurança, a educação digital emerge nesta Estratégia como um pilar estratégico. A promoção da educação e a conscientização sobre cibersegurança são fundamentais para cultivar uma sociedade resiliente, capacitando cidadãos para navegarem com segurança e confiança no ciberespaço. Este compromisso com a literacia digital não é apenas uma medida defensiva, mas também um facilitador de oportunidades, desbloqueando o potencial criativo e empreendedor da nação e assegurando que cada cidadão esteja equipado para prosperar na era digital.

1.2 ANÁLISE DO CONTEXTO ENVOLVENTE

Enquanto nação insular em desenvolvimento, São Tomé e Príncipe enfrenta significativos desafios tecnológicos e a presença de recursos limitados para garantir uma ciberdefesa robusta. A escassez de especialistas na área e a infraestrutura tecnológica ainda em consolidação sublinham a urgência de investimento e formação para a implementação e manutenção de medidas de segurança digital eficazes.

No entanto, o contexto digital em São Tomé e Príncipe tem tido um desenvolvimento notável ao longo das últimas duas décadas, marcado por várias iniciativas e projetos que visam promover a governação eletrónica e a integração das tecnologias de informação e comunicação (TIC) na sociedade.

O início deste percurso remonta a 2002, com a criação do Comité de Governação Eletrónica e Gestão de Conhecimento, seguido pela fundação do Centro de Competências em TIC (CCTIC). Embora o projeto do CCTIC não tenha sobrevivido devido à falta de sustentabilidade financeira, essa época assistiu ao surgimento de iniciativas como o "Internet 4All" e a abertura de cibercafés, facilitando o acesso à Internet a custos reduzidos.

A educação e o setor público também beneficiaram da instalação de novos equipamentos com acesso à Internet, incluindo instituições de ensino como o Liceu Nacional. No entanto, a falta de recursos financeiros continuou a ser um obstáculo, como evidenciado pela criação da Comissão para Sociedade de Informação e Comunicação (COSIC) em 2005, que enfrentou desafios semelhantes.

A legislação desempenhou um papel fundamental no avanço da governação eletrónica. A promulgação da Lei sobre o Sistema de Administração Financeira do Estado (SAFE) em 2007 (Lei nº 03/2007) estabeleceu um quadro legal para a gestão financeira. A Lei nº 15/2017 sobre Cibercrime, juntamente com a Lei de Proteção de Dados Pessoais (Lei nº 3/2016), ajudou a estabelecer diretrizes para a cibersegurança e a proteção de dados. Atualmente existem algumas Leis que se encontram em Projeto de Lei, nomeadamente, a lei da assinatura digital, a lei da criação de um cartão único do cidadão e a lei da videoconferência, o reflete o compromisso com a modernização e eficiência.

A inovação tecnológica também foi evidente com o lançamento do passaporte biométrico em 2008 e o passaporte eletrónico em 2018. A implementação de sistemas como o SIDONIA para a gestão aduaneira e o E-VisaST para solicitação eletrónica de vistos demonstra um compromisso contínuo com a modernização e eficiência.

A colaboração internacional desempenhou um papel vital, com parcerias com o Brasil, Taiwan e a União Europeia, contribuindo para o desenvolvimento de infraestruturas como o Centro de Dados e a Rede do Governo. A adesão ao cabo submarino ACE em 2011 e a entrada da segunda operadora de telecomunicações, UNITEL STP, em 2013, melhoraram significativamente a conectividade e reduziram os custos.

Podem ser referidos vários esforços para impulsionar a governação eletrónica e integrar as TIC em vários setores da sociedade de São Tomé e Príncipe. Um marco importante foi o programa "STP em Rede", lançado em 2010, que visou reforçar a governação eletrónica, integrar TIC na educação, incluir as PME na sociedade da informação e fortalecer o INIC. As iniciativas incluíram melhorias nas infraestruturas de comunicação, formação de utentes / utilizadores, legislação específica e aprimoramento da presença do Governo na Internet. Outro exemplo significativo de tais esforços, foi o início da construção de uma *backbone* de fibra ótica governamental em 2017.

Em 2020 foi idealizada a construção de uma Plataforma de Interoperabilidade para São Tomé e Príncipe, constituindo a mesma uma iniciativa estratégica que visa promover a governação digital, facilitar a interação entre o Governo e a sociedade, e contribuir para a modernização económica de São Tomé e Príncipe. A sua implementação é guiada por um conjunto de políticas e normas que enfatizam a abertura, transparência e eficiência. Em novembro de 2021 foi publicado o Quadro Nacional de Interoperabilidade de São Tomé e Príncipe e, atualmente, encontra-se em Projeto de Lei a Lei de Interoperabilidade.

Em 2023, a Comissão Nacional de Proteção de Dados ("CNPD") aprovou a Diretriz/2023/1 sobre medidas organizativas e de segurança, tendo em vista promover a consciencialização das organizações para a relevância da implementação de políticas de segurança adequadas, clarificando que o número significativo de ataques ocorridos em 2022, radica, na sua maioria, na falta de investimento nesta área – resultando em vulnerabilidades nas infraestruturas e falta de formação dos utilizadores.

Também em 2023, São Tomé e Príncipe lançou o projeto STP Digital, que possui vários objetivos a cumprir a num período máximo de cinco anos. Este projeto o projeto visa melhorar a equidade e sustentabilidade dos serviços de telecomunicações e fortalecer a governança de dados, sistemas de dados e capacidades estatísticas.

Deste modo, o contexto digital em São Tomé e Príncipe reflete um compromisso contínuo com a inovação, a modernização e a inclusão digital, potenciada por uma demografia jovem, propensa à utilização tecnológica, paralelamente a uma acessibilidade crescente a tais recursos. A colaboração internacional, a legislação progressiva e a implementação de tecnologias emergentes são marcos importantes neste percurso. A continuação destes esforços, juntamente com uma gestão eficaz e sustentável, será crucial para alcançar uma sociedade da informação plenamente integrada e segura.

Contudo, a jornada para uma sociedade digital segura não está isenta de obstáculos. Situada no Golfo da Guiné, a localização geográfica de São Tomé e Príncipe e a sua economia em crescimento tornam o país um alvo potencial para ciberataques, especialmente à medida que a digitalização avança a passos largos. Diversas ciberameaças, incluindo ataques de *phishing* e *ransomware*, bem como a exploração de vulnerabilidades em websites, manifestam-se com regularidade e com mais frequência nos últimos anos, pondo em risco a integridade das instituições nacionais e a privacidade dos cidadãos são-tomenses.

Este panorama é agravado pela dependência do país em relação ao alojamento externo de dados e serviços estruturantes, incluindo informações pessoais dos cidadãos e infraestruturas críticas. A crescente necessidade de digitalização dos serviços só vem intensificar este cenário de risco, exacerbado ainda pela falta de infraestrutura adequada e pela insuficiente maturidade digital nos setores público e privado, contribuindo para uma postura de cibersegurança frágil.

Diante deste cenário, é de suma importância abordar prontamente as vulnerabilidades identificadas, desenvolver uma cultura robusta de cibersegurança e investir em tecnologia e formação. Considerando a economia de São Tomé e Príncipe, assente principalmente na exportação de cacau e café e no turismo, a vulnerabilidade a disrupções digitais torna-se um aspeto crítico a ser abordado pela presente Estratégia Nacional. Esta procura, assim, alinhar-se de forma harmoniosa com os objetivos de desenvolvimento económico do país, assegurando a proteção e promoção da inovação e do crescimento sustentável.

1.3 Princípios Orientadores

A Estratégia Nacional de Cibersegurança de São Tomé e Príncipe está ancorada nos seguintes princípios orientadores:

- **Princípio 1 - Legalidade e Respeito pelos Direitos Fundamentais:** A Estratégia adotará as leis nacionais e internacionais vigentes e promoverá a proteção dos direitos fundamentais, liberdades e garantias dos cidadãos são-tomenses no ciberespaço.

- **Princípio 2 - Resiliência e Proatividade**: São Tomé e Príncipe irá desenvolver e manter capacidades para identificar, detetar, responder e recuperar face a ciberameaças, promovendo um ciberespaço seguro e resiliente.

- **Princípio 3 - Cooperação:** A Estratégia fomentará a cooperação e coordenação entre diversos *stakeholders* a níveis nacional e internacional, incluindo o setor privado, organizações civis e entidades governamentais, para a partilha de informação e boas práticas.

- **Princípio 4 - Inclusão e Acesso Universal**: Este princípio assegura que todos os cidadãos de São Tomé e Príncipe terão acesso e poderão utilizar o ciberespaço de forma segura e inclusiva.

- **Princípio 5 - Inovação e Desenvolvimento Sustentável:** São Tomé e Príncipe irá integrar firmemente a cibersegurança nas estruturas básicas da sociedade da informação, promovendo a inovação e o crescimento sustentável da economia digital.

- **Princípio 6 - Educação e Literacia Digital**: A Estratégia deverá promover um ciberespaço seguro, através da implementação de programas educativos que desenvolvam competências nos cidadãos para uma participação segura, responsável e esclarecida no ciberespaço. A ênfase será dada tanto à proteção contra ciberameaças como ao uso eficiente e ético das tecnologias digitais.

2. CAPÍTULO II – VISÃO, MISSÃO E OBJETIVOS

2.1 VISÃO

A atual Estratégia estabelece a seguinte visão para São Tomé e Príncipe:

- São Tomé e Príncipe aspira a ser um país digitalmente seguro e resiliente, onde a integridade, disponibilidade e confiabilidade da informação são fundamentais. Esta visão engloba o impulso para o desenvolvimento sustentável e a inovação, garantindo que a sociedade esteja plenamente consciente e preparada para enfrentar ciberameaças.

2.2 MISSÃO

Quanto à Missão, São Tomé e Príncipe estabelece que:

- A missão de São Tomé e Príncipe consiste em integrar de forma robusta a segurança da informação nas estruturas vitais da sua sociedade da informação. Este compromisso tem como objetivo criar um ciberespaço seguro e fomentar uma cultura de cibersegurança consciente e responsável entre os cidadãos e instituições.

2.3 OBJETIVOS ESTRATÉGICOS E ESPECÍFICOS

Para alcançar a visão e missão da Estratégia Nacional de Cibersegurança de São Tomé e Príncipe, foram definidos **cinco objetivos estratégicos**. Cada um destes objetivos estratégicos é complementado por objetivos específicos, que orientam e especificam as ações necessárias, garantindo um direcionamento focado e eficaz na implementação das medidas de cibersegurança no país.

Objetivo Estratégico 1: Fortalecimento da Coordenação em Cibersegurança

No panorama atual de evolução digital, São Tomé e Príncipe reconhece que a complexidade e a vastidão dos desafios do ciberespaço impõem que uma liderança sólida e transversal seja estabelecida. Este facto é complementado pela necessidade de uma coordenação operacional rápida e eficiente, uma capacidade proativa de resposta e um compromisso contínuo com os recursos, capacidades e competências necessárias.

Este primeiro objetivo estratégico, centrado na consolidação de políticas e no fortalecimento da coordenação em cibersegurança, surge como um marco vital para garantir a integridade digital da nação. Neste contexto, é fundamental para São Tomé e Príncipe estabelecer e fortalecer uma coordenação centralizada em cibersegurança. Atualmente, a falta de uma entidade que centralize e coordene ações nesta área evidencia a necessidade urgente de uma abordagem mais integrada. Assim, a formação do Comité de Cibersegurança representa um passo vital dentro desta Estratégia. Este Comité, além de aconselhar o Governo de São Tomé e Príncipe em decisões relacionadas à cibersegurança, assegurará que a implementação da Estratégia se realize de forma alinhada e eficaz, congregando diferentes especialistas e partes interessadas.

Paralelamente, o desenvolvimento de um Centro Nacional de Resposta a Incidentes de Cibersegurança (CERT) é uma iniciativa também essencial para a resiliência digital de São Tomé e Príncipe. A capacidade de identificar e responder a incidentes no ciberespaço e a implementação de protocolos de gestão de crises revelam-se fundamentais para a proteção da infraestrutura digital nacional.

Outra vertente crucial é a identificação e regulamentação de ativos críticos e operadores em cibersegurança. É essencial que o Governo identifique e proteja as infraestruturas críticas do país uma vez que estas representam os pilares fundamentais para a continuidade das funções essenciais da sociedade, economia e segurança nacional. Qualquer interrupção, falha ou ataque a estas infraestruturas pode resultar em impactos significativos para a população, gerando consequências socioeconómicas, políticas e até humanitárias de grande magnitude.

Por fim, a cibersegurança não pode ser dissociada da Defesa Nacional. Assim, esta Estratégia enfatiza a necessidade de conduzir avaliações meticulosas por parte do Governo de São Tomé e Príncipe para discernir os riscos específicos da cibersegurança que possam afetar a integridade da nossa defesa. Através destas avaliações, será possível formular e implementar estratégias direcionadas, assegurando a robustez e a resiliência da defesa são-tomense perante as ciberameaças.

Com este objetivo estratégico é reforçado o compromisso de São Tomé e Príncipe em evoluir, adaptar-se e fortalecer-se face aos desafios do ciberespaço, consolidando políticas e estabelecendo uma coordenação eficaz em cibersegurança.

Apresentam-se, de seguida, os objetivos específicos para o presente objetivo estratégico.

- **Objetivo Específico 1.1 - Estrutura de Governança e Gestão da Estratégia Nacional de Cibersegurança de São Tomé e Príncipe:** este objetivo específico está relacionado com a criação de um Comité de Cibersegurança para a governança e gestão da Estratégia Nacional de Cibersegurança de São Tomé e Príncipe. O objetivo desta estrutura é estabelecer diretrizes claras e eficazes para a governança e gestão de riscos cibernéticos, assegurando que as práticas de cibersegurança estejam alinhadas com os objetivos estratégicos nacionais. A estrutura incluirá a definição de processos; estruturas organizacionais; funções e responsabilidades; atividades; artefactos de informação; políticas e procedimentos; competências; cultura e comportamentos; e serviços, infraestruturas e aplicações. Esta estrutura é projetada para melhorar a cibersegurança do país, assegurar a conformidade com padrões legais e regulatórios, e fortalecer a resiliência nacional contra ciberameaças.

- **Objetivo Específico 1.2 - Coordenação Integrada e Resposta a Incidentes de Cibersegurança:** o objetivo é estabelecer uma liderança sólida e uma coordenação eficaz em cibersegurança. O Comité de Cibersegurança servirá como ponto centralizado de tomada de decisão e de implementação da Estratégia, bem como de elo de colaboração entre especialistas e partes interessadas. A institucionalização da coordenação é essencial para garantir uma resposta unificada e alinhada contra ciberameaças. A formação contínua dos membros deste Comité é de extrema a importância para manter a liderança atualizada e preparada para os desafios em constante evolução do ciberespaço.

  Além disso, este objetivo inclui também a garantia de uma resposta eficaz a ciberameaças através da implementação do Centro Nacional de Resposta a Incidentes de Cibersegurança de São Tomé e Príncipe (CERT-STP). Este Centro atuará como núcleo de monitorização, deteção e resposta a ameaças em tempo real, proporcionando uma resposta eficaz. Além disso, a implementação de protocolos de gestão de crises garantirá um plano claro e estruturado para lidar com emergências, minimizando danos e restaurando a normalidade rapidamente. O CERT-STP será uma linha de frente na proteção contra ciberameaças, transmitindo confiança ao público e parceiros internacionais sobre a resiliência digital do país. Além disso, o CERT-STP deve também funcionar como um centro de excelência, promovendo a capacitação e a disseminação de melhores práticas em cibersegurança.

- **Objetivo Específico 1.3 - Proteção de Infraestruturas Críticas e Resiliência da Defesa Nacional:** o objetivo é garantir a proteção de ativos, setores e operadores críticos em cibersegurança, identificando-os e regulamentando-os. Isto permitirá que São Tomé e Príncipe concentre esforços nas áreas de maior importância estratégica que, se comprometidas, podem ter um grande impacto no país. A regulamentação assegurará o cumprimento de padrões básicos de cibersegurança e fortalecerá a postura defensiva de São Tomé e Príncipe.

  A resiliência da Defesa Nacional em cibersegurança também é parte deste objetivo, envolvendo a avaliação de impacto e mitigação de riscos para identificar vulnerabilidades e áreas de risco na

Defesa Nacional, permitindo respostas adequadas e estratégias de mitigação. São Tomé e Príncipe procura assim manter uma postura defensiva robusta, adaptável e resiliente.

Objetivo Estratégico 2: Consciencialização e Cultura de Cibersegurança

Com a imersão digital cada vez mais dominante no quotidiano dos são-tomenses e do mundo, o ciberespaço tornou-se central para o desenvolvimento social, económico e político das nações. No entanto, a exposição a potenciais ciberameaças cresce em paralelo com o avanço tecnológico, tornando imperativo para São Tomé e Príncipe garantir que todos os seus cidadãos e instituições estejam munidos das ferramentas e do conhecimento necessários para enfrentar tais desafios.

Face à contínua evolução e à natureza difusa das ciberameaças, é primordial que a sociedade de São Tomé e Príncipe não só entenda os riscos, mas também antecipe e esteja preparada para eles. Esta antecipação passa pela partilha proativa de informação, permitindo uma avaliação precoce e eficaz das ameaças emergentes. Com a capacidade de detetar e conhecer métricas de sucesso associados a potenciais ameaças e em curso, é possível desenvolver medidas que atenuem os riscos antes que as ameaças se manifestem.

Neste sentido, pretende-se que a sociedade de São Tomé e Príncipe desenvolva uma compreensão clara das ameaças que o ciberespaço encerra. Este entendimento não é apenas crucial, mas é a pedra basilar para estabelecer uma cultura sólida e informada de cibersegurança em São Tomé e Príncipe.

Reforçar a consciencialização e a educação em cibersegurança emerge assim como central nesta Estratégia. A promoção de uma cultura de cibersegurança, norteada por princípios éticos, deve ser uma prioridade para que todos possam navegar no ciberespaço com confiança, consciência e segurança. Trata-se de mais do que simplesmente proteger sistemas e redes: é fundamental cultivar uma mentalidade de cibersegurança que permeie todas as camadas da sociedade, desde entidades públicas até empresas e a sociedade civil. Por outro lado, a formação e capacitação, de recursos humanos qualificados será também determinante para enfrentar os complexos desafios do ciberespaço.

Para tal, São Tomé e Príncipe tem como um dos objetivos principais capacitar os seus cidadãos, proporcionando-lhes as competências necessárias para navegar com confiança e segurança no ciberespaço. Este objetivo será alcançado através de uma série de iniciativas específicas, centradas na educação e consciencialização da população em geral, que serão detalhadas no plano de ação.

Para o objetivo estratégico em questão, os objetivos específicos são apresentados de seguida.

- **Objetivo Específico 2.1 - Promoção da Consciencialização e Literacia Digital:** o objetivo é promover a literacia digital e mediática da população de São Tomé e Príncipe através do desenvolvimento de programas de sensibilização específicos. Isso capacitará os cidadãos com competências críticas que lhes permitirão avaliar e discernir o conteúdo online, preparando a sociedade para enfrentar os desafios da era digital, tornando-a mais resiliente contra ataques de engenharia social e ciberameaças.

- **Objetivo Específico 2.2 - Confiança e Segurança em Serviços Online:** reconhecendo a importância da confiança nos serviços online, São Tomé e Príncipe pretende promover a confiança e segurança dos seus cidadãos na Internet. Isso será alcançado através da condução de pesquisas para avaliar a perceção e o sentimento de segurança online, garantindo que os serviços online sejam tecnicamente seguros e transparentes. Além disso, o país implementará canais de denúncia eficientes e acessíveis. Estes canais, além de receberem relatos de atividades suspeitas, serão coordenados entre várias agências, assegurando uma resposta rápida e eficaz a qualquer incidente. Este objetivo sublinha assim o compromisso de São Tomé e Príncipe em envolver seus cidadãos na coletiva e contínua defesa do seu ciberespaço.

Objetivo Estratégico 3: Desenvolvimento e Fortalecimento das Capacidades Nacionais de Cibersegurança

São Tomé e Príncipe, reconhecendo a importância vital das infraestruturas críticas de informação, entende que, numa era de digitalização global, possuir uma infraestrutura de cibersegurança robusta é tão essencial quanto ter fundações físicas sólidas para qualquer construção. Os ataques às infraestruturas críticas podem causar uma disrupção significativa à economia nacional e à integridade da vida e saúde das pessoas. Os danos podem ser amplos, estendendo-se desde o enfraquecimento da segurança territorial até danos à reputação dos indivíduos e instituições são-tomenses.

Nesse sentido, São Tomé e Príncipe pretende evoluir para uma realidade mais robusta e capacitada, com um foco especial na proteção das suas infraestruturas críticas. Inicialmente, é fundamental que se promova uma ampla consciencialização em cibersegurança, envolvendo todos os utilizadores de TICs, sejam eles do setor público, privado ou da sociedade civil. Este movimento requer um plano coordenado onde recursos educativos online, como cursos e seminários, sejam disponibilizados e onde se estabeleçam métricas iniciais para avaliar o impacto destas ações.

Em paralelo, o investimento na formação especializada e na educação nacional em cibersegurança será intensificado. A visão é que, para além da formação inicial, São Tomé e Príncipe incorpore cursos relacionados com cibersegurança em escolas e universidades, fortalecendo assim a sua base educacional.

Adicionalmente, o desenvolvimento do capital humano em cibersegurança é crucial. Através da documentação das necessidades nacionais de profissionais qualificados, São Tomé e Príncipe pretende criar programas de formação específicos, com ênfase na proteção das infraestruturas críticas.

Por fim, São Tomé e Príncipe pretende fortalecer a sua posição no campo da cibersegurança, estabelecendo parcerias de investigação e desenvolvimento tanto a nível nacional como internacional. O objetivo passa essencialmente por se integrar ativamente nas redes de investigação e assegurar uma presença destacada na vanguarda da cibersegurança.

A proteção das infraestruturas críticas e outras infraestruturas de informação de São Tomé e Príncipe é uma responsabilidade partilhada que exige a colaboração de todos os envolvidos. Isto implica uma abordagem integrada, onde entidades públicas, empresas privadas e a sociedade civil trabalham em conjunto para identificar vulnerabilidades, reforçar defesas e garantir a resiliência contra potenciais ciberameaças. Só através de um compromisso coletivo e de uma estratégia bem coordenada é que se pode garantir a segurança e integridade dos ativos digitais vitais do país.

Os objetivos específicos para este objetivo estratégico são detalhados de seguida.

- **Objetivo Específico 3.1 - Formação e Educação em Cibersegurança:** o Governo de São Tomé e Príncipe está empenhado em construir uma cultura de cibersegurança. Para isso, a presente Estratégia prevê o desenvolvimento de um plano coordenado que integra múltiplas partes interessadas, incluindo o Governo, o setor privado e a sociedade civil. Este plano envolverá a criação e disponibilização de recursos educativos online, como cursos e seminários, bem como a integração de cursos relacionados com cibersegurança nos currículos das escolas e universidades nacionais. São Tome e Príncipe também pretende implementar um sistema de métricas para avaliar a eficácia e impacto destas iniciativas, assegurando assim que os esforços realizados correspondam às necessidades reais da população.

- **Objetivo Específico 3.2 - Capacitação Profissional e Inovação em Cibersegurança:** São Tomé e Príncipe está consciente da importância em desenvolver profissionais especializados em cibersegurança e, por isso, pretende avaliar e documentar as necessidades nacionais nesta área. São Tomé e Príncipe tem a pretensão de criar programas de especialização em cibersegurança para elementos de equipas de TI. Além disso, São Tomé e Príncipe tem ainda o objetivo de facilitar o acesso a certificações internacionais reconhecidas, reforçando assim o compromisso do país com

padrões globais de excelência. Para se posicionar na vanguarda da cibersegurança, São Tomé e Príncipe promoverá também a investigação e o desenvolvimento no campo da cibersegurança, tanto a nível nacional quanto através de parcerias internacionais.

Objetivo Estratégico 4: Consolidação do Estrutura Legal e Regulatória em Cibersegurança

São Tomé e Príncipe, tendo em consideração as exigências atuais no ciberespaço, reconhece a imperativa necessidade de robustecer o seu quadro legal e regulatório em cibersegurança. São Tomé e Príncipe já deu passos significativos nesse sentido, como evidenciado pela implementação da Lei nº 15/2017 sobre Cibercrime e da Lei nº 3/2016 de Proteção de Dados Pessoais. Contudo, embora se destaque em algumas áreas, persistem lacunas, como a ausência de uma legislação específica voltada para a proteção de crianças online e a necessidade de modernizar leis de propriedade intelectual à luz do ciberespaço.

O avanço para um cenário mais consolidado, alinhado com padrões internacionais, é mais do que uma meta estabelecida por São Tomé e Príncipe com a presente Estratégia: a implementação de leis e regulamentos não pode ser apenas uma reação a delitos virtuais, mas uma estratégia proativa de prevenção, deteção e repressão das atividades de criminalidade no ciberespaço.

Neste sentido, no domínio legislativo, São Tomé e Príncipe prioriza a adaptação da legislação existente no âmbito da proteção online de crianças, dos consumidores e da propriedade intelectual ao ciberespaço.

Reconhecendo os desafios em capacidade e competência legal e regulatória, São Tomé e Príncipe está ciente de que as forças de segurança, procuradores e tribunais necessitam de recursos e formação especializada para enfrentar o cibercrime. Surge assim a urgência de institucionalizar a capacitação de agentes judiciais em cibercrime e evidências digitais, integrando a formação de modo sistemático na estrutura judicial.

Para concluir, São Tomé e Príncipe contempla na cooperação intersectorial e na partilha de informação em cibersegurança os alicerces para uma abordagem eficaz e coesa. É assim para São Tomé e Príncipe primordial estabelecer mecanismos de colaboração e comunicação contínuos entre os setores público e privado, apoiados por uma legislação apropriada, com o intuito de criar um ciberespaço seguro e protegido para todos os cidadãos são-tomenses.

De seguida, encontraram-se os objetivos específicos associados ao presente objetivo estratégico.

- **Objetivo Específico 4.1 - Adoção e Adaptação de Boas Práticas Legais e Regulatórias:** São Tomé e Príncipe, ao reconhecer a necessidade de um ciberespaço seguro, pretende estabelecer um conjunto claro de padrões e normas legais que delineiam as responsabilidades dos vários atores no ciberespaço. Além de estabelecer padrões obrigatórios, pretende também criar um mecanismo transparente para notificar violações de normas e divulgar vulnerabilidades. Para garantir a eficácia destas medidas, terá de existir clareza nas consequências civis e criminais para aqueles que não cumprirem com estas normas.

  Paralelamente, São Tomé e Príncipe pretende adaptar, rever e expandir a legislação existente relacionada com a cibersegurança e o ciberespaço.

- **Objetivo Específico 4.2 - Capacitação e Cooperação no Contexto do Cibercrime e Cibersegurança:** para que a estrutura legal seja implementada com eficácia, é vital que os que estão na linha de frente da justiça - desde investigadores da polícia até juízes - estejam equipados com o conhecimento necessário para lidar com as questões do cibercrime. Portanto, São Tomé e Príncipe pretende não apenas oferecer formação, mas garantir que esta seja regular e institucionalizada, garantindo que o sistema judicial de São Tomé e Príncipe esteja preparado para lidar com as complexidades do

ciberespaço. Além disso, o país pretende estabelecer canais robustos de cooperação intersectorial e internacional, promulgando legislação de apoio e criando mecanismos eficazes de colaboração.

Objetivo Estratégico 5: Adoção e Implementação de Boas Práticas de Cibersegurança

No cenário atual, onde a digitalização se entrelaça com todos os segmentos da sociedade, a efetiva implementação de normas e tecnologias de cibersegurança em São Tomé e Príncipe é crucial. Tais medidas não só reforçam a defesa da infraestrutura digital do país contra ameaças, mas também instauram confiança entre cidadãos, empresas e parceiros internacionais. Essa confiança é fundamental para impulsionar a prosperidade digital de São Tomé e Príncipe, atraindo investimentos e solidificando a sua presença no panorama digital mundial, garantindo ao mesmo tempo a integridade das informações essenciais para o desenvolvimento nacional.

A necessidade de São Tomé e Príncipe adotar padrões internacionais em cibersegurança é incontornável, neste sentido, a presente Estratégia pretende promover a aplicação destes tanto no setor público quanto no privado. Neste sentido, São Tomé e Príncipe procurará com algumas iniciativas fomentar processos de aquisição e discussões sobre *software* seguro e garantir a qualidade do *hardware* utilizado em São Tomé e Príncipe.

Em paralelo, São Tomé e Príncipe considera a proteção de dados através da implementação de controlos de segurança e criptografia como uma prioridade: aqui a Estratégia irá delinear uma séria de iniciativas para incentivar todos os setores a utilizar os mais seguros protocolos de segurança e utilizar métodos criptográficos adequados.

Com foco no desenvolvimento seguro, São Tomé e Príncipe planeia também compilar um catálogo de plataformas e aplicações seguras a serem utilizadas no país, bem como, implementar políticas para a atualização e manutenção de *software*.

Uma vez que São Tomé e Príncipe reconhece a relevância das infraestruturas críticas, a presente Estratégia prevê também a realização de avaliações de risco para os provedores de serviços de internet e o desenvolvimento de planos de resposta a incidentes em setores críticos também.

Ainda no contexto deste objetivo estratégico, São Tomé e Príncipe reconhece a importância vital de dinamizar mercados ligados à cibersegurança para o progresso nacional. Assim, com a presente Estratégia, o país visa impulsionar diversas iniciativas. Entre elas, destaca-se o incentivo ao surgimento de serviços especializados em consultoria de cibersegurança e a realização de avaliações de risco associadas à terceirização de serviços de TI.

De seguida, são listados os objetivos específicos relacionados com este objetivo estratégico.

- **Objetivo Específico 5.1 - Promoção de Boas Práticas e Dinamização do Ecossistema de Cibersegurança:** São Tomé e Príncipe está empenhado em promover boas práticas de cibersegurança e dinamizar o seu ecossistema de cibersegurança. Isso envolve a adoção de padrões internacionais de cibersegurança nos setores público e privado, bem como a implementação rigorosa de critérios de cibersegurança nos processos de aquisição de *software* e *hardware*. Além disso, São Tomé e Príncipe reforçará a resposta aos riscos de cibersegurança, incluindo o uso da criptografia para proteger dados em trânsito e em repouso, garantindo a privacidade e integridade das informações. São Tomé e Príncipe também incentivará o crescimento da indústria de cibersegurança, promovendo serviços de consultoria especializados e avaliações de risco para terceirização de serviços de TI.

- **Objetivo Específico 5.2 - Promoção do Desenvolvimento Seguro de *Software*:** São Tomé e Príncipe reconhece que a importância do uso de *softwares* seguros e, por isso, projeta a criação de um catálogo de plataformas e aplicações seguras, bem como a criação de políticas para a manutenção e

atualização regular de *software*, garantindo assim que as vulnerabilidades sejam prontamente tratadas.

- **Objetivo Específico 5.3 - Resiliência das Infraestruturas Críticas:** dada a importância vital das infraestruturas de comunicação, São Tomé e Príncipe procurará realizar avaliações de risco abrangentes para identificar potenciais vulnerabilidades. Com base nessas avaliações, planos de resposta a incidentes serão desenvolvidos, garantindo que o país possa responder prontamente e eficazmente a quaisquer ameaças.

3. CAPÍTULO III - IMPLEMENTAÇÃO DA ESTRATÉGIA

3.1 O Comité Nacional de Cibersegurança de São Tomé e Príncipe

3.1.1 Enquadramento

O Comité Nacional de Cibersegurança de São Tomé e Príncipe, atua como órgão que auxiliará as tomadas de decisões do Governo nas questões de cibersegurança, bem como pela implementação e coordenação da Estratégia Nacional de Cibersegurança e Plano de Ação. Esta estrutura é composta por:

- O Diretor de Estudos no Ministério das Infraestruturas, Recursos Naturais e Meio Ambiente;
- O Presidente da AGER;
- O Presidente do INIC;
- O Presidente da ANPDP;
- O Presidente da DGRN;
- O Presidente da DITEI;
- O Presidente do INE;
- O Diretor do Banco Central de São Tomé e Príncipe;
- O Coordenador do projeto STP Digital.

Para lidar com questões técnicas específicas, cada entidade que integra o Comité de Cibersegurança deve eleger dois técnicos especializados. Estes técnicos terão a função de fornecer pareceres detalhados e especializados nas matérias técnicas, garantindo que as decisões e estratégias adotadas sejam fundamentadas em conhecimento técnico aprofundado e atualizado.

A composição e escolha do Presidente do Comité de Cibersegurança são definidas por Resolução do Conselho de Ministros. Deverá ser considerada a possibilidade de rotatividade no exercício da função de Presidente.

Além disso, o Presidente do Comité de Cibersegurança tem a autonomia para, por iniciativa própria ou a pedido de outros membros, convocar titulares de órgãos públicos, representantes de entidades privadas ou outras personalidades de relevo para participar nas reuniões do Comité de Cibersegurança. Esta medida assegura uma visão mais ampla e inclusiva, abrangendo diferentes perspetivas e experiências no campo da cibersegurança.

3.1.2 Objetivos e Responsabilidades

O Papel do Comité Nacional de Cibersegurança de São Tomé e Príncipe será:

- Avaliar e aconselhar o Estado em temas ou questões relevantes que fortaleçam a cibersegurança;
- Desenvolver abordagens para estabelecer estruturas e diretrizes nacionais e regionais eficazes contra o cibercrime;
- Garantir o desenvolvimento de competências institucionais para proteger São Tomé e Príncipe de cibercrimes;
- Estimular a colaboração e alinhamento intergovernamental em questões de cibersegurança;
- Incentivar e fortalecer alianças entre setores público e privado em temas de cibersegurança no território nacional;

- Examinar o panorama atual da cibersegurança no país, identificar áreas de foco prioritário e garantir abordagens adequadas para cada situação;
- Identificar as Infraestruturas Críticas de Informação (ICI) e estabelecer medidas para assegurar sua defesa contra delitos e ciberameaças;
- Detetar lacunas na execução de projetos e mecanismos de cibersegurança;
- Zelar pela concretização das metas e ações previstas na estratégia;
- Instituir um protocolo de coordenação entre os vários setores envolvidos, assegurando uma implementação coesa e resultados consistentes;
- Propor e identificar mecanismos alternativos de financiamento para as atividades ligadas à concretização da estratégia;
- Acompanhar de perto o cumprimento dos prazos estabelecidos para cada ação, garantindo que todos os marcos sejam atingidos dentro do tempo previsto.

3.2 Financiamento e Alocação de Recursos

A concretização efetiva da Estratégia Nacional de Cibersegurança de São Tomé e Príncipe depende fortemente da garantia de recursos e financiamento adequados. Com base nisso, as diretrizes estabelecidas no Plano de Ação indicam as possíveis fontes de financiamento e as entidades responsáveis pelas variadas iniciativas propostas no referido plano.

3.3 Monitorização e Avaliação da Estratégia

A Estratégia Nacional de Cibersegurança de São Tomé e Príncipe, sob a supervisão do Comité de Cibersegurança, será submetida a uma avaliação anual. Esta avaliação terá como foco a verificação dos objetivos estratégicos e do plano de ação, ajustando-os conforme a evolução das circunstâncias e tendo em conta a rápida transformação do ciberespaço.

Para garantir a eficácia desta estratégia, é fundamental estabelecer metas de desempenho anuais, que serão monitorizadas e avaliadas regularmente. Estas metas serão definidas para diversas instituições governamentais e partes interessadas, responsáveis pela implementação de ações específicas. Toda esta informação irá constar no plano de ação.

4. CAPÍTULO IV – PLANO DE AÇÃO

4.1 A IMPORTÂNCIA DO PLANO DE AÇÃO

Tendo em consideração os objetivos estratégicos definidos para São Tomé e Príncipe, reconhece-se a necessidade imperativa de um instrumento orientador e organizador para garantir a realização eficiente desses objetivos. Nesse contexto, foi criado um Plano de Ação, desenhado para estruturar e impulsionar as iniciativas necessárias ao desenvolvimento do país, em especial no setor de TIC.

O Plano de Ação serve assim como uma bússola, fornecendo estruturação e organização, delineando metas específicas, ações, responsáveis pela execução e os prazos essenciais para a concretização. É um instrumento vital para garantir a coordenação e alinhamento entre diferentes entidades e setores envolvidos, assegurando a coesão e a integração de esforços rumo a objetivos comuns.

Por outro lado, o Plano de Ação é fundamental para a monitorização e avaliação do progresso, estabelecendo métricas de sucesso de desempenho claros que permitirão a avaliação regular dos resultados e o ajuste das estratégias conforme necessário. Através deste plano, será possível gerir eficientemente a alocação de recursos, identificando necessidades e otimizando o uso dos mesmos para alcançar os resultados desejados.

Consequentemente, o Plano de Ação fomenta a comunicação e a transparência, constituindo-se como um referencial indispensável para todos os intervenientes, sendo crucial para materializar os objetivos estratégicos de São Tomé e Príncipe em realidades tangíveis e sustentáveis.

O Plano de Ação de São Tomé e Príncipe é organizado em programas de transformação, sendo cada programa constituído por várias iniciativas. Cada uma dessas iniciativas, por sua vez, detalha os objetivos gerais e específicos para os quais está a contribuir, garantindo assim uma estruturação clara e eficaz das ações e metas a serem atingidas.

4.2 Visão Geral do Plano de Ação

Programa I:								
Objetivo do programa:								
Código da Iniciativa	**Iniciativa**	**Objetivo da Iniciativa**	**Objetivo Estratégico**	**Objetivo Específico**	**Entidade Responsável**	**Partes Interessadas envolvidas**	**Horizonte Temporal[1]**	**Métrica de Sucesso**

[1] Curto Prazo - Iniciativas que têm um impacto imediato e que podem ser implementadas rapidamente (3 a 6 meses);
Médio Prazo - Iniciativas que requerem um planeamento e execução mais detalhados e que têm um impacto moderado a significativo (6 meses a 2 anos);
Longo Prazo - Iniciativas estratégicas que requerem um compromisso de longo prazo e que têm um impacto significativo na estrutura de cibersegurança nacional (Mais de 2 anos).

4.3 Monitorização do Plano de Ação

Objetivo Estratégico 1:																	
Objetivo Específico	**Código da Iniciativa**	**Métrica de Sucesso**	**Metas**														
			2023	**Resultados 2023**	**Desvio 2023**	**2024**	**Resultados 2024**	**Desvio 2024**	**2025**	**Resultados 2025**	**Desvio 2025**	**2026**	**Resultados 2026**	**Desvio 2026**	**2027**	**Resultados 2027**	**Desvio 2027**