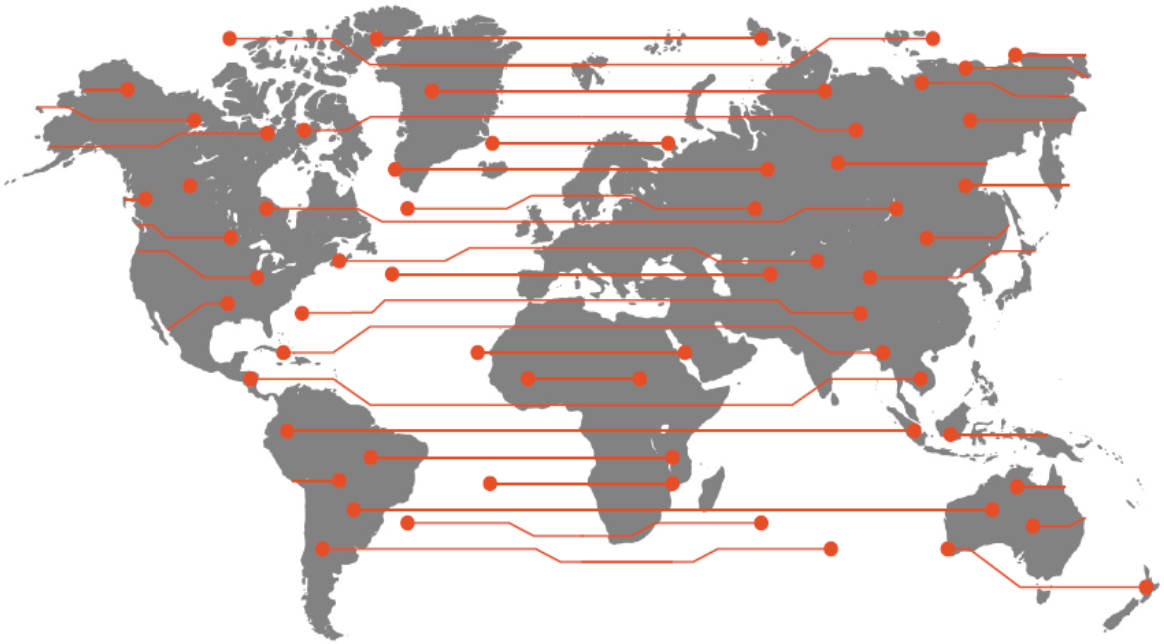
NRD Cyber Security

WORLD BANK GROUP

Projeto

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



D-04

Plano de ação

Versão 1.3

Informações sobre o documento

Título do projeto:	Desenvolvimento da Estratégia Nacional de Cibersegurança e do Plano de Ação para São Tomé e Príncipe		
Título do relatório:	D-4 - Plano de Ação de São Tomé e Príncipe		
Versão:	1.3	**Data da versão:**	25-01-2024
Preparado por:	Equipa da NRD Cyber Security		
Avaliado por:			
Aprovado por:			

Fluxo de informação

Quem	Data	Contacto
NRD Cyber Security		

Cronologia das versões

Versão nº.	Data	Comentários
1.0	15-12-2023	Versão rascunho 1.0
1.1	04-01-2024	Versão rascunho 1.1
1.2	15-01-2024	Versão rascunho 1.2
1.3	25-01-2024	Versão final

Conteúdo

I. Enquadramento

No âmbito da Estratégia Nacional de Cibersegurança de São Tomé e Príncipe, definiram-se diretrizes essenciais que visam fortalecer a infraestrutura digital e a cibersegurança do país, sendo a visão para a cibersegurança em São Tomé e Príncipe concretizada em "Objetivos Gerais" e "Objetivos Específicos". Os Objetivos Gerais delineiam a visão macro do país para o desenvolvimento da cibersegurança, estabelecendo metas amplas e integradoras. Por sua vez, os Objetivos Específicos traduzem-se em metas mais concretas e detalhadas, permitindo um foco em áreas críticas que compõem o panorama da cibersegurança.

Para que estes objetivos sejam atingidos de forma eficaz, é imperativo definir Programas de Melhoria. Estes programas são desenhados para assegurar a implementação bem-sucedida da estratégia, garantindo uma perspetiva clara dos benefícios a serem alcançados. Cada programa enquadra um conjunto de benefícios esperados, recursos necessários e horizonte temporal, permitindo traduzir os objetivos da Estratégia para o plano de ação. Esta abordagem programática é essencial para garantir que cada passo da estratégia seja realizado de maneira coordenada e eficiente.

No contexto da Estratégia Nacional de Cibersegurança de São Tomé e Príncipe foram identificados 8 Programas principais, para os quais foram identificadas 35 iniciativas concretas que irão materializar os objetivos delineados. Estas iniciativas representam ações específicas, projetos e medidas que serão adotadas para promover a cibersegurança no país.

Assim, a relação entre os Objetivos da Estratégia, os Programas e as Iniciativas é intrínseca e sinérgica. Os objetivos fornecem o quadro e a direção, os programas oferecem a estrutura e os meios, e as iniciativas constituem os passos concretos para a realização da visão estratégica.

Este Plano de Ação reflete um compromisso de São Tomé e Príncipe com a cibersegurança, abordando não apenas as necessidades atuais, mas também antecipando desafios futuros. A sua implementação contribuirá significativamente para um ciberespaço mais seguro e resiliente no país, alinhando-se com as melhores práticas internacionais no domínio da cibersegurança.

II. Visão geral do programa

A Estratégia Nacional de Cibersegurança de São Tomé e Príncipe baseia-se numa série de programas estruturados e interligados, cada um abordando um aspeto vital da cibersegurança. Estes programas são a espinha dorsal da estratégia, delineando o caminho a seguir para garantir um ciberespaço seguro, resiliente e inovador no país.

1. **Programa de Governação e Coordenação da Cibersegurança**: Este programa é a pedra angular da estratégia, estabelecendo o quadro de governação necessário para coordenar as várias iniciativas de cibersegurança. O seu objetivo é assegurar uma liderança eficaz, a coordenação interagências e a colaboração entre as diferentes partes interessadas.
2. **Programa de Gestão de Ativos e Operadores Críticos**: Focado na identificação e proteção de ativos digitais críticos e operadores essenciais, este programa visa garantir a continuidade e segurança das infraestruturas vitais do país.
3. **Programa de Educação e Sensibilização para a Cibersegurança**: Este programa tem como objetivo promover a sensibilização e educação para a cibersegurança junto da população e das organizações. A ideia é criar uma cultura de segurança digital, fundamental para a prevenção de incidentes.
4. **Programa de Resposta a Incidentes e Gestão de Riscos**: Desenvolve competências para uma resposta rápida e eficiente a incidentes de cibersegurança, bem como a implementação de práticas de gestão de risco, minimizando potenciais ameaças.
5. **Programa de Formação Profissional e Desenvolvimento Técnico**: Este programa aposta no desenvolvimento de competências e na formação profissional na área da cibersegurança, procurando garantir que o país dispõe dos especialistas necessários para enfrentar os desafios digitais.
6. **Programa de Desenvolvimento Jurídico e Regulamentar**: Visa estabelecer um quadro jurídico e regulamentar sólido e atualizado que apoie as iniciativas de cibersegurança e responda a um ciberespaço em constante evolução.
7. **Programa de Reforço da Infraestrutura Tecnológica, Inovação, Certificação e Normatização:** Procura investir e modernizar a infraestrutura tecnológica, promovendo a inovação e a adoção de novas tecnologias para reforçar a segurança digital e também enfatizar a importância da implementação de padrões e normas de segurança e a certificação de processos e produtos para garantir a confiabilidade e a segurança das soluções tecnológicas.
8. **Programa de Colaboração Internacional e Desenvolvimento da Indústria:** Este programa enfatiza a importância das parcerias internacionais e o desenvolvimento da indústria local de cibersegurança, expandindo as capacidades do país e integrando-o na rede global de cibersegurança.

Cada programa, com as suas especificidades e focos, contribui para uma visão integrada e holística da cibersegurança, abordando não só os desafios atuais, mas também antecipando as necessidades futuras do país na área da segurança digital.

O quadro seguinte apresenta os Programas e identifica as iniciativas que serão implementadas para os concretizar:

Programa	Descrição	Benefícios esperados	Iniciativas	Estimativa de investimento (Valor médio)
P1. Programa de Governação e Coordenação da Cibersegurança	Este programa centra-se na criação de estruturas de liderança e na colaboração entre diferentes setores, que são essenciais para estabelecer uma estratégia unificada de cibersegurança.	• Criar um comité interministerial para liderar a estratégia nacional de cibersegurança. • Promover a colaboração entre várias entidades governamentais e o sector industrial. • Facilitar a comunicação e a ação concertada entre as diferentes partes interessadas.	**P1.1:** Criação do Comité de Liderança e Coordenação da Cibersegurança **P1.2:** Promover a colaboração interdepartamental e intersectorial	**$68,500.00**
P2. Programa de Gestão de Ativos e Operadores Críticos	Este programa é dedicado à identificação e à proteção de ativos e operadores essenciais para a infraestrutura de cibersegurança do país.	• Identificar e catalogar ativos e operadores críticos. • Criar um conjunto de regulamentos para garantir a segurança dos ativos e operadores críticos. • Assegurar protocolos de coordenação eficazes entre a CSIRT e os responsáveis pelas infraestruturas críticas.	**P2.1:** Elaboração de regulamentação em matéria de cibersegurança para os ativos e operadores críticos **P2.2:** Identificação de ativos e operadores críticos **P2.3:** Implementação de protocolos entre o CSIRT e as infraestruturas críticas	**$192,500.00**
P3. Programa de educação e sensibilização para a cibersegurança	O seu objetivo é aumentar a literacia digital em todos os níveis de ensino e sensibilizar o público e as empresas para as melhores práticas de cibersegurança.	• Desenvolver programas curriculares que integrem a literacia digital desde o ensino básico. • Educar o público e as empresas através de workshops e seminários. • Realizar campanhas de sensibilização para a importância da cibersegurança.	**P3.1:** Criação de programas de ensino para promover a literacia digital e a cibersegurança nas escolas **P3.2:** Organizar regularmente seminários e workshops sobre as melhores práticas em matéria de cibersegurança **P3.3:** Parceria para eventos de sensibilização para a literacia mediática **P3.4:** Realizar estudos anuais sobre o nível de confiança dos cidadãos nos serviços online **P3.5:** Criação de uma plataforma de verificação de factos online para combater a desinformação **P3.6:** Campanhas de sensibilização sobre a proteção dos dados pessoais **P3.7:** Avaliação e documentação das necessidades nacionais de competências em matéria de cibersegurança	**$217,500.00**

Programa	Descrição	Benefícios esperados	Iniciativas	Estimativa de investimento (Valor médio)
			P3.8: Guia de boas práticas de cibersegurança para entidades públicas e privadas	
P4. Programa de resposta a incidentes e gestão de riscos	Centra-se na identificação de riscos e no estabelecimento de capacidades de resposta a incidentes para proteger os ativos digitais.	• Criar e reforçar um centro de resposta a incidentes de cibersegurança. • Desenvolver e aplicar uma análise de risco em domínios críticos como a defesa nacional.	**P4.1:** Criação e reforço do CSIRT-STP **P4.2:** Análise exaustiva dos ciber-riscos na defesa nacional **P4.3:** Protocolo de avaliação de riscos para infraestruturas de telecomunicações	**$502,500.00**
P5. Programa de Formação Profissional e Desenvolvimento Técnico	Centra-se no aumento das competências técnicas e profissionais em matéria de cibersegurança, desde a defesa ativa até à formação jurídica para lidar com a cibercriminalidade.	• Melhorar as competências das equipas de TI das instituições públicas e privadas. • Estabelecer parcerias para facilitar o acesso a certificações reconhecidas. • Desenvolver um programa de formação integrado para os agentes judiciais.	**P5.1:** Reforço da capacidade defensiva com formação e equipamento **P5.2:** Programas de formação especializada para equipas de TI **P5.3:** Estabelecer parcerias com instituições internacionais para o intercâmbio de conhecimentos e melhores práticas no domínio da educação em matéria de cibersegurança e da luta contra o cibercrime **P5.4:** Organização de eventos anuais sobre cibersegurança para reunir investigadores, profissionais e partes interessadas para debater e trocar ideias **P5.5:** Formação de agentes judiciais em matéria de cibercrime **P5.6:** Criação de bolsas de estudo ou incentivos para que os estudantes se especializem em cibersegurança	**$422,500.00**
P6. Programa de Desenvolvimento Legal e Regulamentar	Este programa visa atualizar e reforçar o quadro jurídico e regulamentar de proteção contra as ameaças digitais, especialmente para grupos vulneráveis como as crianças e os adolescentes.	• Rever e atualizar a legislação. • Criar a lei sobre o quadro jurídico para a segurança no ciberespaço / cibersegurança.	**P6.1:** Revisão e atualização da legislação existente em matéria de cibersegurança **P6.2:** Criação da Lei do regime Jurídico da Segurança do Ciberespaço / da Cibersegurança **P6.3:** Fortalecimento da legislação relativa à propriedade intelectual para proteger contra violações online	**$85,000.00**

Programa	Descrição	Benefícios esperados	Iniciativas	Estimativa de investimento (Valor médio)
P7. Programa de Fortalecimento da Infraestrutura Tecnológica, Inovação, Certificação e Normalização	O objetivo é reforçar a segurança das infraestruturas tecnológicas e promover a inovação através da investigação e do desenvolvimento, bem como normalizar e elevar o nível de segurança do software e das aplicações através de programas de certificação.	• Implementar um sistema de certificação para plataformas e aplicações. • Lançar uma campanha de sensibilização para a importância de um software seguro e de atualizações regulares. • Assegurar que as infraestruturas tecnológicas cumprem as orientações em matéria de segurança e de cifragem. • Criar um centro nacional de inovação e investigação no domínio da cibersegurança.	**P7.1:** Programa de certificação nacional para plataformas e aplicações **P7.2:** Campanha de sensibilização para software seguro **P7.3:** Centro nacional de investigação e inovação em cibersegurança **P7.4:** Desenvolvimento de selos de segurança ou certificações para serviços online que cumpram normas de segurança rigorosas **P7.5:** Competências em criptografia e controlos de segurança **P7.6:** Auditorias periódicas das infraestruturas tecnológicas	**$312,500.00**
P8. Programa de Colaboração Internacional e Desenvolvimento da Indústria	O objetivo é aumentar a colaboração internacional e promover o desenvolvimento do sector local da cibersegurança.	• Participar ativamente em fóruns e conferências internacionais. • Estabelecer acordos de cooperação para o intercâmbio de informações e de boas práticas. • Promover eventos que atraiam investimentos e incentivem a colaboração intersectorial.	**P9.1:** Colaborações internacionais em redes de investigação e desenvolvimento **P9.2:** Participação internacional de São Tomé e Príncipe no domínio da cibersegurança **P8.3:** Exercícios de simulação com parceiros internacionais **P8.4:** Feiras e eventos nacionais na indústria de cibersegurança	**$167,500.00**

Finalmente, importa referir que estes programas irão garantir que os objetivos gerais e específicos da Estratégia Nacional de Cibersegurança de São Tomé e Príncipe são alcançados. O quadro seguinte apresenta a forma como os programas irão contribuir para os objetivos da estratégia:

	Objetivos Estratégicos da Estratégia Nacional de Cibersegurança de São Tomé e Príncipe				
Programa	**1. Fortalecimento da Coordenação em Cibersegurança** 1.1 - Estrutura de Governança e Gestão da Estratégia Nacional de Cibersegurança de São Tomé e Príncipe 1.2 - Coordenação Integrada e Resposta a Incidentes de Cibersegurança 1.3 - Proteção de Infraestruturas Críticas e Resiliência da Defesa Nacional	**2: Consciencialização e Cultura de Cibersegurança** 2.1 - Promoção da Consciencialização e Literacia Digital 2.2 - Confiança e Segurança em Serviços Online	**3. Desenvolvimento e Fortalecimento das Capacidades Nacionais de Cibersegurança** 3.1 - Formação e Educação em Cibersegurança 3.2 - Capacitação Profissional e Inovação em Cibersegurança	**4: Consolidação do Estrutura Legal e Regulatória em Cibersegurança** 4.1 - Adoção e Adaptação de Boas Práticas Legais e Regulatórias 4.2 - Capacitação e Cooperação no Contexto do Cibercrime e Cibersegurança	**5: Adoção e Implementação de Boas Práticas de Cibersegurança** 5.1 - Promoção de Boas Práticas e Dinamização do Ecossistema de Cibersegurança 5.2 - Promoção do Desenvolvimento Seguro de Software 5.3 - Resiliência das Infraestruturas Críticas
P1. Programa de Governação e Coordenação da Cibersegurança	1.1; 1.2				
P2. Programa de Gestão de Ativos e Operadores Críticos	1.2				5.3
P3. Programa de educação e sensibilização para a cibersegurança		2.1;2.2	3.1;3.2	4.1	5.1
P4. Programa de resposta a incidentes e gestão de riscos	1.2;1.3				5.3
P5. Programa de Formação Profissional e Desenvolvimento Técnico	1.3		3.1; 3.2	4.2	
P6. Programa de Desenvolvimento Legal e Regulamentar				4.1	
P7. Programa de Fortalecimento da Infraestrutura Tecnológica, Inovação, Certificação e Normalização		2.2	3.2		5.1; 5.3
P8. Programa de Colaboração Internacional e Desenvolvimento da Indústria			3.2	4.3	5.1

III. Pormenores das iniciativas

Seguem-se os pormenores das iniciativas que serão realizadas no contexto da Estratégia Nacional de Cibersegurança de São Tomé e Príncipe. Cada iniciativa foi concebida para responder a uma necessidade específica no âmbito do quadro mais vasto da cibersegurança, contribuindo diretamente para a realização dos objetivos estratégicos. As iniciativas abrangem uma vasta gama de domínios, desde a governação e coordenação da cibersegurança, a gestão dos riscos, a educação e a sensibilização, até ao desenvolvimento jurídico, regulamentar e técnico.

Estas ações concretas visam reforçar a infraestrutura digital do país, aumentar a resiliência contra as ciber-ameaças e promover uma cultura de segurança digital sólida e inclusiva.

Nota: *Para cada iniciativa, foi efetuada uma estimativa de investimento, considerando valores mínimos e máximos. As estimativas foram baseadas em valores genéricos de mercado e tiveram em conta a valorização dos recursos humanos e técnicos. No entanto, podem ser potenciadas sinergias entre iniciativas e aproveitados recursos existentes nas organizações envolvidas. Adicionalmente, as iniciativas foram categorizadas num intervalo de orçamento (valor médio), tendo em consideração os seguintes critérios:*

Programa	Descrição	Iniciativas
Baixo investimento	Até $30.000,00	Esta categoria inclui iniciativas com um investimento estimado mais baixo, adequadas a projetos de menor escala ou com custos de funcionamento reduzidos. Em geral, estas iniciativas envolvem atividades essenciais, mas não requerem um investimento substancial.
Investimento moderado	Entre $30.000,00 e $45.000,00	As iniciativas desta categoria têm um investimento estimado moderado, adequado a projetos de média dimensão. Esta categoria pode abranger atividades que requerem recursos significativos, mas que não são altamente complexas ou de grande escala.
Investimento significativo	Entre $45.000,00 e $60.000,00	Esta categoria engloba iniciativas com um investimento estimado significativo, indicando projetos de maior dimensão e complexidade. De um modo geral, estas iniciativas podem abranger atividades que envolvam a aquisição de tecnologia, a formação de equipas especializadas e a implementação de sistemas complexos.
Alto investimento	Acima de $60.000,00	As iniciativas desta categoria têm um investimento estimado elevado, o que sugere projetos de grande escala e altamente complexos. Podem incluir atividades que exigem recursos substanciais para a aquisição de tecnologia de ponta, o desenvolvimento de infraestruturas críticas e a implementação de iniciativas abrangentes de cibersegurança.

Adicionalmente, cada iniciativa foi classificada como sendo uma iniciativa de ***"Implementação" e/ou "Manutenção"****, permitindo desta forma concluir se o investimento será realizado apenas num momento do tempo ou se considera a realização da iniciativa desde o seu lançamento até ao final do prazo da estratégia.*

Este exercício de estimativa destina-se sobretudo a apoiar a tomada de decisão das entidades envolvidas na Estratégia Nacional de Cibersegurança de STP e não dispensa a realização de uma avaliação detalhada dos recursos necessários e custos associados com a realização de cada iniciativa.

P1. Programa de Governação e Coordenação da Cibersegurança

<table>
<tr><td>Código
P1.1</td><td colspan="2">Iniciativa
Criação do Comité de Cibersegurança</td><td>Horizonte temporal
Ano 1-3: Fundações e estruturas iniciais</td></tr>
<tr><td>Objetivo geral
1</td><td>Objetivo específico
1.1</td><td>Programa
1. Programa de Governação e Coordenação da Cibersegurança</td><td>Entidades envolvidas
Ministério das Infraestruturas</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Criar um comité interministerial para dirigir e coordenar a estratégia nacional de cibersegurança.</td><td>Partes interessadas impactadas
INIC
AGER
Sociedade civil
Ministério da Justiça
DPIE (Direção Planeamento e Inovação Educativa)
DGRN</td></tr>
<tr><td colspan="3">Principais atividades
• Identificar e convidar membros interministeriais e líderes em matéria de cibersegurança para formar o Comité.
• Elaboração de uma carta de princípios que defina o âmbito, os objetivos e as responsabilidades do Comité.
• Estabelecer um calendário regular para reuniões e relatórios de progresso.
• Criação de subcomités, se necessário, para se concentrarem em áreas específicas da cibersegurança.</td><td>Métricas de sucesso
Aplicação efetiva da estratégia de cibersegurança.

KPIs
Número de iniciativas lançadas, grau de execução da estratégia nacional.</td></tr>
<tr><td colspan="3">Recursos necessários
• Representantes ministeriais e entidades relevantes de STP
• Peritos em cibersegurança
Financiamento</td><td>Avaliação e revisão
Revisão anual para ajustamentos e melhorias.</td></tr>
<tr><td colspan="3">Detalhes orçamentais
Despesas com recursos humanos:
• Tendo em conta que os membros do Comité podem já fazer parte do governo e que as suas contribuições para o Comité podem fazer parte das suas funções oficiais, o custo adicional pode ser mínimo ou estar relacionado com a compensação de horas extraordinárias ou de aconselhamento especializado.
• Consultores especializados: Podem ser necessários para desenvolver a carta de princípios e outras diretrizes especializadas.
• Coordenação e administração: Pessoal necessário para gerir o Comité e as suas atividades.

Despesas em tecnologia e infraestruturas:
• Podem ser relativamente baixos se tirarem partido das infraestruturas existentes e da proximidade física das entidades governamentais.
• Software de colaboração: Plataformas para videoconferência, partilha de documentos e comunicação.
• Hardware e segurança: Computadores e software seguros para os membros e subcomités do Comité.</td><td>Intervalo orçamental (valor médio)
Baixo investimento</td></tr>
</table>

Despesas em gestão e operações: • Inclui o custo das reuniões, a publicação de relatórios e outras despesas de funcionamento. • Espaço para reuniões: Aluguer de salas para reuniões, se estas não puderem ser realizadas em instalações públicas. • Materiais e serviços: Material de escritório, serviços de impressão e distribuição de relatórios e documentos. **[X] Implementação** **[ ] Manutenção** **Total estimado por ano: $2.000 - $5.000** - um posto a tempo inteiro, como um/a secretário/a	

Observações: Ainda existe discussão sobre quem será o ministério responsável pelo Comité de Cibersegurança.

Deve ser incluída uma margem de contingência para cobrir acontecimentos imprevistos e assegurar a flexibilidade orçamental. A colaboração entre ministérios e a utilização dos recursos e infraestruturas existentes podem reduzir significativamente os custos. A estimativa relativa aos recursos humanos tem em conta a possibilidade de o Comité funcionar com uma estrutura reduzida, dada a menor escala administrativa de um microestado.

<table>
<tr><td>Código
P1.2</td><td colspan="2">Iniciativa
Promover a colaboração interdepartamental e intersectorial</td><td>Horizonte temporal
Ano 1-3: Fundações e estruturas iniciais</td></tr>
<tr><td>Objetivo geral
1 e 4</td><td>Objetivo específico
1.1 e 4.1</td><td>Programa
1. Programa de Governação e Coordenação da Cibersegurança</td><td>Entidades envolvidas
Comité de Cibersegurança</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Promover a colaboração entre diferentes departamentos governamentais e setores industriais para uma abordagem unificada da cibersegurança.</td><td>Partes interessadas impactadas
Entidades com risco de cibersegurança</td></tr>
<tr><td colspan="3">Principais atividades
• Promover a colaboração interdepartamental e intersectorial.
o Identificação das partes interessadas em diferentes departamentos governamentais e setores industriais.
o Desenvolvimento de uma plataforma ou fórum online para facilitar a comunicação permanente entre as partes interessadas.
o Criação de um repositório de boas práticas e de recursos partilhados.
• Organização de reuniões semestrais entre representantes do governo, do sector privado e da sociedade civil.
o Estabelecer uma agenda que inclua a revisão do guia de boas práticas, a discussão de desafios emergentes e a partilha de soluções.
o Documentar as conclusões e recomendações das reuniões e publicar relatórios para promover a transparência.
o Utilizar os conhecimentos adquiridos nas reuniões para informar as políticas públicas e as estratégias de cibersegurança.</td><td>Métricas de sucesso
Estabelecimento de canais de comunicação eficazes, realização de ações de colaboração.
KPIs
Número de acordos de colaboração assinados, nível de participação em workshops.</td></tr>
<tr><td colspan="3">Recursos necessários
• Coordenadores de projetos
• Peritos em cibersegurança
• Financiamento</td><td>Avaliação e revisão
Revisão anual com todas as partes interessadas para ajustamentos e melhorias.</td></tr>
<tr><td colspan="3">Detalhes orçamentais
Despesas com recursos humanos:
• Incluirá o custo do pessoal para organizar eventos, gerir a plataforma online e coordenar o levantamento das partes interessadas.
• Coordenadores de projeto: Para gerir a iniciativa e organizar eventos.
• Especialistas em informática: Para desenvolver e manter a plataforma ou o fórum online (opcional).
• Equipa de comunicação e relações públicas: Para promover eventos e colaborações.</td><td>Intervalo orçamental (valor médio)
Alto investimento</td></tr>
</table>

Despesas em tecnologia e infraestruturas: • Serão necessários investimentos em tecnologia para apoiar a comunicação e a colaboração online. • Desenvolvimento e manutenção da plataforma/fórum online: Custos de criação e suporte técnico **(opcional).** • Equipamento para eventos: Por exemplo, tecnologia de apresentação e sistemas de comunicação. **Despesas em gestão e operações:** • Inclui os custos associados à organização de eventos e à manutenção do repositório de boas práticas. • Logística do evento: Aluguer do local, catering, equipamento audiovisual e material promocional. • Desenvolvimento e manutenção do repositório: Custos associados à criação e atualização de um repositório de boas práticas. **[] Implementação** **[X] Manutenção** **Total estimado: $25.000 - $85.000**	
Observações: A estimativa considera a necessidade de uma abordagem colaborativa e integrada, típica de um microestado como São Tomé e Príncipe. A utilização de espaços e recursos existentes pode ajudar a minimizar os custos, especialmente na organização de eventos. As parcerias com organizações locais e internacionais podem ser uma forma eficaz de reduzir custos e aumentar o alcance das iniciativas. Estes valores são estimativas genéricas e devem ser ajustados com base nas especificidades locais e em orçamentos detalhados.	

P2. Programa de Gestão de Ativos e Operadores Críticos

<table>
<tr><td>Código
P2.1</td><td colspan="2">Iniciativa
Elaboração de regulamentação em matéria de cibersegurança para os ativos e operadores críticos</td><td>Horizonte temporal
Ano 1-3: Fundações e estruturas iniciais</td></tr>
<tr><td>Objetivo geral
1</td><td>Objetivo específico
1.2</td><td>Programa
2. Programa de gestão de ativos e operadores críticos</td><td>Entidades envolvidas
AGER</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Criar um conjunto de regulamentos para garantir a segurança dos ativos e operadores críticos identificados.</td><td>Partes interessadas impactadas
INIC, Ministério da Justiça</td></tr>
<tr><td colspan="3" rowspan="2">Principais atividades
• Elaborar regulamentação específica para a proteção dos ativos e operadores críticos.
• Consultar os peritos em cibersegurança e as partes interessadas durante o processo de elaboração da regulamentação.
• Implementar uma fase de consulta pública para recolher reações aos regulamentos propostos.
• Finalizar e adotar os regulamentos, assegurando a sua comunicação clara e a disponibilização de orientações para a sua aplicação.</td><td>Métricas de sucesso
Aplicação bem-sucedida da regulamentação, redução das vulnerabilidades.</td></tr>
<tr><td>KPIs
Nível de conformidade entre ativos e operadores, redução do número de incidentes.</td></tr>
<tr><td colspan="3">Recursos necessários
• Consultores jurídicos
• Peritos em cibersegurança</td><td>Avaliação e revisão
Revisões anuais, ajustamentos se necessário.</td></tr>
<tr><td colspan="3">Detalhes orçamentais
Despesas com recursos humanos:
• Estes incluem o custo de peritos externos em cibersegurança, advogados e pessoal de apoio.
• Consultoria de peritos em cibersegurança: Para garantir que os regulamentos estão em conformidade com as melhores práticas internacionais.
• Juristas e legisladores: Elaborar regulamentos e assegurar a sua conformidade legal.
• Equipa de consulta pública: Gerir e analisar as reações recebidas durante a fase de consulta pública.</td><td>Intervalo orçamental (valor médio)
Investimento significativo</td></tr>
</table>

Despesas em tecnologia e infraestruturas: • Poderá ser necessário algum investimento em tecnologia para facilitar a consulta pública e a divulgação dos regulamentos. • Plataformas de consulta online: Para acolher a fase de consulta pública e permitir um feedback fácil e organizado. • Sistemas de gestão de documentos: Gerir e arquivar todos os documentos relacionados com o processo de elaboração de regulamentos. **Despesas em gestão e operações:** • Inclui os custos relacionados com a coordenação do projeto e as despesas gerais. • Despesas de funcionamento: Custos de coordenação e gestão do processo de elaboração dos regulamentos. • Publicação e comunicação: Custos de publicação dos regulamentos finais e do material explicativo sobre os mesmos. **[X] Implementação** **[] Manutenção** **Total estimado: $45.000 - $65.000**	
Observações: A estimativa para os recursos humanos tem em conta a necessidade de peritos de alto nível e peritos jurídicos com experiência específica em cibersegurança. O investimento em tecnologia tem por objetivo facilitar uma abordagem inclusiva e transparente durante a consulta pública. As despesas operacionais e de comunicação são fundamentais para garantir que os regulamentos sejam bem compreendidos e efetivamente aplicados. Estes valores são estimativas genéricas que devem ser ajustadas com base em cotações locais e nas necessidades específicas do projeto em São Tomé e Príncipe. Deve ser prevista uma margem de contingência para cobrir eventuais variações de custos.	

<table>
<tr><td>Código
P2.2</td><td colspan="2">Iniciativa
Identificação de ativos e operadores críticos</td><td>Horizonte temporal
Ano 1-3: Fundações e estruturas iniciais</td></tr>
<tr><td>Objetivo geral
1</td><td>Objetivo específico
1.2</td><td>Programa
2. Programa de gestão de ativos e operadores críticos</td><td>Entidades envolvidas
INIC</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Identificar e catalogar os ativos e operadores críticos para o sistema nacional de cibersegurança.</td><td>Partes interessadas impactadas
AGER</td></tr>
<tr><td colspan="3">Principais atividades
• Desenvolvimento da metodologia de identificação do ICI
• Classificar os ativos e os operadores com base no seu nível de importância crítica para a segurança nacional.
• Documentar e manter um registo atualizado destes bens e operadores, que deverá ser revisto periodicamente.</td><td>Métricas de sucesso
Identificação completa e precisa, desenvolvimento de medidas de proteção.
KPIs
Número de ativos e operadores identificados, grau de vulnerabilidade.</td></tr>
<tr><td colspan="3">Recursos necessários
• Peritos</td><td>Avaliação e revisão
Revisões anuais, ajustamentos se necessário.</td></tr>
<tr><td colspan="3">Detalhes orçamentais
Despesas com recursos humanos:
• Incluirá o custo dos peritos externos em cibersegurança e do pessoal de apoio para realizar o estudo, classificar os ativos e mantê-los atualizados.
• Equipa de cartografia e classificação: Especialistas para identificar e classificar os ativos e os operadores.
• Gestão e administração de dados: O pessoal deve manter os registos atualizados e efetuar revisões periódicas.

Despesas em tecnologia e infraestruturas:
• Software de identificação de ativos: Para catalogar e classificar ativos e operadores (opcional).
• Infraestruturas informáticas: Equipamento e sistemas de armazenamento seguro dos dados recolhidos.</td><td>Intervalo orçamental (valor médio)
Alto investimento</td></tr>
</table>

Despesas em gestão e operações: • Inclui os custos associados à coordenação dos projetos e as despesas gerais de funcionamento. • Custos operacionais e logísticos: Custos de organização e gestão da iniciativa. • Publicação e divulgação: Custos para documentar e partilhar os resultados do mapeamento. **[X] Implementação** **[] Manutenção** **Total estimado por ano: $85,000-100 000**	
Observações: A estimativa tem em conta a escala e as necessidades específicas de um microestado como São Tomé e Príncipe. A natureza colaborativa e integrada do governo e dos setores essenciais num microestado pode facilitar o processo de cartografia e reduzir os custos. É importante prever uma margem para imprevistos e variações de custos. Estes valores são estimativas genéricas e devem ser ajustados de acordo com informações locais mais detalhadas e com as especificidades do projeto.	

<table>
<tr><td>Código
P2.3</td><td colspan="2">Iniciativa
Implementação de protocolos entre as CSIRT e as infraestruturas críticas</td><td>Horizonte temporal
Ano 3-4: Reforço das capacidades e resposta a incidentes</td></tr>
<tr><td>Objetivo geral
5</td><td>Objetivo específico
5.3</td><td>Programa
2. Programa de gestão de ativos e operadores críticos</td><td>Entidades envolvidas
CSIRT-STP</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Estabelecer protocolos de coordenação eficazes para responder a incidentes de cibersegurança em infraestruturas críticas.</td><td>Partes interessadas impactadas
Instituições identificadas como gestoras de ativos determinados como críticos para o estado</td></tr>
<tr><td colspan="3">Principais atividades
• Identificar as partes responsáveis pelas infraestruturas críticas e estabelecer canais de comunicação com CSIRT.
• Desenvolver protocolos pormenorizados de coordenação e resposta a incidentes, incluindo planos de emergência.
• Efetuar exercícios regulares para testar e aperfeiçoar os protocolos.
• Avaliar a eficácia dos protocolos após cada incidente e efetuar os ajustes necessários.</td><td>Métricas de sucesso
Resposta rápida a incidentes, minimização de danos.
KPIs
Tempo médio de resposta a incidentes, eficácia da coordenação.</td></tr>
<tr><td colspan="3">Recursos necessários
• Equipa de coordenação
• Mecanismos de comunicação seguros</td><td>Avaliação e revisão
Revisão anual dos protocolos e ajustamentos, se necessário.</td></tr>
<tr><td colspan="3">Detalhes orçamentais
Despesas com recursos humanos: O desenvolvimento de protocolos exige especialistas em cibersegurança e infraestruturas críticas.
Despesas com tecnologia e infraestruturas: Requer sistemas de comunicação eficazes e seguros.
Custos de gestão e de funcionamento: Necessidade de testes regulares e de atualização dos protocolos.

[X] Implementação
[] Manutenção

Total estimado: $35.000 - $55.000</td><td>Intervalo orçamental (valor médio)
Investimento moderado</td></tr>
<tr><td colspan="4">Observações:</td></tr>
</table>

P3. Programa de educação e sensibilização em matéria de cibersegurança

<table>
<tr><td>Código
P3.1</td><td colspan="2">Iniciativa
Criação de programas de ensino para promover a literacia digital e a cibersegurança nas escolas</td><td>Horizonte temporal
Ano 3-4: Reforço das capacidades e resposta a incidentes</td></tr>
<tr><td>Objetivo geral
2</td><td>Objetivo específico
2.1</td><td>Programa
3. Programa de educação e sensibilização em matéria de cibersegurança</td><td>Entidades envolvidas
Ministério da Educação</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Desenvolver e aplicar programas curriculares que promovam a literacia digital e a cibersegurança a partir do ensino básico.</td><td>Partes interessadas impactadas
INIC, AGER, ANPDP</td></tr>
<tr><td colspan="3">Principais atividades
• Realizar um estudo para identificar as necessidades e as lacunas da atual literacia digital no ensino primário.
• Desenvolver programas curriculares integrados que incluam competências digitais e de cibersegurança.
• Formar os educadores para que possam ensinar eficazmente os novos currículos.
• Implementar os currículos por fases, começando por um programa-piloto antes da implementação em grande escala.
• Desenvolvimento de materiais e recursos de apoio para os alunos
• Implementação de um sistema de feedback para avaliar a eficácia dos seminários e workshops.
• Utilizar uma plataforma online para fornecer materiais educativos sobre cibersegurança.</td><td>Métricas de sucesso
Melhorar as competências digitais dos alunos.

KPIs
Número de escolas que aplicam o novo currículo, resultados das avaliações dos alunos.</td></tr>
<tr><td colspan="3">Recursos necessários
• Educadores
• Material didático
• Financiamento</td><td>Avaliação e revisão
Análise e ajustamentos anuais com base no feedback.</td></tr>
<tr><td colspan="3">Detalhes orçamentais
Despesas com recursos humanos: Preparação de currículos por peritos em educação e cibersegurança.
Despesas em tecnologia e infraestruturas: plataformas de aprendizagem eletrónica e materiais didáticos.
Custos de gestão e de funcionamento: Implementação e acompanhamento de programas educativos.

[X] Implementação
[] Manutenção
Total estimado: $25.000 - $50.000</td><td>Intervalo orçamental (valor médio)
Investimento moderado</td></tr>
<tr><td colspan="4">Observações:</td></tr>
</table>

<table>
<tr><td>Código
P3.2</td><td colspan="2">Iniciativa
Organização de seminários e workshops periódicos sobre as melhores práticas em matéria de cibersegurança</td><td>Horizonte temporal
Ano 4-5: Educação, sensibilização e normalização</td></tr>
<tr><td>Objetivo geral
2, 3, 4 e 5</td><td>Objetivo específico
2.1, 3.1, 4.1 e 5.1</td><td>Programa
3. Programa de educação e sensibilização em matéria de cibersegurança</td><td>Entidades envolvidas
Comité de Cibersegurança</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Educar as entidades empresariais e outras sobre as melhores práticas em matéria de literacia digital e cibersegurança.</td><td>Partes interessadas impactadas
Instituições públicas e privadas, ONGs, Comunicação Social</td></tr>
<tr><td colspan="3">Principais atividades
• Criação de workshops e seminários para entidades empresariais sobre as melhores práticas em matéria de literacia digital
○ Identificar temas e conteúdos relevantes para workshops e seminários com base nas necessidades das entidades empresariais.
○ Organizar eventos educativos e criar materiais de formação adequados.
○ Estabelecer parcerias com peritos em cibersegurança para proporcionar formação especializada.
○ Avaliar o impacto da formação e ajustar os eventos futuros com base nas reações.
• Organização de seminários e workshops periódicos sobre as melhores práticas em matéria de cibersegurança, acompanhados da criação e aplicação de métricas de avaliação e feedback.
○ Identificação de temas relevantes e de peritos no domínio da cibersegurança para conduzir as sessões.
○ Planeamento e organização logística de eventos, incluindo plataformas online para workshops virtuais.
○ Desenvolvimento de materiais e recursos de apoio para os participantes.
○ Implementação de um sistema de feedback para avaliar a eficácia dos seminários e workshops.
• Realização de workshops anuais sobre cibersegurança para entidades governamentais, empresas locais e instituições de ensino, com o objetivo de reforçar competências e aplicar o Guia de Boas Práticas em situações reais
○ Planear o conteúdo dos seminários para abordar questões atuais e relevantes em matéria de cibersegurança.
○ Identificar e convidar peritos para conduzir as sessões de formação.
○ Coordenar a participação de entidades governamentais, empresas e instituições de ensino.
○ Realizar simulações e exercícios práticos para aplicar o Guia de Boas Práticas em cenários reais.
Avaliar a eficácia dos seminários e ajustar as sessões futuras com base nas reações recebidas.</td><td>Métricas de sucesso
Aumento das práticas de segurança nas empresas participantes.
KPIs
Número de participantes, feedback pós-evento.</td></tr>
</table>

Recursos necessários	Avaliação e revisão
• Peritos em cibersegurança • Locais para eventos • Material promocional	Revisão anual do programa.
Detalhes orçamentais **Despesas com recursos humanos:** Planeamento e execução de workshops por especialistas. **Despesas em tecnologia e infraestruturas:** Locais para eventos e o equipamento necessário. **Custos de gestão e de funcionamento:** Materiais de promoção e formação. **[] Implementação** **[X] Manutenção** **Total estimado: $20.000 - $45.000**	**Intervalo orçamental (valor médio)** Investimento moderado
Observações:	

<table>
<tr><td>Código
P3.3</td><td colspan="2">Iniciativa
Estabelecer parcerias com organizações locais para promover eventos de sensibilização para a literacia mediática</td><td>Horizonte temporal
Ano 3-4: Reforço das capacidades e resposta a incidentes</td></tr>
<tr><td>Objetivo geral
2</td><td>Objetivo específico
2.1</td><td>Programa
3. Programa de educação e sensibilização em matéria de cibersegurança</td><td>Entidades envolvidas
Comité de Cibersegurança</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Expandir o alcance e o impacto das campanhas de sensibilização para a literacia mediática.</td><td>Partes interessadas impactadas
Comunicação Social, Operadoras de Telecomunicações, Autarquias</td></tr>
<tr><td colspan="3">Principais atividades
• Mapeamento e contacto com organizações locais com interesse e influência na literacia mediática.
• Desenvolver uma série de eventos e materiais de sensibilização em colaboração com estas organizações.
• Promover eventos em vários meios de comunicação, incluindo redes sociais e eventos comunitários.
• Monitorizar e medir a eficácia das campanhas para ajustar as estratégias futuras.</td><td>Métricas de sucesso
Melhoria dos indicadores de literacia mediática na comunidade.
KPIs
Número de parcerias estabelecidas, alcance das campanhas.</td></tr>
<tr><td colspan="3">Recursos necessários
• Coordenador do projeto
• Material promocional
• Financiamento</td><td>Avaliação e revisão
Avaliação anual e ajustamento da estratégia, se necessário.</td></tr>
<tr><td colspan="3">Detalhes orçamentais
Despesas com recursos humanos: Coordenação de parcerias e eventos.
Despesas em tecnologia e infraestruturas: Apoio a campanhas de sensibilização.
Custos de gestão e de funcionamento: Organização de eventos e acompanhamento.
[] Implementação
[X] Manutenção
Total estimado: $15.000 - $30.000</td><td>Intervalo orçamental (valor médio)
Baixo investimento</td></tr>
<tr><td colspan="4">Observações:</td></tr>
</table>

<table>
<tr><td>Código
P3.4</td><td colspan="2">Iniciativa
Realização de inquéritos anuais sobre o nível de confiança dos cidadãos nos serviços online</td><td>Horizonte temporal
Ano 4-5: Educação, sensibilização e normalização</td></tr>
<tr><td>Objetivo geral
2 e 3</td><td>Objetivo específico
2.2 e 3.1</td><td>Programa
3. Programa de educação e sensibilização em matéria de cibersegurança</td><td>Entidades envolvidas
Comité de Cibersegurança</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Avaliar o nível de confiança dos cidadãos nos serviços online.</td><td>Partes interessadas impactadas
INE</td></tr>
<tr><td colspan="3">Principais atividades
• Desenvolvimento de um inquérito para avaliar a confiança nos serviços online.
• Realização de inquéritos e recolha de dados junto dos utilizadores de serviços online.
• Analisar os dados para identificar tendências e áreas de preocupação.
• Publicar relatórios anuais e recomendar melhorias com base nas conclusões.</td><td>Métricas de sucesso
Relatórios anuais publicados e utilizados em estratégias futuras.

KPIs
Número de respostas, nível de confiança medido.</td></tr>
<tr><td colspan="3">Recursos necessários
• Equipa de investigação</td><td>Avaliação e revisão
Revisão anual para avaliar a eficácia e efetuar ajustamentos.</td></tr>
<tr><td colspan="3">Detalhes orçamentais
Despesas com recursos humanos: Inclui a coordenação, os analistas de dados e os especialistas em investigação para desenvolver e efetuar os estudos.
Despesas em tecnologia e infraestruturas: Ferramentas analíticas e plataformas de investigação online (STP tem isto).
Despesas de gestão e de funcionamento: Despesas de publicação de relatórios e recomendações.
[X] Implementação
[] Manutenção
Total estimado por ano: $10.000 - $20.000</td><td>Intervalo orçamental (valor médio)
Baixo investimento</td></tr>
<tr><td colspan="4">Observações:</td></tr>
</table>

<table>
<tr><td>Código
P3.5</td><td colspan="2">Iniciativa
Criação de uma plataforma de verificação de factos online para combater a desinformação</td><td>Horizonte temporal
Ano 4-5: Educação, sensibilização e normalização</td></tr>
<tr><td>Objetivo geral
2</td><td>Objetivo específico
2.1</td><td>Programa
3. Programa de educação e sensibilização em matéria de cibersegurança</td><td>Entidades envolvidas
Comité de Cibersegurança, Universidades</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Criar uma plataforma de verificação de factos online para combater a desinformação.</td><td>Partes interessadas impactadas
Comunicação Social</td></tr>
<tr><td colspan="3">Principais atividades
• Definir os critérios e os processos de verificação dos factos.
• Construir ou adquirir uma plataforma tecnológica para alojar e gerir o serviço de verificação.
• Estabelecer parcerias com os meios de comunicação social, verificadores de factos e peritos para criar uma rede de verificação de factos.
• Lançar campanhas de educação para o público sobre a forma de utilizar a plataforma e a importância da verificação dos factos.</td><td>Métricas de sucesso
Redução da difusão de informações falsas, aumento do número de utilizadores ativos.
KPIs
Número de visitas à plataforma, número de factos verificados.</td></tr>
<tr><td colspan="3">Recursos necessários
• Programadores de software
• Verificadores de factos
• Servidores</td><td>Avaliação e revisão
Revisões semestrais para avaliar a eficácia da plataforma.</td></tr>
<tr><td colspan="3">Detalhes orçamentais
Despesas com recursos humanos: Técnicos informáticos e especialistas em conteúdos para estabelecer critérios de verificação.
Despesas com tecnologia e infraestruturas: Desenvolvimento e manutenção da plataforma de verificação de factos.
Despesas em gestão e operações: Campanhas educativas para promover a utilização da plataforma.
[X] Implementação
[] Manutenção
Total estimado: $30.000 - $60.000</td><td>Intervalo orçamental (valor médio)
Investimento moderado</td></tr>
<tr><td colspan="4">Observações:</td></tr>
</table>

<table>
<tr><td>Código
P3.6</td><td colspan="2">Iniciativa
Desenvolvimento de campanhas de sensibilização sobre a importância da proteção dos dados pessoais</td><td>Horizonte temporal
Ano 1-3: Fundações e estruturas iniciais</td></tr>
<tr><td>Objetivo geral
2</td><td>Objetivo específico
2.1</td><td>Programa
3. Programa de educação e sensibilização em matéria de cibersegurança</td><td>Entidades envolvidas
ANPDP</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Sensibilizar o público para a importância da proteção dos dados pessoais.</td><td>Partes interessadas impactadas
Comité de Cibersegurança, Comunicação Social</td></tr>
<tr><td colspan="3">Principais atividades
• Planeamento estratégico de campanhas, incluindo objetivos, mensagens-chave e segmentação de audiências.
• Criação de materiais de sensibilização, tais como folhetos, vídeos e publicações nas redes sociais.
• Parcerias com organizações da sociedade civil e com o sector privado para alargar o alcance.
• Acompanhamento e avaliação do impacto das campanhas.</td><td>Métricas de sucesso
Maior sensibilização do público, redução das violações de dados.
KPIs
Alcance das campanhas, nível de envolvimento.</td></tr>
<tr><td colspan="3">Recursos necessários
• Especialistas em marketing
• Designers gráficos
• Financiamento da publicidade</td><td>Avaliação e revisão
Análise semestral da eficácia das campanhas.</td></tr>
</table>

Detalhes orçamentais	Intervalo orçamental (valor médio)
Despesas com recursos humanos: • Incluirá o custo de profissionais para planear e executar a campanha, bem como para criar conteúdos. • Equipa de marketing e comunicação: Profissionais para desenvolver e gerir a campanha, incluindo a criação de estratégias e mensagens. • Designers e criadores de conteúdos: Para a produção de materiais de sensibilização, como folhetos, vídeos e posts para redes sociais. **Despesas em tecnologia e infraestruturas:** • Será necessário equipamento e software para criar e distribuir os materiais da campanha. • Software de design e edição: Para criar materiais gráficos e vídeos. • Infraestrutura de TI e alojamento Web: Para apoiar a presença online da campanha. **Despesas em gestão e operações:** • Inclui os custos associados à coordenação dos projetos e as despesas gerais de funcionamento. • Produção de materiais físicos: Impressão de folhetos e outros materiais promocionais. • Custos de publicidade: Custos de promoção da campanha em diferentes plataformas, incluindo as redes sociais. • Parcerias e colaborações: Custos potenciais associados a parcerias com organizações da sociedade civil e com o sector privado. **[X] Implementação** **[X] Manutenção** **Total estimado por ano: $5.000 - $10.000**	Baixo investimento
Observações: A estimativa tem em conta a necessidade de uma abordagem eficaz e com impacto, mesmo num microestado. A colaboração com organizações locais pode ajudar a reduzir os custos e a aumentar o alcance da campanha. A inclusão de uma margem para imprevistos é aconselhável para cobrir variações nos custos. Estes valores são estimativas genéricas que devem ser ajustadas com base em informações locais mais detalhadas e nas necessidades específicas do projeto em São Tomé e Príncipe.	

<table>
<tr><td>Código
P3.7</td><td colspan="2">Iniciativa
Avaliação e documentação das necessidades nacionais em termos de competências em matéria de cibersegurança</td><td>Horizonte temporal
Ano 1-3: Fundações e estruturas iniciais</td></tr>
<tr><td>Objetivo geral
3</td><td>Objetivo específico
3.2</td><td>Programa
3. Programa de educação e sensibilização em matéria de cibersegurança</td><td>Entidades envolvidas
Comité de Cibersegurança</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Compreender as lacunas e as necessidades de competências em matéria de cibersegurança no país.</td><td>Partes interessadas impactadas
Ministério da Educação, Ministério da Justiça, CSIRT</td></tr>
<tr><td colspan="3">Principais atividades
• Realizar inquéritos e entrevistas com profissionais de TI para identificar as competências existentes e as lacunas.
• Analisar o cenário de ciber-ameaças e alinhar as necessidades de competências com os riscos identificados.
• Documentar as competências necessárias a diferentes níveis organizacionais e recomendar percursos de formação.
• Publicar um relatório pormenorizado sobre as necessidades do país em matéria de competências de cibersegurança.</td><td>Métricas de sucesso
Implementação bem-sucedida de estratégias de formação baseadas na avaliação.

KPIs
Integralidade da avaliação, número de lacunas identificadas.</td></tr>
<tr><td colspan="3">Recursos necessários
• Equipa de investigação
• Financiamento de estudos</td><td>Avaliação e revisão
Revisão anual e atualizações, se necessário.</td></tr>
<tr><td colspan="3">Detalhes orçamentais
Despesas com recursos humanos: Consultores para analisar as competências e as lacunas em matéria de cibersegurança.
Despesas em tecnologia e infraestruturas: Sistemas de compilação e análise de dados de inquéritos.
Custos de gestão e de funcionamento: Publicação de relatórios e recomendações de formação.
[X] Implementação
[] Manutenção
Total estimado: $20.000 - $45.000</td><td>Intervalo orçamental (valor médio)
Investimento moderado</td></tr>
<tr><td colspan="4">Observações:</td></tr>
</table>

<table>
<tr><td>Código
P3.8</td><td colspan="2">Iniciativa
Desenvolvimento de um Guia de Boas Práticas de Cibersegurança para orientar as entidades públicas e privadas sobre as normas e responsabilidades básicas no ciberespaço</td><td>Horizonte temporal
Ano 3-4: Reforço das capacidades e resposta a incidentes</td></tr>
<tr><td>Objetivo geral
4</td><td>Objetivo específico
4.1</td><td>Programa
3. Programa de educação e sensibilização em matéria de cibersegurança</td><td>Entidades envolvidas
Comité de Cibersegurança</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Aconselhamento de entidades públicas e privadas sobre as melhores práticas em matéria de cibersegurança.</td><td>Partes interessadas impactadas
Entidades públicas e privadas</td></tr>
<tr><td colspan="3">Principais atividades
• Compilar um conjunto de boas práticas de cibersegurança relevantes para o contexto nacional.
• Desenvolver o guia em colaboração com peritos locais e internacionais em cibersegurança.
• Distribuir o guia e fornecer formação e seminários sobre como implementar as práticas recomendadas.
• Rever e atualizar regularmente o guia para manter a sua relevância e eficácia.</td><td>Métricas de sucesso
Implementação bem-sucedida das práticas recomendadas, redução dos incidentes de segurança.
KPIs
Número de descarregamentos, nível de implementação nas organizações.</td></tr>
<tr><td colspan="3">Recursos necessários
• Equipa de redação e de revisão
• Aconselhamento técnico
• Recursos de publicação</td><td>Avaliação e revisão
Revisão anual para atualizações.</td></tr>
<tr><td colspan="3">Detalhes orçamentais
Despesas com recursos humanos: Peritos para compilar boas práticas e redatores técnicos.
Despesas em tecnologia e infraestruturas: Ferramentas de colaboração e publicação.
Custos de gestão e de funcionamento: Distribuição do guia e seminários de sensibilização.
[X] Implementação
[] Manutenção

Total estimado: $15.000 - $35.000</td><td>Intervalo orçamental (valor médio)
Baixo investimento</td></tr>
<tr><td colspan="4">Observações:</td></tr>
</table>

P4. Programa de resposta a incidentes e gestão de riscos

<table>
<tr><td>Código
P4.1</td><td colspan="2">Iniciativa
Criação e reforço do CSIRT-STP</td><td>Horizonte de tempo
Ano 1-3: Fundações e estruturas iniciais</td></tr>
<tr><td>Objetivo geral
1</td><td>Objetivo específico
1.2</td><td>Programa
4. Programa de resposta a incidentes e gestão de riscos</td><td>Entidades envolvidas
Comité de Cibersegurança, Projeto STP Digital</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Criar um centro de resposta a incidentes de segurança informática para monitorizar, avaliar e reagir a incidentes informáticos.</td><td>Partes interessadas impactadas
Instituições Públicas e privadas</td></tr>
<tr><td colspan="3">Principais atividades
• Definição da infraestrutura tecnológica e dos requisitos de pessoal para o CSIRT-STP.
• Elaboração do modelo de prestação de serviços do CSIRT.
• Recrutamento e formação de especialistas em cibersegurança para operar o CSIRT.
• Implementação de ferramentas e processos para a monitorização contínua e análise de ameaças.
• Estabelecimento de procedimentos para resposta a incidentes e recuperação.</td><td>Métricas de sucesso
Tempo de resposta a incidentes, número de incidentes resolvidos.

KPIs
Estabelecimento de canais de comunicação eficazes, realização de ações de colaboração.</td></tr>
<tr><td colspan="3">Recursos necessários
• Pessoal especializado
• Infraestruturas tecnológicas
• Financiamento</td><td>Avaliação e revisão
Resolução eficiente de incidentes, redução do tempo de resposta.</td></tr>
<tr><td colspan="3">Detalhes orçamentais
Despesas com recursos humanos:
• Peritos em cibersegurança (a tempo inteiro) pelo menos 3 (o ideal 5).
• Peritos subcontratados para a criação do CSIRT

Despesas em tecnologia e infraestruturas:
• Será necessário um investimento inicial significativo em tecnologia para criar o CSIRT.</td><td>Intervalo orçamental (valor médio)
Alto investimento</td></tr>
</table>

• Infraestruturas tecnológicas: Hardware e software para monitorizar e analisar ameaças, incluindo servidores, sistemas de deteção de intrusões e ferramentas de análise de segurança. • Sistemas de comunicação e segurança de dados: Equipamentos para garantir a segurança das comunicações e o armazenamento de dados sensíveis. **Despesas em gestão e operações:** • Formação e desenvolvimento contínuo: Programas de formação para manter a equipa atualizada com as mais recentes práticas e tecnologias de cibersegurança. • Inclui os custos associados ao funcionamento quotidiano do CSIRT e à manutenção das suas capacidades. • Despesas operacionais e logísticas: Custos correntes de manutenção do centro, incluindo serviços públicos, comunicações e segurança. • Procedimentos de resposta e recuperação de incidentes: Desenvolvimento e implementação de protocolos para lidar com incidentes cibernéticos. **[X] Implementação** **[] Manutenção** **Total estimado:** $ 300.000-500.000 (estabelecimento sem salário do pessoal e pilha de tecnologia)	
Observações: A estimativa tem em conta a necessidade de um investimento inicial significativo em tecnologia e formação para estabelecer um CSIRT eficaz. O custo dos recursos humanos reflete a importância de ter uma equipa qualificada e experiente a operar um centro de resposta a incidentes. A colaboração com organizações internacionais de cibersegurança pode oferecer oportunidades para reduzir os custos e melhorar a eficácia. Estes valores são estimativas genéricas que devem ser ajustadas com base nas necessidades específicas e nas cotações locais em São Tomé e Príncipe. É aconselhável uma margem para imprevistos para cobrir eventos imprevistos e variações nos custos.	

<table>
<tr><td>Código
P4.2</td><td colspan="2">Iniciativa
Estabelecimento de um protocolo de avaliação regular dos riscos para as principais infraestruturas de telecomunicações do país</td><td>Horizonte temporal
Ano 3-4: Reforço das capacidades e resposta a incidentes</td></tr>
<tr><td>Objetivo geral
5</td><td>Objetivo específico
5.3</td><td>Programa
4. Programa de resposta a incidentes e gestão de riscos</td><td>Entidades envolvidas
AGER</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Assegurar a integridade e a segurança das principais infraestruturas de telecomunicações do país.</td><td>Partes interessadas impactadas
Comité de Cibersegurança</td></tr>
<tr><td colspan="3">Principais atividades
• Definir uma metodologia de avaliação periódica dos riscos que seja exaustiva e adaptada à realidade nacional.
• Efetuar avaliações de risco a intervalos regulares, envolvendo especialistas de diferentes áreas.
• Rever e atualizar a avaliação dos riscos à medida que surgem novas ameaças e tecnologias.
• Controlo da conformidade das empresas.
• Monitorizar a forma como os requisitos elaborados/definidos são implementados.</td><td>Métricas de sucesso
Redução dos incidentes de segurança nas infraestruturas avaliadas.
KPIs
Número de vulnerabilidades detetadas e resolvidas.</td></tr>
<tr><td colspan="3">Recursos necessários
• Peritos em cibersegurança
• Instrumentos de avaliação dos riscos</td><td>Avaliação e revisão
Revisão anual do protocolo e ajustamentos, se necessário.</td></tr>
<tr><td colspan="3">Detalhes orçamentais
Despesas com recursos humanos: Peritos externos para desenvolver e rever protocolos numa base regular.
Despesas em tecnologia e infraestruturas: Sistemas para efetuar e controlar as avaliações de risco.
Despesas em gestão e operações: Realização de avaliações periódicas e atualização de protocolos.

[X] Implementação
[X] Manutenção

Total estimado: $25.000 - $60.000</td><td>Intervalo orçamental (valor médio)
Investimento moderado</td></tr>
<tr><td colspan="4">Observações:</td></tr>
</table>

<table>
<tr><td>Código
P4.3</td><td colspan="2">Iniciativa
Análise abrangente dos ciber-riscos na defesa nacional</td><td>Horizonte de tempo
Ano 4-5: Educação, sensibilização e normalização</td></tr>
<tr><td>Objetivo geral
1</td><td>Objetivo específico
1.3</td><td>Programa
4. Programa de resposta a incidentes e gestão de riscos</td><td>Entidades envolvidas
Ministério da Defesa Nacional</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Avaliar os ciber-riscos associados à defesa nacional e propor medidas de atenuação.</td><td>Partes interessadas impactadas
Comité Nacional de Cibersegurança</td></tr>
<tr><td colspan="3">Principais atividades
• Realizar um estudo exaustivo dos sistemas de informação da defesa nacional.
• Efetuar uma análise aprofundada dos ciber-riscos utilizando ferramentas analíticas e consultoria especializada.
• Desenvolver um plano de ação estratégico de cibersegurança para a atenuação dos riscos.
• Atualizar e melhorar regularmente as políticas de segurança da defesa nacional.
• Preparar um relatório pormenorizado sobre o panorama das ciber-ameaças.
• Promover a colaboração interagências e a partilha de informações entre as entidades de São Tomé e Príncipe.
• Criar grupos de trabalho conjuntos sobre cibersegurança para esforços coordenados de defesa.
• Implementar a Monitorização Contínua e a Recolha de Informação sobre Ameaças.</td><td>Métricas de sucesso
Identificação e atenuação efetiva dos riscos.

KPIs
Completude da avaliação dos riscos, aplicação das medidas recomendadas.</td></tr>
<tr><td colspan="3">Recursos necessários
• Peritos em cibersegurança
• Financiamento</td><td>Avaliação e revisão
Revisões anuais e após eventos significativos.</td></tr>
<tr><td colspan="3">Detalhes orçamentais
Despesas com recursos humanos: Peritos em cibersegurança para avaliar os riscos e desenvolver planos de ação.
Despesas em tecnologia e infraestruturas: Análise de risco e ferramentas de segurança da informação.
Custos de gestão e de funcionamento: Revisão de políticas e implementação de melhorias.
[X] Implementação
[] Manutenção
Total estimado: $35.000 - $70.000</td><td>Intervalo orçamental (valor médio)
Investimento significativo</td></tr>
<tr><td colspan="4">Observações:</td></tr>
</table>

P5. Programa de Formação Profissional e Desenvolvimento Técnico

<table>
<tr><td>Código
P5.1</td><td colspan="2">Iniciativa
Fortalecimento das capacidades defensivas através de treino e equipamento</td><td>Horizonte temporal
Ano 3-4: Reforço das capacidades e resposta a incidentes</td></tr>
<tr><td>Objetivo geral
1</td><td>Objetivo específico
1.3</td><td>Programa
5. Programa de Formação Profissional e Desenvolvimento Técnico</td><td>Entidades envolvidas
Comité de Cibersegurança</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Melhorar as capacidades defensivas no ciberespaço através da formação e da aquisição de equipamento.</td><td>Partes interessadas impactadas
Instituições públicas e privadas, CSIRT</td></tr>
<tr><td colspan="3" rowspan="2">Principais atividades
• Avaliação das necessidades de formação e de equipamento das equipas de ciberdefesa.
• Desenvolver ou atualizar programas de formação em cibersegurança.
• Aquisição de equipamento e ferramentas de segurança atualizados.
• Realização de exercícios regulares de simulação de ciberataques para testar e melhorar a preparação.</td><td>Métricas de sucesso
Redução dos incidentes, melhoria das competências do pessoal.</td></tr>
<tr><td>KPIs
Nível de capacidade do pessoal, eficiência do equipamento.</td></tr>
<tr><td colspan="3">Recursos necessários
• Formadores
• Equipamento
• Financiamento</td><td>Avaliação e revisão
Revisões anuais, ajustamentos se necessário.</td></tr>
<tr><td colspan="3">Detalhes orçamentais
Despesas com recursos humanos: formadores em cibersegurança e equipa de defesa.
Despesas em tecnologia e infraestruturas: Equipamento e ferramentas de segurança.
Despesas em gestão e operações: SOC e exercícios de simulação.
[X] Implementação
[X] Manutenção
Total estimado: $50.000 - $100.000</td><td>Intervalo orçamental (valor médio)
Alto investimento</td></tr>
<tr><td colspan="4">Observações:</td></tr>
</table>

<table>
<tr><td>Código
P5.2</td><td colspan="2">Iniciativa
Implementação de programas de formação especializada para equipas de TI em instituições públicas e privadas</td><td>Horizonte temporal
Ano 1-3: Fundações e estruturas iniciais</td></tr>
<tr><td>Objetivo geral
3</td><td>Objetivo específico
3.2</td><td>Programa
5. Programa de Formação Profissional e Desenvolvimento Técnico</td><td>Entidades envolvidas
INIC, Universidades</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Melhorar as competências em matéria de cibersegurança das equipas de TI das instituições públicas e privadas.</td><td>Partes interessadas impactadas
Instituições públicas e privadas</td></tr>
<tr><td colspan="3" rowspan="2">Principais atividades
• Desenvolver um currículo de formação em cibersegurança que responda às necessidades específicas identificadas.
• Estabelecer programas de formação contínua para atualizar as competências das equipas de TI.
• Acompanhar e avaliar a eficácia da formação através de testes práticos e avaliações periódicas.
• Adaptar os programas de formação com base no feedback e nas tendências emergentes em matéria de cibersegurança.</td><td>Métricas de sucesso
Melhoria das práticas de cibersegurança nas instituições participantes.</td></tr>
<tr><td>KPIs
Número de formandos, taxa de sucesso nos exames.</td></tr>
<tr><td colspan="3">Recursos necessários
• Formadores
• Material didático
• Infraestruturas de formação</td><td>Avaliação e revisão
Revisões anuais do currículo e da eficácia do programa.</td></tr>
<tr><td colspan="3">Detalhes orçamentais
Despesas com recursos humanos:
• Incluirá o custo de formadores especializados, desenvolvedores de currículos e pessoal de apoio.
• Desenvolvimento curricular: Especialistas para criar um programa de formação que responda a necessidades específicas de cibersegurança.
• Formadores: Profissionais que ministram a formação.
• Gestão e avaliação da formação: Pessoal para organizar programas, monitorizar a participação e avaliar a eficácia.</td><td>Intervalo orçamental (valor médio)
Alto investimento</td></tr>
</table>

Despesas em tecnologia e infraestruturas: • Será necessário algum investimento em tecnologia para apoiar a formação, especialmente se esta decorrer virtualmente. • Plataformas de aprendizagem online e software de formação: Para apoiar a realização de cursos e materiais online. • Equipamento para formação presencial: Incluindo computadores, redes e sistemas de segurança para a formação prática. **Despesas em gestão e operações:** • Inclui os custos associados à organização e ao funcionamento dos programas de formação. • Logística da formação: Se a formação for presencial, inclui o aluguer do espaço, do equipamento e do catering. • Materiais e recursos de formação: Criação e impressão de manuais, folhetos e outros materiais didáticos. • Despesas de controlo e avaliação: Inclui o custo dos testes práticos e dos instrumentos de avaliação. **[X] Implementação** **[] Manutenção** **Total estimado: $80.000 - $100.000**	
Observações: A estimativa considera a necessidade de formação especializada e relevante para as equipas de TI em São Tomé e Príncipe. A formação online pode ser uma opção eficaz e económica, especialmente tendo em conta a escala de um microestado. As parcerias com instituições de ensino ou organizações internacionais de cibersegurança podem ajudar a reduzir os custos e a melhorar a qualidade da formação. Estes valores são estimativas genéricas e devem ser ajustados com base nas necessidades específicas e nas cotações locais. É aconselhável prever uma margem para imprevistos para cobrir eventos imprevistos e variações nos custos.	

<table>
<tr><td>Código
P5.3</td><td colspan="2">Iniciativa
Estabelecer parcerias com instituições internacionais para o intercâmbio de conhecimentos e de melhores práticas no domínio da educação em matéria de cibersegurança e da luta contra o cibercrime</td><td>Horizonte temporal
Ano 4-5: Expansão e inovação tecnológica</td></tr>
<tr><td>Objetivo geral
3 e 4</td><td>Objetivo específico
3.1 e 4.2</td><td>Programa
5. Programa de Formação Profissional e Desenvolvimento Técnico</td><td>Entidades envolvidas
Comité de Cibersegurança</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Facilitar o intercâmbio de conhecimentos e de melhores práticas no domínio da cibersegurança.</td><td>Partes interessadas impactadas
Ministério dos Negócios Estrangeiros, da Cooperação e das Comunidades São Tomé Príncipe, Ministério da Justiça</td></tr>
<tr><td colspan="3">Principais atividades
• Estabelecer parcerias com instituições internacionais para o intercâmbio de conhecimentos e melhores práticas no domínio da educação em matéria de cibersegurança.
○ Identificar e contactar instituições internacionais com programas reconhecidos em matéria de cibersegurança.
○ Desenvolvimento de acordos de colaboração para o intercâmbio de conhecimentos, materiais e práticas.
○ Organização de eventos conjuntos, como conferências e webinars, para facilitar o intercâmbio de experiências.
○ Avaliação periódica da parceria para garantir que está a trazer valor e a atingir os objetivos estabelecidos.
• Estabelecer parcerias com instituições internacionais para o intercâmbio de conhecimentos e de melhores práticas no domínio da cibercriminalidade.
○ Identificar e contactar instituições internacionais com conhecimentos especializados em matéria de cibercrime.
○ Negociar e formalizar acordos de parceria para partilhar conhecimentos e melhores práticas.
○ Organizar eventos e intercâmbios que facilitem a transferência de conhecimentos.
○ Implementar programas conjuntos de formação e desenvolvimento.</td><td>Métricas de sucesso
Melhorar os currículos e as competências em matéria de cibersegurança.
KPIs
Número de parcerias estabelecidas, eficácia das práticas implementadas.</td></tr>
<tr><td colspan="3">Recursos necessários
• Equipa de coordenação
• Fundos para viagens e alojamento</td><td>Avaliação e revisão
Revisão semestral dos acordos e resultados.</td></tr>
<tr><td colspan="3">Detalhes orçamentais
Despesas com recursos humanos: Gestores de relações internacionais para estabelecer e manter parcerias.
Despesas em tecnologia e infraestruturas: Plataformas de comunicação para o intercâmbio de conhecimentos.
Custos de gestão e de funcionamento: Organização de eventos e iniciativas conjuntas.</td><td>Intervalo orçamental (valor médio)
Baixo investimento</td></tr>
</table>

[X] Implementação **[X] Manutenção** **Total estimado: $15.000 - $30.000**	
Observações:	

<table>
<tr><td>Código
P5.4</td><td colspan="2">Iniciativa
Organização de eventos anuais sobre cibersegurança para reunir investigadores, profissionais e partes interessadas para debater e trocar ideias</td><td>Horizonte temporal
Ano 3-4: Reforço das capacidades e resposta a incidentes</td></tr>
<tr><td>Objetivo geral
3</td><td>Objetivo específico
3.2</td><td>Programa
5. Programa de Formação Profissional e Desenvolvimento Técnico</td><td>Entidades envolvidas
Comité de Cibersegurança</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Criar uma plataforma de diálogo, colaboração e intercâmbio de conhecimentos entre investigadores, profissionais e partes interessadas no domínio da cibersegurança.</td><td>Partes interessadas impactadas
Universidades, entidades públicas e privadas</td></tr>
<tr><td colspan="3">Principais atividades
• Planear e organizar eventos anuais que reúnam a comunidade da cibersegurança, incluindo workshops, conferências e fóruns.
• Criar uma agenda que promova o debate aberto, a troca de ideias e a colaboração.
• Facilitar a participação de peritos internacionais para enriquecer o diálogo.
• Assegurar que os eventos produzam resultados tangíveis, tais como publicações conjuntas ou recomendações políticas.</td><td>Métricas de sucesso
Elevado nível de participação, publicações resultantes, novas colaborações estabelecidas.
KPIs
Número de participantes, número de palestras e workshops, reações dos participantes.</td></tr>
<tr><td colspan="3">Recursos necessários
• Equipa de organização
• Local do evento
• Equipamento técnico
• Altifalantes</td><td>Avaliação e revisão
Revisão pós-evento para avaliar o sucesso e as áreas a melhorar.</td></tr>
<tr><td colspan="3">Detalhes orçamentais
Despesas com recursos humanos: Organizadores de eventos e peritos em cibersegurança.
Despesas em tecnologia e infraestruturas: Espaços para conferências e equipamento técnico.
Custos de gestão e de funcionamento: Promoção do evento e gestão pós-evento.
[X] Implementação
[X] Manutenção
Total estimado: $30.000 - $60.000</td><td>Intervalo orçamental (valor médio)
Investimento moderado</td></tr>
<tr><td colspan="4">Observações:</td></tr>
</table>

<table>
<tr><td>Código
P5.5</td><td colspan="2">Iniciativa
Reforço das capacidades dos agentes judiciais em matéria de cibercrime e provas digitais</td><td>Horizonte temporal
Ano 4-5: Educação, sensibilização e normalização</td></tr>
<tr><td>Objetivo geral
4</td><td>Objetivo específico
4.2</td><td>Programa
5. Programa de Formação Profissional e Desenvolvimento Técnico</td><td>Entidades envolvidas
Ministério da Justiça</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Formar agentes judiciais na compreensão e tratamento de casos de cibercriminalidade e provas digitais</td><td>Partes interessadas impactadas
Ordem dos Advogados, Comité de Cibersegurança</td></tr>
<tr><td colspan="3">Principais atividades
• Adquirir as ferramentas de Análise Forense necessárias para a investigação da cibercriminalidade
• Adquirir formação uma vez por ano ou enviar peritos para a formação.
• Estabelecer parcerias com os serviços responsáveis pela aplicação da lei e com peritos forenses digitais.
• Organizar sessões práticas para desenvolver competências em contextos realistas.
• Compilar um conjunto de recursos e melhores práticas para utilização contínua.
• Efetuar avaliações regulares do programa para garantir que este continua a responder às necessidades atuais.</td><td>Métricas de sucesso
Melhoria da capacidade de tratamento dos casos de cibercriminalidade, redução do tempo de resolução dos casos.
KPIs
Número de agentes formados, avaliações da eficácia da formação.</td></tr>
<tr><td colspan="3">Recursos necessários
• Peritos em cibercriminalidade
• Formadores
• Financiamento de materiais e formação</td><td>Avaliação e revisão
Revisões anuais do currículo e dos métodos de ensino.</td></tr>
<tr><td colspan="3">Detalhes orçamentais
Despesas com recursos humanos: Coordenação e formadores no domínio da cibercriminalidade e da investigação forense digital.
Despesas em tecnologia e infraestruturas: Ferramentas de Análise Forense
Custos de gestão e de funcionamento: Parcerias com órgãos judiciais e avaliação de programas e formações.
[X] Implementação
[X] Manutenção
Total estimado: $80.000 - $100.000</td><td>Intervalo orçamental (valor médio)
Alto investimento</td></tr>
<tr><td colspan="4">Observações:</td></tr>
</table>

<table>
<tr><td>Código
P5.6</td><td colspan="2">Iniciativa
Criação de bolsas de estudo ou incentivos para que os estudantes se especializem em cibersegurança</td><td>Horizonte temporal
Ano 4-5: Educação, sensibilização e normalização</td></tr>
<tr><td>Objetivo geral
3</td><td>Objetivo específico
3.1</td><td>Programa
5. Programa de Formação Profissional e Desenvolvimento Técnico</td><td>Entidades envolvidas
Ministério da Educação</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Incentivar o desenvolvimento de competências especializadas no domínio da cibersegurança.</td><td>Partes interessadas impactadas
Universidades, Comité de Cibersegurança</td></tr>
<tr><td colspan="3">Principais atividades
• Definição dos critérios de elegibilidade e de seleção para as bolsas ou incentivos.
• Criação de um fundo ou de parcerias com entidades privadas para financiar bolsas de estudo.
• Promoção do programa de bolsas de estudo para atrair candidaturas de estudantes interessados.
• Acompanhar o progresso académico e profissional dos beneficiários para medir o sucesso do programa.</td><td>Métricas de sucesso
Elevado número de especialistas nos domínios da cibersegurança.
KPIs
Número de bolsas de estudo concedidas, taxa de conclusão dos cursos.</td></tr>
<tr><td colspan="3">Recursos necessários
• Fundos para bolsas de estudo.
• Comité de seleção.</td><td>Avaliação e revisão
Revisões anuais.</td></tr>
<tr><td colspan="3">Detalhes orçamentais
Despesas com recursos humanos: Administração do programa de bolsas e seleção dos candidatos.
Despesas em tecnologia e infraestruturas: Sistemas de gestão de bolsas de estudo e de acompanhamento académico.
Custos de gestão e funcionamento: Promoção do programa e parcerias com instituições de ensino.
[X] Implementação
[] Manutenção

Total estimado: $50.000 - $150.000</td><td>Intervalo orçamental (valor médio)
Alto investimento</td></tr>
<tr><td colspan="4">Observações:</td></tr>
</table>

P6. Programa de Desenvolvimento Legal e Regulamentar

<table>
<tr><td>Código
P6.1</td><td colspan="2">Iniciativa
Revisão da legislação existente em matéria de cibersegurança</td><td>Horizonte de tempo
Ano 1-3: Fundações e estruturas iniciais</td></tr>
<tr><td>Objetivo geral
4</td><td>Objetivo específico
4.1</td><td>Programa
6. Programa de desenvolvimento jurídico e regulamentar</td><td>Entidades envolvidas
Ministério da Justiça</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Reforçar o quadro jurídico da cibersegurança e proteger as crianças e os adolescentes das ameaças e dos riscos no ciberespaço.</td><td>Partes interessadas impactadas
Comité de Cibersegurança, Ministério da Educação, ONGs, organismos nacionais e internacionais que atuam no País</td></tr>
<tr><td colspan="3">Principais atividades
• Análise da legislação existente em matéria de cibersegurança.
o Efetuar uma análise completa da situação atual da legislação em vigor em matéria de cibersegurança para identificar as necessidades de atualização.
o Consultar peritos para garantir que a legislação está em conformidade com as normas internacionais.
o Organizar fóruns de discussão com o público para recolher opiniões sobre as alterações sugeridas.
o Formular e aplicar as alterações legislativas necessárias.
o Acompanhar o impacto das leis atualizada s e considerar futuras revisões, se necessário.
• Rever e atualizar a legislação existente para incluir proteções específicas para as crianças e adolescentes no ciberespaço.
o Analisar a legislação atual para identificar lacunas na proteção das crianças e adolescentes online.
o Elaborar propostas de alterações legislativas para reforçar a proteção deste grupo vulnerável.
o Consultar peritos de vários domínios para obter contribuições multidisciplinares.
o Trabalhar com os legisladores para que as alterações propostas sejam aprovadas.
o Divulgar informações sobre as novas proteções jurídicas e educar o público.</td><td>Métricas de sucesso
Aprovação efetiva dos aditamentos, redução dos crimes contra menores online.
KPIs
Número de consultas públicas realizadas, tempo de aprovação, taxas de cibercriminalidade contra menores.</td></tr>
<tr><td colspan="3">Recursos necessários
• Equipa jurídica
• Peritos em cibersegurança</td><td>Avaliação e revisão
Avaliação anual para verificar a eficácia das medidas e os ajustamentos necessários.</td></tr>
</table>

Detalhes orçamentais	Intervalo orçamental (valor médio)
Despesas com recursos humanos: Peritos externos, advogados especializados em direito tecnológico e proteção de menores. **Despesas em tecnologia e infraestruturas:** Recursos para a investigação jurídica e o desenvolvimento legislativo. **Custos de gestão e de funcionamento:** Processos de consulta pública e aplicação de novas leis. **[X] Implementação** **[] Manutenção** **Total estimado: $25.000 - $50.000**	Investimento moderado
Observações:	

<table>
<tr><td>Código
P6.2</td><td colspan="2">Iniciativa
Criação da Lei do regime Jurídico da Segurança do Ciberespaço / da Cibersegurança</td><td>Horizonte temporal
Ano 1-3: Fundações e estruturas iniciais</td></tr>
<tr><td>Objetivo geral
4</td><td>Objetivo específico
4.1</td><td>Programa
6. Programa de desenvolvimento jurídico e regulamentar</td><td>Entidades envolvidas
Ministério da Justiça</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Criação de uma lei sobre o quadro jurídico da segurança do ciberespaço</td><td>Partes interessadas impactadas
ANPDP, Comité de Cibersegurança, Operadores de Telecomunicações</td></tr>
<tr><td colspan="3">Principais atividades
• Consultar peritos internacionais para compreender os requisitos que devem ser cumpridos nesta lei (será completado no âmbito da iniciativa anterior)
• Consultar peritos de vários domínios para obter contribuições multidisciplinares.
• Elaborar um projeto de lei.</td><td>Métricas de sucesso
Aprovação efetiva das alterações, redução dos cibercrimes.

KPIs
Número de consultas públicas efetuadas, prazo de aprovação.</td></tr>
<tr><td colspan="3">Recursos necessários
• Equipa jurídica
• Peritos em cibersegurança
• Financiamento para a redação/desenvolvimento</td><td>Avaliação e revisão
Avaliação anual para verificar a eficácia das medidas e ajustamentos necessários.</td></tr>
<tr><td colspan="3">Detalhes orçamentais
Custos dos recursos humanos: Peritos externos, juristas e consultores de cibersegurança para a redação da lei.
Despesas em tecnologia e infraestruturas: Recursos para a investigação jurídica e o desenvolvimento legislativo.
Custos de gestão e de funcionamento: Evolução da legislação.

[X] Implementação
[] Manutenção

Total estimado: $40,000 - $ 60,000</td><td>Intervalo orçamental (valor médio)
Baixo investimento</td></tr>
<tr><td colspan="4">Observações:</td></tr>
</table>

<table>
<tr><td>Código
P6.3</td><td colspan="2">Iniciativa
Fortalecimento da legislação relativa à propriedade intelectual para proteger contra violações online</td><td>Horizonte temporal
Ano 4-5: Educação, sensibilização e normalização</td></tr>
<tr><td>Objetivo geral
4</td><td>Objetivo específico
4.1</td><td>Programa
6. Programa de desenvolvimento jurídico e regulamentar</td><td>Entidades envolvidas
Ministério da Justiça</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Reforçar a legislação existente em matéria de propriedade intelectual, a fim de abordar especificamente os desafios e riscos associados ao ciberespaço.</td><td>Partes interessadas impactadas
SENAPIQ-STP, Comité de Cibersegurança</td></tr>
<tr><td colspan="3">Principais atividades
• Examinar a legislação atual em matéria de propriedade intelectual para abordar questões no ciberespaço.
• Colaborar com peritos para desenvolver um quadro jurídico sólido contra as violações online.
• Colaborar com as partes interessadas para garantir a eficácia e a aplicabilidade da legislação.
• Realizar ações de sensibilização sobre as novas disposições legais.</td><td>Métricas de sucesso
Diminuição das violações da propriedade intelectual online, aplicação efetiva da lei.
KPIs
Número de casos de infração resolvidos, taxa de aprovação da legislação.</td></tr>
<tr><td colspan="3">Recursos necessários
• A equipa jurídica deve analisar a legislação atual.
• Peritos em propriedade intelectual</td><td>Avaliação e revisão
Avaliação anual para verificar a eficácia das medidas e ajustamentos necessários.</td></tr>
<tr><td colspan="3">Detalhes orçamentais
Despesas com recursos humanos: Consultores jurídicos para rever a legislação atual.
Despesas em tecnologia e infraestruturas: Instrumentos de análise jurídica.
Custos de gestão e de funcionamento: Campanhas de sensibilização.
[X] Implementação
[] Manutenção
Total estimado: $20.000 - $45.000</td><td>Intervalo orçamental (valor médio)
Investimento moderado</td></tr>
<tr><td colspan="4">Observações:</td></tr>
</table>

P7. Programa de Fortalecimento da Infraestrutura Tecnológica, Inovação, Certificação e Normalização

<table>
<tr><td>Código
P7.1</td><td colspan="2">Iniciativa (opcional)
Criação de um Programa de certificação nacional para plataformas e aplicações, centrado na segurança</td><td>Horizonte temporal
Ano 3-4: Reforço das capacidades e resposta a incidentes</td></tr>
<tr><td>Objetivo geral
5</td><td>Objetivo específico
5.2</td><td>Programa
7. Programa de Fortalecimento da Infraestrutura Tecnológica, Inovação, Certificação e Normalização</td><td>Entidades envolvidas
Comité de Cibersegurança</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Normalizar e melhorar o nível de segurança das plataformas e aplicações nacionais.</td><td>Partes interessadas impactadas
INIC, SENAPIQ</td></tr>
<tr><td colspan="3">Principais atividades
• Desenvolver um conjunto de normas de segurança para plataformas e aplicações.
• Criar um processo de certificação que avalie e verifique a conformidade com estas normas.
• Incentivar os promotores a aderirem ao programa de certificação.
• Acompanhar e atualizar as normas de certificação para garantir que continuam a ser pertinentes e eficazes.</td><td>Métricas de sucesso
Adoção generalizada da certificação no mercado.

KPIs
Número de plataformas e aplicações certificadas.</td></tr>
<tr><td colspan="3">Recursos necessários
• Equipa de avaliação
• Ferramentas de teste de segurança</td><td>Avaliação e revisão
Revisão anual do programa.</td></tr>
<tr><td colspan="3">Detalhes orçamentais
Despesas com recursos humanos: Peritos em segurança para desenvolver normas.
Despesas em tecnologia e infraestruturas: Plataforma de certificação e ferramentas de avaliação.
Custos de gestão e de funcionamento: Acompanhamento e atualização das normas.

[X] Implementação
[] Manutenção

Total estimado: $25.000 - $50.000</td><td>Intervalo orçamental (valor médio)
Investimento moderado</td></tr>
<tr><td colspan="4">Observações:</td></tr>
</table>

<table>
<tr><td>Código
P7.2</td><td colspan="2">Iniciativa (opcional)
Lançamento de uma campanha de sensibilização para a importância de um software seguro e de atualizações regulares</td><td>Horizonte temporal
Ano 4-5: Expansão e inovação tecnológica</td></tr>
<tr><td>Objetivo geral
5</td><td>Objetivo específico
5.2</td><td>Programa
7. Programa de Fortalecimento da Infraestrutura Tecnológica, Inovação, Certificação e Normalização</td><td>Entidades envolvidas
INIC</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Sensibilizar o público e as organizações para a importância de utilizar software seguro e de manter as atualizações em dia.</td><td>Partes interessadas impactadas
Universidades, Comunicação Social
Entidades públicas, privadas e ONGs</td></tr>
<tr><td colspan="3">Principais atividades
• Conceber a campanha que destaca os riscos de software inseguro e a importância de atualizações regulares.
• Criar materiais informativos e educativos para distribuir através de vários canais de comunicação.
• Planear sessões de informação e workshops para diferentes grupos-alvo, incluindo escolas, empresas e o público em geral.
• Monitorizar o impacto da campanha e ajustar as estratégias, se necessário, para melhorar a sensibilização.</td><td>Métricas de sucesso
Aumento da utilização de software seguro e atualizado.
KPIs
Número de participantes nos seminários, alcance da campanha.</td></tr>
<tr><td colspan="3">Recursos necessários
• Equipa de marketing
• Altifalantes
• Material publicitário</td><td>Avaliação e revisão
Análise semestral da eficácia da campanha.</td></tr>
<tr><td colspan="3">Detalhes orçamentais
Custos dos recursos humanos: Equipa de marketing e comunicação.
Despesas em tecnologia e infraestruturas: Material informativo e sessões de informação.
Despesas em gestão e operações: Controlo do impacto.
[X] Implementação
[] Manutenção
Total estimado: $20.000 - $40.000</td><td>Intervalo orçamental (valor médio)
Baixo investimento</td></tr>
<tr><td colspan="4">Observações:</td></tr>
</table>

<table>
<tr><td>Código
P7.3</td><td colspan="2">Iniciativa (opcional)
Criação de um centro nacional de investigação e inovação em matéria de cibersegurança</td><td>Horizonte temporal
Ano +5: Expansão e inovação tecnológica</td></tr>
<tr><td>Objetivo geral
3</td><td>Objetivo específico
3.2</td><td>Programa
7. Programa de Fortalecimento da Infraestrutura Tecnológica, Inovação, Certificação e Normalização</td><td>Entidades envolvidas
Comité de Cibersegurança</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Criar um centro nacional de investigação, desenvolvimento e inovação no domínio da cibersegurança.</td><td>Partes interessadas impactadas
Entidades públicas e privadas, Universidades</td></tr>
<tr><td colspan="3">Principais atividades
• Definir o âmbito e os objetivos do centro de investigação e inovação.
• Identificar as fontes de financiamento e os recursos necessários.
• Recrutar uma equipa multidisciplinar de peritos em cibersegurança.
• Promover a colaboração entre o centro, as universidades, a indústria e as instituições governamentais.
• Acompanhar e avaliar o impacto da investigação e das inovações desenvolvidas pelo centro.</td><td>Métricas de sucesso
Contribuição significativa para o domínio da cibersegurança.

KPIs
Número de projetos de investigação, publicações e patentes.</td></tr>
<tr><td colspan="3">Recursos necessários
• Equipa de investigação
• Equipamento
• Fundos para construção e funcionamento</td><td>Avaliação e revisão
Revisões e ajustamentos anuais com base no feedback e nos resultados.</td></tr>
<tr><td colspan="3">Detalhes orçamentais
Despesas com recursos humanos: Equipa de investigação multidisciplinar.
Despesas em tecnologia e infraestruturas: Equipamentos e laboratórios de investigação.
Custos de gestão e de funcionamento: Gestão do centro e acompanhamento dos resultados.
[X] Implementação
[] Manutenção

Total estimado: $100.000 - $200.000</td><td>Intervalo orçamental (valor médio)
Alto investimento</td></tr>
<tr><td colspan="4">Observações:</td></tr>
</table>

<table>
<tr><td>Código
P7.4</td><td colspan="2">Iniciativa
Desenvolvimento de selos de segurança ou certificações para serviços online que cumpram normas de segurança rigorosas</td><td>Horizonte de tempo
Ano 4-5: Educação, sensibilização e normalização</td></tr>
<tr><td>Objetivo geral
2 e 5</td><td>Objetivo específico
2.2 e 5.1</td><td>Programa
7. Programa de Fortalecimento da Infraestrutura Tecnológica, Inovação, Certificação e Normalização</td><td>Entidades envolvidas
INIC</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Criar e aplicar um sistema de certificação para os serviços online.</td><td>Partes interessadas impactadas
ANPDP, Comité de Cibersegurança, SENAPIQ</td></tr>
<tr><td colspan="3">Principais atividades
• Desenvolvimento de selos de segurança ou certificações para serviços online que cumpram normas de segurança rigorosas.
  ○ Definição das normas de segurança que os serviços online devem cumprir.
  ○ Desenvolvimento de um processo de avaliação e auditoria para serviços online.
  ○ Implementação de um sistema de controlo para garantir a manutenção das normas.
• Criação de um selo de garantia para o software desenvolvido no país que cumpra critérios rigorosos de segurança.
  ○ Definir os critérios de segurança rigorosos que o software deve cumprir para obter o selo de garantia.
  ○ Desenvolver um processo de avaliação e certificação de software.
  ○ Promover o selo de garantia junto dos promotores e do público.
  ○ Efetuar controlos regulares para garantir a manutenção das normas.</td><td>Métricas de sucesso
Aumento anual do número de serviços certificados, feedback positivo dos utilizadores.
KPIs
Número de serviços certificados, taxa de conformidade.</td></tr>
<tr><td colspan="3">Recursos necessários
• Peritos em cibersegurança para definir normas e avaliar serviços
• Ferramentas de auditoria</td><td>Avaliação e revisão
Revisão anual do sistema de certificação para atualizações e melhorias.</td></tr>
<tr><td colspan="3">Detalhes orçamentais
Despesas com recursos humanos: Equipa para definir normas e avaliar serviços.
Despesas em tecnologia e infraestruturas: Ferramentas de avaliação e selos de segurança.
Despesas em gestão e operações: Sistema de controlo.
[X] Implementação
[] Manutenção
Total estimado: $15.000 - $35.000</td><td>Intervalo orçamental (valor médio)
Baixo investimento</td></tr>
<tr><td colspan="4">Observações:</td></tr>
</table>

<table>
<tr><td>Código
P7.5</td><td colspan="2">Iniciativa
Desenvolvimento e promoção de competências em criptografia e controlos de segurança para infraestruturas tecnológicas</td><td>Horizonte de tempo
Ano +5: Expansão e inovação tecnológica</td></tr>
<tr><td>Objetivo geral
5</td><td>Objetivo específico
5.1</td><td>Programa
7. Programa de Fortalecimento da Infraestrutura Tecnológica, Inovação, Certificação e Normalização</td><td>Entidades envolvidas
Comité de Cibersegurança</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Capacitar profissionais de TI e de telecomunicações em técnicas criptográficas avançadas.</td><td>Partes interessadas impactadas
INIC, DITEI, Universidades, ANPDP</td></tr>
<tr><td colspan="3">Principais atividades
• Definir diretrizes claras para a implementação de criptografia e controlos de segurança nas infraestruturas tecnológicas, tanto em entidades governamentais quanto em empresas privadas.
• Promover formação especializada para profissionais de TI em criptografia avançada, segurança de infraestruturas e melhores práticas de cibersegurança.
• Atualizar continuamente as diretrizes para refletir as novas ameaças e tecnologias emergentes.</td><td>Métricas de sucesso
Adoção generalizada das orientações e melhorias nos indicadores de segurança.
KPIs
Número de entidades que aplicam as orientações, redução dos incidentes de segurança.</td></tr>
<tr><td colspan="3">Recursos necessários
• Equipa de redação técnica
• Peritos em cibersegurança</td><td>Avaliação e revisão
Revisão anual das orientações com a possibilidade de atualizações.</td></tr>
<tr><td colspan="3">Detalhes orçamentais
Despesas com recursos humanos: Formadores em criptografia e segurança.
Despesas em tecnologia e infraestruturas: Plataformas de formação e recursos educativos.
Despesas em gestão e operações: Custos associados à formação e à atualização contínua das diretrizes.
[X] Implementação
[X] Manutenção

Total estimado: $20.000 - $40.000</td><td>Intervalo orçamental (valor médio)
Baixo investimento</td></tr>
<tr><td colspan="4">Observações:</td></tr>
</table>

<table>
<tr><td>Código
P7.6</td><td colspan="2">Iniciativa
Realização de auditorias periódicas das principais infraestruturas tecnológicas para garantir a correta aplicação dos controlos de segurança e da criptografia</td><td>Horizonte temporal
Ano 3-4: Educação, sensibilização e normalização</td></tr>
<tr><td>Objetivo geral
5</td><td>Objetivo específico
5.1</td><td>Programa
7. Programa de Fortalecimento da Infraestrutura Tecnológica, Inovação, Certificação e Normalização</td><td>Entidades envolvidas
Comité de Cibersegurança, ANPDP</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Estabelecer um conjunto de orientações e normas para a aplicação de medidas de segurança e criptografia em entidades governamentais e empresas privadas.</td><td>Partes interessadas impactadas
Entidades com infraestruturas tecnológicas (exemplo: INIC, DITEI, DGRN, SMF, Banco Central, Assembleia Nacional, AGER, Alfandegas, MECC, EMAE, Operadoras, bancos, etc)</td></tr>
<tr><td colspan="3">Principais atividades
• Elaborar um plano de auditoria que identifique todas as infraestruturas tecnológicas essenciais.
• Definir a frequência das auditorias e as normas específicas de criptografia e segurança a avaliar.
• Realização de auditorias e elaboração de relatórios pormenorizados sobre os resultados.
• Recomendar melhorias e acompanhar a aplicação de ações corretivas.</td><td>Métricas de sucesso
Maior capacidade para lidar com questões de encriptação nas organizações.
KPIs
Número de profissionais formados, avaliações positivas do curso.</td></tr>
<tr><td colspan="3">Recursos necessários
• Formadores
• Material didático
• Local de formação</td><td>Avaliação e revisão
Revisão anual do curso e ajustamentos, se necessário.</td></tr>
<tr><td colspan="3">Detalhes orçamentais
Custos dos recursos humanos: Equipa de auditoria e especialistas em segurança.</td><td>Intervalo orçamental (valor médio)</td></tr>
</table>

Despesas em tecnologia e infraestruturas: Ferramentas de auditoria. **Despesas em gestão e operações:** Custos administrativos relacionados com as auditorias regulares e com a aplicação de medidas corretivas. **[X] Implementação** **[X] Manutenção** **Total estimado: $25.000 - $55.000**	Investimento moderado
Observações:	

P8. Programa de Colaboração Internacional e Desenvolvimento da Indústria

<table>
<tr><td>Código
P8.1</td><td colspan="2">Iniciativa
Promoção de colaborações internacionais através da participação em redes de pesquisa e desenvolvimento em cibersegurança</td><td>Horizonte de tempo
Ano 4-5: Educação, sensibilização e normalização</td></tr>
<tr><td>Objetivo geral
3</td><td>Objetivo específico
3.2</td><td>Programa
8. Programa de Colaboração Internacional e Desenvolvimento da Indústria</td><td>Entidades envolvidas
Comité de Cibersegurança</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Estabelecer parcerias estratégicas com entidades internacionais para promover a investigação e o desenvolvimento no domínio da cibersegurança.</td><td>Partes interessadas impactadas
Ministério dos Negócios Estrangeiros, da Cooperação e das Comunidades</td></tr>
<tr><td colspan="3">Principais atividades
• Identificar as redes internacionais relevantes que se dedicam à investigação e desenvolvimento no domínio da cibersegurança.
• Estabelecer contactos e formalizar acordos de colaboração com estas entidades.
• Participar ativamente em projetos de investigação conjuntos, contribuindo com conhecimentos e recursos locais.
• Divulgar os resultados da colaboração e aplicar as conclusões para reforçar as capacidades nacionais.</td><td>Métricas de sucesso
Realização de projetos conjuntos, publicações conjuntas, partilha de recursos.
KPIs
Número de parcerias estabelecidas, projetos conjuntos iniciados.</td></tr>
<tr><td colspan="3">Recursos necessários
• Equipa diplomática especializada
• Financiamento de viagens e alojamento
• Recursos jurídicos para a formalização de acordos</td><td>Avaliação e revisão
Revisões semestrais para ajustes e otimizações.</td></tr>
<tr><td colspan="3">Detalhes orçamentais
Despesas com recursos humanos: Gestores de projetos de colaboração.
Despesas em tecnologia e infraestruturas: Ferramentas de colaboração.
Despesas em gestão e operações: Divulgação de resultados.
[X] Implementação
[X] Manutenção

Total estimado: $20.000 - $45.000</td><td>Intervalo orçamental (valor médio)
Investimento moderado</td></tr>
<tr><td colspan="4">Observações:</td></tr>
</table>

<table>
<tr><td>Código
P8.2</td><td colspan="2">Iniciativa
Fomento de participação ativa de São Tomé e Príncipe em fóruns e conferências internacionais de cibersegurança</td><td>Horizonte temporal
Ano 3-4: Reforço das capacidades e resposta a incidentes</td></tr>
<tr><td>Objetivo geral
4</td><td>Objetivo específico
4.2</td><td>Programa
8. Programa de Colaboração Internacional e Desenvolvimento da Indústria</td><td>Entidades envolvidas
Comité de Cibersegurança</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Aumentar a visibilidade e a colaboração internacional de São Tomé e Príncipe no domínio da cibersegurança.</td><td>Partes interessadas impactadas
Ministério dos Negócios Estrangeiros, Cooperação, outras entidades públicas</td></tr>
<tr><td colspan="3">Principais atividades
• Promover a participação ativa de São Tomé e Príncipe nos fóruns e conferências internacionais sobre cibersegurança.
  ○ Fazer o levantamento dos fóruns e conferências internacionais relevantes no domínio da cibersegurança e elaborar planos anuais.
  ○ Desenvolver materiais e apresentações que destaquem as iniciativas locais no domínio da cibersegurança.
  ○ Partilhar os resultados dos eventos com a comunidade da cibersegurança
• Estabelecimento de acordos de cooperação internacional no domínio da cibersegurança para o intercâmbio de informações e de melhores práticas.
  ○ Definir áreas prioritárias de cooperação e troca de informações em matéria de cibersegurança (já existe na CPLP - Comunidade dos Países de Língua Portuguesa).
  ○ Formalizar acordos de cooperação com parceiros internacionais.
  ○ Estabelecer canais de comunicação seguros para a partilha de informações.
  ○ Avaliar periodicamente a eficácia dos acordos e efetuar os ajustamentos necessários.</td><td>Métricas de sucesso
Melhoria das relações internacionais, adoção das melhores práticas.

KPIs
Número de eventos em que se participou, acordos ou parcerias estabelecidas.</td></tr>
<tr><td colspan="3">Recursos necessários
• Pessoal especializado
• Recursos financeiros para deslocação, alojamento e participação
• Equipa de negociação
• Apoio jurídico
• Recursos financeiros</td><td>Avaliação e revisão
Avaliação anual da eficácia e ajustamentos necessários.</td></tr>
<tr><td colspan="3">Detalhes orçamentais Despesas com recursos humanos: peritos para representar o país e gestores de relações internacionais.
Despesas com tecnologia e infraestruturas: Despesas de deslocação e participação em eventos internacionais.
Custos de gestão e de funcionamento: Planeamento estratégico e acompanhamento das ações pós-evento.</td><td>Intervalo orçamental (valor médio)
Baixo investimento</td></tr>
</table>

[X] Implementação **[X] Manutenção** **Total estimado: $20.000 - $40.000**	
Observações: Este investimento poderá ser reduzido ao mínimo através de vários meios: candidaturas de oradores, participação em programas de bolsas, etc. Dirigir-se às organizações ITU, First.org e GFCE para obter patrocínio.	

<table>
<tr><td>Código
P8.3</td><td colspan="2">Iniciativa
Promoção de exercícios de simulação de cibersegurança com parceiros internacionais</td><td>Horizonte temporal
Ano +5: Expansão e inovação tecnológica</td></tr>
<tr><td>Objetivo geral
4</td><td>Objetivo específico
4.2</td><td>Programa
8. Programa de Colaboração Internacional e Desenvolvimento da Indústria</td><td>Entidades envolvidas
INIC, Comité de Cibersegurança</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Melhorar as capacidades de resposta a incidentes de cibersegurança através de exercícios de simulação com parceiros internacionais.</td><td>Partes interessadas impactadas
Ministério da Defesa Nacional, CSIRT, Ministério da Justiça e da Polícia</td></tr>
<tr><td colspan="3">Principais atividades
• Planear e organizar exercícios de simulação conjuntos com parceiros internacionais.
• Desenvolver cenários que reflitam ameaças cibernéticas reais e potenciais.
• Analisar os resultados dos exercícios para identificar áreas de melhoria na resposta a incidentes.
• Integrar as lições aprendidas nos protocolos nacionais de resposta a incidentes.</td><td>Métricas de sucesso
Melhoria das capacidades de resposta a incidentes, feedback positivo dos participantes.

KPIs
Número de simulações efetuadas, nível de preparação alcançado.</td></tr>
<tr><td colspan="3">Recursos necessários
• Equipa técnica especializada
• Infraestrutura para simulação
• Recursos financeiros</td><td>Avaliação e revisão
Análise semestral do programa e ajustamentos necessários.</td></tr>
<tr><td colspan="3">Detalhes orçamentais
Despesas com recursos humanos: Organizadores de exercícios e especialistas em segurança.
Despesas em tecnologia e infraestruturas: Cenários de simulação e ferramentas de análise.
Despesas em gestão e operações: Integração das lições aprendidas.

[X] Implementação
[] Manutenção

Total estimado: $30.000 - $60.000</td><td>Intervalo orçamental (valor médio)
Investimento moderado</td></tr>
<tr><td colspan="4">Observações:</td></tr>
</table>

<table>
<tr><td>Código
P8.4</td><td colspan="2">Iniciativa
Organização de feiras e eventos nacionais centrados no sector da cibersegurança, para atrair investimentos e promover a colaboração entre setores</td><td>Horizonte de tempo
Ano +5: Expansão e inovação tecnológica</td></tr>
<tr><td>Objetivo geral
5</td><td>Objetivo específico
5.1</td><td>Programa
8. Programa de Colaboração Internacional e Desenvolvimento da Indústria</td><td>Entidades envolvidas
Comité de Cibersegurança</td></tr>
<tr><td colspan="3">Objetivo da iniciativa
Promover o sector local da cibersegurança, atrair investimentos e facilitar a colaboração entre setores.</td><td>Partes interessadas impactadas
Entidades públicas e privadas, ONGs, Universidades</td></tr>
<tr><td colspan="3">Principais atividades
• Planear e organizar feiras e eventos que destaquem o sector local da cibersegurança.
• Criar oportunidades de ligação em rede e de colaboração entre empresas e investidores.
• Promover a inovação e os últimos desenvolvimentos no domínio da cibersegurança.
• Avaliar o impacto dos eventos na atração de investimentos e no reforço do sector.</td><td>Métricas de sucesso
Aumento do interesse no sector local da cibersegurança, aumento das parcerias e dos investimentos.

KPIs
Número de expositores, participantes, volume de negócios gerado durante os eventos.</td></tr>
<tr><td colspan="3">Recursos necessários
• Equipa de organização
• Financiamento das infraestruturas e da organização de eventos</td><td>Avaliação e revisão
Revisão pós-evento para melhorias futuras.</td></tr>
<tr><td colspan="3">Detalhes orçamentais
Despesas com recursos humanos: Equipa de organização de eventos.
Despesas com tecnologia e infraestruturas: Espaço para eventos e material promocional.
Despesas de gestão e de funcionamento: Avaliação do impacto.
[X] Implementação
[X] Manutenção

Total estimado: $40.000 - $80.000</td><td>Intervalo orçamental (valor médio)
Investimento significativo</td></tr>
<tr><td colspan="4">Observações:</td></tr>
</table>

IV. Roteiro Estratégico do Plano de ação

Este capítulo apresenta o "Plano de Ação para a Cibersegurança", um roteiro estratégico concebido para orientar São Tomé e Príncipe na construção de um ecossistema digital seguro e resiliente nos próximos cinco anos. Este plano representa o compromisso do país em garantir a integridade, a confidencialidade e a disponibilidade dos ativos digitais e das infraestruturas críticas, bem como em capacitar os cidadãos e as entidades para navegarem em segurança no ciberespaço.

O plano tem em conta os diferentes programas e iniciativas definidos no contexto da Estratégia Nacional de Cibersegurança e, para cada iniciativa, foram definidos objetivos específicos e indicadores-chave de desempenho (KPI) para garantir uma execução eficaz e quantificável.

Reconhece-se que a cibersegurança é um domínio em constante evolução, que exige uma resposta adaptável e progressiva. Assim, este plano não se limita a uma série de ações pré-determinadas, mas pretende ser um guia estratégico que deve ser revisto e ajustado periodicamente para responder aos desafios e necessidades emergentes. Esta abordagem flexível garantirá que São Tomé e Príncipe esteja sempre um passo à frente na identificação, proteção, deteção, resposta e recuperação de ciber-ameaças.

Por último, o sucesso deste plano está diretamente ligado ao empenho e à colaboração entre o Governo de São Tomé e Príncipe, o sector privado, outras instituições, o meio académico e os cidadãos. A união de esforços permitirá criar um ciberespaço seguro para São Tomé e Príncipe, protegendo não só as infraestruturas tecnológicas, mas também o bem-estar e a privacidade de cada cidadão.

	Ano 1-3: Fundações e estruturas iniciais	**Ano 3-4: Reforço das capacidades e resposta a incidentes**	**Ano 4-5: Educação, sensibilização e normalização**	**Ano +5: Expansão e inovação tecnológica**
Estimativa de investimento por horizonte temporal (Valores médios)	**$766,000.00**	**$716,000.00**	**$405,000.00**	**$386,500.00**
Programas				
1. Programa de Governação e Coordenação da Cibersegurança	P1.1: Criação do Comité de Liderança e Coordenação da Cibersegurança P1.2: Promoção de colaborações interdepartamentais e intersectoriais			
2. Programa de Gestão de Ativos e Operadores Críticos	P2.1: Elaboração de regulamentação em matéria de cibersegurança para os ativos e operadores críticos P2.2: Identificação de ativos e operadores críticos	P2.3: Implementação de protocolos entre as CSIRT e as infraestruturas críticas		

	Ano 1-3: Fundações e estruturas iniciais	Ano 3-4: Reforço das capacidades e resposta a incidentes	Ano 4-5: Educação, sensibilização e normalização	Ano +5: Expansão e inovação tecnológica
3. Programa de educação e sensibilização para a cibersegurança	P3.6: Campanhas de sensibilização sobre a proteção dos dados pessoais P3.7: Avaliação e documentação das necessidades nacionais de competências em matéria de cibersegurança	P3.1: Criação de programas de ensino para promover a literacia digital e a cibersegurança nas escolas P3.2: Organizar regularmente seminários e workshops sobre as melhores práticas em matéria de cibersegurança P3.3: Parceria para eventos de sensibilização para a literacia mediática P3.8: Guia de boas práticas de cibersegurança para entidades públicas e privadas	P3.4: Realizar estudos anuais sobre o nível de confiança dos cidadãos nos serviços online P3.5: Criação de uma plataforma de verificação de factos online para combater a desinformação	
4. Programa de resposta a incidentes e gestão de riscos	P4.1: Criação e reforço do CSIRT-STP	P4.3: Protocolo de avaliação de riscos para infraestruturas de telecomunicações (mudar de comunicação para telecomunicações)	P4.2: Análise exaustiva dos ciber-riscos na defesa nacional	
5. Programa de Formação Profissional e Desenvolvimento Técnico	P5.2: Programas de formação especializados para equipas de TI	P5.1: Formação e equipamento de defesa P5.4: Organização de eventos anuais sobre cibersegurança para reunir investigadores, profissionais e partes interessadas para debater e trocar ideias	P5.5: Formação de agentes judiciais em matéria de cibercrime P5.6: Criação de bolsas de estudo ou incentivos para que os estudantes se especializem em cibersegurança	P5.3: Estabelecer parcerias com instituições internacionais para o intercâmbio de conhecimentos e melhores práticas no domínio da educação em matéria de cibersegurança e da luta contra o cibercrime
6. Programa de desenvolvimento jurídico e regulamentar	P6.1: Revisão e atualização da legislação existente relacionada com a cibersegurança P6.2: Criação da Lei do regime Jurídico da Segurança do Ciberespaço / da Cibersegurança		P6.3: Fortalecimento da legislação relativa à propriedade intelectual para proteger contra violações online	

	Ano 1-3: Fundações e estruturas iniciais	Ano 3-4: Reforço das capacidades e resposta a incidentes	Ano 4-5: Educação, sensibilização e normalização	Ano +5: Expansão e inovação tecnológica
7. Programa de Fortalecimento da Infraestrutura Tecnológica, Inovação, Certificação e Normalização		P7.1: Programa de certificação nacional para plataformas e aplicações	P7.2: Campanha de sensibilização para software seguro P7.4: Desenvolvimento de selos de segurança ou certificações para serviços online que cumpram normas de segurança rigorosas	P7.3: Centro nacional de investigação e inovação em cibersegurança P7.5: Competências em criptografia e controlos de segurança P7.6: Auditorias periódicas das infraestruturas tecnológicas
8. Programa de Colaboração Internacional e Desenvolvimento da Indústria		P8.2: Participação internacional de São Tomé e Príncipe na cibersegurança	P8.1: Colaborações internacionais em redes de investigação e desenvolvimento	P8.3: Exercícios de simulação com parceiros internacionais P8.4: Feiras e eventos nacionais no sector da cibersegurança