Relatório de Modelos de Governança

Estudo de viabilidade sobre Modelos de Governança de Cibersegurança e Proteção de Dados, Manual de Operações, bem como Apoio à Capacitação em Crime Cibernético na Guiné-Bissau

Para: Programa Regional de Integração Digital da África Ocidental Guiné-Bissau (WARDIP)

Feito por: BS Innovations e GoSecure 05/2024

RFP No: WARDIP – C – 15 - 2023

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

Índice

Lista de figuras

Lista de figuras

Definição de acrónimos

BSI	BS Innovations
WARDIP	Programa Regional de Integração Digital da África Ocidental
DGTED	Instituto de Modernização Administrativa Direção Geral de Telecomunicações e economia digital
ITMA	Instituto Tecnológico para a Modernização Administrativa
CEDEAO	Comunidade Económica dos Estados da África Ocidental
UEMOA	União Económica e Monetária da África Ocidental
UA	União Africana
CPLP	Comunidade dos Países de Língua Portuguesa
LGPD	Lei Geral de Proteção de Dados Pessoais
SOC	Centro de Operações de Segurança
CII	infraestrutura s críticas da informação
IR	Resposta a incidentes
ASIN	Agência dos Sistemas de Informação e de Numeração
bjCSIRT	Equipa de resposta a incidentes de segurança informática do Benim
APDP	Autoridade de Proteção de Dados de Carácter Pessoal
SOP	Procedimentos Operacionais Normalizados
TIC	Tecnologias da Informação e da Comunicação
KPIs	Indicadores-chave de desempenho
INACOM	Instituto Nacional de Comunicações
NCS	Secretariado Nacional de Cibersegurança
CERT	Equipa de Resposta a Emergências Informáticas
CGI	Imagens geradas por computador
GCI	Índice Mundial de Cibersegurança
LGPD	Lei Geral sobre a Proteção de Dados
NCSI	Índice Nacional de Cibersegurança
OEA	Organização dos Estados Americanos
UIT	União Internacional das Telecomunicações
ANSI	Agência Nacional para a Sociedade da Informação
ANSSI	Agência Nacional para a Segurança dos Sistemas de Informação
GDPR	Regulamento Geral sobre a Proteção de Dados
CA	Autoridade das Comunicações
ANACOM	Autoridade Nacional de Comunicações
CIRT	Equipa de Resposta a Incidentes Informáticos
ANRT	Agência Nacional de Regulação das Telecomunicações
ARN	Agência Nacional de Regulação
OCDE	Organização para a Cooperação e Desenvolvimento Económico
ISO	Organização Internacional de Normalização
SGSI	Sistema de Gestão da Segurança da Informação
NIST	Instituto Nacional de Normas e Tecnologia
GTM	Guiné Telecom
CSF	Quadro de Cibersegurança
RBAC	Controlo de acesso baseado em funções

EAGB	Eletricidade e Águas da Guiné-Bissau
CGB	Correios da Guiné-Bissau
MFA	Autenticação multi-fator
INCIBE	Instituto Nacional de Cibersegurança de Espanha
CISO	Diretor de Segurança da Informação
CIO	Diretor da Informação
CRO	Organismos de Investigação Contratados
LOB	Linha de negócios
CNCS	Centro Nacional de Cibersegurança

I. SUMÁRIO EXECUTIVO

Com a evolução das tecnologias, o mundo enfrenta crescentes ameaças à segurança no mundo digital. O crescimento exponencial do número de ciberataques, que tem sido acompanhado por um grau de complexidade e sofisticação progressivos, representam sérias ameaças a infraestruturas críticas e serviços na nuvem.

Uma governança eficaz garante a conformidade, a responsabilização e a proteção dos sistemas e dos dados pessoais que tratam, quer sejam armazenados, processados ou transmitidos. Um modelo de governança robusto facilita a execução harmoniosa das responsabilidades em todos os níveis do país, do seu governo e de todas as organizações, capacitando e fortalecendo a sua estrutura existente.

Este estudo de viabilidade investiga e analisa os benefícios globais da governança, abordando especificamente as complexidades da cibersegurança e da privacidade de dados no âmbito de um quadro de governança mais amplo. Partindo de bases de conhecimento global, o estudo apresenta vários modelos de governança normalmente distinguidos no discurso académico. No entanto, reconhecendo que nem todas as opções teóricas são adequadas a todos os contextos, o estudo avalia e discute meticulosamente os modelos mais pertinentes. Em última análise, recomenda uma abordagem adaptada para implementação na Guiné-Bissau, considerando as necessidades e dinâmicas únicas do governo e dos seus constituintes.

A. Visão geral dos objetivos

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

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

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

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

A fase inicial do projeto, Etapa 1, envolve a realização de um estudo de viabilidade dos modelos de governança da cibersegurança e da proteção de dados. Este estudo começará com uma exploração das bases de conhecimentos mundiais sobre modelos de governança. Posteriormente, será identificada uma seleção de modelos considerados mais adequados para aplicação nacional A partir deste subconjunto selecionado, o grupo de

trabalho recomendará o modelo de governança mais adequado às circunstâncias e aspirações únicas da Guiné-Bissau.
O modelo de governança a ser recomendado baseia-se-á em estudos comparativos e nas realidades da Guiné-Bissau, tendo em conta os desafios internos e externos. O modelo foi adaptado ao contexto específico da Guiné-Bissau e a sua estrutura foi feita sob medida.

B. Definição de governança de cibersegurança e de proteção de dados

No panorama em rápida evolução das tecnologias da informação e de comunicação, a cibersegurança e a proteção de dados tornaram-se questões críticas para empresas, governos e indivíduos. Compreender estes conceitos, juntamente com os modelos de governança que os supervisionam é essencial para uma gestão eficaz dos riscos e para a conformidade regulamentar. Este estudo fornece uma definição estruturada de cibersegurança, proteção de dados, modelos de governança e explora as diferenças entre cibersegurança e proteção de dados.

Cibersegurança

Definição:
A cibersegurança engloba as práticas, tecnologias e processos concebidos para proteger os sistemas informáticos, redes, programas e dados contra ataques, danos ou acesso não autorizado. Inclui a segurança da informação, a segurança da rede, a segurança das aplicações e a segurança do sistema.

Objetivos:
Confidencialidade: Garantir que as informações sejam acessíveis apenas a pessoas autorizadas.
Integridade: Garantir que a informação e os sistemas só podem ser alterados de forma autorizada e exacta.
Disponibilidade: Assegurar que a informação e os sistemas estão acessíveis aos utilizadores autorizados quando necessário.
Meios:
Tecnológicos: Firewalls, sistemas de deteção de intrusão, criptografia, sistemas de antivírus, etc.
Organizacional: Políticas de segurança, formação, auditorias de segurança, etc.
Humanos: sensibilização dos utilizadores, formação e reforço de capacidade das equipas de segurança, etc.

Proteção de dados

Definição:
A proteção de dados ou proteção de dados pessoais engloba as medidas e técnicas destinadas a garantir que os dados pessoais dos indivíduos são recolhidos, processados e armazenados de forma segura e em conformidade com as leis e regulamentos. Dá ênfase à privacidade e aos direitos dos indivíduos relativamente aos seus dados pessoais.

Objetivos:
Privacidade: Garantir que os dados pessoais são tratados de forma a respeitar a privacidade das pessoas.
Transparência: Garantir que as pessoas são informadas sobre a forma como os seus dados são utilizados.
Controlo: Permitir que as pessoas controlem a utilização dos seus dados pessoais.
Meios:
Legislativas: Leis e regulamentos, como o GDPR (Regulamento Geral de Proteção de Dados) na Europa, a CCPA (Lei de Privacidade do Consumidor da Califórnia) na Califórnia, etc.
Técnica: Anonimização, pseudonimização, encriptação, etc.
Organizacional: Políticas de privacidade, consentimento informado, gestão dos direitos dos indivíduos, etc.

Modelos de governança

Definição:
Os modelos de governança em matéria de cibersegurança e proteção de dados são quadros que definem as estruturas, responsabilidades, políticas e procedimentos necessários para gerir e controlar os riscos relacionados com a segurança da informação e a proteção de dados. Garantem a conformidade com a regulamentação e as melhores práticas.

Com base no livro Rational Cybersecurity for Business (Cibersegurança Racional para Empresas), as principais funções da governança são:
Criar um estatuto ou mandato para o programa de

segurança: Definir "segurança", "cibersegurança" ou "proteção de dados" para uma organização em termos da sua missão, governança, estrutura de comunicação e princípios operacionais. Especificar formalmente que organizações ou funções dentro da empresa têm autoridade sobre a estratégia, política, projetos, orçamentos, comités e operações de segurança.

Gerir, controlar e comunicar o risco: Identificar, acompanhar, gerir e comunicar os riscos de informação ao nível executivo ou à autoridade designada, juntamente com outros riscos empresariais ou estatais. Assegurar que a estratégia de segurança e a carteira de projetos estão alinhadas com os riscos empresariais ou estatais.

Coordenar Projetos de segurança e gerir problemas: Organizar, patrocinar e presidir a fóruns que envolvam várias partes interessadas, incluindo o Diretor de Segurança da Informação (CISO) ou equivalente, o Diretor da Informação (CIO) ou equivalente, os Organismos de Investigação Contratados (CRO) ou equivalente, o chefe de auditoria ou equivalente e os executivos dos sectores Linha de negócios (LOB) ou estratégicos essenciais para o êxito dos Projetos e processos. Mediar as questões que são encaminhadas para o nível de governança da cibersegurança do Estado.

Gerir a política de segurança: Trabalhar com o Estado, as entidades críticas, os recursos-chave de TI e outras áreas para desenvolver políticas, normas, processos e procedimentos de segurança, obter acordo e adoção formal e gerir o ciclo de vida das políticas.

Atribuir orçamentos e recursos de segurança: Decidir como pagar as despesas operacionais e de capital do programa de segurança. Atribuir fundos e recursos à(s) organização(ões) de segurança e a outros grupos responsáveis pela execução de Projetos ou serviços de segurança. Aprovar os orçamentos propostos e as principais despesas.

Diferenças entre cibersegurança e proteção de dados

Embora a cibersegurança e a proteção de dados estejam estreitamente relacionadas e se sobreponham frequentemente, diferem nos seus objetivos e âmbito.

Cibersegurança:

- **Âmbito:** Proteção de sistemas informáticos, redes, aplicações e dados contra ameaças e ataques.
- **Objetivos principais:** Confidencialidade, integridade e disponibilidade de informações e sistemas.

Proteção de dados:

- **Âmbito de aplicação:** Proteção dos dados pessoais das pessoas, gestão dos direitos das pessoas sobre os seus dados.
- **Objetivos principais:** Privacidade, respeito pela privacidade, transparência e controlo individual sobre os seus dados.

A cibersegurança e a proteção de dados são disciplinas complementares, mas distintas, essenciais para proteger a informação num ambiente digital cada vez mais complexo. Embora ambas sejam cruciais para preservar a confiança e a integridade dos dados, a proteção de dados alarga o seu âmbito para abranger o aspeto mais vasto das preocupações com a privacidade e a conformidade. Os modelos de governança desempenham um papel crucial, fornecendo as estruturas e os procedimentos necessários para gerir eficazmente estas áreas e garantir a conformidade com os regulamentos aplicáveis. Compreender as diferenças entre a cibersegurança e a proteção de dados permite uma abordagem mais abrangente e integrada à gestão do risco e à proteção da informação.

A combinação da governança da cibersegurança e da proteção de dados num único modelo pode oferecer vantagens significativas. Esta abordagem integrada simplifica os processos, melhora a conformidade e reforça a proteção global da informação. Eis os principais benefícios de um modelo de governança unificado:

- Aumento da eficiência operacional
- Conformidade regulamentar melhorada
- Redução de custos
- Melhoria da gestão dos riscos
- Cultura de segurança reforçada[1]

A abordagem integrada permite que as organizações protejam melhor as suas informações e respondam mais eficazmente aos desafios da segurança digital. No presente relatório serão fornecidos mais pormenores sobre os modelos de governança.

[1]**Source:** https://link.springer.com/article/10.1007/s10207-021-00534-3

II. MODELOS DE GOVERNANÇA DA CIBERSEGURANÇA

Os modelos de governança existem numa variedade de formas, cada um com o seu próprio conjunto de vantagens e desvantagens. Compreender estes modelos é crucial para determinar a abordagem mais eficaz para uma organização.

As vantagens de um modelo de governança bem escolhido incluem uma maior responsabilização, melhores processos de tomada de decisão e um melhor alinhamento de interesses entre as partes interessadas. Por outro lado, as desvantagens podem envolver complexidade, tomada de decisões mais lenta devido à burocracia e potenciais conflitos entre as estruturas de governança e a cultura organizacional.

Antes de selecionar um modelo de governança, é essencial compreender completamente a estrutura, os objetivos, a cultura e o ambiente regulamentar da organização. Um único modelo pode ser suficiente para alguns, no entanto, outros podem beneficiar de uma abordagem híbrida que combine elementos de vários modelos. Esta solução personalizada pode fornecer a flexibilidade necessária para atender às necessidades organizacionais específicas, aproveitando os pontos fortes de várias estruturas de governança.

Em última análise, a escolha do modelo de governança ou a combinação dos mesmos deve facilitar a capacidade da organização para cumprir a sua missão, aderir aos requisitos de conformidade e atingir os objetivos estratégicos.

Iremos explorar os três principais modelos de governança:

- Centralizado também chamado de modelo de governança hierárquico
- Modelo de governança descentralizado
- Híbrido também designado por modelo de governança matricial

Qualquer um dos três modelos pode funcionar se for aplicado da forma correta no local certo. No entanto, em alguns casos, as estruturas de governança da segurança resultam mais do acaso e de personalidades do que de um pensamento organizacional bem pensado e, por isso, podem não estar devidamente alinhadas com o negócio ou com a cultura do Estado.

Figura 1: As três principais estruturas de governança[2]

Para além dos três principais modelos de governança, existem outros que não serão detalhados nas principais secções do presente relatório por serem demasiado complexos para serem aplicados e mantidos a nível estatal.

- Modelo de governança baseado em comités
- Modelo de governança colaborativa[3]
- Modelo de governança da rede
- Modelo de governança adaptativo
- Modelo de governança integrado

Alguns pormenores desses modelos constam dos anexos do presente relatório.

[2] https://link.springer.com/chapter/10.1007/978-1-4842-5952-8_3#Sec6

[3] https://www.pdx.edu/policy-consensus-center/sites/policyconsensuscenter.web.wdt.pdx.edu/files/2020-06/1-Building-a-Collaborative-Governance--Framework.pdf

A. Modelo de Governança Centralizado ou Hierárquico

O modelo de governança centralizado é uma forma tradicional de estrutura organizacional que é frequentemente visualizada como uma pirâmide. No topo desta pirâmide está o mais alto nível de autoridade, normalmente ocupado por uma função de gestão de alto nível. Este indivíduo ou grupo detém o maior poder e toma as decisões mais importantes para a organização.

Abaixo do nível superior, existem níveis sucessivos de gestão. Cada nível tem o seu próprio conjunto de responsabilidades e autoridade, que diminui à medida que se desce na pirâmide. Estes níveis podem incluir a gestão de topo, a gestão intermédia e a gestão inferior, cada uma supervisionando uma parte específica das operações da organização.

Na base da pirâmide está a força de trabalho geral. Estes são os indivíduos que executam as tarefas quotidianas da organização. Apesar de estarem na base da pirâmide, o seu papel é crucial para o funcionamento da organização. O modelo é caracterizado por linhas claras de autoridade e uma cadeia de comando bem definida, assegurando que todos conhecem o seu papel e responsabilidades dentro da organização. Esta estrutura permite uma tomada de decisões eficiente e um fluxo de comunicação de cima para baixo.

No caso de um governo, o modelo centralizado significaria ter uma única agência central de cibersegurança e proteção de dados. Esta agência define políticas e procedimentos para todos os ministérios e agências. É também responsável pela gestão de todos os incidentes.

Vantagens do modelo de governança centralizado ou hierárquico

Linhas claras de autoridade:
Na estrutura centralizada, cada nível tem deveres e obrigações distintos. Esta explicitação proporciona uma compreensão clara de quem detém as rédeas e de quem é responsável pela tomada de decisões. É esta clareza que garante que todos dentro da organização estão cientes das suas funções e das funções dos outros, promovendo um sentido de ordem e estrutura.

A autoridade para tomar decisões não é distribuída uniformemente, mas sim em cascata, dos níveis mais altos da hierarquia para baixo. Isto cria uma cadeia de comando bem estabelecida, em que as instruções e decisões fluem dos níveis superiores para os inferiores. Esta estrutura garante que todas as decisões tomadas estão alinhadas com os objetivos e estratégias globais da organização.

Eficiência na tomada de decisões:
A abordagem descendente numa estrutura hierárquica permite acelerar a tomada de decisões. Aqueles que detêm os níveis mais elevados de autoridade podem tomar decisões rapidamente, assegurando que a organização possa se adaptar e responder às circunstâncias em mudança de forma eficiente.

Em situações em que é necessária uma ação imediata, este processo de tomada de decisão simplificado revela-se altamente benéfico. Facilita respostas rápidas, permitindo que a organização resolva problemas ou aproveite oportunidades sem atrasos desnecessários. Esta eficiência é uma das principais vantagens de uma abordagem top-down numa estrutura hierárquica.

Percurso profissional definido:
Dentro da organização, os colaboradores têm uma compreensão lúcida da sua progressão na carreira. Estão conscientes do caminho que precisam percorrer no seu percurso profissional dentro da organização, o que traz clareza e objetivo às suas funções.

As vias de promoção dentro da organização estão claramente delineadas. Esta clareza não só dá aos colaboradores um sentido de orientação, como também serve de fonte de motivação. Conhecer os passos para a progressão pode inspirar os empregados a lutar pela excelência e a atingir os seus objetivos de carreira.

Fidelidade ao departamento:
É comum os empregados nutrirem um profundo sentimento de lealdade para com os seus respetivos departa-

mentos dentro da organização. Esta lealdade traduz-se muitas vezes numa forte ligação entre os membros da equipa, reforçando o espírito de trabalho em equipa dentro destas unidades.

A lealdade que os empregados sentem pelos seus departamentos pode aumentar significativamente a colaboração dentro do departamento. Quando os funcionários são leais à sua equipa, é mais provável que trabalhem em conjunto de forma eficaz, aumentando a produtividade geral e a harmonia dentro da unidade. Este sentimento de lealdade e camaradagem é um ativo valioso em qualquer organização.

Desvantagens do modelo de governança centralizado ou hierárquico

Falta de flexibilidade:
A estrutura inflexível inerente a uma organização hierárquica pode colocar desafios à adaptabilidade. Quando o ambiente empresarial ou estatal sofre alterações, esta rigidez pode atuar como uma barreira, dificultando o ajustamento e a evolução da organização em conformidade.

Além disso, a natureza hierárquica da organização pode potencialmente travar a inovação. A abordagem descendente e a clara definição de funções e responsabilidades podem limitar o pensamento criativo e as ideias novas, que são a força vital da inovação. Isto pode resultar num ambiente menos inovador, afetando potencialmente a competitividade da organização a longo prazo.

- **Participação limitada:**

Numa estrutura hierárquica, os indivíduos ou grupos dos níveis inferiores podem ter uma participação mínima no processo de tomada de decisões. A concentração do poder de decisão nos níveis superiores pode muitas vezes fazer com que os que estão na base sintam que o seu contributo não é valorizado ou considerado.
Esta falta de envolvimento em decisões-chave pode resultar num sentimento de desinteresse entre os empregados. Quando os empregados sentem que as suas vozes não são ouvidas ou que as suas opiniões não são valorizadas, isso pode levar à insatisfação e a uma diminuição do moral. Isto pode ter um impacto potencial na sua produtividade e no seu empenhamento na organização.

- **Potencial para a burocracia:**

A existência de vários níveis de gestão pode levar ao desenvolvimento de procedimentos burocráticos. Esta estrutura, embora possa fornecer linhas claras de autoridade e responsabilidade, pode também introduzir um nível de complexidade que pode não ser necessário para as operações da organização.
Por outro lado, a presença de burocracia, um subproduto comum da burocracia, pode impedir a rapidez da tomada de decisões. Este facto pode levar a um aumento dos custos operacionais, uma vez que se gasta tempo e recursos para ultrapassar estes obstáculos administrativos. Isto afeta não só a eficiência da organização, mas também a sua rentabilidade.

- **Risco de mentalidade de silo:**

Os departamentos podem tornar-se insulares, concentrando-se apenas nos seus próprios objetivos e não nos objetivos gerais da organização.

Essencialmente, embora o modelo centralizado possa proporcionar estabilidade e clareza, também pode dificultar a adaptabilidade e a inclusão. As organizações que considerem este modelo devem ponderar cuidadosamente estes fatores para determinar se está de acordo com os seus objetivos estratégicos e necessidades operacionais.

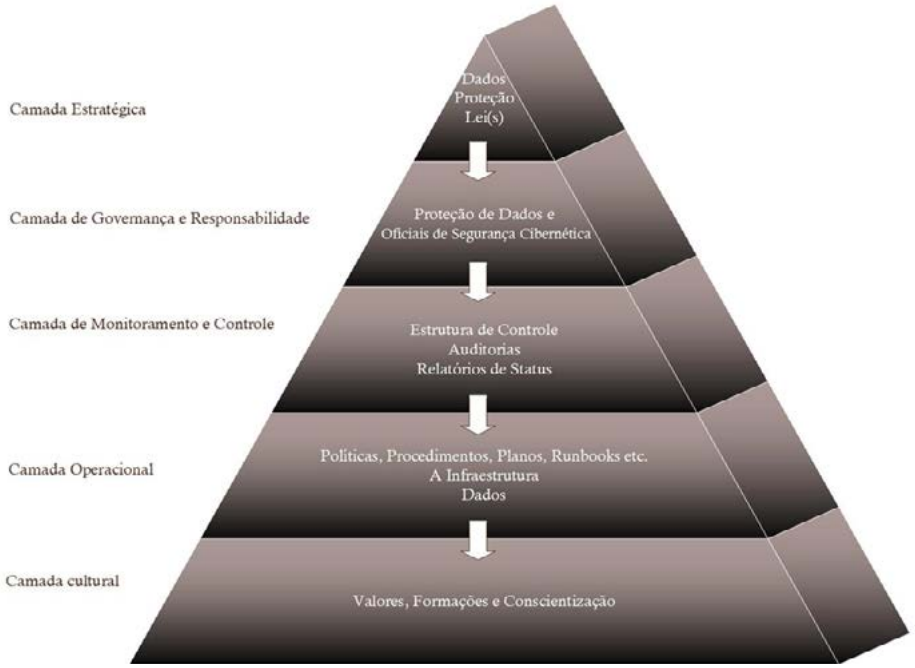

Figura 2: Diagrama em pirâmide do modelo centralizado ou hierárquico

O modelo tradicional de governança é caracterizado por uma abordagem descendente, em que a autoridade e o poder de decisão estão concentrados nos níveis superiores de gestão. Este modelo é predominante nas organizações que têm um controlo centralizado e estruturas formalizadas. A cadeia de comando é clara e as decisões fluem do topo para os níveis inferiores da organização.

A governança hierárquica é outro aspeto deste modelo, que se distingue pela aplicação direta da autoridade do Estado a populações-alvo. Esta forma de governança entra em ação quando os Estados impõem regras ou normas de comportamento a outros actores. Estas regras e normas são aplicadas através de um sistema de sanções e recompensas.

O objetivo final da governança centralizada é atingir objetivos colectivos. O Estado usa a sua autoridade para regular o comportamento e garantir o cumprimento das suas regras e normas. Este modelo, embora tradicional, continua a ser comum em muitas organizações e Estados devido à sua estrutura clara e funções definidas.

Figura 3: Ilustração simples do modelo centralizado ou hierárquico

Legenda: A caixa verde representa as entidades que serão afetadas pelas regras provenientes do topo da pirâmide. Enquanto a caixa laranja representa a entidade que toma as decisões.

No contexto da instabilidade política da Guiné-Bissau, um modelo de governança centralizado para a cibersegurança e proteção de dados oferece vantagens cruciais ao permitir uma coordenação eficaz entre diferentes entidades governamentais e setores críticos, garantindo assim uma resposta rápida e consistente às ciberameaças. No entanto, a centralização pode levar a uma concentração excessiva de poder e recursos, um ponto único de falha, tornando o sistema vulnerável a abusos e corrupção, especialmente num ambiente em que as mudanças de regime podem ser frequentes devido à instabilidade política. Além disso, a rigidez de uma estrutura centralizada pode atrasar a tomada de decisões e a adaptação a novas ameaças, enquanto a falta de competências e recursos locais pode limitar a eficácia da implementação.

B. Modelo de governança descentralizada

Um modelo de governança descentralizada é um sistema em que os poderes de tomada de decisão são distribuídos longe de uma autoridade central. Este modelo é frequentemente utilizado em organizações ou comunidades para dar poder às unidades individuais, permitindo uma tomada de decisões mais localizada e reactiva. Neste modelo, cada unidade funciona de forma semi-independente, tomando decisões com base nas suas necessidades e circunstâncias únicas. Isto pode levar a uma organização mais flexível e adaptável que pode responder rapidamente às mudanças no seu ambiente.

O modelo de governança descentralizada não se limita a distribuir o poder, trata-se também de promover um sentido de propriedade e responsabilidade entre as unidades individuais. Ao dar às unidades a autonomia para tomarem as suas próprias decisões, elas tornam-se mais interessadas nos resultados dessas decisões. Isto pode levar a uma maior motivação e envolvimento entre os membros da organização ou comunidade.
No caso de um governo, o modelo descentralizado significaria ter agências de cibersegurança ao nível de cada ministério ou agência. Estas agências serão completamente autónomas e não receberão directivas de lado nenhum.

Vantagens da governança descentralizada

- **Maior capacidade de resposta:**

Num modelo de governança descentralizada, as unidades locais têm autonomia para tomar decisões que estão mais em sintonia com as suas necessidades e circunstâncias específicas. Isto significa que podem responder mais rápida e eficazmente a questões locais ou a mudanças no seu ambiente. Não estão vinculadas a uma política de tamanho único ditada por uma autoridade central, que pode não compreender ou apreciar totalmente as nuances da sua situação específica.

- **Inovação reforçada:**

As unidades descentralizadas têm a liberdade de experimentar e inovar. Podem testar novas ideias e abordagens no seu contexto local, aprender com os seus sucessos e fracassos e adaptar-se mais rapidamente a novos desafios ou oportunidades. Isto pode levar a uma organização mais inovadora e dinâmica, capaz de encontrar novas soluções para problemas complexos.

- **Melhoria da eficiência:**

As decisões tomadas mais perto do ponto de ação podem ser implementadas mais rapidamente, conduzindo a uma maior eficiência operacional. Quando a tomada de decisões é descentralizada, há menos necessidade de a informação fluir para cima e para baixo na hierarquia, reduzindo os atrasos e melhorando a velocidade de execução. Além disso, as decisões são tomadas por quem tem o melhor conhecimento da situação, o que conduz a resultados mais eficazes e eficientes.

- **Capacitação:**

A governança descentralizada pode levar a um maior envolvimento e motivação entre os membros, uma vez que estes têm uma influência direta nas decisões que os afetam. Esta sensação de poder pode melhorar a moral, aumentar o compromisso com os objetivos da organização e aumentar a produtividade.

Desvantagens da governança descentralizada

- **Risco de incoerência:**

Sem um forte controlo central, pode haver uma falta de uniformidade nas decisões das diferentes unidades. Isto pode levar a potenciais conflitos, ineficiências e confusão. Também pode dificultar a garantia de que todas as unidades estão alinhadas com a estratégia e os objetivos gerais da organização.

- **Coordenação complexa:**

A coordenação de atividades e políticas entre unidades descentralizadas pode ser um desafio. Pode exigir recursos adicionais para gerir a comunicação e a coordenação entre as unidades. Existe também um risco de duplicação de esforços, uma vez que diferentes unidades podem empreender iniciativas semelhantes de forma independente.

- **Potencial de má afetação de recursos:**

Numa estrutura descentralizada, várias unidades dentro da organização podem encontrar-se em competição pelos mesmos recursos. Esta concorrência pode potencialmente levar a uma má afetação de recursos, em que algumas unidades podem receber mais do que precisam enquanto outras ficam a faltar. Além disso, existe o risco de duplicação de esforços, em que várias unidades realizam iniciativas semelhantes de forma independente, levando a uma repetição desnecessária e ao desperdício de recursos.

Sem uma autoridade central para gerir e supervisionar a distribuição de recursos, existe o risco de estes recursos não serem utilizados da forma mais eficiente ou eficaz. A ausência de um controlo central pode fazer com que os recursos sejam atribuídos a áreas onde não são tão necessários, enquanto outras áreas que poderiam beneficiar mais desses recursos são ignoradas. Esta falta de controlo pode ter um impacto potencial na produtividade e eficácia globais da organização.

- **Dificuldade em estabelecer objetivos comuns:**

Alinhar os diversos objetivos das várias unidades com a estratégia global da organização pode ser difícil. Cada unidade pode ter as suas próprias prioridades e objetivos, que nem sempre se alinham com os objetivos mais amplos da organização. Isto pode dificultar a garantia de que todas as unidades estão a trabalhar para o mesmo objetivo final.

Apesar destes desafios, os modelos de governança descentralizada podem ser particularmente vantajosos em ambientes dinâmicos, onde a capacidade de adaptação e resposta rápida é crucial. No entanto, requerem canais de comunicação robustos e uma forte cultura organizacional para mitigar os riscos de fragmentação e garantir o alinhamento com os objetivos globais da organização. É importante encontrar um equilíbrio entre a autonomia das unidades individuais e a necessidade de coordenação e alinhamento em toda a organização.

A governança descentralizada é um sistema em que o poder de tomar decisões é distribuído por diferentes níveis ou unidades dentro de uma organização. Esta estrutura proporciona a cada unidade um certo grau de autonomia e flexibilidade, permitindo-lhes responder mais rápida e eficazmente às suas necessidades e circunstâncias específicas. Ao dar poder às unidades locais, este modelo promove uma organização mais reactiva e adaptável que pode navegar melhor pelas complexidades do seu ambiente.

No entanto, embora a governança descentralizada ofereça muitos benefícios, também apresenta alguns desafios. Um dos principais problemas é a coordenação de atividades e políticas entre as várias unidades. Sem uma autoridade centralizada, pode ser difícil garantir que todas as unidades estão a trabalhar em harmonia para os mesmos objetivos. Além disso, alinhar os diversos objetivos de cada unidade com a estratégia global da organização também pode constituir um desafio. Apesar destes potenciais obstáculos, com uma comunicação eficaz e uma liderança forte, um modelo de governança descentralizada pode conduzir a uma organização mais dinâmica e resiliente.

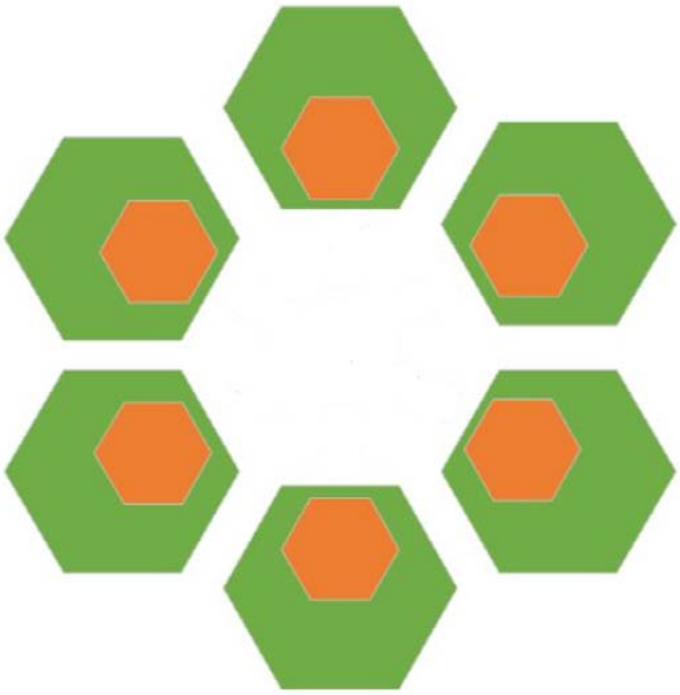

Figura 4: Ilustração simples do modelo descentralizado

Legenda: A caixa verde representa as entidades que serão afetadas pelas regras provenientes do topo da pirâmide. Enquanto a caixa laranja representa as entidades que tomam as decisões.

Um modelo de governança descentralizada permitiria, no contexto da Guiné-Bissau, distribuir as responsabilidades e os recursos por diferentes entidades e regiões, reduzindo assim o risco de concentração de poder, de corrupção e de ponto único de falha. Este modelo promove a resiliência e a adaptabilidade ao permitir uma tomada de decisão mais rápida e local face a ameaças específicas, o que é essencial num ambiente em constante mudança. Cada unidade operacional ou regional pode ter as suas próprias políticas, procedimentos e responsabilidades de segurança.

Por outro lado, esse modelo pode levar à fragmentação dos esforços de cibersegurança, dificultando a coordenação e a comunicação entre as diferentes entidades, o que pode enfraquecer a resposta global às ciberameaças. A disparidade de recursos e competências entre regiões pode criar zonas vulneráveis, onde os níveis de proteção variam consideravelmente.

C. Modelo de governança híbrido

O modelo de governança híbrido ou matricial é uma mistura única de estruturas centralizadas e descentralizadas. É frequentemente utilizado nas organizações para gerir projetos complexos que necessitam de colaboração multifuncional. Neste modelo, a autoridade e os poderes de decisão são partilhados entre uma liderança central e unidades ou departamentos individuais. Isto permite um equilíbrio entre as directivas de cima para baixo e as iniciativas de baixo para cima, criando uma estrutura organizacional dinâmica e flexível.

Este modelo é particularmente útil na gestão de projetos complexos que abrangem diferentes departamentos ou funções. Ao permitir a partilha de autoridade e responsabilidade, o modelo híbrido facilita uma melhor coordenação e colaboração entre diversas equipas. Permite que a organização aproveite os pontos fortes das estruturas centralizadas e descentralizadas, criando um sistema mais resistente e adaptável.

Num contexto governamental, o modelo híbrido pode consistir numa agência central responsável pela defi-

nição de orientações para a cibersegurança e a proteção de dados. Os incidentes graves devem também ser geridos pela agência central em coordenação com os ministérios e agências terceiras. Os organismos dos ministérios e agências são autónomos na definição das políticas locais, respeitando as orientações e a gestão dos incidentes não graves. No entanto, devem ser estabelecidos protocolos de comunicação muito bons.

Eis um resumo das suas vantagens e desvantagens:

Vantagens da governança híbrida

- **Flexibilidade:**

O modelo híbrido oferece um equilíbrio entre as abordagens do topo para a base e da base para o topo, proporcionando flexibilidade na tomada de decisões. Isto significa que, embora as decisões estratégicas possam ser tomadas a um nível central, as decisões operacionais podem ser tomadas mais perto do terreno, permitindo uma ação mais rápida e mais reactiva.

- **Otimização de recursos:**

O modelo híbrido permite uma utilização eficiente dos recursos, permitindo que os membros da equipa trabalhem em múltiplos projetos em diferentes departamentos. Isto não só otimiza a utilização dos recursos humanos, como também permite uma melhor atribuição e utilização de outros recursos, como o tempo e o orçamento.

- **Colaboração melhorada:**

O modelo híbrido incentiva a colaboração e a partilha de conhecimentos entre diferentes departamentos e equipas. Ao eliminar os silos e fomentar a colaboração interfuncional, promove uma cultura de aprendizagem e inovação.

- **Agilidade:**

O modelo híbrido pode adaptar-se rapidamente à evolução das necessidades e dos ambientes empresariais. Ao distribuir os poderes de decisão, permite que a organização responda rapidamente a novos desafios ou oportunidades.

Desvantagens da governança híbrida

- **Complexidade:**

A estrutura híbrida pode ser complexa, levando a uma potencial confusão de papéis e responsabilidades. Com a autoridade e a responsabilidade partilhadas entre a direção central e as unidades individuais, pode ser difícil definir claramente quem é responsável por quê.

- **Potencial de conflito:**

O modelo híbrido pode levar à sobreposição de autoridades e à duplicação das linhas de comunicação, o que pode resultar em conflitos e lutas pelo poder. Esta situação pode potencialmente dificultar a tomada de decisões e afetar a moral da equipa.

- **Atrasos na tomada de decisões:**

A necessidade de consenso entre as várias partes interessadas no modelo híbrido pode atrasar os processos de tomada de decisão. Com várias partes envolvidas, chegar a um acordo pode levar tempo, atrasando potencialmente decisões importantes.

- **Desafios de gestão:**

A coordenação de atividades e a comunicação entre diferentes equipas numa estrutura híbrida pode ser um desafio. É necessária uma liderança forte e canais de comunicação eficazes para garantir um funcionamento sem problemas.

Num contexto governamental, o modelo híbrido poderia ajudar a integrar vários departamentos e agências para trabalharem em conjunto no desenvolvimento e implementação de políticas. No entanto, exigiria diretrizes claras, canais de comunicação eficazes e uma liderança forte para evitar que os potenciais inconvenientes ofusquem os benefícios. Apesar dos seus desafios, quando implementado corretamente, o modelo de governança híbrido pode conduzir a uma organização mais flexível, colaborativa e eficiente.

O modelo híbrido é uma mistura única de estruturas organizacionais hierárquicas e descentralizadas. Apresenta linhas de reporte duplas e equipas multifuncionais,

integrando elementos de ambos os tipos de estruturas. Este modelo foi concebido para fomentar a colaboração e facilitar a troca de informações entre os vários segmentos da organização, eliminando os silos e promovendo uma abordagem mais integrada do trabalho.

No entanto, embora o modelo híbrido ofereça muitas vantagens, também apresenta alguns desafios. A duplicação das linhas de reporte pode levar à complexidade e criar ambiguidade em torno das funções e responsabilidades. Isto pode fazer com que seja difícil para os membros da equipa compreenderem os seus deveres e a quem devem prestar contas. Apesar destes desafios, com uma comunicação clara e uma liderança forte, o modelo matricial pode conduzir a uma organização mais colaborativa e eficiente.

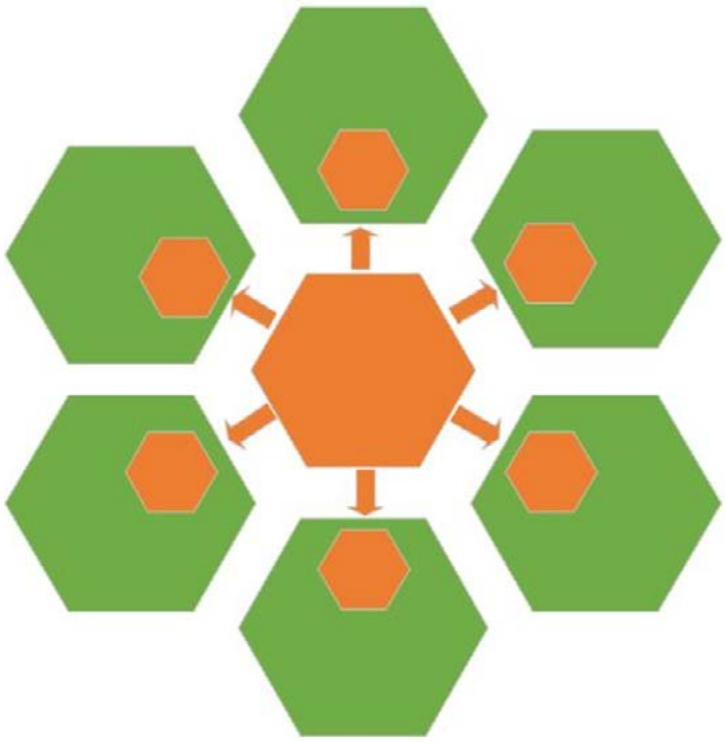

Figura 5: Ilustração simples do modelo híbrido

Legenda: A caixa verde representa as entidades que serão afetadas pelas regras provenientes do topo da pirâmide. Enquanto a caixa laranja representa a entidade que toma as decisões.

Um modelo de governança híbrido para a cibersegurança e a proteção de dados no contexto da Guiné-Bissau oferece um equilíbrio ótimo ao combinar as vantagens dos modelos centralizado e descentralizado. Este modelo permite uma coordenação central para definir políticas, normas e respostas às principais ameaças, garantindo a coerência nacional e a utilização eficiente dos recursos. Ao mesmo tempo, permite uma descentralização parcial, permitindo que as entidades locais se adaptem rapidamente a ameaças específicas e respondam às necessidades regionais, promovendo a resiliência e a adaptabilidade.

III. CONTEXTO E QUADRO ANALÍTICO

A. Descrição da situação atual na Guiné-Bissau

A Guiné-Bissau está a progredir rapidamente em termos tecnológicos e tem registado um aumento da penetração da Internet nos últimos anos. Esta melhoria do acesso à Internet abre a porta a avanços tecnológicos como:

- A digitalização dos serviços públicos
- A digitalização da identidade
- A proliferação de plataformas de serviços electrónicos, comércio eletrónico, pagamentos electrónicos e muito mais

Estes novos serviços irão consumir dados que terão de ser protegidos. Além disso, para poderem contar com estes serviços, devem ser resistentes às ciberameaças. Atualmente, na Guiné-Bissau, existem algumas entidades sob a tutela do Ministério dos Transportes, Telecomunicações e Economia Digital que estão envolvidas na criação de serviços digitais governamentais. O organigrama seguinte ilustra a sua estrutura.

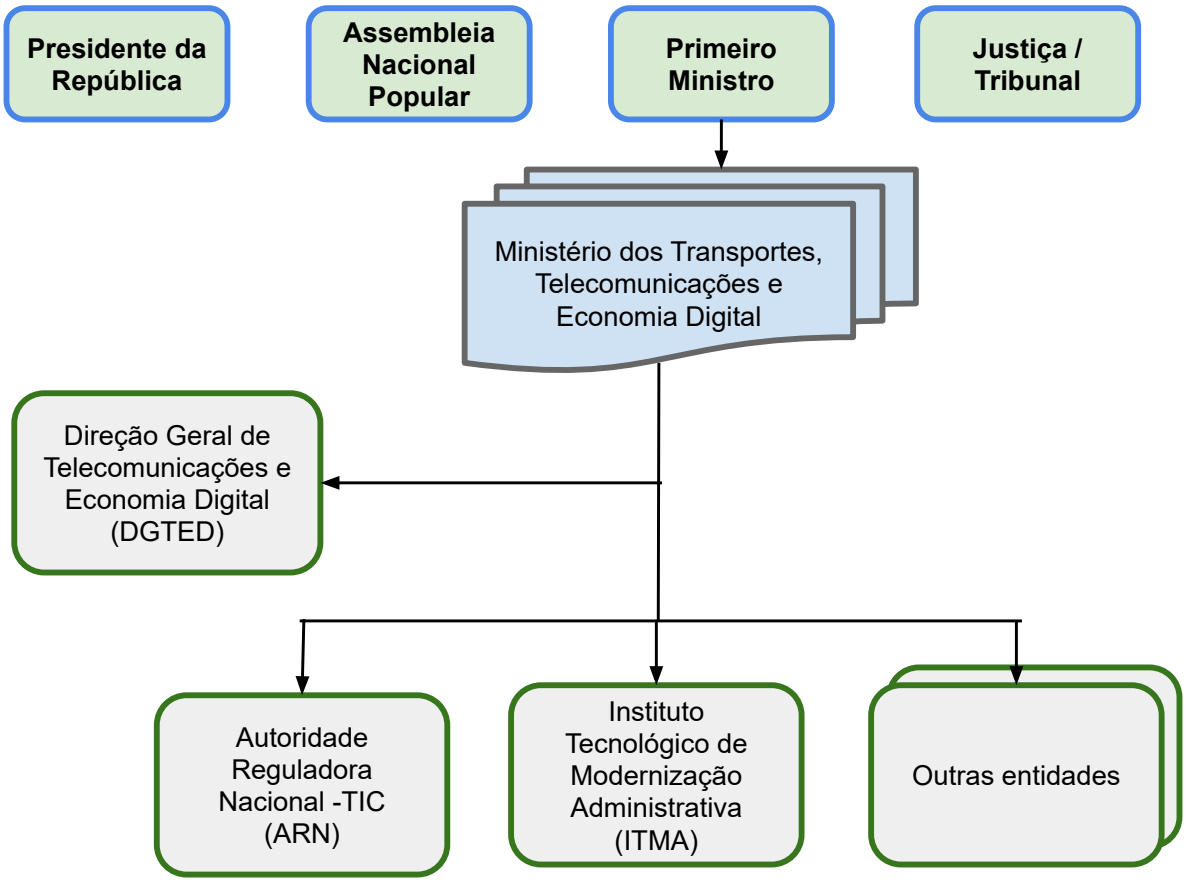

Figura 6: Organograma da atual estrutura de governança na Guiné-Bissau

Conforme declarado no Artigo 59 da Constituição[4], são órgãos de soberania **o Presidente da República, a Assembleia Nacional Popular, o Governo e os Tribunais.** A organização do poder político baseia-se na separação e independência dos órgãos de soberania, e na subordinação de todos eles à Constituição.

O Presidente da República é o Chefe de Estado, símbolo da unidade, garante a independência nacional e da Constituição e Comandante Supremo das Forças Armadas.

O Presidente da República representa a República da Guiné-Bissau (Ref. Artigo 62 da Constituição).

As funções de Presidente da República são incompatíveis com quaisquer outras de natureza pública ou privada. (Ref. Artigo 65ºda Constituição)

Algumas das funções exclusivas do Presidente da

[4]https://www.constituteproject.org/constitution/Guinea_Bissau_1996

República (Ref. Artigo 68ºda Constituição) :

- Nomear e exonerar o Primeiro-Ministro, tendo em conta os resultados eleitorais e ouvidas as forças políticas representadas pela Assembleia Nacional Popular;
- Confirmar a nomeação do Primeiro-Ministro;
- Nomear e exonerar os restantes membros do governo, , sob proposta do Primeiro-Ministro, e dar lhes posse ;
- Criar e extinguir ministérios e secretarias de Estado, sob proposta do Primeiro-Ministro;
- Presidir o Conselho de Estado;
- Presidir o Conselho de Ministros, quando entender ;
- Empossar os juízes do Supremo Tribunal de Justiça;
- Nomear e exonerar, sob proposta do Governo, o Chefe do Estado-Maior General das Forças Armadas;
- Nomear e exonerar, ouvido o Governo, o Procurador-Geral da República;

O Presidente da República é igualmente competente para (Ref. Artigo 69 da Constituição) :

- Dissolver a Assembleia Nacional Popular, em caso de grave crise política, após consulta ao Presidente da Assembleia Nacional Popular e aos partidos políticos nela presentes, e dentro dos limites estabelecidos pela presente Constituição;
- Demitir o Governo, nos termos do artigo 104.º,n.º2, da Constituição;
- Promulgar ou vetar, no prazo de 30 dias a contar da receção de qualquer diploma emanado da Assembleia Nacional Popular ou do Governo para promulgação.

O veto do Presidente da República sobre as leis da Assembleia Nacional Popular pode ser suportado por voto favorável da maioria de dois terços dos deputados em efectividade de funções (Ref. Artigo 69ºnº2 da Constituição).

Conforme o Artigo 71ºda Constituição, em caso de ausência para o estrangeiro ou de impedimento temporário, o Presidente da Assembleia Nacional Popular substitui temporariamente o Presidente da República.
O Presidente da Assembleia Nacional Popular assume as funções do Presidente da República em caso de morte ou impedimento definitivo; em caso de impedimento do primeiro, o seu próprio substituto assume as funções até a tomada de posse do novo Presidente eleito.

O novo Presidente será eleito no prazo de 60 dias.
O Presidente da República interino não pode, em caso algum, exercer as atribuições previstas nas alíneas g), i), m), n), o), s), v) e x) do artigo 68ºe nas alíneas a), b) e c) do nº1 do artigo 69ºda Constituição.
O Presidente da República interino só pode usar os poderes estabelecidos na alínea j) do artigo 68ºpara cumprir o disposto no nº3 do presente artigo."

A Assembleia Nacional Popular é o órgão supremo legislativo e de fiscalização política representativo de todos os cidadãos guineenses. Decide sobre todas as questões fundamentais da política interna e externa do Estado (Ref. Artigo 76ºda Constituição).
Conforme o artigo 81ºda Constituição, um deputado tem o direito de apresentar inquéritos ao Governo, oralmente ou por escrito, e deve receber uma resposta na sessão ou num prazo de 15 dias, por escrito, se forem necessárias mais investigações.

Se o Programa de Governo não for aprovado pela Assembleia Nacional Popular, será realizado um novo debate no prazo de 15 dias.
O voto de confiança perante a Assembleia Nacional deve ser efectuado pelo Primeiro-Ministro, após deliberação do Conselho de Ministros;
A iniciativa de moção de censura requer um terço dos deputados em efectividade de funções;
A não aprovação de uma moção de confiança ou a aprovação de uma moção de censura por maioria absoluta implica a destituição do Governo.
A Assembleia Nacional Popular tem competência exclusiva para legislar sobre:

- A organização da defesa nacional;
- O sistema monetário;
- Organização judiciária e estatuto dos magistrados;
- Definição dos crimes, penas e outras medidas de segurança e processo criminal;

Conforme declarado no Artigo 94 da Constituição, "A Assembleia Nacional Popular não pode ser dissolvida

nos 12 meses posteriores à eleição, nos últimos seis meses de um mandato do Presidente da República ou durante a vigência do estado de
sítio ou de emergência.
A dissolução da Assembleia Nacional Popular não impede a subsistência do mandato dos deputados até a abertura da legislatura subsequente às novas eleições.

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

A Comissão Permanente é competente para:
Acompanhar todas as actividades do Governo e da Administração;
Exercer os poderes da Assembleia Nacional Popular relativamente ao mandato dos deputados;
Convocar a Assembleia Nacional Popular sempre que necessário;
Preparar a abertura das sessões ;
Pronunciar-se sobre qualquer imposição de lei marcial ou declaração de estado de emergência.
A Comissão Permanente responde e presta contas de todas as suas actividades perante a Assembleia Nacional Popular".

A Justiça / Tribunal, também designada por Tribunais, é um órgão de soberania com competência para administrar a justiça em nome do povo (Ref. artigo 119.ºda Constituição).
O artigo 120ºda Constituição estabelece que:

- O Supremo Tribunal de Justiça é a instância judicial suprema da República. O Conselho Superior da Magistratura nomeia os seus juízes.
- Os juízes do Supremo Tribunal de Justiça são empossados pelo Presidente da República.
- Compete ao Supremo Tribunal de Justiça e aos tribunais instituídos por lei o exercício da função jurisdicional.
- No exercício da sua função jurisdicional, os tribunais são independentes e apenas estão sujeitos à lei.
- O Conselho Superior da Magistratura é o órgão superior de gestão e disciplina da magistratura judicial.
- O Conselho Superior da Magistratura contará, pelo menos, com representantes do Supremo Tribunal de Justiça, dos demais tribunais e da Assembleia Nacional Popular, nos termos estabelecidos na lei.

No artigo 125ºé referido que:

- O Ministério Público é o órgão do Estado responsável, juntamente com os tribunais, pela fiscalização do Estado de Direito e pela representação dos interesses públicos e sociais, competindo-lhe a propositura de ações penais.
- O Ministério Público organiza-se segundo uma estrutura hierarquizada, sob a direção do Procurador-Geral da República.
- O Procurador-Geral da República é nomeado pelo Presidente da República, ouvido o Governo.

O Primeiro-Ministro é nomeado pelo Presidente da República, de acordo com os resultados eleitorais e ouvido os partidos políticos representados na Assembleia Nacional Popular. (Ref. Artigo 98 da Constituição)
O Primeiro-Ministro faz parte do Governo. Conforme o artigo 96ºda Constituição, "O Governo é o órgão supremo executivo e administrativo da República da Guiné-Bissau.

O Governo executa as políticas gerais do país de acordo com o seu Programa, aprovado pela Assembleia Nacional Popular.

Compete ainda ao Primeiro-Ministro, sem prejuízo de outras atribuições que lhe são conferidas pela Constituição e pela lei, informar o Presidente da República sobre as questões relativas à política interna e externa do país.
Tal como consta no artigo 100ºda Constituição, algumas das competências do Governo são:

- Dirigir a Administração Pública, coordenar e controlar as actividades dos Ministérios e demais organismos da Administração Central e os do Poder Local;

- Organizar e dirigir a realização das actividades políticas, económicas, culturais, científicas, sociais, de defesa e segurança, de acordo com o seu Programa;
- Elaborar o Plano de Desenvolvimento Nacional e o Orçamento Geral do Estado, e executá-lo;
- Legislar por meio de decretos-leis e decretos sobre as matérias respeitantes à sua organização e funcionamento, bem como sobre as matérias não reservadas à Assembleia Nacional Popular;
- Aprovar propostas de lei e submetê-los à Assembleia Nacional Popular;
- O Governo é politicamente responsável perante o Presidente da República e perante a Assembleia Nacional Popular. (Ref. Artigo 103.ºda Constituição)

Conforme estabelecido no artigo 104 da Constituição, "A demissão do Governo acarreta-se:"

- O início de nova legislatura;
- A não aprovação do programa de Governo pela segunda vez consecutiva;
- A aceitação pelo Presidente da República do pedido de demissão apresentado pelo Primeiro-Ministro;
- A aprovação de uma moção de censura ou a não aprovação de uma moção de confiança por maioria absoluta dos Deputados em efectividade de funções;
- A morte ou a indisponibilidade física prolongada do Primeiro-Ministro.
- O Presidente da República pode demitir o Governo em caso de grave crise política que ponha em causa o normal funcionamento das instituições da República, ouvidos o Conselho de Estado e os partidos políticos com assento parlamentar.

O Ministério dos Transportes, Telecomunicações e Economia Digital é membro do Governo e é efetivamente responsável pela cibersegurança e pela privacidade dos dados.

A Direção-Geral das Telecomunicações e da Economia Digital (DGTED) está sob a tutela do Ministério dos Transportes, das Telecomunicações e da Economia Digital. É responsável por propor directivas ao ministério que podem ser apresentadas ao conselho de ministros e seguidas até à assembleia nacional para serem votadas como lei.
Para conhecer as directrizes correctas a propor ao ministério, a DGTED participa em conferências, debates com países terceiros e outras instituições. A DGTED também recebe directivas do seu ministério de tutela para os aspectos políticos relacionados com o programa de governo.

Na ausência de um modelo de governança estruturado, a DGTED e a ARN cobrem parcialmente alguns aspectos da cibersegurança. Mas não cobre todos os aspectos da cibersegurança e da governança de proteção de dados. Na verdade, em caso de incidente de segurança no sector público, não existe um procedimento, uma entidade de acompanhamento ou qualquer outra entidade para o gerir. Além disso, não existe atualmente qualquer mecanismo ou obrigação de comunicação de incidentes na administração pública.
As mesmas deficiências foram encontradas no sector privado. Quer se trate de bancos ou de qualquer outra entidade privada de importância crítica na Guiné-Bissau, estes não têm qualquer obrigação legal de comunicar incidentes de segurança.
Não existem padrões, normas ou leis que exijam que as entidades públicas ou privadas mantenham os dados críticos seguros em trânsito, durante o processamento ou em repouso.

O Instituto Tecnológico de Modernização Administrativa (ITMA) está sob a tutela do Ministério dos Transportes, Telecomunicações e Economia Digital. É uma pessoa colectiva de direito público, criada para operacionalizar as iniciativas governamentais de modernização tecnológica e de redes privadas na administração central e local do Estado, reforçando a participação e o envolvimento dos diferentes actores e instituições na prestação de serviços públicos. O ITMA é dotado de personalidade jurídica e goza de autonomia administrativa, financeira e patrimonial.
O ITMA também trabalha na implementação de políticas de digitalização nos sectores públicos.

A Agência Reguladora Nacional (ARN) das telecomunicações está sob a responsabilidade do Ministério dos

Transportes, Telecomunicações e Economia Digital. Tem o mandato de regulamentar as TIC. Por exemplo, garante que os operadores de telecomunicações respeitam a sua largura de banda e o seu acordo de serviço com os consumidores. A ARN trabalha em colaboração com a Polícia Judiciária para efetuar investigações quando existem problemas de segurança relacionados com os serviços de telecomunicações. A título de exemplo, podemos referir os casos de extravio de telemóveis.

Entidades terceiras como Correios Guiné-Bissau (CGB), Guiné Telecom, GTM, Sociedade de Cabos da Guiné-Bissau não são de interesse para este estudo.

De acordo com os nossos inquéritos no território, a DGTED, o ITMA e a ARN constituem as únicas entidades governamentais cujo mandato está próximo da segurança. Esta proximidade com a segurança não significa a existência de um modelo de governança para a cibersegurança e a proteção de dados. Podemos, portanto, concluir que não existe atualmente um modelo de governança para a cibersegurança e proteção de dados na Guiné-Bissau. O nosso estudo de viabilidade terá este aspeto em consideração ao propor o modelo de governança. No entanto, iremos aprender a forma como a DGTED, ITMA, ARN são governadas e interagem entre si no ecossistema da Guiné-Bissau.

B. Objetivos do estudo de viabilidade e metodologia utilizada

Objetivo do estudo de viabilidade

O principal objetivo deste estudo de viabilidade é conduzir a Guiné-Bissau à identificação de um modelo de governança da cibersegurança e da proteção de dados adequado ao contexto da Guiné-Bissau. Adicionalmente, o estudo irá apoiar o desenvolvimento de políticas e regulamentos nacionais, bem como a implementação de programas estratégicos que precisam de ser melhorados para remover os obstáculos à governança. Isto permitirá o surgimento de um sistema de governança nacional integrado e robusto, que pode posicionar o país de forma competitiva no mercado digital regional e global.

Para atingir estes objetivos, é essencial estabelecer um modelo de governança sólido que inclua elementos essenciais como a estrutura, os mecanismos de supervisão, as políticas e os processos.

Metodologia utilizada

A metodologia utilizada no nosso estudo consiste, em primeiro lugar, em definir o que é a cibersegurança, a proteção de dados e a governança. Em seguida, apresentaremos as nuances entre estes termos e a forma como se articulam. Concluiremos esta secção referindo se o mesmo modelo de governança pode ser utilizado para todos estes aspetos ou se devem ser distintos.

Em segundo lugar, apresentaremos os diferentes modelos de governança. Destacamos as suas vantagens e desvantagens. Serão propostas estatísticas sobre o desempenho de certos modelos de governança.

Em terceiro lugar, identificaremos o estado atual da governança da cibersegurança e da proteção de dados na Guiné-Bissau. Esta etapa incluirá a recolha de dados no terreno com base num inquérito por questionário. Será proposta uma análise das particularidades da Guiné-Bissau que podem influenciar a governança.

Em seguida, faremos uma análise comparativa de alguns países que têm semelhanças com a Guiné-Bissau e que já implementaram um modelo de governança há pelo menos um ano.

Por fim, identificaremos os fatores de decisão e proporemos um modelo de governança.

IV. ANÁLISE DO AMBIENTE ATUAL

A. Avaliação da governança existente em matéria de cibersegurança e proteção de dados

Para realizar este estudo, foi necessário fazer um balanço da situação em termos de cibersegurança e proteção de dados. Para recolher informações, reunimo-nos com alguns intervenientes públicos e privados envolvidos em aspetos de cibersegurança e proteção de dados, como a DGTED, o ITMA, a ARN, a Energia (EAGB), a Polícia Judiciária, os Bancos e as Operadoras de Telecomunicação. A recolha de dados foi efectuada através de um inquérito por questionário que abrangia os seguintes aspetos principais:

- **Informação geral sobre cibersegurança:** Permite ao inquirido fazer a sua leitura da cibersegurança na Guiné-Bissau
- **Políticas e regulamentos:** Discute o estado das leis e o seu reforço
- **Capacidades técnicas e infraestruturas:** fala sobre o estado das infraestruturas face aos ciberataques
- **Reforço de capacidades:** fala sobre planos de formação
- **Gestão de Incidentes e Resiliência:** fala sobre a resposta a incidentes e a continuidade das atividades
- **Cooperação e parcerias:** conversas sobre acordos assinados

Informações gerais sobre cibersegurança:

De forma unânime, os inquiridos informaram-nos da inexistência de infraestruturas de cibersegurança no país e da falta de uma estratégia nacional de cibersegurança. No que diz respeito à estratégia nacional de segurança, está em curso um projeto para resolver esta questão.
Os principais actores (públicos e privados) envolvidos na cibersegurança no país não estão claramente definidos. Os debates permitiram estabelecer uma lista parcial:

- No sector público:
  - Ministério dos Transportes, das Telecomunicações e da Economia Digital
  - Polícia Judiciária,
  - ARN
- No sector privado, a identificação ainda não foi feita

Não existe uma entidade para gerir as informações sobre as ameaças à cibersegurança dos cidadãos e das empresas. Algumas empresas privadas registaram alguns ataques. Mas a falta de leis que as obriguem a comunicar com o governo e/ou com o público torna impossível obter pormenores sobre esses ataques e sobre a forma como foram tratados.
O nível de sensibilização e de formação em matéria de cibersegurança entre os cidadãos e as empresas é baixo, mesmo os que trabalham no domínio das TIC sabem pouco sobre cibersegurança.

A avaliação dos ativos críticos na Guiné-Bissau ainda não foi efectuada.

Políticas e regulamentos :
Não existem leis e regulamentos específicos sobre cibersegurança atualmente em vigor no país. No entanto, está em curso um projeto WARDIP sobre o desenvolvimento de leis de cibersegurança.

Esta situação provoca a inexistência de agências de aplicação da lei e de serviços de informação no que diz respeito à cibersegurança.

Capacidades técnicas e infraestruturais :
O nível de desenvolvimento e de sofisticação das infraestruturas das tecnologias da informação e das telecomunicações no país é baixo.

Os programas de investigação e desenvolvimento em matéria de cibersegurança são inexistentes.

A capacidade das redes de comunicação (Internet, telefone) para resistir a ciberataques é muito baixa.

Atualmente, não existe uma identificação e classificação das infraestruturas e dos ativos críticos do país.

O atual nível de investimento público em cibersegurança é muito baixo.

Reforço das capacidades :
Não existem programas específicos de formação de recursos.

Gestão de incidentes e resiliência :
Não existe uma equipa nacional de resposta a emergências informáticas (CERT) ou uma estrutura equivalente para responder a incidentes de cibersegurança. O projeto WARDIP cobre atualmente este aspeto.

No entanto, as entidades privadas, como os bancos e as operadoras de telecomunicações, têm as suas próprias ferramentas de gestão da cibersegurança e de alerta em caso de tentativas de ataque com base nas políticas do grupo de entidades.

Se o país sofrer incidentes de cibersegurança com um impacto significativo na economia, poderá não os gerir corretamente devido à ausência de CERT.
As empresas enfrentam muitos obstáculos na implementação de medidas eficazes de cibersegurança devido à falta de políticas, orientações e legislação no país e também à falta de recursos formados e competentes neste domínio.

Cooperação e parcerias :
As parcerias internacionais existentes no domínio da cibersegurança abrangem muito mais o aspeto da formação e do reforço das capacidades. Os principais parceiros são a CEDEAO, a UEMOA, a UA e a UTI.

Não existe cooperação entre os sectores público e privado para gerir a cibersegurança.

Os meios de comunicação social e os jornalistas ainda não estão a desempenhar o seu papel na sensibilização e comunicação sobre as questões de cibersegurança devido à falta de orientações claras em matéria de cibersegurança.

As empresas e as agências governamentais não partilham informações sobre ameaças e incidentes de cibersegurança.

B. Desafios e lacunas identificados no sistema atual

No estado atual da cibersegurança e proteção de dados na Guiné-Bissau, o maior desafio é a gestão da mudança num contexto em que não existem directrizes, normas, padrões ou regulamentos. Quaisquer propostas que visem a atualização nesta área implicarão mudanças notáveis nos processos e hábitos de muitas organizações, tanto públicas como privadas. Para além disso, gerará custos adicionais para todas as entidades envolvidas.

A falta de formação adequada e acessível em matéria de cibersegurança e proteção de dados para um grande número de guineenses continua a ser um dos principais desafios para qualquer modelo que venha a ser proposto.
A disponibilidade orçamental é outro desafio, porque uma boa implementação do modelo exigirá um investimento maciço, uma vez que não havia nada em vigor.

C. Análise das infraestruturas e recursos existentes

Atualmente, a Guiné-Bissau não dispõe de infraestruturas e recursos tecnológicos para conter as ciberameaças. Constatámos a ausência de:

- CERT
- Centro Nacional de Dados
- Centro Nacional de Operações de Segurança (SOC Nacional)
- Agência de Segurança Nacional
- Cada ministério gere os seus servidores de forma isolada, sem directivas e orientações claras.

A ausência destes elementos contribui para a falta de visibilidade do estado real das ciberameaças a que o país está exposto.

D. Visão geral da postura no ciberespaço da Guiné-Bissau

O ciberespaço da Guiné-Bissau pode ser considerado subdesenvolvido, caracterizado pela ausência de legislação específica contra os cibercrimes e de uma estratégia nacional de cibersegurança. Esta falta de estratégias e de instituições responsáveis pela sua implementação

expõe o ciberespaço da Guiné-Bissau a riscos significativos. Em 2020, de acordo com o Índice Global de Cibersegurança (GCI) da UIT, a Guiné-Bissau ocupa a 161.ºposição a nível mundial e a 36.ºem África, o que evidencia a ausência de políticas sólidas de proteção do ciberespaço (fonte: ITU GCI 2020).

Nome do país	Pontuação	Classificação
Belize	10.29	159
Mali	10.14	160
Guiné-Bissau	9.85	161
Libéria	9.72	162

Quadro 1: A Guiné-Bissau na UIT 2020

Além disso, a Guiné-Bissau tem uma presença reduzida na Dark Web devido à sua infraestrutura de Internet subdesenvolvida e às suas capacidades limitadas em matéria de cibersegurança. Este baixo nível de digitalização reduz significativamente o impacto das ciberameaças no país. No entanto, o ciberespaço da Guiné-Bissau enfrenta várias ameaças notáveis, o que a coloca entre os dez principais países em risco em termos de ciberameaças, de acordo com a Kaspersky (fonte: Kaspersky Cybermap). Esta posição sublinha os grandes desafios que o país deve enfrentar para reforçar a sua segurança digital e proteger as infraestruturas críticas contra os ciberataques.

Este facto sublinha a urgência de desenvolver políticas sólidas de cibersegurança, melhorar a sua infraestrutura digital e reforçar as capacidades de cibersegurança para enfrentar os desafios crescentes do ciberespaço da Guiné-Bissau.

E. Análise das características da Guiné-Bissau que afetam a governança

Com base na definição de governança da cibersegurança e da proteção de dados, identificámos alguns aspetos específicos na Guiné-Bissau que podem afetar o modelo selecionado. Temos de abordar o desafio que estes aspetos representam para que o modelo de governança proposto tenha todas as hipóteses de ser persistente e relevante. A lista seguinte dos aspetos específicos pode não ser exaustiva, mas baseia-se no nosso inquérito e na nossa compreensão do contexto:

- Instabilidade política
- Aspeto cultural, incluindo religiões, composição étnica e populacional
- Geolocalização e Acordos assinados pelo país
- Situação económica do país
- Disponibilidade de tecnologias e recursos qualificados
- Estado de direito e capacidade de o fazer cumprir

Estes elementos são pormenorizados a seguir.

Instabilidade política

Na Guiné-Bissau, o governo está dividido em três ramos:

- O poder executivo é composto pelo Presidente e pelo Primeiro-Ministro. São responsáveis pelas tarefas executivas.
    - Da Constituição[6] da Guiné-Bissau, o Presidente é eleito para mandatos de 5 anos por maioria absoluta de votos, num sistema de duas voltas no máximo. O Presidente não pode candidatar-se a um terceiro mandato consecutivo, nem durante os cinco anos que se seguem ao termo do seu segundo mandato. Em caso de demissão do Presidente, este não pode candidatar-se a eleições imediatas, nem às que se realizem nos cinco anos seguintes à sua demissão. Como em muitos países em desenvolvimento, a Presidência da Guiné-Bissau está exposta ao risco de derrube por movimentos de ideias. Este facto já foi constatado na história recente do país.

Em caso de mudança, seja ela brusca durante o mandato ou no fim do mandato, as funções políticas sob o controlo do Presidente podem ser remodeladas. Essa mudança afectará diretamente todas as partes do modelo de governação da cibersegurança e da proteção de dados que está sob a supervisão da Presidência. Isto pode ter um grande impacto no funcionamento, na visão e na existência da entidade de governação afetada.

- Da Constituição[7] da Guiné-Bissau, é nomeado e exonerado pelo Presidente da República, tendo em conta os resultados eleitorais e depois de ouvidas as forças políticas representadas pela Assembleia Nacional Popular. Compete-lhe propor ao Presidente da República os restantes membros do Governo. Na história da Guiné-Bissau, é de notar que existe uma forte possibilidade de migração dos representantes da Assembleia do campo maioritário para um campo não maioritário. Isto pode levar a que um campo anteriormente minoritário se torne um campo maioritário. Estas migrações podem ocorrer durante o mandato dos deputados. Esta situação pode levar a uma substituição do Primeiro-Ministro e, consequentemente, do gabinete ministerial. Assim, todas as componentes políticas do modelo de governação que seria proposto e que responderia perante o Primeiro-Ministro poderiam ser enfraquecidas na sequência deste tipo de mudança.

- O ramo judicial é responsável pelas decisões do supremo tribunal e pela constituição do ramo judicial do governo[8]. O membro deste tribunal é nomeado pelo conselho superior da magistratura. De acordo com o artigo 120ºda Constituição[9] da Guiné-Bissau, o Presidente da República dá posse aos juízes do Supremo Tribunal de Justiça. Dado que os membros deste ramo não provêm de uma eleição com um mandato fixo, este ramo confere uma certa estabilidade a todos os aspectos da governação que dele dependem. O risco de mudança é muito reduzido neste caso, uma vez que não está diretamente ligado a mudanças políticas. O risco de mudança é muito mínimo neste caso, uma vez que não está diretamente ligado a mudanças políticas.
- O poder legislativo é responsável por constituir o poder legislativo do governo. Os 102 deputados são eleitos através de um sistema de representação proporcional de lista fechada. Uma vez eleitos, tal como previsto no artigo 79 da Constituição[10] da Guiné-Bissau, têm um mandato de 4 anos. O único risco de instabilidade que registámos até à data é a dissolução do Parlamento pelo Presidente. O seu objetivo é aprovar as leis promulgadas pelo poder executivo e depois enviá-las para o poder judicial para serem transcritas para a lei.

O risco de instabilidade está presente em todos os sectores do aspecto político analisado. Para ser sustentável, o modelo de governança proposto deverá fazer face a estes riscos. Identificámos vários países africanos com um modelo de governança que adoptaram o mesmo modelo político e que estão expostos aos mesmos riscos de instabilidade. Entre estes países, podemos citar: A República Democrática do Congo[11], Portugal, entre outros.

Aspeto cultural, incluindo religiões, composição étnica e populacional

A consideração de fatores culturais é crucial no desenvolvimento de estratégias de cibersegurança na Guiné-Bissau para garantir que as iniciativas são eficazes, bem recebidas e alinhadas com as normas e valores locais. A cultura da Guiné-Bissau é uma mistura de tradições africanas, portuguesas e indígenas, com uma parte significativa da população a seguir crenças animistas tradicionais, juntamente com o cristianismo e o islamismo. Eis algumas considerações culturais a ter em conta:

- **Língua e comunicação:** A comunicação é feita sobretudo nas línguas locais, como o crioulo ou o português (língua oficial), o que pode ser mais eficaz para sensibilizar a população em geral para as questões da cibersegurança. A utilização de mensagens e canais culturalmente adequados, como programas de rádio ou reuniões comunitárias, pode aumentar o envolvimento e a compreensão. Para permitir o envolvimento de todas as partes interes-

[7] https://www.constituteproject.org/constitution/Guinea_Bissau_1996
[8] https://globaledge.msu.edu/countries/guinea-bissau/government
[9] https://www.constituteproject.org/constitution/Guinea_Bissau_1996
[10] https://www.constituteproject.org/constitution/Guinea_Bissau_1996
[11] https://republique.cd/le-gouvernement

sadas, o modelo de governança deve estar disponível em pelo menos uma destas línguas. O aspeto linguístico deve ser tido em consideração tanto nos intercâmbios internos como externos. Os outros países de língua portuguesa são: Angola, Brasil, Cabo Verde, Moçambique, Portugal, São Tomé e Príncipe, Timor-Leste e, desde 2014, Guiné Equatorial.

- **Confiança e autoridade:** O respeito pela autoridade e pelas estruturas hierárquicas é importante na cultura da Guiné-Bissau. O recurso a figuras de confiança, como os líderes comunitários ou religiosos, para apoiar as iniciativas de cibersegurança pode aumentar a credibilidade e encorajar a participação.
- **Composição da população:** Com base nas estatísticas do Banco Mundial, em 2022, a população da Guiné-Bissau era de cerca de 2.105.666 habitantes. Esta população deverá aumentar ao longo dos anos. Constatamos uma taxa de analfabetismo elevada, como na maioria dos países da região. Algumas pessoas não compreendem o português. A educação é muito valorizada na Guiné-Bissau e há um interesse crescente pela tecnologia e pela literacia digital. Investir em programas de educação e sensibilização para a cibersegurança que atendam a diferentes faixas etárias e habilitações literárias pode capacitar os indivíduos para se protegerem online e contribuir para uma sociedade mais ciber consciente.

Estes aspetos garantirão o envolvimento das partes interessadas, a sua compreensão do modelo de governança, a sua participação e evitarão conflitos culturais. Alguns países também partilham este aspeto e foram capazes de construir um modelo de governança. Na lista, temos Angola, Guiné Equatorial, entre outros.

Geolocalização e Acordos assinados pelo país

Situada em África, mais concretamente na região da África Ocidental, a Guiné-Bissau é membro de algumas organizações regionais. Com esta proximidade, uma grande quantidade de dados digitais pode ser trocada com os países vizinhos. Para proteger os dados da população, algumas organizações, incluindo a Guiné-Bissau, estabeleceram acordos. A Guiné-Bissau assinou a Convenção da União Africana sobre Cibersegurança e Proteção de Dados Pessoais (conhecida como Convenção de Malabo). A Convenção de Malabo visa promover a cibersegurança e a proteção de dados em toda a África. Além disso, a Guiné-Bissau é membro de comunidades ou organizações económicas regionais que têm disposições de proteção de dados nos seus quadros. Como membro da Comunidade Económica dos Estados da África Ocidental (CEDEAO), a Guiné-Bissau está sujeita à Lei Complementar da CEDEAO sobre a Proteção de Dados Pessoais. A Guiné-Bissau também ratificou o Pacto Internacional sobre os Direitos Civis e Políticos (PIDCP). O PIDCP é um dos principais instrumentos internacionais de direitos humanos que consagra os direitos civis e políticos, com o objetivo de proteger e promover as liberdades fundamentais e as liberdades individuais em todo o mundo. Note-se que, na Guiné-Bissau, a Constituição protege o direito à privacidade nos artigos 34.ºA e 38. Atualmente, a Guiné-Bissau não dispõe de legislação sobre proteção de dados no direito interno, nem de legislação conexa, como a legislação sobre cibercrimes ou transações eletrônicas.

Muitos países, com modelos de governança existentes, como o Gana, o Benim e o Togo, têm os mesmos critérios e podem inspirar este estudo de viabilidade.

Situação económica do país

Tendo em conta os desafios económicos, é crucial um modelo de governança que promova o desenvolvimento económico através de práticas transparentes e responsáveis. Para tal, é necessário combater a corrupção, incentivar o investimento estrangeiro e assegurar uma alocação eficaz dos recursos.

Os fatores socioeconómicos influenciam o acesso à tecnologia e aos recursos de cibersegurança na Guiné-Bissau. O desenvolvimento de soluções de cibersegurança

acessíveis e a preços módicos que respondam às necessidades dos diferentes grupos socioeconómicos pode promover a inclusão e o acesso equitativo à segurança digital.

Além disso, o modelo de governança proposto deve ser viável com o orçamento disponível para a Guiné-Bissau. O Produto Interno Bruto da Guiné-Bissau era de 1,63 mil milhões de euros em 2022. "A Guiné-Bissau registou um défice do Orçamento do Estado igual a 5,50 por cento do Produto Interno Bruto do país em 2022. O Orçamento do Estado na Guiné-Bissau foi em média de -3,72 por cento do PIB de 2002 até 2022, atingindo um máximo histórico de 3,60 por cento do PIB em 2009 e um mínimo histórico de -9,80 por cento do PIB em 2020". O nosso parâmetro de referência terá em conta este aspeto na seleção dos países.

Disponibilidade de tecnologias e recursos qualificados

Na verdade, a Guiné-Bissau não dispõe de tecnologias para ajudar na governança da cibersegurança e proteção de dados. Algumas das entidades privadas, como bancos ou outras multinacionais, têm firewalls e outros equipamentos. Uma vez que não existe qualquer exigência por parte do governo, as multinacionais seguem as normas da sua sede.

Os recursos em matéria de cibersegurança são limitados na Guiné-Bissau. Este facto deve-se provavelmente à falta de formação disponível localmente. Durante os nossos inquéritos no terreno, a maioria das pessoas com quem nos reunimos reconheceu uma falta de qualificações que deve ser resolvida em matéria de cibersegurança e proteção de dados. Para que o modelo de governança funcione, as pessoas qualificadas devem estar nas posições certas na cadeia de governança.

A Guiné-Bissau não é a única a enfrentar este desafio. Há muitos países com perfis semelhantes que têm ou tiveram este desafio. Alguns deles conseguiram superá-lo através de vários meios que veremos mais detalhadamente na seção sobre a avaliação comparativa.

Estado de direito e capacidade de o fazer cumprir

O desenvolvimento e a implementação de leis e regulamentos sólidos em matéria de cibersegurança e privacidade de dados são essenciais para proteger os direitos dos indivíduos e promover a confiança nas tecnologias digitais. A Guiné-Bissau precisa de rever e atualizar o seu quadro jurídico para fazer face à evolução das ciberameaças e alinhar-se com as normas e padrões internacionais.

Note-se que, na Guiné-Bissau, a Constituição protege o direito à privacidade nos artigos 34.ºA e 38. Atualmente, a Guiné-Bissau não dispõe de legislação sobre proteção de dados no direito interno, nem de legislação conexa, como a legislação sobre cibercrimes ou transações electrónicas.

A falta de lei e de entidades que controlam a execução das leis faz com que, por exemplo, hoje em dia, não se tenha informação sobre os ataques existentes na Guiné-Bissau.

Durante as nossas investigações, a maioria das instituições encontradas não foi capaz de fornecer um retrato real dos ataques. O modelo de governança proposto deve ser suficientemente flexível para funcionar, no início da sua aplicação, num ambiente em que ainda não existem leis fortes. O modelo de governança deve, nomeadamente, fazer recomendações sobre as leis que devem ser implementadas e aplicadas para que cada entidade possa cumprir a sua missão. A maioria dos países da África Ocidental com um modelo de governança da cibersegurança e da proteção de dados enfrentou este desafio.

V. ESTUDOS DE CASOS INTERNACIONAIS

A governança da cibersegurança desempenha um papel crucial na proteção das infraestruturas e dos dados digitais contra as ciberameaças em constante evolução. Numa era em que a interconexão digital permeia todos os aspetos da vida moderna, são imperativas medidas sólidas de cibersegurança para garantir a integridade, a confidencialidade e a disponibilidade dos ativos digitais.

A Guiné-Bissau é um país significativamente ligado às comunidades internacionais e regionais de que faz parte, nomeadamente a CEDEAO e a CPLP (Comunidade dos Países de Língua Portuguesa). Tendo em conta as relações diplomáticas da Guiné-Bissau com outros países, nomeadamente os países membros destas duas organizações, podemos identificar cinco países cujos modelos e estratégias se revelaram eficazes. Estes países são o Benim, o Brasil, o Gana, Portugal e o Togo. Cada um destes países enfrenta um desafio formidável: proteger os seus ecossistemas digitais contra uma miríade de riscos cibernéticos, que vão desde violações de dados e ataques de ransomware a sofisticadas campanhas de ciberespionagem. No centro dos seus esforços está a formulação e implementação de quadros de governança da cibersegurança que orientam o desenvolvimento de políticas, a aplicação da regulamentação, a coordenação institucional e os investimentos tecnológicos.

A. Apresentação de modelos de governança utilizados em países com ambientes semelhantes

Para identificar os países semelhantes que podem ser relevantes para o nosso estudo, utilizamos os seguintes critérios:

- **C1:** Ter um modelo de governança da cibersegurança e da proteção de dados implementado há, pelo menos, um ano
- Partilhar com a Guiné-Bissau, pelo menos, uma das seguintes características que existia antes de implementarem o seu modelo de governança e que pode afetar ou afetar a governança da cibersegurança e da proteção de dados
  - Instabilidade política
    - **C2 :** A instabilidade do Presidente
    - **C3 :** A instabilidade do Primeiro-Ministro
  - Aspeto cultural, incluindo religiões, composição étnica e populacional
    - **C4 :** Grande parte da população não compreende a língua oficial
    - **C5 :** Pelo menos três religiões coexistem no país
  - Geolocalização e Acordos assinados pelo país
    - **C6 :** Membro da CEDEAO
    - **C7 :** Membros dos países de língua portuguesa
    - **C8 :** Membro da África Unida (Assinou a Convenção de Malabo)
    - **C9 :** Ratificou o Pacto Internacional sobre os Direitos Civis e Políticos (ICCPR)
  - Situação económica do país
    - **C10 :** O orçamento nacional é frequentemente deficitário
  - Disponibilidade de tecnologias e recursos qualificados
    - **C11 :** Falta de competências
    - **C12 :** Falta de tecnologia
  - Estado de direito e capacidade de o fazer cumprir
    - **C13 :** Falta de legislação para fazer cumprir a cibersegurança e a proteção de dados
    - **C14 :** Falta de entidade de controlo e de aplicação da lei

Eis o quadro de seleção

	Modelo de governança implementado	Política		Culturais		Geolocalização e acordos				Economia	Tecnologia e competências		Estado de direito	
País	**C1**	**C2**	**C3**	**C4**	**C5**	**C6**	**C7**	**C8**	**C9**	**C10**	**C11**	**C12**	**C13**	**C14**
Guiné-Bissau	Não	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim	Sim
Português	Sim	Não	Sim	Não	Sim	Não	Sim	Não	Sim[1]	Sim[2]	Não	Não	Não	Não
Brasil	Sim	Sim	Sim	Não	Sim	Não	Sim	Não	Sim[3]	Sim[4]	Não	Não	Não	Não
Togo	Sim	Não	Não	Sim	Sim	Sim	Não	Sim[5]	Sim[6]	Sim[7]	Não	Sim	Não	Não
Gana	Sim	Não	Não	Sim	Sim	Sim	Não	Sim[8]	Sim[9]	Sim[10]	Não	Sim	Não	Não
Benim	Sim	Não	Não	Sim	Sim	Sim	Não	Sim[11]	Sim[12]	Sim[13]	Não	Sim	Não	Não

[4] https://ijrcenter.org/wp-content/uploads/2020/02/Portugal-Factsheet.pdf
[5] https://tradingeconomics.com/portugal/government-budget
[6] https://ijrcenter.org/wp-content/uploads/2018/04/Brazil-Factsheet.pdf
[7] https://tradingeconomics.com/brazil/government-budget-value
[8] https://www.uneca.org/stories/republic-of-togo-and-the-united-nations-economic-commission-for-africa-sign-a-memorandum-of
[9] https://www.pgaction.org/es/news/togo-second-optional-protocol.html
[10] https://tradingeconomics.com/togo/government-budget
[11] https://dataprotection.africa/malabo-convention-set-to-enter-force/
[12] https://www.pgaction.org/campaigns/adp/gha.html
[13] https://tradingeconomics.com/ghana/government-budget#:~:text=Ghana%20recorded%20a%20Government%20Budget,percent%20of%20GDP%20in%202008.
[14] https://dataprotection.africa/malabo-convention-set-to-enter-force/
[15] https://en.wikipedia.org/wiki/International_Covenant_on_Civil_and_Political_Rights#States_which_are_neither_signatories_nor_parties
[16] https://tradingeconomics.com/benim/government-budget

Com base na seleção dos países anteriores, exploramos o seu modelo de governança para comparar, em primeiro lugar, a forma como estão estruturados. É importante notar que nem todos os países mencionam explicitamente o modelo de governança que utilizam. Deduzimo-lo com base no nosso conhecimento da sua estrutura e na informação que disponibilizam ao público. Esta análise dos modelos de governança destes países explora as complexidades dos seus quadros de governança. Examina até que ponto aderem a abordagens centralizadas, descentralizadas ou híbridas. Serão explorados os mecanismos de governança, os quadros jurídicos, as estruturas institucionais, as infraestruturas tecnológicas, as capacidades de resposta a incidentes e as iniciativas de colaboração destes países.

Benim :

Apresentação das características do Benim :

Figura 7: Panorâmica do índice do Benim em 2022[17]

Modelo de governança :

O Benim utiliza um modelo centralizado de governança da cibersegurança, com a Agência dos Sistemas de Informação e do Digital (ASIN) a supervisionar a estratégia e as políticas nacionais de cibersegurança.

Quadro jurídico e regulamentos:

As principais leis e regulamentos incluem:

1. Ato Digital: Define e penaliza a cibercriminalidade e estabelece medidas de cibersegurança.
2. Lei de Proteção de Dados: Regula o tratamento e a proteção dos dados pessoais.

Estrutura institucional:

A principal instituição responsável pela cibersegurança no Benim é a Agência dos Sistemas de Informação e do Digital (ASIN em francês), que tem por missão coordenar e aplicar as políticas de cibersegurança. A agência acolhe a Equipa de Resposta a Incidentes de Segurança Informática do Benim (bjCSIRT), que é responsável pela resposta a incidentes de segurança informática.

A Autoridade para a Proteção dos Dados Pessoais (APDP) é responsável pelo controlo e regulamentação da proteção dos dados pessoais na República do Benim.

infraestruturas tecnológicas:

O Benim está a investir nas suas infraestruturas de TIC, concentrando-se na melhoria da conetividade à Internet e na segurança dos seus sistemas digitais. O país está a aumentar a desmaterialização de todos os procedimentos de pedido de documentos administrativos e está também a investir fortemente na operacionalização da sua PKI nacional.

Resposta e gestão de incidentes:

A Equipa de Resposta a Incidentes de Segurança Informática do Benim (bjCSIRT) gere os incidentes de cibersegurança, oferecendo coordenação e apoio na resposta a incidentes.

Cooperação internacional:

O Benim participa em fóruns internacionais de cibersegurança e colabora com organizações regionais como a Comunidade Económica dos Estados da África Ocidental (CEDEAO) e entidades mundiais como a UIT.

Evolução da cibersegurança e da proteção de dados ao longo dos anos

A figura seguinte mostra a evolução da estrutura da cibersegurança e da proteção de dados ao longo dos anos.

[17] https://ncsi.ega.ee/country/bj_2022/

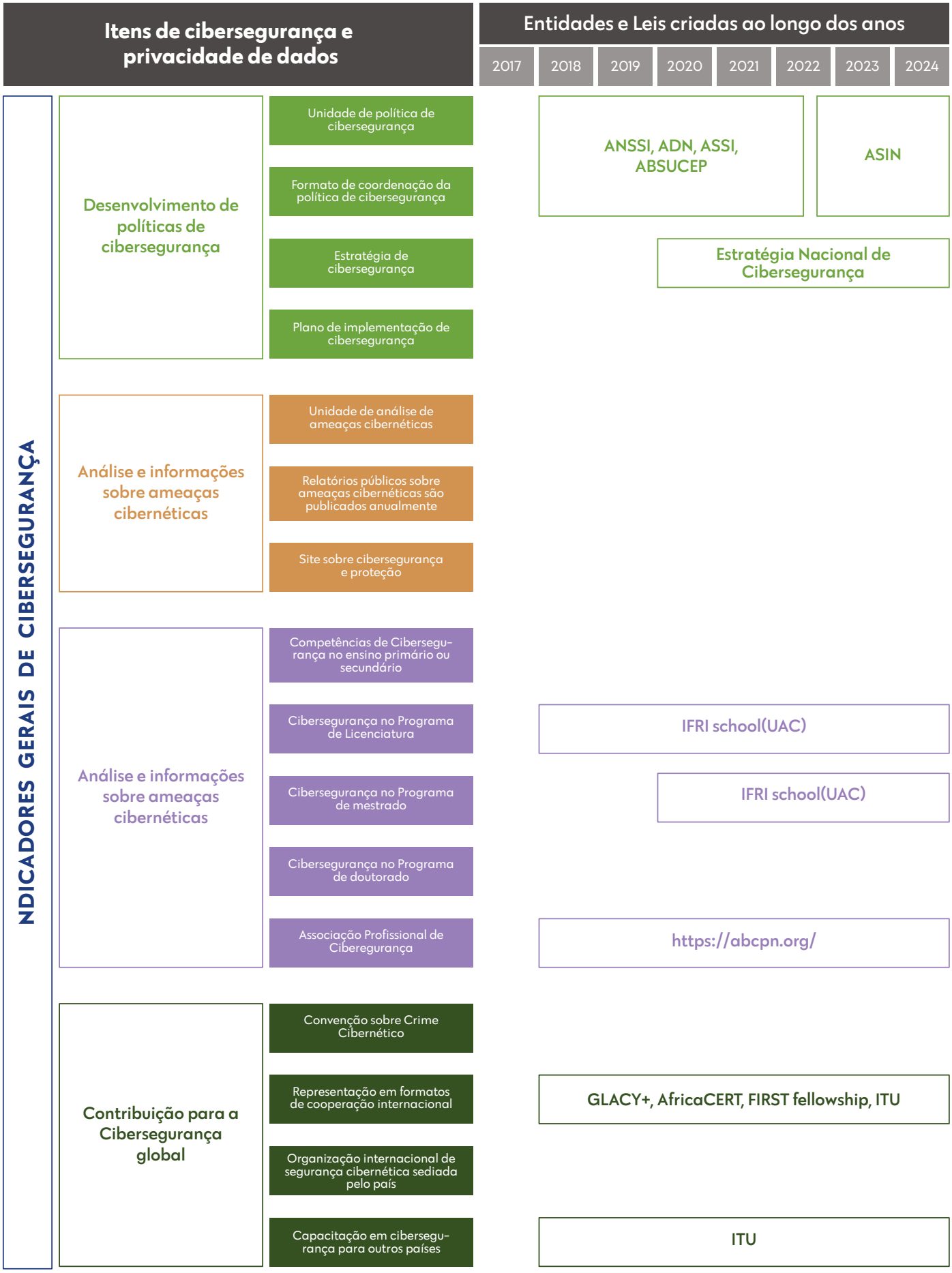

Figura 8: Indicador geral de cibersegurança no Benim ao longo dos anos

INDICADORES DE BASE DE CIBERSEGURANÇA	Itens de cibersegurança e privacidade de dados		Entidades e Leis criadas ao longo dos anos
			2017 / 2018 / 2019 / 2020 / 2021 / 2022 / 2023 / 2024
	Proteção de serviços digitais	Responsabilidade de cibersegurança para provedores de serviços digitais	
		Padrão de cibersegurança para o setor público	
		Autoridade de supervisão competente	ANSSI / ASIN
	Proteção de serviços essenciais	Operadores de serviços essenciais são identificados	Artigos 82- 86 https://sgg.gouv.bj/doc/loi-2017-20/
		Requisitos de cibersegurança para operadores de serviços essenciais	
		Autoridade de supervisão competente	ANSSI / ASIN
		Monitoramento regular das medidas de segurança	
	Serviços de Confiança Identificação Eletrônica	Identificador persistente unico	ANIP, RAVIP
		Requisitos para criptosistemas	
		Identificação eletrônica	Artigos 278 - 283 https://sgg.gouv.bj/doc/loi-2017-20/
		Assinatura Eletrônica	Artigos 284 - 298 https://sgg.gouv.bj/doc/loi-2017-20/
		Carimbo de data e hora	Artigos 299 - 300 https://sgg.gouv.bj/doc/loi-2017-20/
		Serviço de entrega eletrônica registrada	
		Autoridade de supervisão competente	Artigos 317 - 325 https://sgg.gouv.bj/doc/loi-2017-20/
	Contribuição para a Cibersegurança global	Organização internacional de segurança cibernética sediada pelo país	O livro 5 da lei https://sgg.gouv.bj/doc/loi-2017-20/
		Capacitação em cibersegu-rança para outros países	APDP e Artigos 462 https://sgg.gouv.bj/doc/loi-2017-20/

Figura 9: Indicador de base da cibersegurança no Benim ao longo dos anos

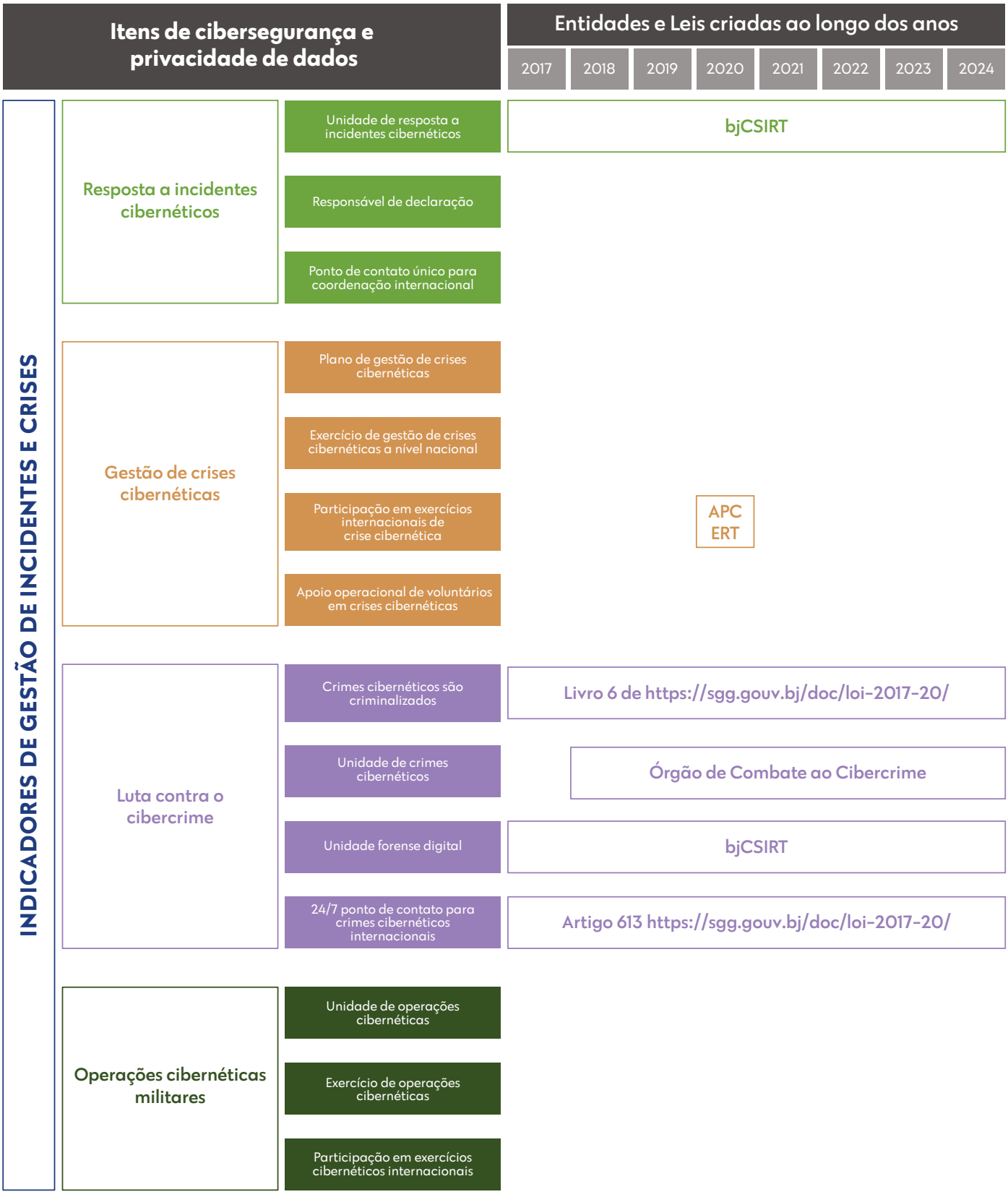

Figura 10: Indicadores de gestão de incidentes e crises no Benim ao longo dos anos[18]

[18] https://ncsi.ega.ee/country/bj_1/?selectedCountryIndex=652#details

Brasil :

Apresentação das características do Brasil :

Figura 11 : Panorama do índice Brasil em 2022[19]

Modelo de governança:
A governança da segurança cibernética no Brasil é híbrida, envolvendo várias partes interessadas, incluindo entidades governamentais, o setor privado e a sociedade civil. O Comité Gestor da Internet no Brasil (CGI.br) coordena as políticas relacionadas à Internet, enquanto o Comando de Defesa Cibernética concentra-se na proteção de infraestruturas críticas.

Quadro jurídico e regulamentos:
Os principais quadros jurídicos do Brasil em matéria de cibersegurança incluem:

1. Marco Civil da Internet: Marco Civil da Internet: regulamentação da utilização da Internet.
2. Lei Geral de Proteção de Dados (LGPD): Regula a proteção de dados e a privacidade.

Estrutura institucional:
O Comité Gestor da Internet no Brasil (CGI.br) e o Comando de Defesa Cibernética são instituições-chave responsáveis pela coordenação de políticas de segurança cibernética e pela proteção de infraestruturas críticas.

infraestruturas tecnológicas:
O Brasil tem uma infraestrutura tecnológica robusta, com redes de telecomunicações avançadas e vários centros de dados.

Resposta e gestão de incidentes:
A Equipe Nacional de Resposta a Emergências em Computadores (CERT.br) e o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Governo Brasileiro (CTIR Gov-BR) são responsáveis pelo gerenciamento e resposta a incidentes.

Cooperação internacional:
O Brasil participa ativamente de iniciativas internacionais de segurança cibernética e colabora com organizações como a Organização dos Estados Americanos (OEA) e a União Internacional de Telecomunicações (UIT).

Evolução da cibersegurança e da proteção de dados ao longo dos anos
A figura seguinte mostra a evolução da estrutura da cibersegurança e da proteção de dados ao longo dos anos.

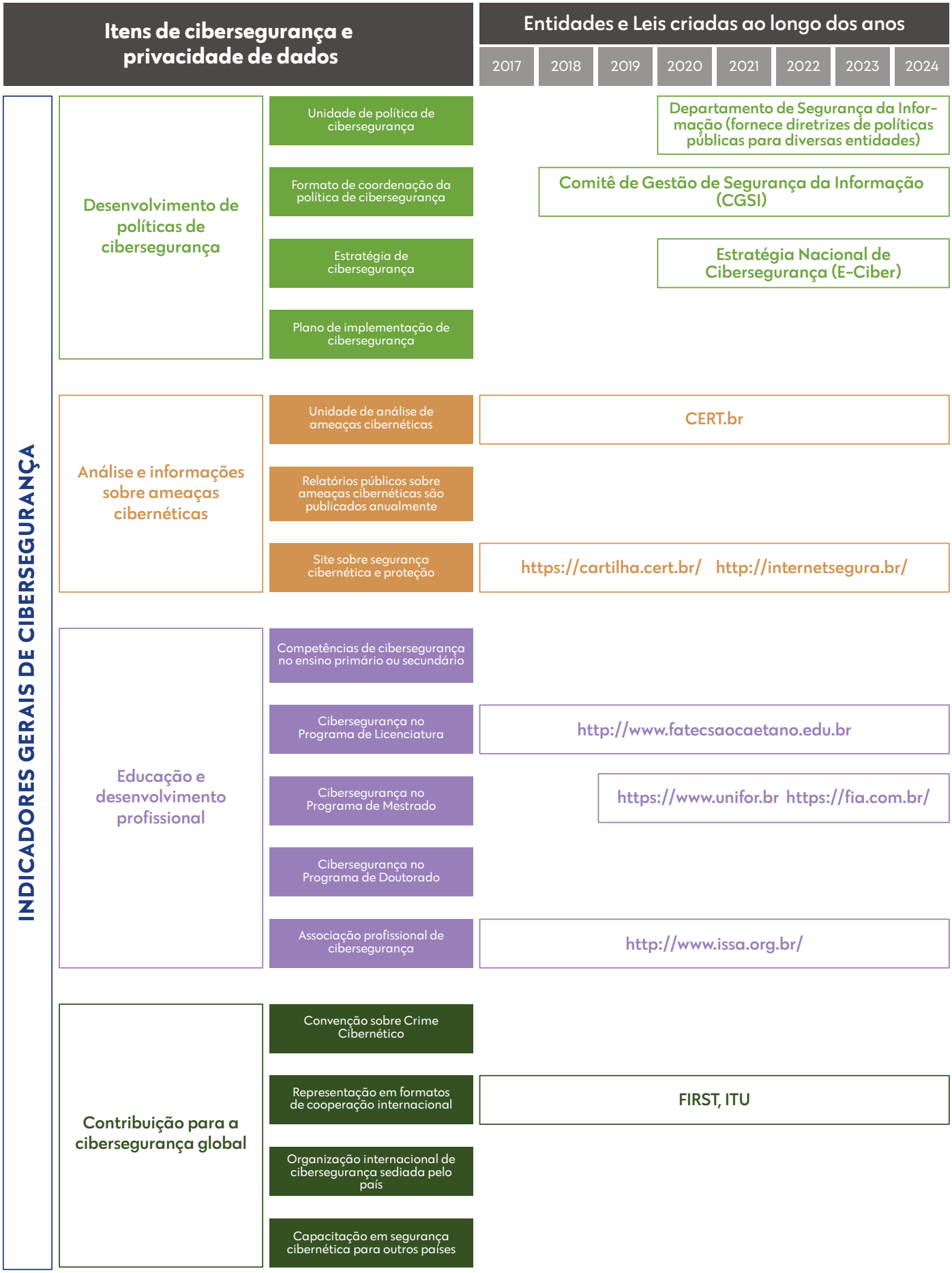

Figura 12 : Indicador geral de cibersegurança no Brasil ao longo dos anos[20]

[20] https://ncsi.ega.ee/country/br_1/?selectedCountryIndex=40#details

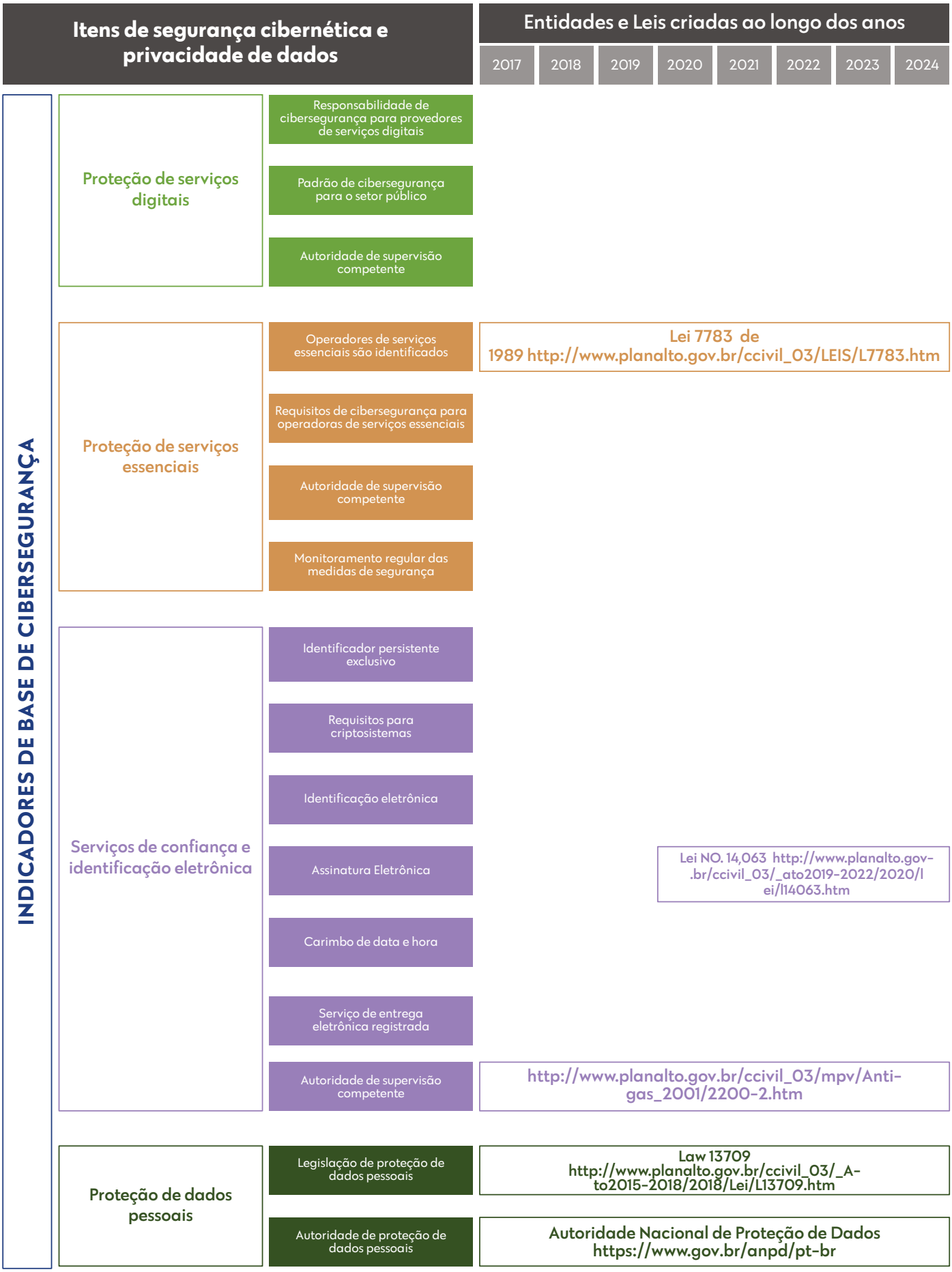

Figura 13 : Indicador de base da cibersegurança no Brasil ao longo dos anos[21]

[21] https://ncsi.ega.ee/country/br_1/?selectedCountryIndex=40#details

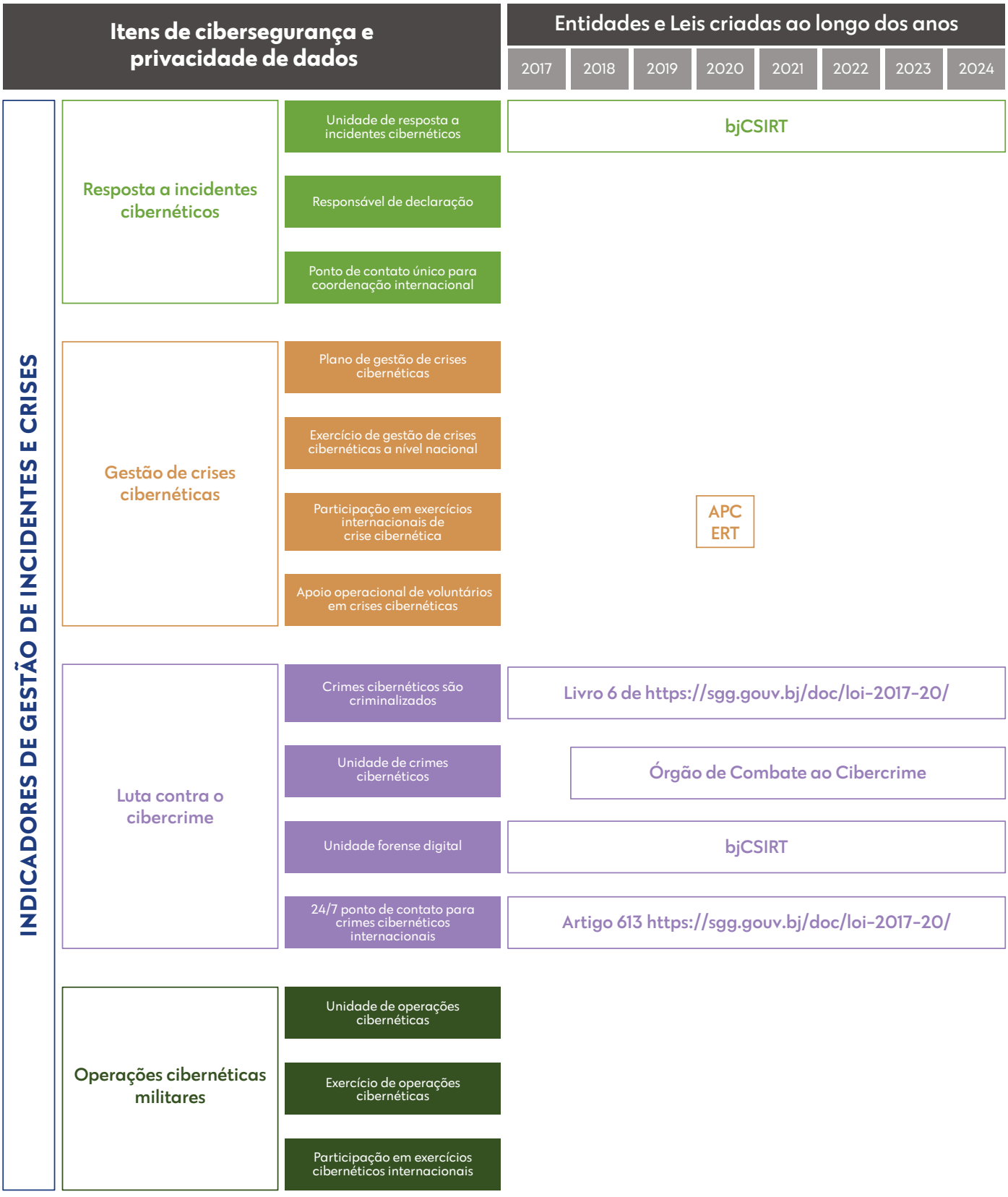

Figura 14: Indicadores de gestão de incidentes e crises no Brasil ao longo dos anos[22]

[22] https://ncsi.ega.ee/country/br_1/?selectedCountryIndex=40#details

Gana :

Apresentação das características do Gana :

Figura 15 : Panorâmica do índice do Gana em 2024[23]

Modelo de governança:
O Gana utiliza um modelo de governança centralizado, com a Autoridade de Cibersegurança (CSA) e o Centro Nacional de Cibersegurança (NCSC) a supervisionar todas as atividades de cibersegurança sob a tutela do Ministério das Comunicações e da Digitalização.

Quadro jurídico e regulamentos:
As principais leis do Gana em matéria de cibersegurança incluem:

1. Lei das Transações Electrónicas: Regula as transações e comunicações electrónicas.
2. Lei da Proteção de Dados: Garante a privacidade dos dados pessoais.
3. Lei da Cibersegurança, 2020: Legislação abrangente que aborda vários aspetos da cibersegurança.

Estrutura institucional:
A Autoridade de Cibersegurança (CSA) e o Centro Nacional de Cibersegurança (NCSC) são as principais entidades responsáveis pela cibersegurança no Gana. A CSA está encarregada de regulamentar e promover a cibersegurança, enquanto o NCSC coordena os esforços nacionais para garantir a cibersegurança. A Comissão de Proteção de Dados (PDC) protege os direitos e a privacidade das pessoas.

infraestruturas tecnológicas:
O Gana está a expandir as suas infraestruturas de TIC, concentrando-se na melhoria do acesso à Internet e das capacidades de cibersegurança.

Resposta e gestão de incidentes:
O CERT-GH do Gana é responsável pela resposta a incidentes, proporcionando um ponto centralizado para a gestão de incidentes de cibersegurança.

Cooperação internacional:
O Gana participa em colaborações regionais e internacionais no domínio da cibersegurança, nomeadamente com a CEDEAO e a UIT.

Evolução da cibersegurança e da proteção de dados ao longo dos anos
A figura seguinte mostra a evolução da estrutura de cibersegurança e proteção de dados ao longo dos anos.

[23] https://ncsi.ega.ee/country/gh/

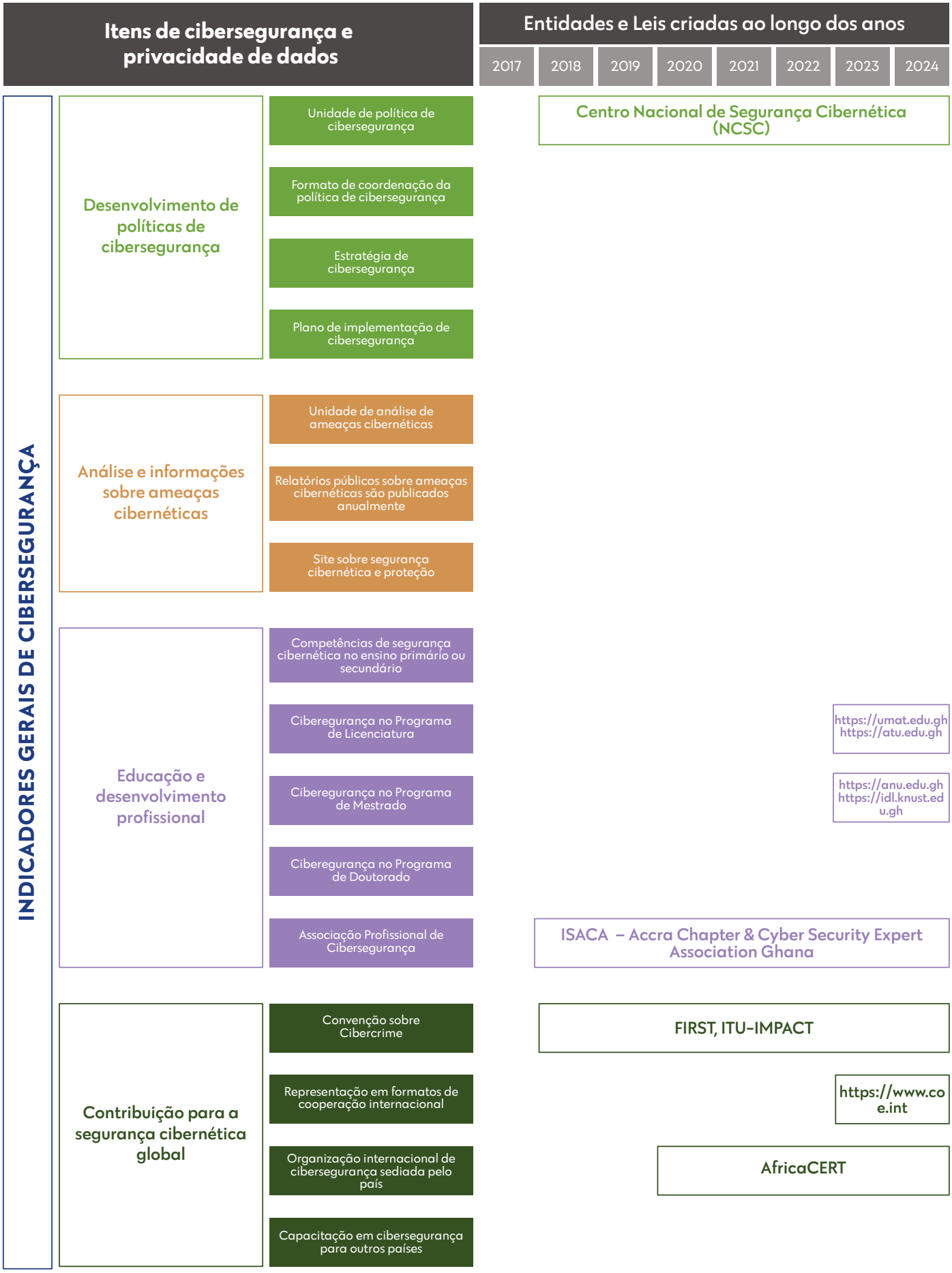

Figura 16 : Indicador geral de cibersegurança no Gana ao longo dos anos[24]

[24] https://ncsi.ega.ee/country/gh_1/?selectedCountryIndex=473#details

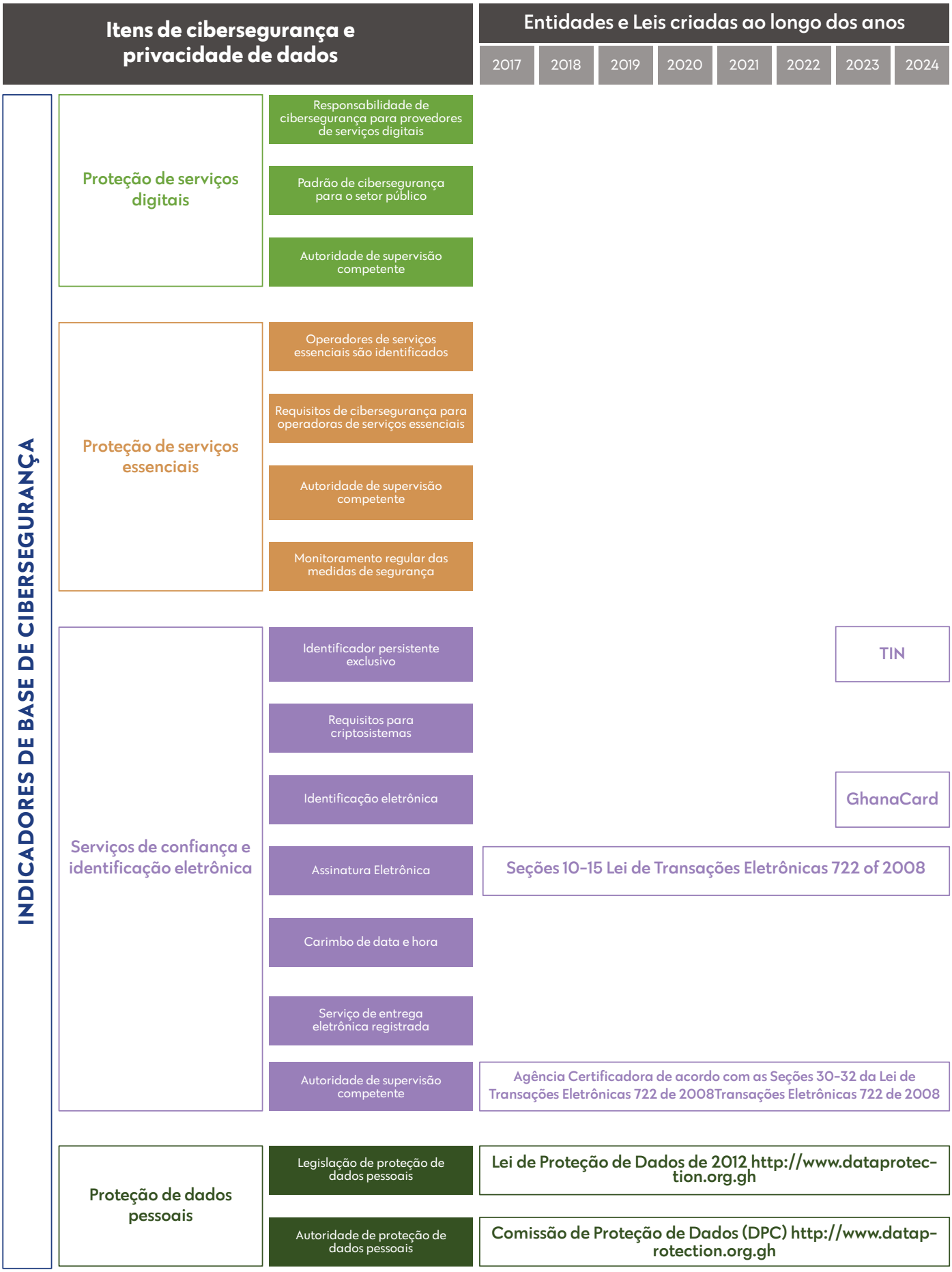

Figura 17: Indicador de base da cibersegurança no Gana ao longo dos anos[25]

[25] https://ncsi.ega.ee/country/gh_1/?selectedCountryIndex=473#details

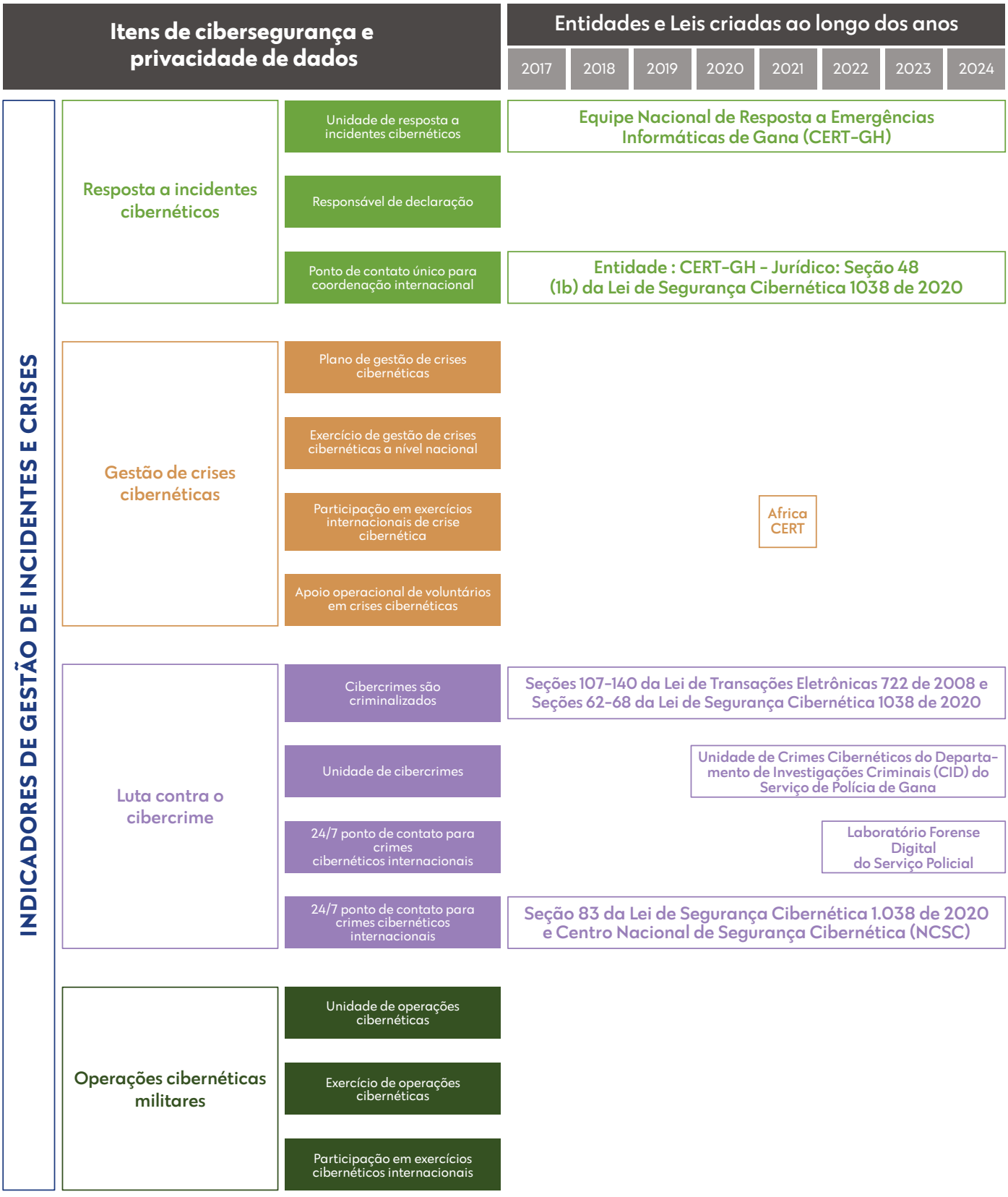

Figura 18 : Indicadores de gestão de incidentes e crises no Gana ao longo dos anos[26]

[26] https://ncsi.ega.ee/country/gh_1/?selectedCountryIndex=473#details

Portugal :

Apresentação das características de Portugal :

Figura 19 : Panorâmica do índice de Portugal em 2021[27]

Modelo de governança:
Portugal utiliza um modelo de governança híbrido, com uma direção política centralizada do Centro Nacional de Cibersegurança (CNCS) e funções operacionais descentralizadas a cargo de vários intervenientes, incluindo a Autoridade Nacional de Comunicações (ANACOM).

Quadro jurídico e regulamentos:
Os principais quadros jurídicos de Portugal em matéria de cibersegurança incluem:

1. Regulamento Geral sobre a Proteção de Dados (RGPD): Regulamento de proteção de dados à escala da UE.
2. Lei da Cibersegurança: Legislação nacional alinhada com a Lei da Cibersegurança da UE.
3. Vários decretos e leis nacionais: Regulamentos específicos que abordam diferentes aspetos da cibersegurança.

Estrutura institucional:
O Centro Nacional de Cibersegurança (CNCS), sob a tutela do Ministério da Defesa Nacional, coordena as políticas e iniciativas de cibersegurança. A Autoridade Nacional de Comunicações (ANACOM) é uma entidade administrativa independente. Desempenha um papel importante na regulação do sector das comunicações, das comunicações electrónicas e postais.

infraestruturas tecnológicas:
Portugal dispõe de infraestruturas TIC avançadas, com uma extensa cobertura de banda larga e centros de dados sofisticados.

Resposta e gestão de incidentes:
O CNCS opera o CERT nacional (CERT.PT), que é responsável pela gestão e resposta a incidentes de cibersegurança. A Comissão Nacional de Proteção de Dados (CNPD) protege os direitos e a privacidade dos indivíduos.

Cooperação internacional:
Portugal participa ativamente em fóruns internacionais de cibersegurança, cooperando com a UE, a NATO e outras organizações mundiais.

Evolução da cibersegurança e da proteção de dados ao longo dos anos
A figura seguinte mostra a evolução da estrutura da cibersegurança e da proteção de dados ao longo dos anos.

[27] https://ncsi.ega.ee/country/pt_2022/

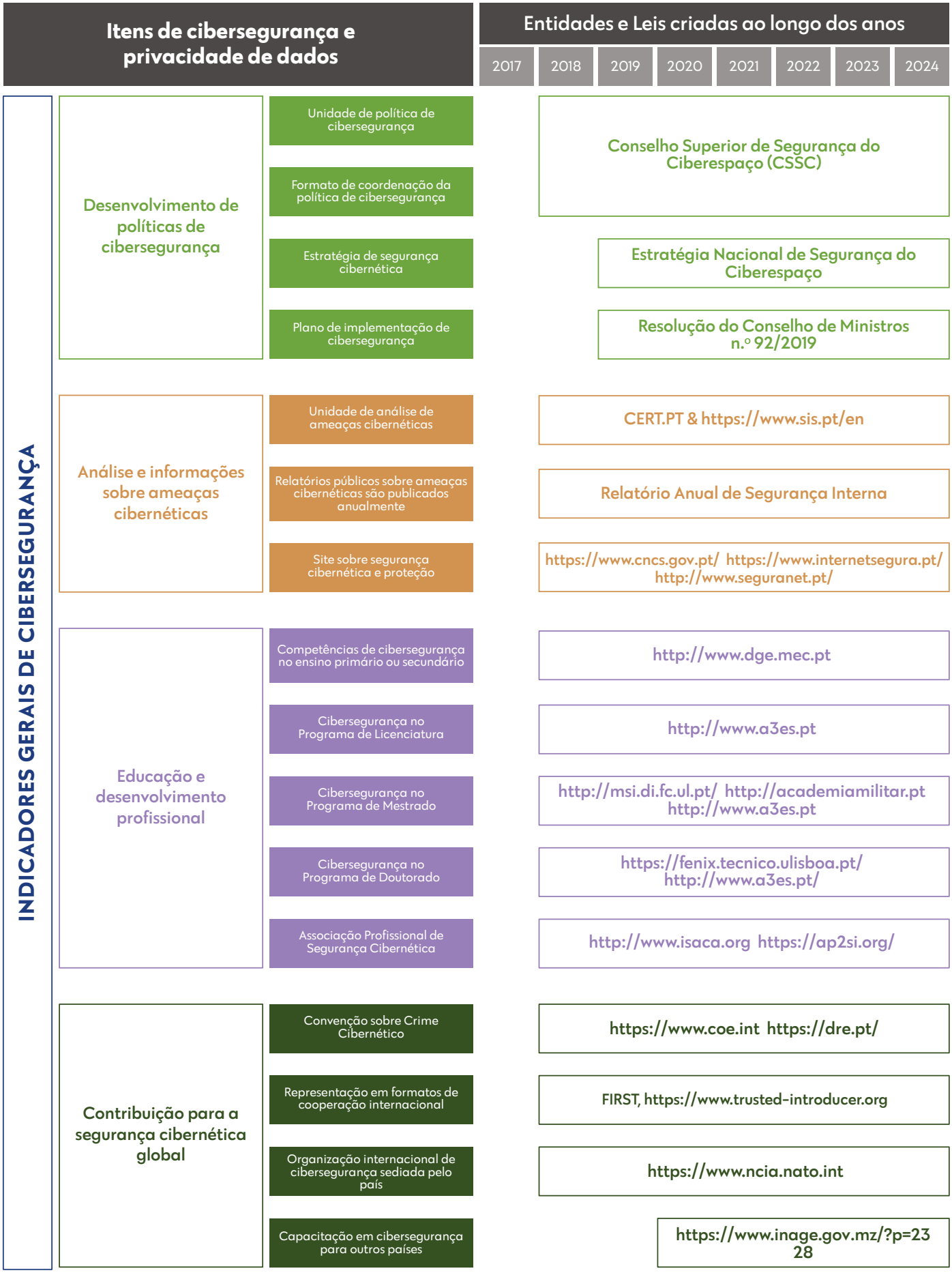

Figura 20 : Indicador geral de cibersegurança em Portugal ao longo dos anos[28]

[28] https://ncsi.ega.ee/country/pt_1/?selectedCountryIndex=525#details

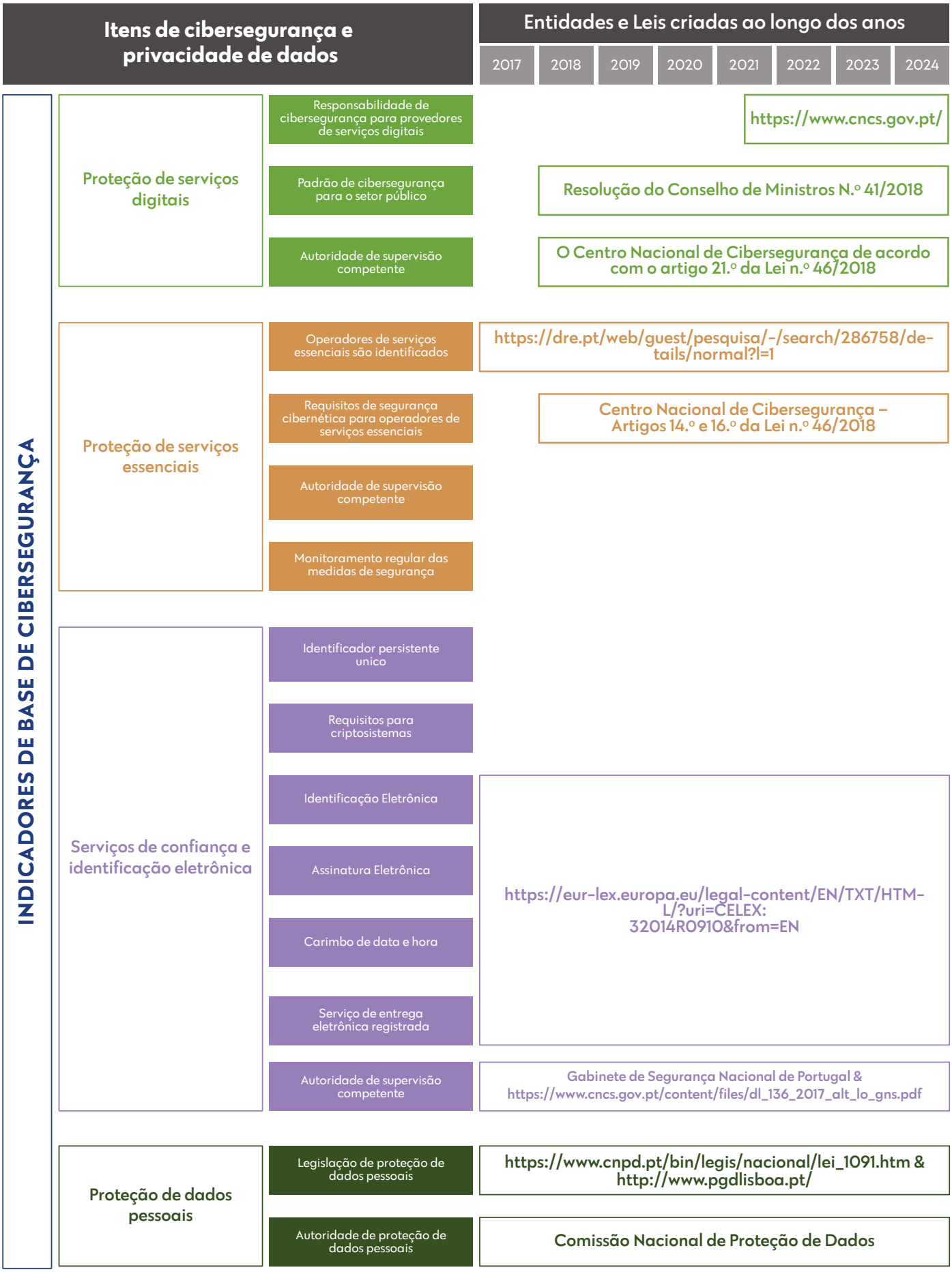

Figura 21: Indicador de base da cibersegurança em Portugal ao longo dos anos[29]

[29] https://ncsi.ega.ee/country/pt_1/?selectedCountryIndex=525#details

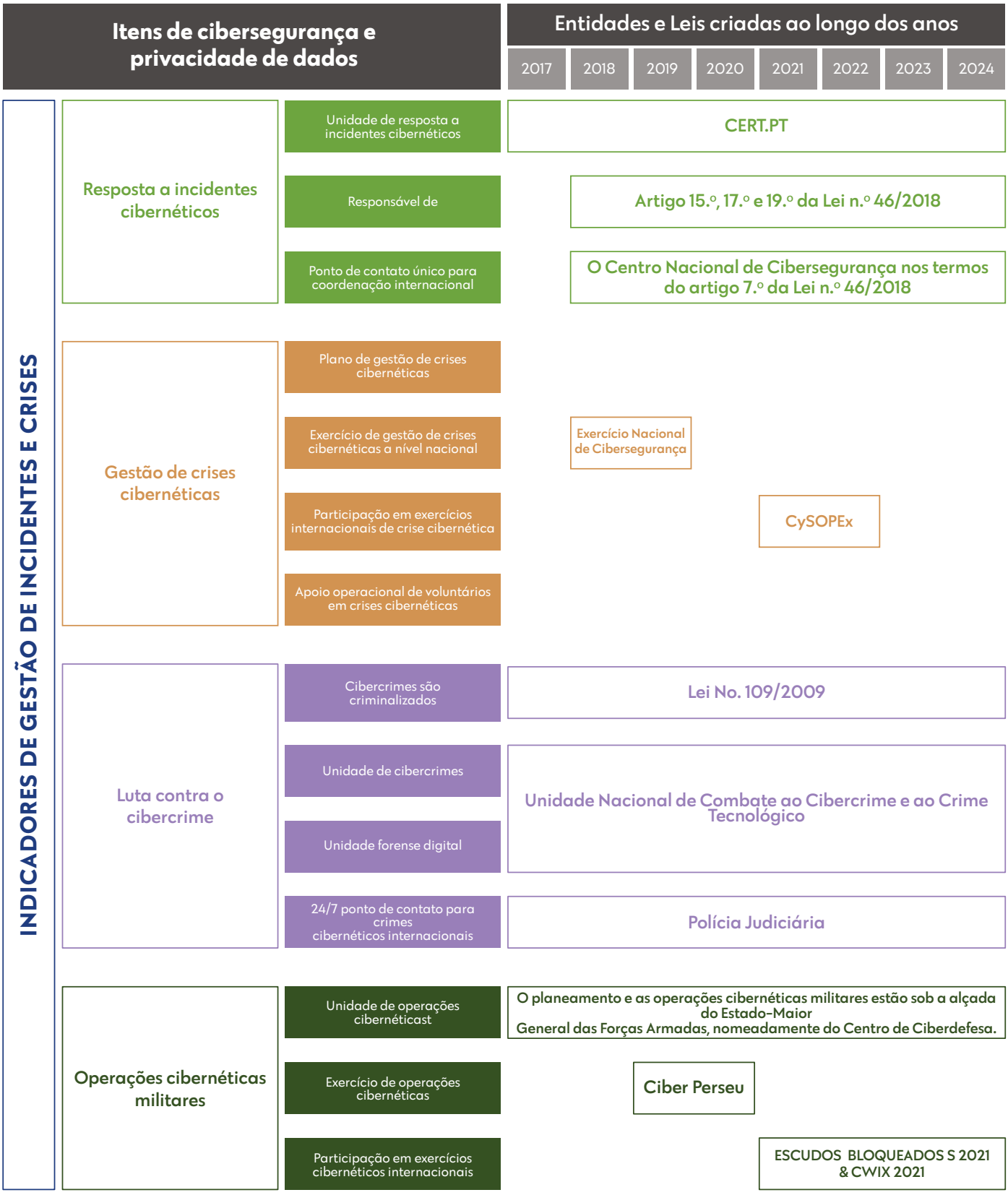

Figura 22 : Indicadores de gestão de incidentes e crises em Portugal ao longo dos anos[30]

[30] https://ncsi.ega.ee/country/pt_1/?selectedCountryIndex=525#details

Togo :

Apresentação das características do Togo :

Figura 23 : Panorâmica do índice do Togo em 2023[31]

Modelo de governança:
O Togo segue um modelo centralizado de governança da cibersegurança, sendo a Agência Nacional de Cibersegurança (Agence Nationale de la Cybersécurité - ANCy) a principal entidade responsável pela supervisão e coordenação dos esforços de cibersegurança.

Quadro jurídico e regulamentos:
1. Lei da Cibersegurança: Define os cibercrimes, as sanções e estabelece quadros regulamentares para a cibersegurança.
2. Lei de Proteção de Dados: Regula o tratamento e a proteção dos dados pessoais.
3. Lei das transacões electrónicas: Regula as transacões electrónicas e as assinaturas digitais para garantir a segurança do comércio em linha.

Estrutura institucional:
A Agência Nacional de Cibersegurança (ANCy): A entidade central responsável pela formulação e implementação de políticas nacionais de cibersegurança, pela coordenação de esforços entre as várias partes interessadas e pela garantia do cumprimento da regulamentação em matéria de cibersegurança.

Ministério da Economia Digital e da Transformação Digital: Proporciona uma orientação política global e apoia o desenvolvimento de infraestruturas digitais e iniciativas de cibersegurança.

Infraestruturas tecnológicas:
O Togo está a investir ativamente na sua infraestrutura tecnológica para melhorar a conetividade digital e as capacidades de cibersegurança. Isto inclui a expansão do acesso à Internet, a melhoria dos serviços digitais e a implantação de tecnologias avançadas de cibersegurança.

Estão em curso iniciativas para desenvolver uma sólida infraestrutura nacional de chave pública (PKI) para proteger as comunicações e transações electrónicas.

Resposta e gestão de incidentes:
Equipa Nacional de Resposta a Incidentes de Cibersegurança (CERT-TG): trata de incidentes de cibersegurança, fornece estratégias de análise e atenuação e coordena os esforços de resposta. A CERT-TG funciona sob a orientação da ANCy para garantir uma abordagem coesa da gestão de incidentes.

O Togo está concentrado no desenvolvimento de capacidades para uma resposta eficaz a incidentes através de programas de formação e colaborações internacionais.

Cooperação internacional:
O Togo participa em iniciativas e fóruns regionais e internacionais de cibersegurança, como a Comunidade Económica dos Estados da África Ocidental (CEDEAO)

[31] https://ncsi.ega.ee/country/tg/

e a União Internacional das Telecomunicações (UIT). Estas colaborações visam partilhar as melhores práticas, melhorar os conhecimentos técnicos e coordenar as respostas às ciberameaças transnacionais.

Evolução da cibersegurança e da proteção de dados ao longo dos anos

O Togo não dispõe de muitos anos de dados históricos que possamos recolher. A agência ANCy está a tratar de toda a governança da cibersegurança e da proteção de dados num modelo centralizado.

B. Análise comparativa: sucessos, fracassos e lições aprendidas

Ao avaliar os modelos de governança da cibersegurança do Benim, Brasil, Togo, Gana e Portugal, emergem vários sucessos, desafios e lições importantes. A abordagem centralizada do Benim facilitou a implementação eficaz de políticas através da ASIN, apoiada por quadros jurídicos sólidos como o Ato Digital e a Lei de Proteção de Dados. No entanto, os desafios em termos de infraestruturas e a necessidade de melhorar as capacidades de resposta a incidentes continuam a ser áreas a melhorar, apesar da participação ativa em fóruns internacionais de cibersegurança. A pontuação da ITU GCI do Benim para 2020 foi de 0,463, colocando-o globalmente na posição 99.

O modelo de governança híbrido do Brasil promove um amplo envolvimento das partes interessadas, apoiado por quadros jurídicos avançados, como o Marco Civil da Internet e a LGPD, juntamente com uma infraestrutura TIC robusta. Os desafios de coordenação entre as entidades e a necessidade de melhorar as capacidades de resposta a incidentes em todo o país destacam as áreas de melhoria em curso. O Brasil alcançou uma pontuação GCI da UIT de 0,765 em 2020, classificando-se em 18º lugar no mundo.

O modelo centralizado do Gana, liderado pela CSA e pelo NCSC, garante esforços simplificados de cibersegurança e um quadro jurídico sólido com a Lei da Cibersegurança, embora as limitações de recursos e as lacunas na sensibilização do público continuem a ser desafios. As lições a tirar incluem a necessidade crítica de recursos adequados, financiamento e programas abrangentes de sensibilização do público. A pontuação da ITU GCI do Gana para 2020 foi de 0,569, colocando-o globalmente na posição 69.

O modelo de governança híbrido de Portugal equilibra a direção política centralizada com operações descentralizadas, apoiadas por infraestruturas TIC avançadas e quadros jurídicos rigorosos como o RGPD e a Lei da Cibersegurança. As questões de coordenação e a necessidade de melhorar as capacidades de resposta a incidentes sublinham as necessidades de melhoria em curso. Portugal alcançou uma pontuação ITU GCI de 0,748 em 2020, classificando-se em 22ºlugar a nível mundial.

O modelo centralizado do Togo é supervisionado pela Agência Nacional de Cibersegurança (ANCY). O quadro legal inclui a Lei do Cibercrime, que define e penaliza as infrações cibernéticas, e a Lei de Proteção de Dados, que regula o processamento e a proteção de dados pessoais. O país investiu em infraestruturas de TIC para melhorar a conetividade e a segurança da Internet. A Equipa de Resposta a Incidentes de Segurança Informática do Togo (CERT-TG) é responsável pela resposta a incidentes. O Togo participa em colaborações regionais e internacionais no domínio da cibersegurança. A pontuação da ITU GCI do Togo para 2020 foi de 0,466, colocando-o em 96ºlugar a nível mundial.

A pontuação de cada país no Índice Global de Cibersegurança (GCI) da UIT fornece uma referência comparativa, refletindo os diferentes níveis de preparação para a cibersegurança e a eficácia institucional a nível mundial. Estas análises destacam as diversas abordagens e os esforços em curso nesses países para reforçar as estruturas de cibersegurança, enfrentar os desafios e adaptar-se à evolução das ameaças à cibersegurança à escala regional e internacional.

Para ter uma visão clara de cada país e da classificação do seu modelo, basear-nos-emos na pontuação NCSI. A pontuação NCSI é calculada com base na notação

do país em vários domínios.
Existem três categorias que estão divididas num total de doze subcategorias. Essas subcategorias também são divididas para serem mais granulares. A presença de cada item de governança dará uma pontuação.

Assim, a pontuação NCSI é a percentagem da soma dos pontos obtidos em relação ao total de pontos possíveis. Quanto mais elevada for a pontuação, melhor será a classificação, indicando uma forte postura de cibersegurança.

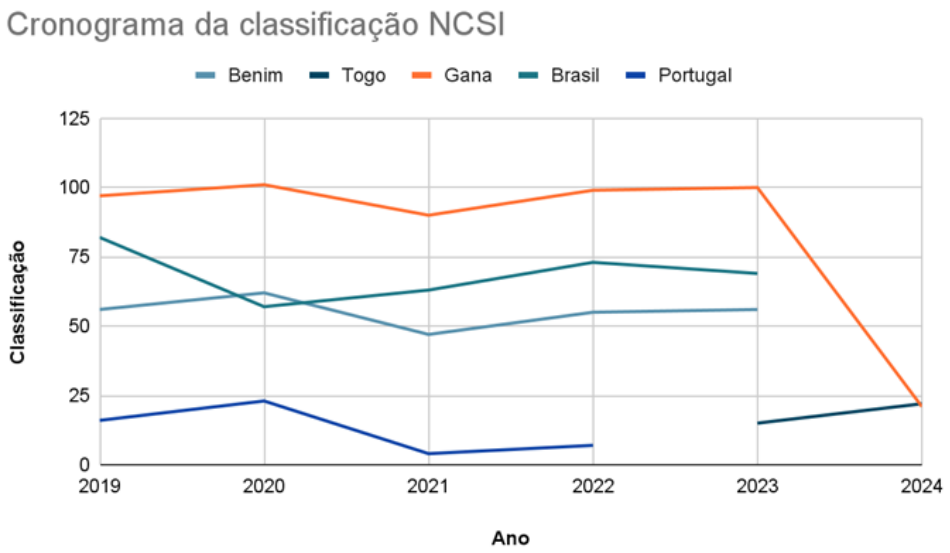

Figura 24 : Calendário da classificação NCSI para os países selecionados[32,33,34,35,36]

Ano	Benim	Togo	Gana	Brasil	Portugal
2019	56		97	82	16
2020	62		101	57	23
2021	47		90	63	4
2022	55		99	73	7
2023	56	15	100	69	
2024		22	21		

Quadro 3: Dados da classificação NCSI para os países seleccionados

O gráfico anterior foi elaborado com base nos dados recolhidos no portal NCSI. Se a visão mudar e certas entidades forem abolidas ou tiverem o seu mandato alterado drasticamente, desviando-se do seu objetivo principal, a pontuação será diretamente afetada. Esta mudança de visão pode resultar de instabilidade ou de qualquer outro motivo.

A evolução da classificação de cada país selecionado é apresentada no gráfico. Alguns dos países da nossa lista não tinham dados, porque por vezes a informação não está disponível ao público.

Podemos ver que Portugal, com o seu modelo de governança híbrido, se destaca. Este facto pode ser explicado pela maturidade do sistema, pelo orçamento atribuído e pela flexibilidade do seu modelo para ser escalável ao longo dos anos e tornar-se melhor.

[32] https://ncsi.ega.ee/country/pt_2022/
[33] https://ncsi.ega.ee/country/bj_2022/
[34] https://ncsi.ega.ee/country/tg_2022/
[35] https://ncsi.ega.ee/country/gh_2022/
[36] https://ncsi.ega.ee/country/br_2022/

VI. PRINCÍPIOS E FATORES DE DECISÃO

A. Discussão sobre os princípios que regem a seleção dos modelos de governança

A escolha de um modelo de governança adequado para a cibersegurança e a proteção de dados num país deve ser orientada por princípios bem definidos que garantam não só a eficácia, mas também o alinhamento com os objetivos nacionais e os valores culturais. Particularmente no caso da Guiné-Bissau, temos de considerar fatores que abordem tanto as realidades práticas como os objetivos estratégicos, a fim de criar um quadro forte, reativo e sustentável que responda tanto às necessidades actuais como aos desafios futuros:

- **Transparência**

O modelo de governança deve garantir que os processos e as decisões de governança estão abertos ao escrutínio, reforçando a confiança do público. Por exemplo, todos os pormenores sobre as iniciativas de cibersegurança devem ser regularmente atualizados e acessíveis ao público.

- **Responsabilidade**

O modelo de governança deve responsabilizar os indivíduos e as organizações pelas suas ações, garantindo que cumprem as suas obrigações e respondem perante as pessoas afetadas pelas suas decisões. Deve impor a criação de um organismo independente de supervisão da cibersegurança que não só audite as práticas de cibersegurança nos sectores público e privado, mas que também tenha autoridade para impor o cumprimento e penalizar o incumprimento. Esta entidade publicará relatórios anuais de avaliação da postura de cibersegurança do país.

- **Inclusão**

No caso da Guiné-Bissau, o envolvimento de universidades locais e de parceiros internacionais na África Ocidental ou na CPLP (Comunidade dos Países de Língua Portuguesa) poderia ajudar a integrar perspectivas e conhecimentos diversos.

- **Eficácia e eficiência**

Este princípio garante que o modelo de governança atinge os seus objetivos de forma atempada e eficiente em termos de recursos, simplificando os processos, assegurando que as políticas são orientadas para os resultados e apoiadas por recursos adequados e realizando avaliações regulares do desempenho.

- **Adaptabilidade**

O modelo deve permitir que as estruturas de governança respondam de forma dinâmica aos novos desafios e à evolução das ameaças no domínio da cibersegurança e da proteção de dados. Por exemplo, devemos desenvolver uma estratégia nacional de cibersegurança que inclua uma disposição específica para revisão e ajustamento periódicos com base nas ameaças emergentes e nos avanços tecnológicos.

A Guiné-Bissau poderia estabelecer um protocolo em que as suas políticas de cibersegurança fossem revistas de dois em dois anos, em consulta com especialistas internacionais em cibersegurança e vizinhos regionais, para se adaptarem ao cenário de ameaças cibernéticas da África Ocidental.

- **Integridade**

Este princípio promove o comportamento ético e a tomada de decisões, assegurando que as ações são tomadas com base na equidade e na justiça, sem ganhos pessoais. O modelo deve ajudar a criar um código de conduta claro para todo o pessoal da cibersegurança, particularmente para os que ocupam posições-chave na gestão de dados sensíveis. A formação regular e a aplicação rigorosa destes códigos, juntamente com mecanismos transparentes para denunciar comportamentos pouco éticos, podem ajudar a mitigar a corrupção, que tem sido um desafio na Guiné-Bissau.

- **Coesão e coordenação**

Este princípio garante uma ação unificada e harmoniosa entre as várias entidades governamentais e não governamentais envolvidas na cibersegurança e na proteção de dados. O modelo deve ajudar a facilitar a colaboração entre agências, estabelecendo forças-tarefa conjuntas e criando bases de dados centralizadas para a partilha de informações. Por exemplo, poderia-se criar um centro de comando centralizado para a cibersegurança que coordenasse vários departamentos governamentais, o sector privado e organismos interna-

cionais. Este centro poderia servir de plataforma para a partilha de informações sobre ameaças e coordenação de respostas em diferentes sectores, racionalizando esforços e evitando duplicações.

B. Fatores que influenciam as decisões sobre a governança da cibersegurança e da proteção de dados

Muitos fatores influenciam o processo de tomada de decisão durante a implementação do modelo de governança da cibersegurança e da proteção de dados. Especialmente no caso da Guiné-Bissau, estes fatores serão moldados por uma combinação de recursos limitados, instabilidade sociopolítica e normas culturais específicas. Eis os principais fatores particularmente relevantes.

Constrangimentos económicos
As limitações financeiras podem constituir um desafio significativo, afetando a capacidade de investir em infraestruturas sólidas de cibersegurança e em medidas de proteção dos dados. Por conseguinte, o modelo de governança tem de ser eficaz em termos de custos, centrando-se na maximização dos recursos limitados para cobrir as necessidades essenciais de segurança e privacidade.

Instabilidade política
As frequentes mudanças de governo ou agitações políticas perturbarão o planeamento a longo prazo e a implementação de estratégias de cibersegurança. O modelo de governança deve ser suficientemente resistente e flexível para resistir às perturbações políticas e continuar a funcionar eficazmente.

Infraestruturas tecnológicas
Com base nas nossas entrevistas e pesquisas, parece que o sector público da Guiné-Bissau pode ter uma infraestrutura tecnológica subdesenvolvida, o que pode limitar a sua capacidade de implementar medidas avançadas de cibersegurança. Os modelos de governança podem ter de dar prioridade a melhorias fundamentais na infraestrutura de TI para apoiar iniciativas mais sofisticadas de cibersegurança.

Quadro jurídico e regulamentar
A falta de um quadro jurídico que trate especificamente da cibersegurança e da proteção de dados é comum. A criação ou o reforço de quadros jurídicos deve ser uma prioridade para servir de base ao modelo de governança e garantir o alinhamento com as normas internacionais.

Parcerias internacionais
As parcerias com organizações internacionais e outros países fornecerão um apoio fundamental, incluindo financiamento, tecnologia e conhecimentos especializados. O modelo de governança deve integrar mecanismos para alavancar a cooperação internacional, a fim de melhorar as capacidades e alinhar-se com as melhores práticas mundiais.

Educação e sensibilização
A sensibilização e a compreensão das questões de cibersegurança e de proteção de dados são muito reduzidas. O modelo de governança tem de incorporar amplas campanhas de sensibilização do público e iniciativas educativas para aumentar a compreensão e o apoio às medidas de cibersegurança.

Reforço das capacidades
A Guiné-Bissau carece de competências locais em matéria de cibersegurança e proteção de dados. A formação e o desenvolvimento de talentos locais podem ser essenciais para uma governança sustentável e eficaz.

Atitudes culturais em matéria de cibersegurança e privacidade
Na Guiné-Bissau as normas culturais podem influenciar as perceções de privacidade e a importância de proteger as informações pessoais. O modelo deve ter em conta as atitudes locais e concentrar-se potencialmente na educação da população sobre os benefícios da proteção de dados.

Envolvimento do sector privado
Não há participação do sector privado nas iniciativas de cibersegurança. O modelo de governança deve incentivar ou impor a participação do sector privado para reforçar a resiliência global da cibersegurança nacional.

Adaptabilidade e escalabilidade

O cenário das ciberameaças está em constante evolução, com novas ameaças a surgirem rapidamente. O modelo de governança deve ser adaptável e escalável, permitindo respostas rápidas a novas ameaças e tecnologias em mudança.

VII. CRENÇAS E CONVICÇÕES FUNDAMENTAIS

A. As nossas crenças e convicções fundamentais que orientam o estudo de viabilidade e influenciam a escolha do modelo de governança.

Com base nas nossas análises, será mais benéfico para a Guiné-Bissau implementar o Modelo de Governança Híbrido para a cibersegurança e a proteção de dados. Esta decisão decorre da convicção de que um quadro de governança flexível, reativo e inclusivo é essencial para enfrentar eficazmente os desafios únicos da cibersegurança do país, bem como informada por referências bem sucedidas de países com estruturas e desafios de governança relacionáveis, especificamente Benim, Togo, Gana, Brasil e Portugal. Reflecte também um alinhamento estratégico tanto com a dinâmica sociopolítica única da nação como com as práticas internacionais bem sucedidas.
Este modelo é particularmente adequado devido à sua capacidade de equilibrar a supervisão centralizada com a execução descentralizada, oferecendo um quadro flexível mas robusto que pode navegar pelas complexidades da paisagem política diversa e ocasionalmente instável da Guiné-Bissau.

A abordagem híbrida é escolhida porque optimiza a utilização de recursos limitados, aumentando a capacidade de estabelecer prioridades e atribuir esforços onde eles são mais necessários, ao mesmo tempo que promove a colaboração entre um vasto leque de partes interessadas, incluindo organismos governamentais, o sector privado e a sociedade civil. Este modelo também apoia a escalabilidade e a sustentabilidade das iniciativas de cibersegurança, garantindo que possam evoluir com a evolução das tecnologias e das ameaças. Além disso, facilita a cooperação internacional, permitindo que a Guiné-Bissau integre as melhores práticas e normas globais na sua governança, o que é vital para abordar as dimensões internacionais das ameaças à cibersegurança. A adoção do Modelo de governança Híbrido reflecte a crença na criação de um quadro de governança resiliente, adaptável e colaborativo que se alinha tanto com os valores culturais como com os objetivos estratégicos da Guiné-Bissau, estabelecendo uma base para a segurança nacional a longo prazo e para a conformidade com as normas globais de cibersegurança.

B. O modelo de governança selecionado

A seleção e implementação do modelo de governança não só reforça a capacidade da Guiné-Bissau para gerir eficazmente os riscos de cibersegurança, como também apoia a sua visão de se tornar uma nação mais conectada e digitalmente segura, ao mesmo tempo que adere aos princípios de transparência, responsabilidade e inclusão. Eis as principais características do Modelo de Governança Híbrido e a forma como se alinham com os objetivos e valores do país: Supervisão Centralizada

A criação de uma entidade central responsável pela definição de normas, políticas e orientações estratégicas nacionais em matéria de cibersegurança, que assegure a coerência e a conformidade com as normas internacionais, ajudando a Guiné-Bissau a reforçar a sua posição global e a sua postura em matéria de segurança, o que é crucial para a soberania e a segurança nacionais.

Implementação descentralizada

Gestão localizada das iniciativas de cibersegurança, permitindo que as autoridades regionais ou as agências sectoriais específicas adaptem as estratégias de implementação às necessidades e condições locais.
Esta caraterística respeita e incorpora os costumes e as estruturas administrativas locais, promovendo a participação da comunidade e garantindo que as medidas de cibersegurança são culturalmente adequadas e amplamente aceites.

Uma avaliação dos recursos da Guiné-Bissau será necessária para identificar claramente a estrutura destas entidades descentralizadas. Em função das limitações de recursos, financeiros, técnicos, humanos ou outros, a modelização pode resultar na criação de agências que serão responsáveis por um grupo homogéneo de entidades. Isto deverá permitir uma boa otimização da estrutura sem tornar o modelo demasiado complexo.

Otimização de recursos

Combina recursos a nível nacional para grandes investimentos, permitindo simultaneamente às zonas locais otimizar e alargar os recursos existentes para necessidades específicas.

A utilização eficiente dos recursos é fundamental em contextos de recursos limitados como a Guiné-Bissau, garantindo a sustentabilidade e a viabilidade económica das iniciativas de cibersegurança.

Redes de colaboração

O modelo incentiva a colaboração entre várias partes interessadas, incluindo entidades governamentais, sector privado, universidades e parceiros internacionais, para partilhar conhecimentos, recursos e melhores práticas.

Esta caraterística reforça a capacidade coletiva de resposta às ameaças à cibersegurança e alinha-se com o valor cultural da cooperação comunitária e da parceria internacional.

Resposta rápida e flexível

O modelo permite uma rápida adaptação e resposta às ameaças emergentes através de poderes de decisão locais, embora continue a ser orientado por uma estratégia centralizada. Garante que o modelo de governança pode adaptar-se rapidamente às mudanças, reflectindo a natureza dinâmica da paisagem política do país e do ambiente cibernético global.

Reforço das capacidades e formação

Dá ênfase ao desenvolvimento de competências locais e a programas de formação regulares, tanto a nível nacional como local.

Isso ajudará a construir uma força de trabalho resiliente e informada, capacitando as comunidades locais e melhorando as capacidades de segurança nacional, o que é crucial para a sustentabilidade a longo prazo.

Mecanismos de transparência e de responsabilização

Este modelo inclui mecanismos de informação e supervisão a vários níveis para garantir que as acções são tomadas de forma responsável e em conformidade com a lei.

Promove a confiança na capacidade do governo para proteger os dados dos cidadãos e manter a privacidade, que são valores culturais fundamentais.

VIII. CONCLUSÃO

A. Resumo das principais conclusões

À medida que a digitalização dos serviços se expande rapidamente na Guiné-Bissau e a exposição ao ambiente web aumenta em geral, os dados ficarão mais expostos e os ataques às infraestruturas críticas aumentarão. Além disso, os avanços em tecnologias como a inteligência artificial (IA) estão a acelerar o surgimento de novas soluções e novas ameaças. Um país que pretenda estar seguro neste cenário em evolução deve implementar medidas adequadas para navegar com sucesso nesta transição.

Sabemos que os dados são cruciais nas telecomunicações. Estes dados podem ser sensíveis ao ponto de afetar a segurança nacional e afetar a privacidade das populações se caírem em mãos erradas. Seja durante o seu trânsito, o seu tratamento ou o seu armazenamento, a sua segurança deve ser garantida. Além disso, devem ser utilizados apenas para os fins para os quais foram recolhidos, respeitando o quadro de utilização definido no momento da recolha. Isto é válido tanto para o sector público como para o sector privado.

Para permitir um ambiente digital saudável, deve ser identificado um modelo de governança que respeite as realidades da Guiné-Bissau. Este modelo deve ser capaz de abranger todas as entidades sensíveis do país que estão ou podem estar no ecossistema digital. Sendo o objetivo deste estudo precisamente a realização de um estudo de viabilidade de diferentes modelos de governança, considerando um contexto de instabilidade política e repleto de fatores que demonstram um clima de fácil mudança, o modelo de governança proposto deve ter grande resiliência. Neste sentido, propomos o modelo híbrido. Em função dos recursos disponíveis, este modelo poderia ser implementado por etapas. Neste caso, pode assemelhar-se a um modelo centralizado no início da sua implementação, mas gradualmente, à medida que as entidades descentralizadas são adicionadas, transformar-se-á num modelo híbrido.

Na fase seguinte deste projeto, abordaremos mais pormenorizadamente a aplicação do modelo escolhido.

B. Etapas futuras

Uma vez escolhido um modelo de governança ou uma combinação de modelos, a atividade seguinte consiste em implementar os elementos de governança na estrutura do modelo. Os elementos habituais de governança são descritos no diagrama abaixo.

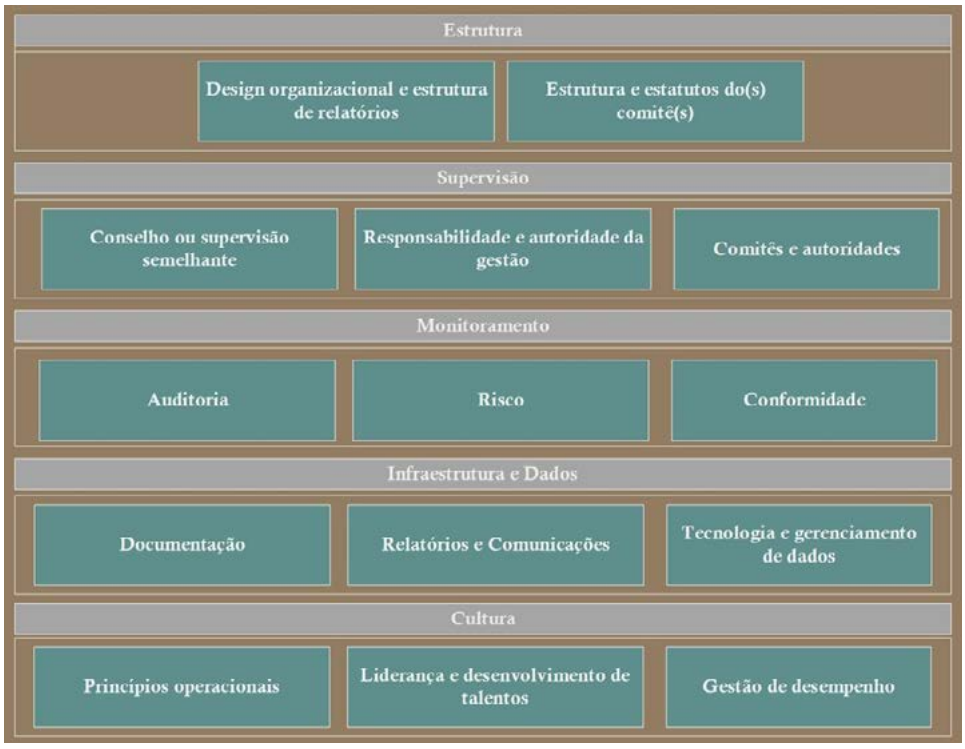

Figura 25: Estrutura pormenorizada da governança

Uma vez escolhido um modelo de governança, os passos seguintes envolvem a integração dos elementos habituais de governança no modelo para garantir a sua eficácia e alinhamento com os objetivos da organização. Esses elementos normalmente incluem:

Estrutura:
Isto envolve a conceção organizacional, as estruturas de informação e a composição dos comités e das cartas.

Responsabilidades de supervisão:
Estabelecer a supervisão do conselho de administração, a responsabilidade da gestão e definir a autoridade e as responsabilidades dos vários comités.

Controlo:
A monitorização assegura a transparência, a eficiência dos recursos e a melhoria contínua. É uma rede de segurança que mantém as organizações responsáveis e no caminho certo

infraestruturas e dados:
Desenvolver os sistemas, processos e políticas necessários para apoiar as atividades de governança.

Talento e cultura:
Garantir que as pessoas certas estão no lugar e que a cultura organizacional apoia o modelo de governança.

A incorporação destes elementos exige um plano pormenorizado que inclua:

Definição de funções e responsabilidades:
Articular claramente quem é responsável por quê no âmbito do quadro de governança para evitar sobreposições e lacunas na responsabilização.

Estabelecimento de processos de tomada de decisão:
Criar processos transparentes e eficientes para a tomada de decisões que se alinhem com os objetivos do modelo de governança.

Desenvolvimento de políticas e procedimentos:
Formular políticas e procedimentos que apoiem a estrutura de governança e facilitem o seu funcionamento.
Configuração dos canais de comunicação:
Implementar mecanismos de comunicação que garantam que a informação flui eficazmente entre os diferentes níveis da organização.

Acompanhamento e avaliação:
Criar sistemas de acompanhamento do desempenho do modelo de governança e de avaliação regular da sua eficácia.

A integração destes elementos no modelo de governança escolhido é crucial para criar uma estrutura robusta que possa orientar a organização no sentido de atingir os seus objetivos estratégicos. É um processo que requer um planeamento cuidadoso, uma comunicação clara e uma avaliação contínua para se adaptar às circunstâncias em mudança.

Esta questão será abordada nas fases subsequentes do presente projeto.

IX. ANEXOS: OUTROS MODELOS DE GOVERNANÇA NÃO CONSIDERADOS COMO CANDIDATOS NO PRESENTE ESTUDO

A. Modelo de governança baseado em comités:

O modelo de governança baseado em comités é um sistema em que as funções de tomada de decisão ou de aconselhamento são atribuídas a um grupo de indivíduos, conhecidos coletivamente como um comité. Este modelo é frequentemente utilizado em organizações onde as decisões ou recomendações sobre assuntos específicos requerem sabedoria coletiva. O comité é normalmente composto por indivíduos com diversas formações e conhecimentos, o que permite uma abordagem abrangente à resolução de problemas e à tomada de decisões.

Neste modelo, os membros do comité trabalham em conjunto para tomar decisões ou apresentar recomendações sobre assuntos específicos. O processo de tomada de decisão coletiva foi concebido para tirar partido dos diversos conhecimentos e perspectivas dos membros do comité. Esta abordagem colaborativa pode conduzir a decisões mais informadas e equilibradas, uma vez que tem em conta uma vasta gama de pontos de vista e conhecimentos especializados.

Eis as vantagens e desvantagens deste modelo:

Vantagens da governança baseada em comités

Agrupamento de pareceres:
Os comités reúnem indivíduos de diversas origens, o que conduz a uma base de conhecimentos mais ampla. Esta diversidade de perspectivas pode melhorar a qualidade das decisões, uma vez que permite uma compreensão mais abrangente das questões em causa. A conjugação de opiniões pode conduzir a decisões mais sólidas e completas que tenham em conta vários aspetos de um problema ou situação.

Cooperação melhorada:
Num modelo baseado em comités, os membros tendem a respeitar os pontos de vista uns dos outros, promovendo a cooperação e a coordenação dentro da organização. Este respeito mútuo pode conduzir a um ambiente de trabalho mais harmonioso, em que os indivíduos se sentem valorizados e ouvidos. Pode também aumentar a eficácia do comité, uma vez que é mais provável que os membros trabalhem em conjunto para atingir objetivos comuns.

Motivação:
A participação nas deliberações dos comités pode aumentar a motivação e o empenho dos membros. Fazer parte de uma entidade decisória pode incutir um sentido de responsabilidade e de propriedade, o que pode aumentar a moral e o empenhamento. Esta motivação acrescida pode conduzir a um melhor desempenho e produtividade.

Representação:
Os comités podem proporcionar um resultado equilibrado ao representarem diferentes interesses e opiniões. Esta representação garante que as várias perspectivas sejam consideradas no processo de tomada de decisão, conduzindo a resultados mais equitativos e inclusivos.

Desvantagens da governança baseada em comités

Tempo e custo:
Os comités podem ser morosos e dispendiosos devido à sua estrutura, que permite uma participação equitativa nos debates. A necessidade de consenso e o tempo necessário para discussões exaustivas podem atrasar a tomada de decisões. Além disso, os recursos necessários para facilitar as reuniões dos comités podem aumentar os custos da organização.

Potencial de conflito:
A necessidade de consenso e a presença de opiniões diversas podem dar origem a conflitos. As diferenças de pontos de vista podem dar origem a desacordos, o que pode atrasar o processo de tomada de decisão e criar tensão no seio do comité.

Risco de inatividade:
Alguns membros da comissão podem tornar-se inativos, o que conduz a um desequilíbrio interno. Esta inatividade pode atrasar a realização dos objetivos e afetar a eficácia global da comissão.

Complexidade:

A estrutura administrativa de um modelo baseado em comités pode tornar-se complexa, conduzindo a potenciais sobreposições de jurisdição e confusão de funções. Esta complexidade pode dificultar a definição clara das responsabilidades e a gestão eficaz do comité.

Num contexto governamental, os comités são frequentemente utilizados para tratar de questões específicas, como a elaboração do orçamento, o desenvolvimento de políticas ou a supervisão das funções governamentais. Podem reforçar a participação democrática e assegurar a consideração de uma variedade de perspectivas. No entanto, os potenciais inconvenientes, como a ineficiência e o risco de conflito, devem ser geridos de forma eficaz para garantir a boa governança. Orientações claras, comunicação eficaz e uma liderança forte são essenciais para a implementação bem sucedida de um modelo de governança baseado em comités.

Nesta estrutura de governança, o poder de tomar decisões é confiado a comités ou grupos de trabalho. Estes grupos são constituídos por representantes de vários segmentos da organização, assegurando um leque diversificado de perspectivas no processo de tomada de decisões. O modelo foi concebido para fomentar a colaboração e a sabedoria coletiva, com cada comité ou grupo de trabalho a trazer para a mesa as suas perspectivas únicas.

Estes comités são responsáveis pela supervisão de funções ou áreas específicas da organização, tais como finanças, gestão de riscos ou planeamento estratégico. São responsáveis por deliberar sobre assuntos relacionados com as respectivas áreas e fazer recomendações à equipa de liderança mais alargada. Desta forma, a liderança mais alargada pode tomar decisões informadas com base nos conhecimentos e recomendações fornecidos por estes comités especializados.

Figura 26: Ilustração simples do modelo de comité

B. Modelo de governança colaborativa

O modelo de governança colaborativa é um sistema em que várias partes interessadas se reúnem para tomar decisões e resolver problemas. Este modelo é frequentemente utilizado na administração pública, em organizações sem fins lucrativos e em grupos comunitários para resolver questões sociais complexas. É um modelo que enfatiza a cooperação, a tomada de decisões partilhadas e a resolução coletiva de problemas. Ao reunir diversas partes interessadas, garante uma abordagem abrangente à tomada de decisões, tendo em conta uma vasta gama de perspectivas e conhecimentos.

Neste modelo, as partes interessadas de várias origens e setores trabalham em conjunto para um objetivo

comum. Partilham os seus conhecimentos, recursos e experiência para tomar decisões informadas e desenvolver soluções eficazes. Esta abordagem de colaboração não só conduz a melhores resultados, como também fomenta um sentido de comunidade e de responsabilidade partilhada entre as partes interessadas.

Eis um resumo das suas vantagens e desvantagens:

Vantagens da governança colaborativa

Tomada de decisões informada:
O modelo de governança colaborativa envolve diversas partes interessadas, conduzindo a uma tomada de decisões mais abrangente. Ao incorporar várias perspectivas e conhecimentos especializados, garante que as decisões são bem informadas e têm em conta todos os fatores relevantes. Isto pode conduzir a soluções mais eficazes e sustentáveis.

Aumento da adesão das partes interessadas:
Quando as partes interessadas fazem parte do processo de tomada de decisões, é mais provável que apoiem e participem ativamente na implementação de políticas ou iniciativas. Este sentimento de apropriação pode levar a um maior empenhamento e envolvimento, aumentando a eficácia das soluções implementadas.

Utilização optimizada de recursos:
A governança colaborativa permite a partilha de recursos, maximizando a eficiência e a eficácia. Ao partilhar recursos, as partes interessadas podem conseguir mais em conjunto do que individualmente. Isto pode levar à redução de custos e à melhoria dos resultados.

Resolução inovadora de problemas:
A inteligência coletiva de diversas partes interessadas pode conduzir a soluções criativas e inovadoras. Ao reunir diferentes ideias e abordagens, a governança colaborativa pode promover a inovação e impulsionar o progresso.

Reforço das relações e das redes:
A colaboração contínua cria confiança e promove a cooperação entre as partes interessadas. Isto pode levar a relações e redes mais fortes, criando um ecossistema de apoio que pode aumentar a capacidade da organização ou da comunidade para enfrentar desafios futuros.

Desvantagens da governança colaborativa

Elevados custos de transação:
A governança colaborativa pode ser intensiva em termos de recursos, consumindo muito tempo e energia. A necessidade de coordenação e de criação de consensos entre diversas partes interessadas pode levar a custos de transação elevados. Isto pode ser um desafio significativo, especialmente para organizações ou comunidades com recursos limitados.

Dificuldade na tomada de decisões:
Chegar a um acordo e coordenar num modelo de colaboração pode ser um desafio. Com a participação de várias partes interessadas, a tomada de decisões pode tornar-se complexa e morosa. Este facto pode abrandar o processo e atrasar potencialmente a implementação de decisões ou iniciativas.

Risco de conflito:
Pode haver conflitos de interesses num modelo de governança em colaboração e as partes interessadas poderosas podem potencialmente dominar o processo. Esta situação pode conduzir a desequilíbrios de poder e a conflitos, comprometendo a eficácia do processo de colaboração.

Questões de aplicação:
Os processos de colaboração podem ter dificuldade em impor compromissos e garantir a aplicação das soluções acordadas. Sem uma autoridade central, pode ser difícil responsabilizar as partes interessadas e garantir que cumprem os seus compromissos.

Em conclusão, embora a governança colaborativa possa conduzir a uma tomada de decisões mais inclusiva e eficaz, também requer uma gestão cuidadosa para evitar ineficiências e conflitos. Trata-se de um ato de equilíbrio delicado entre o aproveitamento dos benefícios da ação coletiva e a redução dos riscos associados à

colaboração. Com uma liderança eficaz, uma comunicação clara e um forte empenhamento de todas as partes interessadas, a governança colaborativa pode ser uma ferramenta poderosa para abordar questões sociais complexas.

A governança colaborativa sublinha a importância da parceria e da cooperação entre várias partes interessadas. Estas partes interessadas podem ir desde departamentos internos de uma organização a parceiros externos e comunidades. Este modelo promove uma cultura de colaboração, em que cada parte interessada tem um papel a desempenhar no processo de tomada de decisões. Promove um sentido de unidade e de objetivo partilhado, o que é particularmente benéfico em ambientes complexos e interligados.

Este modelo de governança encoraja a tomada de decisões partilhadas e a construção de consensos, assegurando que todas as vozes são ouvidas e consideradas. Também enfatiza a responsabilidade mútua, em que cada parte interessada é responsável não só pelas suas próprias acções, mas também pelo resultado coletivo. Este sentido de responsabilidade mútua promove uma cultura de responsabilidade e integridade, que é crucial para o sucesso de qualquer projeto de colaboração.

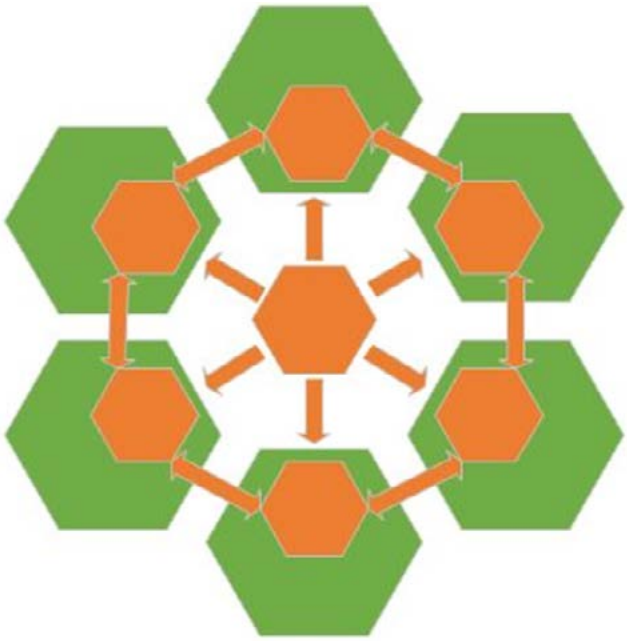

Figura 27: Ilustração simples do modelo de colaboração

C. Modelo de governança da rede:

O modelo de governança em rede é uma estrutura única que envolve várias organizações ou grupos que colaboram para atingir objetivos comuns. Este modelo é caracterizado por um elevado grau de interdependência e cooperação entre as entidades participantes. Foi concebido para potenciar os pontos fortes colectivos de todos os participantes, permitindo-lhes trabalhar em conjunto e de forma coordenada para atingir objetivos comuns.

Neste modelo, os processos de tomada de decisão e de resolução de problemas são distribuídos por toda a rede, permitindo uma abordagem mais inclusiva e participativa. O modelo de governança em rede é particularmente eficaz em ambientes complexos, onde as questões não podem ser tratadas eficazmente por uma única organização ou grupo. Promove um sentido de responsabilidade partilhada e de responsabilização mútua, reforçando a capacidade coletiva de resolver problemas complexos.

Vantagens da governança da rede

Melhoria da aprendizagem e da inovação:
O modelo de governança em rede promove a aprendizagem e a inovação ao reunir diversas perspectivas e conhecimentos especializados. Ao facilitar a troca de

ideias e conhecimentos entre os participantes, cria um ambiente propício à aprendizagem e à inovação. Isto pode levar ao desenvolvimento de novas soluções e abordagens, melhorando a capacidade coletiva de resolução de problemas da rede.

Utilização eficiente dos recursos:
O modelo de governança da rede promove uma utilização mais eficiente dos recursos. Ao reunir recursos e conhecimentos, a rede pode alcançar uma escala e um impacto maiores do que as organizações ou grupos individuais poderiam alcançar sozinhos. Isto pode levar a uma maior eficiência e eficácia na resolução de problemas complexos.

Maior competitividade:
As redes podem aumentar a competitividade através da prestação de melhores serviços a clientes e consumidores. Ao combinar os pontos fortes e os recursos de várias organizações ou grupos, as redes podem oferecer uma gama mais alargada de serviços, satisfazer diversas necessidades dos clientes e adaptar-se rapidamente às mudanças no mercado ou no ambiente.

Flexibilidade:
O modelo de governança da rede permite a adaptabilidade e a capacidade de resposta a ambientes e necessidades em mudança. As redes podem adaptar-se rapidamente a novos desafios ou oportunidades, o que as torna mais resistentes e ágeis do que as estruturas hierárquicas tradicionais.

Desvantagens da governança em rede

Instabilidade relativa:
A flexibilidade da rede também pode levar à instabilidade, uma vez que o equilíbrio de poder e as relações podem mudar frequentemente. Este facto pode criar incerteza e dificultar a manutenção de políticas e práticas coerentes em toda a rede.

Dinâmica de controlo complexa:
Num modelo de governança de rede, é necessário estabelecer um equilíbrio entre controlo excessivo e insuficiente. Isto pode ser um desafio, uma vez que um controlo excessivo pode sufocar a inovação e a participação, enquanto um controlo insuficiente pode conduzir ao caos e à ineficiência.

Questões de responsabilidade:
Garantir a responsabilidade numa rede pode ser difícil. Com várias organizações ou grupos envolvidos, pode não ser claro quem é responsável por determinadas ações ou decisões. Isto pode dificultar a responsabilização dos participantes e garantir que as ações acordadas sejam levadas a cabo.

Preocupações com a legitimidade:
As redes precisam de estabelecer uma legitimidade interna e externa. Isto implica criar confiança e credibilidade entre os participantes e as partes interessadas, o que pode ser um processo complexo e moroso.

Em conclusão, embora a governança em rede possa conduzir a uma abordagem mais dinâmica e colaborativa da gestão e da resolução de problemas, também apresenta desafios em termos de estabilidade, controlo e responsabilidade. Estes desafios têm de ser cuidadosamente geridos para garantir a eficácia e a sustentabilidade da rede. Apesar destes desafios, quando implementada de forma eficaz, a governança em rede pode ser uma ferramenta poderosa para abordar questões complexas e atingir objetivos comuns.

A governança em rede é um modelo que transcende os limites de uma única entidade e incorpora uma variedade de partes interessadas. Estas podem incluir organismos governamentais, organizações sem fins lucrativos, empresas comerciais e grupos comunitários. Esta abordagem alargada permite um esforço mais abrangente e colaborativo na tomada de decisões e na resolução de problemas.

Estas redes são criadas com o objetivo de abordar objetivos ou dificuldades comuns. Aproveitam as competências e os recursos variados dos participantes, criando uma força coletiva mais capaz e com mais recursos. Esta abordagem colaborativa não só aumenta a eficácia da rede, como também fomenta um sentido de responsabilidade partilhada e de benefício mútuo entre os participantes.

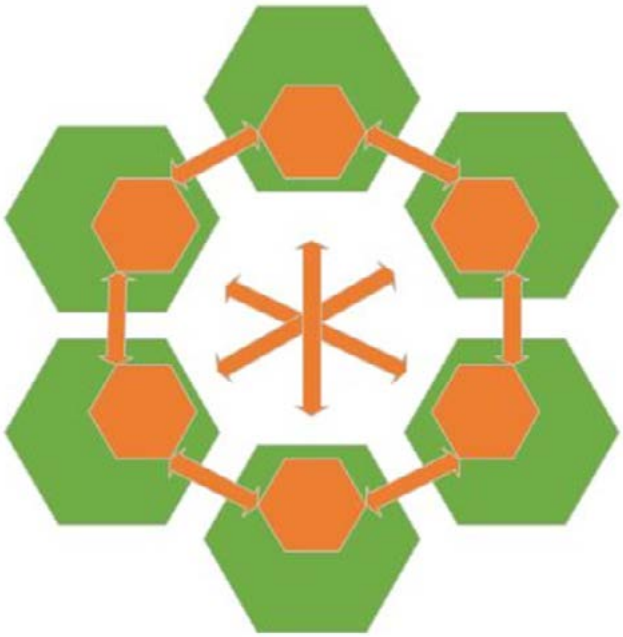

Figura 28: Ilustração simples do modelo de rede

D. Modelo de governança adaptativo:

O modelo de governança adaptativa é uma abordagem dinâmica e flexível da governança, concebida para responder eficazmente às mudanças no ambiente e na sociedade. Este modelo caracteriza-se pela sua ênfase na aprendizagem e no ajustamento das políticas com base em novas informações e circunstâncias variáveis. É um modelo que valoriza a adaptabilidade e a resiliência, permitindo às organizações navegar na incerteza e na complexidade de forma mais eficaz.

Neste modelo, a governança não é um processo estático, mas sim um processo dinâmico que evolui em resposta a mudanças no ambiente interno e externo. As políticas e estratégias não são gravadas em pedra, mas são continuamente ajustadas com base no feedback e na aprendizagem. Este processo contínuo de aprendizagem e adaptação permite que as organizações se mantenham relevantes e eficazes num mundo em rápida mudança.

O modelo de governança adaptativa não tem apenas a ver com flexibilidade e adaptabilidade; tem também a ver com aprendizagem e inovação. Incentiva as organizações a experimentar, a aprender com os seus êxitos e fracassos e a melhorar continuamente as suas estratégias e políticas. Esta cultura de aprendizagem e inovação pode conduzir a soluções mais eficazes e sustentáveis para problemas complexos.

Eis algumas vantagens e desvantagens deste modelo:

Vantagens da governança adaptativa

Capacidade de resposta à mudança:
A governança adaptativa permite que as organizações respondam rapidamente a novas informações e circunstâncias em mudança. Esta capacidade de reação permite que as organizações se mantenham à frente da curva e adaptem as suas estratégias e políticas para enfrentar novos desafios e oportunidades.

Aprendizagem contínua:
O modelo de governança adaptativa promove uma cultura de aprendizagem e melhoria contínua. O feedback é utilizado não só para corrigir erros, mas também para aperfeiçoar estratégias e políticas, tornando-as mais eficazes e relevantes. Este processo de aprendizagem contínua promove uma cultura de melhoria e excelência dentro da organização.

Inovação:
Ao incentivar a experimentação, a governança adaptativa pode conduzir a soluções inovadoras para problemas complexos. Esta cultura de inovação pode

impulsionar o progresso e ajudar as organizações a manterem-se competitivas num mundo em rápida mudança.

Coordenação reforçada:
O modelo de governança adaptativa pode melhorar a coordenação entre as várias partes interessadas, promovendo a comunicação e a colaboração. Ao reunir diversas partes interessadas e facilitar a sua colaboração, pode aumentar a capacidade coletiva da organização para resolver problemas complexos.

Desvantagens da governança adaptativa

Complexidade:
A implementação do modelo de governança adaptativa pode ser complexa, uma vez que exige sistemas robustos de monitorização, feedback e ajustamento. Esta complexidade pode colocar desafios em termos de implementação e gestão, exigindo uma liderança forte e sistemas de gestão eficazes.

Potencial de instabilidade:
Mudanças frequentes nas políticas e estratégias podem levar à instabilidade e à incerteza. Embora a adaptabilidade seja um ponto forte do modelo de governança adaptativa, demasiadas mudanças podem criar confusão e incerteza, comprometendo a eficácia do processo de governança.

Intensidade de recursos:
A governança adaptativa pode ser intensiva em recursos, exigindo um investimento significativo na recolha, análise e gestão de dados. Esta intensidade de recursos pode colocar desafios, especialmente para organizações com recursos limitados.

Risco de concentração no curto prazo:
Existe o risco de que a ênfase na adaptabilidade possa levar a um pensamento a curto prazo em detrimento dos objetivos a longo prazo. Embora a adaptabilidade seja importante, é também crucial manter uma perspetiva de longo prazo e garantir que as adaptações de curto prazo não prejudiquem os objetivos e estratégias de longo prazo.

Em resumo, embora a governança adaptativa ofereça uma abordagem proactiva e resistente à gestão da mudança, também apresenta desafios em termos de complexidade, estabilidade e atribuição de recursos. Estes desafios têm de ser cuidadosamente geridos para garantir a eficácia e a sustentabilidade do processo de governança. Apesar destes desafios, quando implementada eficazmente, a governança adaptativa pode ser uma ferramenta poderosa para navegar na complexidade e na mudança.

A governança adaptativa é um modelo que dá prioridade à flexibilidade, à aprendizagem e à capacidade de adaptação em resposta a circunstâncias variáveis e incertezas. Esta abordagem é caracterizada pela sua natureza dinâmica, permitindo ajustes rápidos e modificações nas estratégias e políticas com base no ambiente em evolução. É um modelo que valoriza a aprendizagem contínua e a capacidade de se adaptar em resposta a novas informações ou mudanças no contexto.

Este modelo é particularmente eficaz em ambientes dinâmicos onde as abordagens tradicionais hierárquicas ou de comando e controlo podem ser insuficientes. Em sistemas complexos ou indústrias sujeitas a mudanças rápidas, o modelo de governança adaptativa brilha. Permite uma abordagem mais reactiva e resistente à governança, capaz de navegar pelas complexidades e incertezas inerentes a esses ambientes.

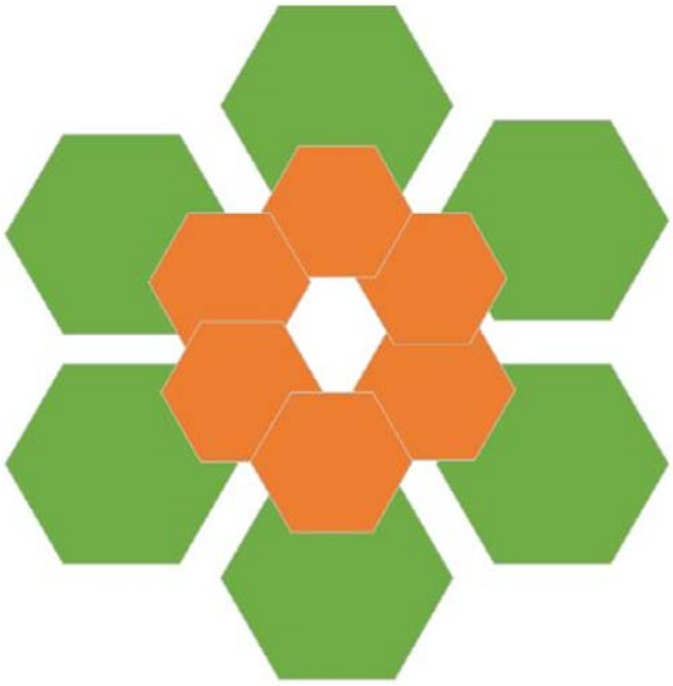

Figura 29: Ilustração simples do modelo adaptativo

E. Modelo integrado de governança:

O modelo de governança integrada é uma estrutura abrangente que reúne vários mecanismos de governança para formar um sistema coeso. Este modelo é meticulosamente concebido para alinhar os objetivos estratégicos com os processos operacionais, assegurando que a governança é consistente e unificada em toda a organização. É um modelo que valoriza a integração e o alinhamento, permitindo às organizações navegar na complexidade de forma mais eficaz.

Neste modelo, a governança não é vista como uma série de atividades isoladas, mas como um sistema interligado em que diferentes componentes trabalham em conjunto para um objetivo comum. O modelo de governança integrada foi concebido para garantir que todos os aspetos da governança – desde o planeamento estratégico à gestão do risco e à conformidade – estão alinhados e integrados. Esta abordagem integrada pode conduzir a uma governança mais eficaz e eficiente, uma vez que assegura que todas as atividades de governança são coordenadas e alinhadas com os objetivos estratégicos da organização.

O modelo de governança integrada não se trata apenas de integração; trata-se também de alinhamento e consistência. Garante que todas as atividades de gestão estão alinhadas com os objetivos estratégicos da organização e que estas atividades são consistentes em toda a organização. Esta consistência pode aumentar a eficácia da governança e garantir que todas as partes da organização estão a trabalhar para os mesmos objetivos.

Eis algumas vantagens e desvantagens do modelo de governança integrada:

Vantagens da governança integrada

Abordagem holística:
O modelo de governança integrada proporciona uma visão holística da governança, integrando a gestão do risco, a conformidade e o planeamento estratégico. Esta abordagem holística garante que todos os aspetos da governança são considerados e integrados, conduzindo a uma governança mais abrangente e eficaz.

Melhoria do processo de tomada de decisões:
Ao consolidar a informação proveniente de várias fontes, o modelo de governança integrada apoia a tomada de decisões mais bem informadas. Esta consolidação da informação pode melhorar a qualidade das decisões, uma vez que garante que estas se baseiam numa com-

preensão abrangente da situação.

Otimização de processos:
O modelo de governança integrada elimina as atividades sem valor acrescentado e simplifica os processos para reduzir o tempo de atraso e a variação. Esta otimização dos processos pode conduzir a uma governança mais eficiente e eficaz, uma vez que reduz o desperdício e melhora a rapidez e a qualidade da tomada de decisões.

Atribuição de recursos:
O modelo de governança integrada ajuda a identificar áreas de redundância e ineficiência, permitindo uma alocação mais eficaz do capital financeiro e humano. Esta afetação eficiente de recursos pode aumentar a eficácia da governança e garantir que os recursos são utilizados da forma mais produtiva.

Proteção da reputação:
A gestão eficaz do risco no modelo de governança integrada melhora a reputação da empresa. Ao gerir os riscos de forma eficaz, a organização pode proteger a sua reputação e criar confiança junto das partes interessadas.

Desvantagens da governança integrada

Complexidade de implementação:
A integração de vários componentes de governança pode ser complexa e difícil. Esta complexidade pode colocar desafios em termos de implementação e gestão, exigindo uma liderança forte e sistemas de gestão eficazes.

Potencial de sobreposição:
Num modelo de governança integrada, pode haver sobreposições de funções e responsabilidades, o que gera confusão. Esta sobreposição pode criar ambiguidade e confusão, prejudicando a eficácia do processo de governança.

Custos iniciais elevados:
A configuração inicial e a manutenção de um sistema de governança integrado podem ser dispendiosas. Estes custos podem representar um desafio significativo, especialmente para organizações com recursos limitados.

Resistência à mudança:
As partes interessadas podem resistir às mudanças necessárias para implementar uma abordagem integrada. Esta resistência à mudança pode constituir um desafio significativo para a implementação do modelo de governança integrada.

Em resumo, embora o modelo de governança integrada possa conduzir a uma governança mais eficiente e eficaz, exige um planeamento e execução cuidadosos para ultrapassar os desafios associados à sua complexidade e à necessidade de mudança organizacional. Apesar destes desafios, quando implementado eficazmente, o modelo de governança integrada pode ser uma ferramenta poderosa para melhorar a governança e alcançar objetivos estratégicos.

A governança integrada é um modelo que visa reunir várias funções de governança, incluindo o planeamento estratégico, a gestão do risco, a conformidade e a gestão do desempenho, numa estrutura unificada. Esta abordagem foi concebida para criar um quadro sem descontinuidades em que todas estas funções funcionam em harmonia, aumentando a eficácia global da governança.

Este modelo promove a coerência e consistência nos processos de tomada de decisão, assegurando que todas as decisões estão alinhadas com os objetivos estratégicos da organização. Além disso, garante que todas as atividades de governança, desde o planeamento à gestão do desempenho, apoiam a realização dos objetivos da organização. Este alinhamento e apoio não só aumentam a eficácia da governança, como também contribuem para a obtenção do sucesso organizacional.

Figura 30: Ilustração simples do modelo integrado

RFP No: WARDIP – C – 15 - 2023

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