Presidência da República

Comitê Nacional de Cibersegurança (CNCiber)

Modelo de Ciber-Maturidade Brasileiro – Nacional (CIMBRA-N)

(v1a)

Brasília - 2026

SUMÁRIO

1 APRESENTAÇÃO

1.1 Introdução

Com o objetivo de permitir uma melhor consciência situacional da realidade da cibersegurança e da ciber-resiliência brasileiras o Comitê Nacional de Cibersegurança (CNCiber) criou um Grupo de Trabalho Temático (GTT) para elaborar dois modelos de maturidade em cibersegurança adequados às condições brasileiras: um de avaliação das condições nacionais e outro de avaliação das condições institucionais.

O início das atividades do GTT Maturidade foi pautado pelo nivelamento técnico e conceitual necessário para a realização da tarefa delegada ao grupo. Foram estudados conceitos de modelos, arcabouços (frameworks), maturidade e conformidade, e modelos prescritivos e descritivos. Foram estudados ainda diversos modelos e arcabouços (*frameworks*), tanto de maturidade quanto de conformidade, ou até de boas práticas, envolvendo as mais variadas temáticas ligadas à cibersegurança, passando pela segurança da informação, desenvolvimento de software, governança de TI, que pudessem prover elementos a serem incorporados à proposta de modelos de avaliação da maturidade brasileira em cibersegurança, nacional ou institucional.

2 O MODELO CIBERMATURIDADE BRASILEIRA – CIMBRA

Após o nivelamento técnico-conceitual dos integrantes do GTT e a pesquisa dos modelos e arcabouços mais usados internacionalmente, decidiu-se que a proposta seria fundamentada em um mix de características de diferentes origens, cujo detalhamento é apresentado nos próximos capítulos.

2.1 O que é uma “cimbra”

Cimbra é uma palavra usada em português e espanhol para designar uma estrutura de madeira ou metal usada para fazer arcos, abóbadas, lajes ou vigas. Portanto, um elemento estruturante que suporta a construção de armações permanentes de longa duração.

Suas principais funções são:

- Sustentação: Suporta o peso do concreto fresco, das fôrmas, dos equipamentos e dos operários até que a estrutura atinja a resistência necessária.
- Moldagem: Mantém a geometria correta do projeto (curvaturas de arcos, nivelamento de lajes, etc.).
- Segurança: Garante que a estrutura não sofra deformações ou desabamentos durante a fase crítica de cura do concreto.

É uma palavra curta, com sentido próprio, associável à contração da denominação Ciber Maturidade Brasileira.

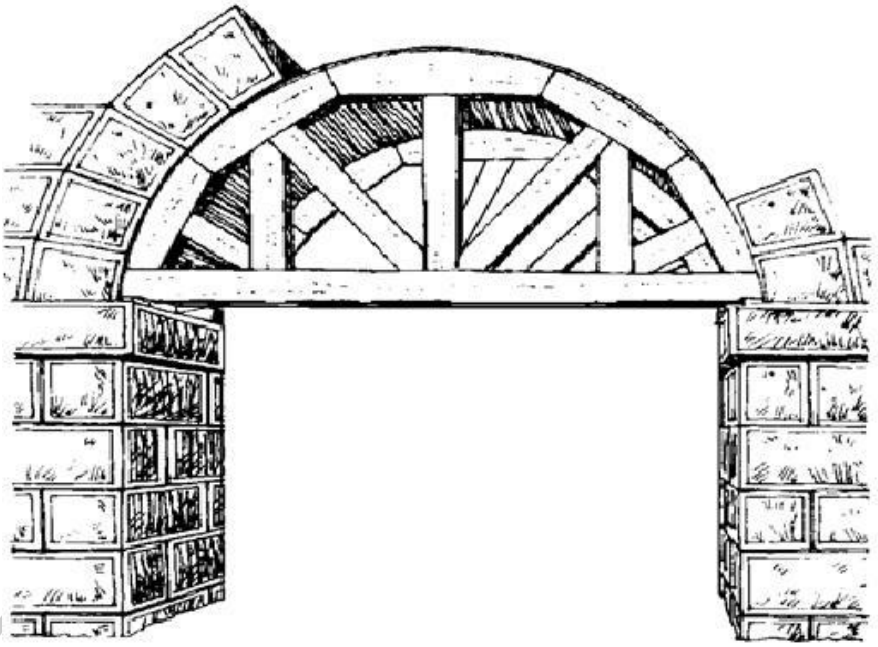

Figura 1- Exemplo de Cimbra

Por essas razões o nome CIMBRA foi adotado pelo GTT para o Modelo de Ciber Maturidade Brasileiro. Suas duas variantes seriam:

- Cimbra-Nacional (ou Cimbra-N): tem como finalidade a mensuração da maturidade nacional em cibersegurança ao longo do tempo, permitindo identificar pontos fortes, fracos e de atenção, que possam representar riscos ou oportunidades para a cibersegurança do País.
- Cimbra-Institucional (ou Cimbra-I): tem por finalidade a mensuração da maturidade institucional em cibersegurança, refletindo o grau de implementação das diferentes práticas em instituições de diferentes setores e portes, públicas ou privadas. A análise de informações de instituições de um mesmo setor permitirá o mapeamento da maturidade setorial em cibersegurança.

3 A ESCALA DE MATURIDADE

A escala de maturidade do CIMBRA foi estruturada com 6 <Níveis> (estágios) aplicáveis cumulativamente:

Nível	Características de Gestão	Características de Abordagem
0-Inicial	As <Práticas> não são realizadas	Não são identificáveis evidências de implementações de todas as <Práticas> exigidas para o nível Fundamental
1-Fundamental	As <Práticas> são realizadas, mas podem ser ad hoc, sem coordenação central	São identificáveis implementações básicas de todas as <Práticas> classificadas como nível Fundamental, e possivelmente de algumas práticas do nível Médio
2-Básico	As <Práticas> são formalizadas e documentadas	São identificáveis implementações completas de todas as <Práticas> dos níveis Fundamental e Médio, e possivelmente de algumas práticas do nível Evoluído.

Nível	Características de Gestão	Características de Abordagem
3-Médio	As <Práticas> são guiadas por políticas (ou outras diretrizes organizacionais) Recursos adequados são fornecidos para apoiar o <Processo>	São identificáveis implementações completas de todas as <Práticas> dos níveis Fundamental e Médio, e possivelmente de algumas práticas do nível Evoluído.
4-Evoluído	Responsabilidade, prestação de contas e autoridade pela execução das <Práticas> são atribuídas Implementações são guiadas por prioridades e análise de riscos O pessoal que executa as <Práticas> tem habilidades e conhecimentos adequados e verificados	São identificáveis implementações completas de todas as <Práticas> dos níveis Fundamental, Médio e Evoluído, e possivelmente de algumas práticas do nível Avançado.
5-Avançado	A eficácia das <Práticas> é avaliada e rastreada Políticas, <Processos> e <Práticas> são aprimoradas com base em lições aprendidas, de forma sistemática, indicando capacidade de adaptação rápida a novas ameaças	São identificáveis implementações completas de todas as <Práticas> dos níveis Fundamental, Médio, Evoluído e Avançado.

Tabela 1 – Níveis de Maturidade do CIMBRA

Entende-se que, para o contexto do CIMBRA, a adoção do modelo de Maturidade deve observar a característica cumulativa, segundo a qual a progressão entre níveis ocorre de forma sequencial e condicionada. Isso significa que o atingimento de um <Nível> de maturidade subsequente está necessariamente vinculado à plena implementação e à evidência objetiva de todas as práticas, controles e requisitos estabelecidos para o <Nível> imediatamente anterior.

Dessa forma, assegura-se consistência evolutiva, consolidação das capacidades institucionais e a construção estruturada de competências ao longo do tempo, evitando lacunas ou sobreposições no desenvolvimento do modelo.

Como exemplo hipotético, pode-se citar a situação em que se demande a existência de Planos Setoriais elaborados pelas autoridades reguladoras setoriais para se atingir o <Nível> Evoluído de maturidade. Se um único setor regulado não dispuser desse plano setorial o país tem sua avaliação prejudicada nesse quesito, pois não terá cumprido a exigência e não há uma ponderação do quesito.

4 HIERARQUIA EM 3 NÍVEIS

O Cimbra-N teve como referência básica os dois modelos de maturidade nacionais considerados (Oxford Cyber Maturity Model – CMM e UIT Global Cybersecurity Index – GCI), incorporando elementos entendidos como relevantes derivados dos demais modelos de referência: COBIT, ITIL, CIS e ISO.

Foi elaborado com uma estrutura baseada em 3 níveis hierarquizados conforme se segue.

4.1 <Eixo>

Um <Eixo> representa um domínio do conhecimento, a categoria que agrupa capacidades relacionadas.

Partindo-se das 5 dimensões do CMM e dos 5 pilares do GCI entendeu-se que havia compatibilidade direta de 3 deles. Assim, 2 daqueles do GCI foram adicionados aos 5 do CMM. Posteriormente, entendeu-se que seria interessante separar os conceitos integrantes de 1 deles, desdobrando-o em dois subconjuntos, resultando num total de 8 eixos temáticos.

4.2 <Processo>

Um <Processo> é um conjunto de <Ações> articuladas dentro de um <Eixo>.

4.3 <Ação>

Uma <Ação> consiste no nível mais granular e operacional da hierarquia, indicando "o quê" deve ser feito para se implementar um <Processo>. É nesse nível que será avaliada a maturidade da execução das <Práticas> de cibersegurança que compõem o CIMBRA-I.

4.4 <Evidência>

Uma <Evidência>, embora prevista no modelo, não caracteriza uma hierarquia do modelo. <Evidências> são apenas **exemplos** de elementos de prova que podem ser utilizados para se comprovar a materialização de um <Aspecto>.

5 FOCO NO DESENVOLVIMENTO DE CAPACIDADES

A proposta do CIMBRA incorpora tanto uma perspectiva prescritiva quanto uma perspectiva descritiva. Isso porque nos níveis iniciais, onde a maturidade é menor, as instituições costumam ser menores e com menor capacidade de investimento, beneficiando-se de "receitas prontas" para acelerarem seu amadurecimento. No entanto, tradicionalmente, os níveis mais elevados de maturidade em cibersegurança demandam maior customização e adaptação dos <Processos> e <Ações> às diferentes realidades institucionais, conforme o nível de maturidade coloca exigências maiores de governança, controle e resposta, implicando em investimentos mais significativos.

Dessa forma, desenha-se o CIMBRA com a perspectiva de que tenha as seguintes características associadas a cada nível:

Nível	Característica
Inicial	Prescritivo
Fundamental	Prescritivo
Básico	Prescritivo
Médio	Prescritivo
Evoluído	Descritivo
Avançado	Descritivo

Tabela 2 – Modelagem Prescritiva-Descritiva do CIMBRA por Nível de Maturidade

6 DETALHAMENTO DO CIMBRA-NACIONAL (CIMBRA-N)

Legenda:
Em fundo VERDE são os Eixos.
Em fundo AMARELO são os Vetores.
Em fundo AZUL são os Aspectos.
Em fundo BRANCO são as Evidências.

E1-Estratégia

Política e Estratégia

Detalhamento:

Considera a capacidade do país de desenvolver e implementar uma Política e/ou Estratégia Nacional de Cibersegurança, bem como sua capacidade de fortalecer a cibersegurança e a ciberdefesa nacionais.

E1-Estratégia-1

Estratégia Nacional de Cibersegurança

Detalhamento:

Avalia a existência, qualidade e maturidade da Política e/ou Estratégia Nacional de Cibersegurança. Avalia também o engajamento na análise das congêneres internacionais e seus eventuais impactos na Política e/ou Estratégia nacionais.

E1-Estratégia-1-A

Existência da Estratégia

Detalhamento:

Aborda a existência de uma estratégia nacional, a alocação de autoridades de implementação entre os setores e a sociedade civil, e a compreensão dos riscos e ameaças à cibersegurança que impulsionam o desenvolvimento de capacidades a nível nacional.

Níveis de Maturidade:

Inicial:
Não existe estratégia nacional de cibersegurança.

Fundamental:
Processos de desenvolvimento iniciados; consultas parciais.

Básico:
Estratégia concluída, aguardando publicação.

Médio:
Estratégia publicada.

Evoluído:
Atualizações orientadas por métricas e análise de riscos.

Avançado:
Revisão contínua.

Evidências

Existência de Estratégia Nacional de Cibersegurança formalmente publicada.

E1-Estratégia-1-B

Qualidade (Conteúdo) da Estratégia

Detalhamento:

Aborda o conteúdo da estratégia nacional de cibersegurança e se esta está explicitamente ligada a riscos, prioridades e objetivos nacionais, tais como segurança nacional, sensibilização do público e

mitigação do cibercrime, capacidade de resposta a incidentes e proteção de infraestruturas nacionais críticas.

Níveis de Maturidade:

Inicial:
Políticas dispersas e pouco integradas.

Fundamental:
Conteúdo alinhado a prioridades, porém, de forma limitada.

Básico:
Conteúdo alinhado a prioridades, de forma ampla.

Médio:
Conteúdo abrange SEICs, resposta a incidentes e conscientização.

Evoluído:
Metas mensuráveis e sustentabilidade considerada.

Avançado:
Estratégia incorpora tendências emergentes e cooperação global.

Evidências

Integração da estratégia de cibersegurança com planos de continuidade de governo (COOP/COG).

Integração entre estratégia de cibersegurança e estratégia de transformação digital do governo.

Política nacional para proteção de processos democráticos e integridade da informação eleitoral.

Integração entre a estratégia e a Políticas Nacional de Cibersegurança.

E1-Estratégia-1-C
Implementação e Revisão

Detalhamento:

Aborda a existência de um plano abrangente de coordenação da implementação estratégia e elevação da maturidade nacional em cibersegurança, incluindo um órgão/organismo responsável pela sua coordenação, com um orçamento consolidado.

Níveis de Maturidade:

Inicial:
Não existe plano de implementação.

Fundamental:
Plano em construção.

Básico:
Plano elaborado, mas sem órgão coordenador ou com recursos indefinidos.

Médio:
Plano publicado com órgão coordenador e orçamento.

Evoluído:
Avaliação baseada em métricas e ajustes periódicos.

Avançado:
Reorientação rápida diante de mudanças estratégicas amplas.

Evidências

Estratégia nacional acompanhada de plano de implementação com metas e cronograma.

Existência de canal institucionalizado de participação de operadores de SEICs na revisão da Estratégia Nacional de Cibersegurança.

Existência de mapa consolidado de programas e iniciativas públicas de cibersegurança para evitar duplicidades.

Linha orçamentária exclusiva para cibersegurança no orçamento público.

Revisão periódica da estratégia (ex.: a cada 2 ou 3 anos).

E1-Estratégia-1-D
Engajamento Internacional

Detalhamento:

Explora até que ponto o país acompanha debates internacionais sobre políticas e/ou estratégias de cibersegurança e como esses debates e questões relacionadas afetam os interesses e a posição internacional do país.

Níveis de Maturidade:

Inicial:
Baixa participação em debates globais.

Fundamental:
Participação ocasional e geralmente passiva.

Básico:
Participação moderada.

Médio:
Participação ativa em fóruns e redes internacionais.

Evoluído:
País promove iniciativas e comunidades internacionais.

Avançado:
País lidera debates e cria mecanismos de cooperação.

Evidências

Análises comparadas da estratégia com aquelas de outros países.

Participação em debates, eventos e mecanismos bi e multilaterais; regionais e globais.

E1-Estratégia-2

Cibersegurança e Ciberdefesa Nacionais

Detalhamento:

Explora se o País tem a capacidade de conceber e implementar uma integração e cooperação entre cibersegurança e ciberdefesa nacionais. Também analisa o nível de capacidade de cibersegurança dentro do sistema de segurança e defesa nacional, e os acordos de colaboração em cibersegurança entre entidades civis e de defesa.

E1-Estratégia-2-A

Estratégia de Cibersegurança na Defesa Nacional

Detalhamento:

Aborda a existência de uma estratégia para apoiar a cibersegurança no âmbito da defesa nacional, e se esta estratégia é amparada por autoridades legais apropriadas, doutrina operacional relevante e regras de engajamento.

Níveis de Maturidade:

Inicial:
O impacto potencial da cibersegurança sobre a defesa nacional pode ter sido considerado, mas não foi formalmente articulado.

Fundamental:
O impacto potencial da cibersegurança sobre a defesa nacional foi avaliado, e uma estratégia para enfrentar esses riscos está em desenvolvimento. Essa análise inclui riscos à capacidade das forças de defesa nacional de operar em um ambiente cibernético contestado.

Básico:
Uma estratégia de cibersegurança para a defesa nacional foi formalmente adotada (de forma autônoma ou integrada a outro documento). A estratégia carece de bases legais apropriadas, doutrina operacional relevante ou regras de engajamento, consistentes com o direito internacional humanitário.

Médio:
Uma estratégia de cibersegurança para a defesa nacional foi formalmente adotada (de forma autônoma ou integrada a outro documento). A estratégia é sustentada por bases legais apropriadas, doutrina operacional relevante e regras de engajamento, consistentes com o direito internacional humanitário.

Evoluído:
A dependência das entidades de defesa nacional em relação à cibersegurança de outras partes da infraestrutura crítica nacional é compreendida e tratada na estratégia de cibersegurança de defesa. Considerações de cibersegurança informam outros elementos da estratégia de defesa nacional, incluindo dissuasão.

Avançado:
A defesa e a comunidade de defesa nacional do país participam ativamente do debate global sobre o direito internacional humanitário e normas de comportamento aplicáveis ao conflito no ciberespaço. Estratégias e doutrinas são adaptativas e projetadas para promover estabilidade no ciberespaço, prevendo e influenciando ações e reações de aliados e adversários.

Evidências

Estratégia nacional de dissuasão e resposta a ataques patrocinados por Estados.

Integração explícita de cibersegurança em políticas de defesa.

Programas de capacitação militar em operações cibernéticas.

E1-Estratégia-2-B
Estratégia de Cibersegurança na Segurança Nacional

Detalhamento:

Aborda a existência de uma estratégia para apoiar a cibersegurança no âmbito da segurança nacional, e se esta estratégia é amparada por autoridades legais apropriadas, doutrina operacional relevante e regras de engajamento.

Níveis de Maturidade:

Inicial:
O impacto potencial da cibersegurança sobre a segurança nacional pode ter sido considerado, mas não foi formalmente articulado.

Fundamental:
O impacto potencial da cibersegurança sobre a segurança nacional foi avaliado, e uma estratégia para enfrentar esses riscos está em desenvolvimento. Essa análise inclui riscos à capacidade dos ativos de segurança nacional de operar em um ambiente cibernético contestado.

Básico:
Uma estratégia de cibersegurança para a segurança nacional foi formalmente adotada (de forma autônoma ou integrada a outro documento). A estratégia carece de bases legais apropriadas, doutrina operacional relevante ou regras de engajamento.

Médio:
Uma estratégia de cibersegurança para a segurança nacional foi formalmente adotada (de forma autônoma ou integrada a outro documento). A estratégia é sustentada por bases legais apropriadas, doutrina operacional relevante e regras de engajamento.

Evoluído:
A dependência das entidades de segurança nacional em relação à cibersegurança de outras partes da infraestrutura crítica nacional é compreendida e tratada na estratégia de cibersegurança. Considerações de cibersegurança informam outros elementos da estratégia de segurança nacional, incluindo dissuasão.

Avançado:
A defesa e a comunidade de segurança nacional do país participam ativamente do debate global sobre o direito internacional humanitário e normas de comportamento aplicáveis ao conflito no ciberespaço. Estratégias e doutrinas são adaptativas e projetadas para promover estabilidade no ciberespaço, prevendo e influenciando ações e reações de aliados e adversários.

Evidências

Integração explícita de cibersegurança em políticas de segurança nacional.

Política nacional para contraterrorismo cibernético.

Política nacional para proteção a eleições.

E1-Estratégia-2-C
Capacidade de Cibersegurança das Instituições de Defesa Nacional

Detalhamento:

Analisa o nível de capacidade de cibersegurança e as estruturas organizacionais dentro do aparato de defesa nacional.

Níveis de Maturidade:

Inicial:
A capacidade especializada em cibersegurança dentro do aparato de defesa nacional é limitada.

Fundamental:
As necessidades de capacidade especializada em cibersegurança são compreendidas, e estruturas organizacionais relevantes foram definidas. Passos iniciais foram tomados para estabelecê-las.

Básico:
As capacidades e estruturas organizacionais de cibersegurança da defesa nacional estão em vigor, mas ainda não foram adequadamente testadas. O financiamento é incerto ou indefinido. Doutrina operacional e regras de engajamento estão parcialmente incorporadas ao treinamento.

Médio:
As capacidades e estruturas organizacionais da cibersegurança na defesa nacional estão em vigor e foram testadas. O financiamento é garantido por meio do orçamento militar nacional ou processo equivalente. Doutrina operacional e regras de engajamento estão plenamente incorporadas ao treinamento. Recursos de inteligência especializados apoiam as operações.

Evoluído:
Mecanismos de colaboração com aliados estão estabelecidos e testados. Capacidades de dissuasão e defesa/resiliência estão integradas à estratégia de cibersegurança de defesa nacional. A cibersegurança está incorporada ao treinamento operacional e de comando.

Avançado:
As capacidades de ciberdefesa do país sustentam respostas multilaterais a desafios compartilhados de defesa nacional e coletiva.

Evidências

Doutrina de ciberdefesa estabelecida para as Forças Armadas.

Estratégia de ciberdefesa formalizada para as Forças Armadas.

Participação das Forças Armadas em exercícios e foruns internacionais de ciberdefesa.

Órgão de ciberdefesa dentro da estrtutura regimental das Forças Armadas .

Rúbrica orçamentária para ciberdefesa dentro do orçamento das Forças Armadas.

E1-Estratégia-2-D
Capacidade de Cibersegurança das Instituições de Segurança Nacional

Detalhamento:

Analisa o nível de capacidade de cibersegurança e as estruturas organizacionais dentro do aparato de segurança nacional.

Níveis de Maturidade:

Inicial:
A capacidade especializada em cibersegurança dentro do aparato de segurança nacional é limitada.

Fundamental:
As necessidades de capacidade especializada em cibersegurança são compreendidas, e estruturas organizacionais relevantes foram definidas. Passos iniciais foram tomados para estabelecê-las.

Básico:
As capacidades e estruturas organizacionais de cibersegurança da segurança nacional estão em vigor, mas ainda não foram adequadamente testadas. O financiamento é incerto ou indefinido. Doutrina operacional e regras de engajamento estão parcialmente incorporadas ao treinamento.

Médio:
As capacidades e estruturas organizacionais da cibersegurança na segurança nacional estão em vigor e foram testadas. O financiamento é garantido por meio do orçamento da segurança nacional ou processo equivalente. Doutrina operacional e regras de engajamento estão plenamente incorporadas ao treinamento. Recursos de inteligência especializados apoiam as operações.

Evoluído:
Mecanismos de colaboração com aliados estão estabelecidos e testados. Capacidades de dissuasão e defesa/resiliência estão integradas à estratégia de cibersegurança de segurança nacional. A cibersegurança está incorporada ao treinamento operacional e de comando.

Avançado:
As capacidades de cibersegurança do país sustentam respostas multilaterais a desafios compartilhados de segurança nacional e coletiva.

Evidências

Doutrina de cibersegurança estabelecida para as instituições civis de Estado ligadas à segurança nacional.

Existência de estruturas de cibersegurança em instituições civis de Estado ligadas à segurança nacional.

Participação das instituições civis de Estado ligadas à segurança nacional em exercícios e foruns internacionais de cibersegurança.

Participação das instituições civis de Estado ligadas à segurança nacional na formulação da política e/ou estratégia nacional de cibersegurança.

E1-Estratégia-2-E
Coordenação da relação civil-defesa

Detalhamento:

Examina a colaboração em matéria de cibersegurança entre entidades civis e de defesa, bem como a existência de recursos adequados.

Níveis de Maturidade:

Inicial: A colaboração em cibersegurança entre entidades civis e de defesa é limitada.
Fundamental: Pode haver colaboração informal em cibersegurança entre entidades civis e de defesa, mas ela não é formalizada, e as entidades de defesa não foram oficialmente dotadas de recursos para essa função.
Básico: A colaboração em cibersegurança entre entidades civis e de defesa foi formalizada, mas ainda não há procedimentos nacionais de gestão de crises.
Médio: A colaboração em cibersegurança entre entidades civis e de defesa existe e foi formalizada. Papéis e responsabilidades estão definidos nos procedimentos nacionais de gestão de crises.
Evoluído: Mecanismos formais determinam dependências cibernéticas militares e de segurança nacional em relação a infraestruturas civis e críticas. Recursos necessários foram avaliados e alocados. A colaboração civil-defesa está incorporada ao planejamento estratégico de ambos os setores.
Avançado: O país lidera o debate internacional sobre melhores práticas de colaboração cibernética intergovernamental, civil e de defesa. Mecanismos permitem que defesa e segurança nacional aproveitem as competências da economia e da sociedade (por exemplo, por meio de uma força cibernética de reserva).

Evidências

Coordenação formal entre defesa, setor civil e inteligência.

Normas para uso e controle de criptografia.

Programas de formação conjunta entre militares, civis e reguladores em cibersegurança.

E2-Cultura

Cultura e Sociedade

Detalhamento:

Analisa elementos importantes de uma mentalidade ou cultura de cibersegurança responsável, como a compreensão dos ciber-riscos na sociedade, o nível de confiança no ambiente digital e a compreensão dos usuários sobre a proteção de dados pessoais online.

Além disso, explora a existência e utilização de mecanismos de denúncia que funcionam como canais para os usuários relatarem crimes e ciberincidentes.

Adicionalmente, analisa o papel da mídia e das mídias sociais na formação de valores, atitudes e comportamentos relacionados à cibersegurança.

Por fim, analisa a existência de mecanismos de conscientização pública sobre ciber-higiene e cibersegurança.

E2-Cultura-1

Mentalidade de Cibersegurança

Detalhamento:

Avalia o grau em que a cibersegurança é priorizada e incorporada aos valores, atitudes e práticas do governo, do setor privado e dos usuários em geral.

E2-Cultura-1-A

Prioridade da Cibersegurança

Detalhamento:

Examina em que medida o governo, o setor privado e os usuários priorizam a cibersegurança.

Níveis de Maturidade:

Inicial:
O governo, o setor privado e os usuários não reconhecem a necessidade de priorizar a cibersegurança. Não existem métricas ou pesquisas que documentem o nível de prioridade da cibersegurança.

Fundamental:
Órgãos e empresas líderes reconhecem a necessidade de priorizar a cibersegurança. Uma pequena proporção de usuários reconhece essa necessidade. Pesquisas e métricas nacionais são limitadas ou ad hoc.

Básico:
Uma parte minoritária dos órgãos governamentais e empresas privadas em todos os níveis considera a cibersegurança uma prioridade. Existem poucas pesquisas e métricas nacionais para avaliar o conhecimento e a priorização da cibersegurança.

Médio:
A maioria dos órgãos governamentais e empresas privadas em todos os níveis está tornando a cibersegurança uma prioridade. Um número crescente de usuários faz o mesmo. Existem métricas e pesquisas nacionais para avaliar o conhecimento e prioridade da cibersegurança.

Evoluído:
Governos, empresas e usuários priorizam rotineiramente a cibersegurança e reavaliam prioridades diante de novas ameaças.

Avançado:
Todos os níveis de governo, setor privado e sociedade tratam a cibersegurança como prioridade estratégica contínua, incorporando-a em políticas públicas, práticas corporativas e hábitos pessoais, com revisões regulares baseadas em dados e ameaças emergentes.

Evidências

Engajamento formal de ONGs, academia e setor privado.

Inclusão explícita de cibersegurança em planos plurianuais e leis orçamentárias.

Programas de reconhecimento público de boas práticas de segurança.

Programas para consumo responsável de tecnologia.

E2-Cultura-1-B
Práticas de Cibersegurança

Detalhamento:

Examina se o governo, o setor privado e os usuários seguem boas práticas de cibersegurança.

Níveis de Maturidade:

Inicial:
Boas práticas de cibersegurança são praticamente inexistentes no governo, setor privado e entre os usuários.

Fundamental:
Alguns órgãos, empresas e usuários adotam boas práticas de forma limitada e reativa.

Básico:
Entre 25% e 50% das instituições governamentais e das empresas privadas adotam práticas seguras de cibersegurança de forma consistente, e um número crescente de usuários segue orientações básicas.

Médio:
O governo e as empresas privadas adotam práticas seguras de cibersegurança de forma consistente, e um número crescente de usuários segue orientações básicas.

Evoluído:
Práticas seguras estão amplamente integradas em processos, operações e comportamento dos usuários. Há campanhas de educação e incentivos à adoção de boas práticas.

Avançado:
O país apresenta cultura consolidada de cibersegurança, com práticas seguras naturalizadas no cotidiano do governo, das empresas e dos cidadãos, apoiadas por educação contínua, inovação e aprendizado coletivo.

Evidências

Ações educativas sobre segurança em portais SEICs.

Disponibilização de material educativo em múltiplos idiomas (incluindo línguas indígenas e de imigração) sobre cibersegurança em SEICs.

Guia nacional em linguagem simples sobre como identificar sites, aplicativos e centrais de atendimento falsos de empresas de SEICs.

Incentivo público à adoção de autenticação multifator.

Iniciativas de estímulo à participação de mulheres e minorias em ações de cibersegurança.

Iniciativas de gamificação para ensinar boas práticas de cibersegurança a jovens.

Monitoramento de desinformação.

Monitoramento de tendências de crimes digitais emergentes contra usuários.

Programas educativos para pequenas e médias empresas que prestam serviços a SEICs, abordando segurança básica e responsabilidade compartilhada.

E2-Cultura-2

Conhecimento dos riscos em Cibersegurança

Detalhamento:

Avalia o grau de conhecimento dos riscos oferecidos pelo ciberespaço para o governo, setor privado e sociedade em geral.

E2-Cultura-2-A

Consciência dos Riscos

Detalhamento:

Examina o nível de conscientização sobre os riscos de cibersegurança no governo, no setor privado e entre os usuários.

Níveis de Maturidade:

Inicial:
O governo possui nível mínimo ou inexistente de consciência sobre riscos de cibersegurança. O setor privado tem nível mínimo ou inexistente de consciência sobre riscos de cibersegurança. Usuários possuem nível mínimo ou inexistente de consciência sobre riscos de cibersegurança.

Fundamental:

Principais órgãos governamentais e empresas líderes têm consciência limitada sobre riscos de cibersegurança. Uma pequena proporção de usuários da Internet demonstra alguma consciência sobre ciber-riscos.

Básico:
Há alguma conscientização sobre riscos de cibersegurança na maioria dos órgãos governamentais e empresas privadas. Menos de 50% de usuários da sociedade reconhecem esses riscos.

Médio:
Há ampla conscientização sobre riscos de cibersegurança na maioria dos órgãos governamentais e empresas privadas. Mais de 50% dos usuários da sociedade reconhecem esses riscos.

Evoluído:
Órgãos governamentais e empresas privadas em todos os níveis estão plenamente conscientes dos riscos de cibersegurança e antecipam novas ameaças. Usuários também estão plenamente cientes dos riscos e procuram antecipar novas ameaças.

Avançado:
Órgãos governamentais, empresas e usuários utilizam continuamente a consciência de riscos para atualizar políticas, práticas operacionais e comportamentos, adaptando-se proativamente às mudanças no cenário de ameaças.

Evidências

Pesquisas periódicas sobre percepção pública de ciberameaças.

Produção de indicadores de percepção de ciber-risco específicos para usuários de SEICs.

E2-Cultura-2-B
Avaliação Crítica de conteúdo

Detalhamento:

Examina se os usuários da Internet avaliam criticamente o que veem ou recebem online.

Níveis de Maturidade:

Inicial:
Poucos usuários de Internet avaliam criticamente o que veem ou recebem online. Eles geralmente não acreditam possuir capacidade para usar a Internet de forma segura. Não há programas para apoiar habilidades de letramento digital e midiático.

Fundamental:
Uma proporção limitada, mas crescente, de usuários avalia criticamente o que vê online. Alguns acreditam ter capacidade para se proteger. Programas de capacitação digital estão sendo desenvolvidos.

Básico:
Menos da metade dos usuários avalia criticamente o que vê online e compreende como se proteger contra desinformação. Programas de letramento digital e midiático estão em operação, mas com alcance limitado.

Médio:
A maioria dos usuários avalia criticamente o que vê online e compreende como se proteger contra desinformação. Programas de letramento digital e midiático estão em operação.

Evoluído:

A maioria dos usuários reconhece informações duvidosas e toma medidas para verificá-las. Programas de capacitação digital são coordenados entre provedores de plataformas, reguladores e sociedade civil.

Avançado:
Quase todos os usuários avaliam rotineiramente os riscos do uso de serviços online e ajustam seus comportamentos conforme a qualidade da informação recebida. Programas colaborativos entre plataformas, reguladores e sociedade civil são contínuos.

Evidências

Autoridade reguladora com poderes de auditoria e fiscalização para proteção de crianças e adolescentes.

Programas de letramento digital para consumidores e usuários de SEICs com foco em segurança de aplicativos, portais e contas online.

E2-Cultura-3

Confiança em Serviços Online

Detalhamento:

Avalia o nível de conhecimento dos riscos oferecidos pelo ciberespaço para o governo, setor privado e sociedade em geral.

E2-Cultura-3-A

Confiança e Segurança em Buscas e Informações Online

Detalhamento:

Examina se os usuários confiam no uso seguro da internet com base em indicadores de legitimidade do site.

Níveis de Maturidade:

Inicial:
A maioria dos usuários não confia ou confia cegamente em websites e conteúdo online. Poucos se sentem confiantes no uso da Internet. Não há métricas sobre confiança online.

Fundamental:
Uma pequena proporção de usuários confia no uso da Internet e se sente minimamente segura. Há métricas limitadas ou ad hoc.

Básico:
Menos da metade dos usuários confia no uso seguro da Internet e reconhece indicadores de legitimidade de sites. Métricas e pesquisas estão em vigor.

Médio:
A maioria dos usuários confia no uso seguro da Internet e reconhece indicadores de legitimidade de sites. Métricas e pesquisas são realizadas ao menos anualmente.

Evoluído:
A maioria dos usuários tem confiança aprendida no uso da Internet e reconhece sites legítimos. Pesquisas sobre confiança são realizadas rotineiramente.

Avançado:
Quase todos os usuários confiam em seu uso seguro da Internet, ajudam outros e verificam informações. Pesquisas nacionais são referência internacional.

Evidências

Mecanismos de engajamento com associações de classe para identificar e divulgar padrões recorrentes de fraude digital.

Mecanismos de engajamento com associações de consumidores para identificar e divulgar padrões recorrentes de fraude digital.

Mecanismos de engajamento com associações empresariais para identificar e divulgar padrões recorrentes de fraude digital.

E2-Cultura-3-B
Combate à Desinformação

Detalhamento:

Examina a existência de ferramentas e recursos para combater a desinformação online.

Níveis de Maturidade:

Inicial:
Provedores de plataformas não tratam da desinformação. A sociedade civil carece de ferramentas e recursos. O governo não aborda o problema.

Fundamental:
Abordagens iniciais de plataformas e sociedade civil surgem para lidar com desinformação. O governo inicia programas limitados, centrados em filtragem e conscientização.

Básico:
Políticas e ferramentas são aplicadas por plataformas e sociedade civil. Programas governamentais buscam preparar o público sem censura.

Médio:
Políticas e ferramentas são desenvolvidas e aplicadas por plataformas e sociedade civil, respeitando direitos humanos. Programas governamentais prepararam o público sem censura.

Evoluído:
Políticas das plataformas e iniciativas civis consolidam-se. O país apoia planos nacionais, regionais e internacionais contra desinformação, protegendo a liberdade de expressão.

Avançado:
O país lidera esforços regionais/globais, com planos e diretrizes que equilibram combate à desinformação e proteção da Internet aberta, empoderando usuários.

Evidências

Campanhas públicas para desmistificar desinformação sobre falhas em SEICs, equilibrando transparência e prevenção de pânico.

Campanhas sazonais, por exemplo no horário eleitoral gratuito no rádio e na TV, destinadas à identificação de desinformação e deep fakes

Monitoramento do impacto de desinformação em temas de segurança pública e saúde.

E2-Cultura-3-C
Confiança do usuário em serviços de governo eletrônico

Detalhamento:

Examina se existem serviços eletrônicos governamentais oferecidos, se há confiança na prestação segura desses serviços e se estão sendo feitos esforços para promover essa confiança na aplicação de medidas de segurança.

Níveis de Maturidade:

Inicial:
O governo oferece poucos ou nenhum e-serviço e não promove sua segurança. Não há métricas de confiança.

Fundamental:
O governo inicia e-serviços com medidas básicas de segurança. Pequeno número de usuários demonstra confiança.

Básico:
Serviços de governo eletrônico estão em funcionamento. Pesquisas de confiança e publicações de segurança são eventuais.

Médio:
Serviços de governo eletrônico estão em funcionamento e têm ampla adoção. Pesquisas de confiança e publicações de segurança são regulares.

Evoluído:
e-Gov é o modo predominante de prestação de serviços públicos. A maioria dos usuários confia e os utiliza. Autoridades coordenam e divulgam medidas de segurança e privacidade.

Avançado:
O país é reconhecido internacionalmente pela qualidade e segurança de seus e-serviços. Pesquisas são contínuas e os serviços são revisados e aprimorados proativamente.

Evidências

Indicador nacional de confiança em governo eletrônico.

Indicadores de confiança social em serviços digitais.

E2-Cultura-3-D
Confiança do usuário em serviços de comércio eletrônico

Detalhamento:

Examina se os serviços de comércio eletrônico são oferecidos e estabelecidos em um ambiente seguro e se inspiram confiança nos usuários.

Níveis de Maturidade:

Inicial:
Serviços de e-commerce não são oferecidos. Usuários não confiam em sua utilização. Não há métricas de confiança.

Fundamental:
Serviços limitados começam a ser oferecidos e adotados por poucos usuários. Setor privado reconhece a necessidade de medidas de segurança.

Básico:
E-commerce estabelecido por alguns atores. Usuários confiam e pesquisas avaliam esporadicamente essa confiança.

Médio:
E-commerce estabelecido por múltiplos atores em ambiente seguro. Usuários confiam e pesquisas avaliam regularmente essa confiança.

Evoluído:
e-Commerce é amplamente aceito e seguro. A maioria dos usuários confia e utiliza. Investimentos em proteção de dados e feedback do usuário são frequentes.

Avançado:
O país é reconhecido internacionalmente por seus serviços de e-commerce seguros e confiáveis. Pesquisas orientadas a resultados aprimoram continuamente os sistemas.

Evidências

Indicadores de confiança em comércio eletrônico.

Indicadores de confiança em identidade digital.

E2-Cultura-4

Compreensão sobre a proteção de informações pessoais online

Detalhamento:

Analisa se os usuários da Internet e as partes interessadas dos setores público e privado reconhecem e compreendem a importância da proteção de informações pessoais online e se são sensíveis aos seus direitos e deveres de privacidade.

E2-Cultura-4-A

Compreensão do usuário da Internet sobre a proteção de informações pessoais online

Detalhamento:

Analisa se os usuários da Internet reconhecem e compreendem a importância da proteção de informações pessoais online, inclusive em plataformas de IA, e se são sensíveis aos seus direitos de privacidade.

Níveis de Maturidade:

Inicial:
Usuários não possuem ou têm conhecimento mínimo sobre como as informações pessoais são tratadas online, nem acreditam que existam medidas adequadas para protegê-las. Não há discussões sobre proteção de informações pessoais online e inexistem padrões de privacidade que orientem práticas na Internet e redes sociais.

Fundamental:
Usuários têm algum conhecimento geral sobre como as informações pessoais são tratadas online e podem adotar boas práticas de cibersegurança para proteger suas informações. Discussões iniciais ocorrem sobre a proteção de dados e o equilíbrio entre segurança e privacidade. Políticas e ações concretas começam a ser desenvolvidas.

Básico:

Uma minoria dos usuários possui habilidades para gerenciar sua privacidade online e se proteger contra intrusões, interferências ou acessos indesejados. O debate público sobre proteção de informações e equilíbrio entre segurança e privacidade é inconstante ou muito básico. Políticas de privacidade não são amplamente estabelecidas.

Médio:
A maioria dos usuários possui habilidades para gerenciar sua privacidade online e se proteger contra intrusões, interferências ou acessos indesejados. O debate público sobre proteção de informações e equilíbrio entre segurança e privacidade é considerável. Políticas de privacidade são amplamente estabelecidas.

Evoluído:
Todos os atores têm informação, confiança e capacidade para proteger suas informações pessoais online e manter controle sobre sua distribuição. Usuários e instituições reconhecem amplamente a importância da proteção de dados e estão cientes de seus direitos de privacidade. Mecanismos públicos e privados moldam práticas na Internet e redes sociais para garantir que privacidade e segurança não sejam concorrentes.

Avançado:
Políticas e mecanismos são revisados proativamente para assegurar que privacidade e segurança se reforcem mutuamente em um ambiente em constante mudança. Essas políticas são informadas por feedback dos usuários e debates públicos. Novos mecanismos, como "privacidade por padrão" (privacy by default), são implementados e promovidos como ferramentas de transparência e confiança.

Evidências

Ações educativas específicas para proteção de dados pessoais e dados sensíveis.

Campanhas voltadas a pacientes e profissionais de saúde sobre proteção de dados em prontuários eletrônicos e telemedicina.

Guias de cibersegurança para o público em geral.

Programas de orientação sobre proteção de dados e cibersegurança para conselhos de saúde, educação e assistência social.

E2-Cultura-4-B

Compreensão do usuário do setor público sobre a proteção de informações pessoais online

Detalhamento:

Analisa se usuários do setor público reconhecem e compreendem a importância da proteção de informações pessoais online, inclusive em plataformas de IA, e se são sensíveis aos seus direitos de privacidade.

Níveis de Maturidade:

Inicial:
Partes interessadas do setor público não possuem ou têm conhecimento mínimo sobre como as informações pessoais são tratadas online, nem acreditam que existam medidas adequadas para protegê-las. Não há discussões sobre proteção de informações pessoais online e inexistem padrões de privacidade que orientem práticas na Internet e redes sociais.

Fundamental:
Partes interessadas do setor público têm algum conhecimento geral sobre como as informações pessoais são tratadas online e podem adotar boas práticas de cibersegurança para proteger suas informações. Discussões iniciais ocorrem sobre a proteção de dados e o equilíbrio entre segurança e privacidade. Políticas e ações concretas começam a ser desenvolvidas.

Básico:
Uma minoria dos usuários do setor público possui habilidades para gerenciar sua privacidade online e se proteger contra intrusões, interferências ou acessos indesejados. O debate público sobre proteção de informações e equilíbrio entre segurança e privacidade é inconstante ou muito básico. Políticas de privacidade não são amplamente estabelecidas no setor público.

Médio:
A maioria dos usuários do setor público possui habilidades para gerenciar sua privacidade online e se proteger contra intrusões, interferências ou acessos indesejados. O debate público sobre proteção de informações e equilíbrio entre segurança e privacidade é considerável. Políticas de privacidade são amplamente estabelecidas no setor público.

Evoluído:
Todos os atores têm informação, confiança e capacidade para proteger suas informações pessoais online e manter controle sobre sua distribuição. Usuários e instituições reconhecem amplamente a importância da proteção de dados e estão cientes de seus direitos de privacidade. Mecanismos públicos moldam práticas na Internet e redes sociais para garantir que privacidade e segurança não sejam concorrentes.

Avançado:
Políticas e mecanismos no setor público são revisados proativamente para assegurar que privacidade e segurança se reforcem mutuamente em um ambiente em constante mudança. Essas políticas são informadas por feedback dos usuários e debates públicos. Novos mecanismos, como "privacidade por padrão" (privacy by default), são implementados e promovidos como ferramentas de transparência e confiança.

Evidências

Ações educativas específicas para proteção de dados pessoais e dados sensíveis no serviço público.

Campanhas voltadas a servidores públicos sobre proteção de dados em processos e procedimentos.

Guias de cibersegurança para servidores públicos.

E2-Cultura-4-C
Compreensão do usuário do setor privado sobre a proteção de informações pessoais online

Detalhamento:

Analisa se usuários do setor privado reconhecem e compreendem a importância da proteção de informações pessoais online, inclusive em plataformas de IA, e se são sensíveis aos seus direitos de privacidade.

Níveis de Maturidade:

Inicial:

Partes interessadas do setor privado não possuem ou têm conhecimento mínimo sobre como as informações pessoais são tratadas online, nem acreditam que existam medidas adequadas para protegê-las. Não há discussões sobre proteção de informações pessoais online e inexistem padrões de privacidade que orientem práticas na Internet e redes sociais.

Fundamental:
Partes interessadas do setor privado têm algum conhecimento geral sobre como as informações pessoais são tratadas online e podem adotar boas práticas de cibersegurança para proteger suas informações. Discussões iniciais ocorrem sobre a proteção de dados e o equilíbrio entre segurança e privacidade. Políticas e ações concretas começam a ser desenvolvidas.

Básico:
Uma minoria dos usuários do setor privado possui habilidades para gerenciar sua privacidade online e se proteger contra intrusões, interferências ou acessos indesejados. O debate público sobre proteção de informações e equilíbrio entre segurança e privacidade é inconstante ou muito básico. Políticas de privacidade não são amplamente estabelecidas no setor privado.

Médio:
A maioria dos usuários do setor privado possui habilidades para gerenciar sua privacidade online e se proteger contra intrusões, interferências ou acessos indesejados. O debate público sobre proteção de informações e equilíbrio entre segurança e privacidade é considerável. Políticas de privacidade são amplamente estabelecidas no setor privado.

Evoluído:
Todos os atores do setor privado têm informação, confiança e capacidade para proteger suas informações pessoais online e manter controle sobre sua distribuição. Usuários e instituições reconhecem amplamente a importância da proteção de dados e estão cientes de seus direitos de privacidade. Mecanismos do setor privado moldam práticas na Internet e redes sociais para garantir que privacidade e segurança não sejam concorrentes.

Avançado:
Políticas e mecanismos no setor privado são revisados proativamente para assegurar que privacidade e segurança se reforcem mutuamente em um ambiente em constante mudança. Essas políticas são informadas por feedback dos usuários e debates públicos. Novos mecanismos, como "privacidade por padrão" (privacy by default), são implementados e promovidos como ferramentas de transparência e confiança.

Evidências

Ações educativas específicas para proteção de dados pessoais e dados sensíveis no setor privado.

Campanhas voltadas a servidores de empresas privadas sobre proteção de dados em processos e procedimentos.

Guias de cibersegurança para servidores de empresas privadas.

E2-Cultura-5

Mecanismos de Denúncia

Detalhamento:

Explora a existência de mecanismos de denúncia que funcionam como canais para os usuários relatarem crimes e incidentes relacionados à internet, como fraudes online, cyberbullying, abuso infantil online, roubo de identidade, violações de privacidade e segurança e outros incidentes.

E2-Cultura-5-A

Mecanismos de Denúncia

Detalhamento:

Explora a existência de mecanismos de denúncia que funcionam como canais para os usuários relatarem crimes relacionados à internet, como fraudes online, cyberbullying, abuso infantil online, roubo de identidade, violações de privacidade e segurança e outros incidentes.

Níveis de Maturidade:

Inicial:
Não existem mecanismos oficiais de relato disponíveis, embora discussões possam ter sido iniciadas. Usuários não utilizam canais de mídia social para relatar danos ou problemas cibernéticos. Não há métricas sobre incidentes relatados.

Fundamental:
Setores público e/ou privado oferecem alguns canais para relatar danos cibernéticos (como fraudes online, cyberbullying, abuso infantil, roubo de identidade, violações de privacidade e segurança, entre outros), mas esses canais não são coordenados e são utilizados de forma ad hoc. Usuários utilizam canais de mídia social para alertar outros usuários de maneira não estruturada. Métricas sobre incidentes relatados estão sendo desenvolvidas.

Básico:
Mecanismos de relato foram estabelecidos, mas são pouco promovidos ou não usados regularmente. Usuários da Internet utilizam eventualmente canais de mídia social para informar outros usuários. Existem métricas iniciais sobre incidentes relatados.

Médio:
Mecanismos de relato foram estabelecidos, promovidos e são usados regularmente. Usuários da Internet utilizam amplamente canais de mídia social para informar outros usuários. Existem métricas consistentes sobre incidentes relatados.

Evoluído:
Mecanismos coordenados de relato são amplamente utilizados e promovidos. Usuários utilizam rotineiramente canais de mídia social para compartilhar informações e alertas. Métricas de danos cibernéticos são utilizadas para revisar e promover novas políticas e práticas. Mecanismos são desenvolvidos para coordenar a resposta a incidentes relatados entre as forças de segurança e a capacidade nacional de resposta a incidentes.

Avançado:
Usuários da Internet utilizam habitualmente canais de mídia social para informar outros e compartilhar boas práticas. Métricas são rotineiramente usadas para subsidiar políticas e decisões. O país demonstra capacidade integrada e adaptativa de aprendizado com incidentes e de comunicação pública eficiente para prevenção de danos futuros.

Evidências

Canais anônimos para denúncias.

Mecanismos de feedback do cidadão sobre experiências com fraudes e ataques.

Mecanismos públicos de denúncia de cibercrimes e fraudes.

E2-Cultura-5-B
Mecanismos de Apoio às Vítimas

Detalhamento:

Explora a existência de mecanismos de apoio às vítimas que denunciam crimes e outros incidentes por meio dos canais oficiais de denúncia.

Níveis de Maturidade:

Inicial:
Não existem mecanismos oficiais de apoio às vítimas, embora discussões possam ter sido iniciadas.

Fundamental:
Mecanismos de apoio podem existir, mas são poucos ou estruturados ad hoc. Métricas sobre os apoios prestados estão sendo desenvolvidas.

Básico:
Mecanismos de apoio foram estabelecidos, mas não são usados regularmente ou o são apenas em poucos casos. Existem métricas iniciais sobre os apoios prestados.

Médio:
Mecanismos de apoio foram estabelecidos, promovidos e são usados regularmente. Existem métricas consistentes sobre os apoios prestados.

Evoluído:
Mecanismos coordenados de apoio às vítimas são amplamente utilizados e promovidos. Mecanismos são desenvolvidos para coordenar o apoio a vítimas de incidentes relatados.

Avançado:
Vítimas recebem apoio regularmente. Métricas são rotineiramente usadas para subsidiar políticas e decisões. O país demonstra capacidade integrada e adaptativa de aprendizado com incidentes e de comunicação pública eficiente para prevenção de danos futuros.

Evidências

Núcleos de apoio psicológico e jurídico para vítimas de cibercrimes.

Programas de orientação técnica gratuita para vítimas.

E2-Cultura-6
Mídia e Plataformas Online

Detalhamento:

Explora se a cibersegurança é um tema comum de discussão na mídia tradicional e um assunto para ampla discussão nas mídias sociais.

Além disso, analisa o papel da mídia na transmissão de informações sobre cibersegurança ao público, moldando assim seus valores, atitudes e comportamento online em relação à cibersegurança.

E2-Cultura-6-A
Cibersegurança como tema comum

Detalhamento:

Explora se a cibersegurança é um tema comum de discussão na mídia tradicional e um assunto para ampla discussão nas mídias sociais.

Níveis de Maturidade:

Inicial:
A mídia tradicional raramente cobre informações sobre cibersegurança ou reporta temas como violações de segurança ou cibercrimes. Raramente há discussões sobre cibersegurança nas redes sociais. Qualquer retrato de denunciantes (ou notificantes) é negativo, baseado em estereótipos criminais ou depreciativos.

Fundamental:
Há cobertura pontual e esporádica da mídia tradicional sobre cibersegurança, com informações limitadas e foco em questões específicas, como proteção infantil online ou cyberbullying. Há discussões limitadas sobre cibersegurança nas redes sociais. Casos positivos de impacto construtivo de denunciantes começam a surgir.

Básico:
A cibersegurança torna-se um tema eventual na mídia tradicional, com reduzida disseminação de informações sobre violações de segurança, cibercrimes e boas práticas. Há pouca discussão sobre cibersegurança nas mídias sociais. Reconhece-se parcialmente o papel positivo dos denunciantes.

Médio:
A cibersegurança torna-se um tema recorrente na mídia tradicional, com ampla disseminação de informações sobre violações de segurança, cibercrimes e boas práticas. Há ampla discussão sobre cibersegurança nas mídias sociais. Reconhece-se o papel positivo dos denunciantes.

Evoluído:
A cobertura da mídia se estende além do relato de ameaças, abordando medidas proativas e práticas de cibersegurança, bem como seus impactos econômicos e sociais. Há discussões frequentes sobre cibersegurança nas mídias sociais, e indivíduos compartilham experiências online. Transparência e denúncia são incentivadas.

Avançado:
Discussões amplas nas mídias tradicionais e sociais sobre experiências e atitudes pessoais influenciam a formulação de políticas e promovem mudanças sociais. As mídias sociais tornam-se um componente central no monitoramento e enfrentamento de danos cibernéticos. A denúncia (ou notificação) é incentivada e protegida como instrumento de responsabilidade social.

Evidências

Parcerias com influenciadores digitais para disseminar conteúdos de cibersegurança.

Parcerias com veículos de mídia de massa para disseminar conteúdos de cibersegurança.

E2-Cultura-6-B
Papel da mídia na formação de valores

Detalhamento:

Analisa o papel da mídia na transmissão de informações sobre cibersegurança ao público, moldando assim seus valores, atitudes e comportamento online em relação à cibersegurança.

Níveis de Maturidade:

Inicial:
A mídia tradicional raramente divulga boas práticas de cibersegurança ao público. Raramente há publicação de matérias sobre cibersegurança na imprensa. Referências a denunciantes (ou notificantes) são negativas, baseadas em estereótipos criminais ou depreciativos.

Fundamental:
Há cobertura pontual e esporádica da mídia tradicional sobre cibersegurança, com informações limitadas e foco em questões específicas. Há discussões limitadas sobre valores, atitudes e comportamentos online em relação à cibersegurança

Básico:
Valores, atitudes e boas práticas de cibersegurança são um tema apenas eventual na mídia tradicional.

Médio:
Valores, atitudes e boas práticas de cibersegurança são um tema recorrente na mídia tradicional.

Evoluído:
A cobertura da mídia se estende além do relato de ameaças, incluindo valores, atitudes, boas práticas e medidas proativas de cibersegurança, bem como seus impactos econômicos e sociais.

Avançado:
Discussões amplas nas mídias tradicionais e sociais sobre experiências e atitudes pessoais influenciam a formulação de valores, atitudes e práticas na sociedade.

Evidências

Parcerias com plataformas digitais para campanhas preventivas.

Participação ativa da mídia na disseminação de conteúdo seguro.

Presença de conteúdos oficiais em redes sociais com respostas rápidas.

Programas de formação em cibersegurança para jornalistas que cobrem temas ligados a SEICs.

Programas de prevenção de violência de gênero e discursos de ódio na Internet.

Programas voltados à conscientização de jornalistas sobre segurança da informação.

E2-Cultura-7

Conscientização em Cibersegurança

Detalhamento:

Analisa a disponibilidade de programas que aumentem a conscientização sobre cibersegurança em todo o país, com foco nos riscos e ameaças à cibersegurança e nas maneiras de lidar com eles.

E2-Cultura-7-A

Programa nacional de conscientização sobre cibersegurança

Detalhamento:

Examina a existência de um programa nacional coordenado de conscientização sobre cibersegurança, conduzido pelo setor público, que abrange uma ampla gama de grupos e questões demográficas, desenvolvido em consulta com partes interessadas de vários setores.

Níveis de Maturidade:

Inicial:
Não há programa nacional abrangente de conscientização em cibersegurança desenvolvido pelo governo. A necessidade de conscientização sobre ameaças e vulnerabilidades cibernéticas ainda não é reconhecida ou está apenas em discussão inicial.

Fundamental:
Um programa nacional coordenado de conscientização em cibersegurança está em desenvolvimento, com participação de partes interessadas do governo, setor privado e sociedade civil. Programas, cursos e seminários iniciados pelo governo estão disponíveis, mas ainda não totalmente incorporados à estratégia nacional de cibersegurança. Recursos são limitados e mecanismos de avaliação são ad hoc.

Básico:
Um programa nacional coordenado de conscientização em cibersegurança, com plano de implementação genérico orientado por uma estratégia nacional, foi publicado. Inexiste um órgão coordenador com autoridade e recursos adequados.

Médio:
Um programa nacional coordenado de conscientização em cibersegurança, com plano de implementação detalhado e vínculo explícito à estratégia nacional, é publicado. Existe um órgão coordenador com autoridade e recursos adequados. Processos de revisão e métricas orientadas a resultados estão em vigor.

Evoluído:
O programa nacional está totalmente integrado a programas setoriais (indústria, academia, sociedade civil, mulheres e crianças). Riscos emergentes são regularmente avaliados e usados para atualizar o programa. Métricas são aplicadas para ajustar as ações e a estratégia nacional.

Avançado:
O programa nacional de conscientização é revisado proativamente com partes interessadas públicas e privadas, levando em conta desenvolvimentos estratégicos nacionais (políticos, econômicos, sociais, técnicos, legais e ambientais).

Evidências

Ações educativas sobre cyberbullying e crimes contra a honra na Internet.

Biblioteca digital centralizada com materiais verificáveis sobre cibersegurança.

Campanhas de cibersegurança nas instituições de ensino fundamental, médio e técnico que usem exemplos reais de riscos em cibersegurança.

Campanhas de conscientização com linguagem adaptada a diferentes faixas etárias.

Campanhas de prevenção a golpes de phishing e vishing que se aproveitam de marcas de autarquias federais.

ampanhas preventivas de ransomware voltadas ao cidadão comum.
Criação de um portal unificado de governo federal com alertas atualizados sobre fraudes e campanhas maliciosas contra usuários de SEICs.
Disseminação de conteúdos de cibersegurança em múltiplos idiomas e formatos acessíveis.
Estrutura nacional de educação parental sobre riscos digitais infantis.
Indicadores de alcance de campanhas de conscientização em diferentes regiões do país.
Iniciativas específicas de conscientização para comunidades rurais sobre segurança de soluções de pagamento digital e serviços públicos remotos.
Materiais acessíveis em formatos inclusivos (audiodescrição, Libras, leitura fácil).
Medição regular do impacto social de campanhas de conscientização.
Política nacional de inclusão digital segura.
Presença de portais oficiais com recomendações atualizadas de segurança ao cidadão.
Produção de conteúdo audiovisual educativo acessível.
Programas nacionais de literacia digital para população em vulnerabilidade social.
Programas nacionais permanentes de conscientização em cibersegurança.
Programas públicos voltados à cibersegurança de crianças e adolescentes.
Programas públicos voltados à cibersegurança de idosos.

Programas públicos voltados à cibersegurança de pessoas neurodivergentes.

E2-Cultura-7-B
Programas privados de conscientização sobre cibersegurança

Detalhamento:

Examina a existência de programas de sensibilização promovidos pelo setor privado e a medida em que estão alinhados com as iniciativas governamentais e da sociedade civil.

Níveis de Maturidade:

Inicial:
O setor privado não demonstra consciência ou capacidade de desenvolver programas de conscientização em cibersegurança.

Fundamental:
Algumas empresas líderes começam a desenvolver programas de conscientização, mas de forma isolada e sem coordenação com o governo ou sociedade civil.

Básico:
Programas de conscientização conduzidos pelo setor privado são ocasionalmente realizados, alinhados parcialmente com iniciativas governamentais e de sociedade civil.

Médio:
Programas de conscientização conduzidos pelo setor privado estão regularmente em operação, alinhados parcialmente com iniciativas governamentais e da sociedade civil.

Evoluído:
Programas privados estão plenamente integrados ao programa nacional de conscientização e incluem mecanismos de avaliação e métricas de impacto.

Avançado:
Esforços conjuntos com o governo e a sociedade civil produzem impacto mensurável na redução do panorama de ameaças.

Evidências

Campanhas de prevenção a golpes de phishing e vishing que se aproveitam de marcas de instituições privadas.

Campanhas nacionais específicas de conscientização sobre golpes relacionados a serviços financeiros digitais, incluindo PIX, cartões e open banking.

Materiais educativos nacionais que expliquem riscos de manipulação de faturas, leituras e medidores inteligentes conectados.

Programas de conscientização voltados a motoristas, transportadoras e operadores logísticos sobre riscos de ataques a sistemas de rastreamento e roteamento.

E2-Cultura-7-C
Programas de conscientização sobre cibersegurança da sociedade civil

Detalhamento:

Este aspeto examina a existência de programas de conscientização em cibersegurança promovidos pela sociedade civil e a medida em que estão alinhados com as iniciativas governamentais e do setor privado.

Níveis de Maturidade:

Inicial:
A necessidade de conscientização em cibersegurança na sociedade civil não é reconhecida ou está apenas em discussão inicial.

Fundamental:
A sociedade civil começa a perceber seu papel em programas, cursos e campanhas, mas sem resultados concretos. Um sistema inicial de métricas pode existir.

Básico:
Esforços colaborativos entre governo e setor privado surgem para compartilhar informações e identificar práticas seguras.

Médio:
Esforços colaborativos entre governo e setor privado para compartilhar informações e identificar práticas seguras estão consolidados e em ampliação. Papéis e mecanismos de coordenação são definidos.

Evoluído:
Processos de revisão e métricas orientadas a resultados estão em vigor e financiados, com resultados compartilhados entre governo e setor privado. A efetividade dos esforços conjuntos é regularmente avaliada.

Avançado:
Iniciativas da sociedade civil são totalmente integradas ao programa nacional. Lições aprendidas alimentam novos programas. Os esforços conjuntos têm impacto mensurável na redução do cibe-risco.

Evidências

Guia nacional de cibersegurança para organizações da sociedade civil que atuam em defesa de direitos em saúde, meio ambiente, água e energia.

Programas de mentoria em cibersegurança para organizações da sociedade civil.

E2-Cultura-7-D
Sensibilização de Executivos

Detalhamento:

Examina os esforços para aumentar a conscientização de executivos sobre questões de cibersegurança nos setores público, privado, acadêmico e da sociedade civil, bem como a forma como os riscos de cibersegurança podem ser abordados.

Níveis de Maturidade:

Inicial:
A conscientização sobre cibersegurança entre executivos é limitada ou inexistente. Eles desconhecem responsabilidades perante acionistas, clientes e funcionários.

Fundamental:

Executivos são informados sobre questões gerais de cibersegurança, mas não compreendem como ameaças específicas afetam suas organizações.

Básico:
Executivos de setores considerados SEICs estão conscientes dos riscos, mas suas organizações ainda não os gerenciam adequadamente.

Médio:
Executivos de setores considerados SEICs estão conscientes dos riscos e de como suas organizações os gerenciam, mas sem foco estratégico.

Evoluído:
A conscientização executiva abrange riscos, métodos de ataque e implicações estratégicas, sendo incorporada em treinamentos e planos de crise.

Avançado:
A conscientização executiva é contínua e integrada à gestão estratégica e à governança corporativa, resultando em decisões alinhadas à cibersegurança organizacional.

Evidências

Mapeamento das competências essenciais de cibersegurança exigidas para cargos públicos estratégicos.

Programas de capacitação em segurança para conselheiros e altos executivos estatais.

Programas de sensibilização voltados a micro e pequenos empreendedores.

E2-Cultura-8

Conscientização em Ciber-higiene

Detalhamento:

Analisa a disponibilidade de programas que aumentem a conscientização em ciber-higiene em todo o país.

E2-Cultura-8-A

Iniciativas Governamentais

Detalhamento:

Examina a existência de um programa nacional coordenado de conscientização sobre ciber-higiene, conduzido pelo governo.

Níveis de Maturidade:

Inicial:
Não há programa nacional abrangente de conscientização em ciber-higiene desenvolvido pelo governo.

Fundamental:
Um programa nacional coordenado de conscientização em ciber-higiene está em desenvolvimento, com participação de partes interessadas do governo, setor privado e sociedade civil.

Básico:

Um programa nacional coordenado de conscientização em ciber-higiene, com plano de implementação detalhado e vínculo explícito à estratégia nacional, foi publicado. Inexiste um órgão coordenador com autoridade e recursos adequados.

Médio:
Um programa nacional coordenado de conscientização em ciber-higiene, com plano de implementação detalhado e vínculo explícito à estratégia nacional, é publicado. Existe um órgão coordenador com autoridade e recursos adequados. Processos de revisão e métricas orientadas a resultados estão em vigor.

Evoluído:
O programa nacional está totalmente integrado a programas setoriais (indústria, academia, sociedade civil, mulheres e crianças). Riscos emergentes são regularmente avaliados e usados para atualizar o programa. Métricas são aplicadas para ajustar as ações e a estratégia nacional.

Avançado:
O programa nacional de conscientização é revisado proativamente com partes interessadas públicas e privadas, levando em conta desenvolvimentos estratégicos nacionais (políticos, econômicos, sociais, técnicos, legais e ambientais).

Evidências

Disponibilidade de cursos EAD gratuitos de alfabetização em cibersegurança.

Guia nacional de boas práticas para uso seguro de redes Wi-Fi públicas.

Guias de higiene digital obrigatórios para serviços públicos.

Materiais e guias públicos sobre boas práticas de ciber-higiene.

Programas para prevenção de golpes financeiros e engenharia social.

Veiculação de campanhas de ciber-higiene em instituições de ensino fundamental, médio e técnico, incluindo vídeos transmitidos nas salas de aula e panfletos/cartilhas distribuídos aos pais e alunos.

Veiculação de propagandas rápidas sobre medidas de ciber-higiene.

E3-Capacidades

Capacidades e Conhecimentos

Detalhamento:

Analisa a disponibilidade, a qualidade, a adesão e a continuidade de programas de educação e qualificação para diversos grupos de interesses, incluindo o governo, o setor privado e a população em geral, e relaciona-se com programas formais de educação em cibersegurança e programas de treinamento profissional.

Considera também a capacidade de desenvolvimento do ecossistema de cibersegurança na formação de talentos, pesquisa avançada e colaboração intersetorial, com foco na criação de capacidades técnicas e científicas

E3-Capacidades-1

Educação em Cibersegurança

Detalhamento:

Aborda a disponibilidade, oferta, qualidade, continuidade e adesão a programas de educação formal e profissional em cibersegurança.

Considera também a existência de um número suficiente de professores e palestrantes qualificados.

Adicionalmente, examina a necessidade de aprimorar a educação em cibersegurança nos níveis nacional e institucional.

Por fim, analisa a colaboração entre governo e indústria para garantir que os investimentos em educação atendam às necessidades do ambiente de educação em cibersegurança em todos os setores.

E3-Capacidades-1-A

Oferta de programas de cibereducação

Detalhamento:

Explora se existem ofertas educacionais formais em cibersegurança e programas de qualificação para educadores disponíveis que proporcionem uma compreensão dos riscos atuais e das necessidades de competências.

Níveis de Maturidade:

Inicial:
Não há programas de qualificação para docentes. Cursos de ciência da computação podem conter algum componente de segurança, mas não há disciplinas específicas de cibersegurança. Não existe sistema de acreditação para educação em cibersegurança.

Fundamental:
Programas de qualificação para educadores estão sendo explorados. Alguns cursos relacionados à cibersegurança (segurança da informação, redes, criptografia) são oferecidos, mas ainda não há cursos específicos de cibersegurança. A demanda por educação em cibersegurança é evidenciada por matrículas e feedback de alunos.

Básico:

A qualificação e oferta de educadores em cibersegurança começa a surgir. Cursos especializados em cibersegurança começam a ser oferecidos e acreditados em nível universitário. Módulos de conscientização sobre ciber-riscos são incluídos em cursos universitários. Universidades e instituições correlatas promovem palestras e seminários eventuais sobre cibersegurança voltados a não especialistas.

Médio:
A qualificação e oferta de educadores em cibersegurança está disponível. Cursos especializados em cibersegurança são oferecidos e acreditados em nível universitário. Módulos de conscientização sobre ciber-riscos são incluídos em diversos cursos universitários. Universidades e instituições correlatas promovem palestras e seminários regulares sobre cibersegurança voltados a não especialistas.

Evoluído:
A educação em cibersegurança abrange todos os níveis — do ensino fundamental e médio até o superior e pós-graduação, incluindo educação técnica e profissional. Passos são dados para incorporar a estrutura STEM (Ciência, Tecnologia, Engenharia e Matemática) com foco em cibersegurança. Educadores são recrutados também da indústria e governo, com incentivos específicos. Cursos acreditados em cibersegurança são integrados em todos os currículos de ciência da computação.

Avançado:
São oferecidos cursos e programas de graduação especificamente em cibersegurança, abrangendo componentes técnicos e não técnicos (como políticas públicas e abordagens multidisciplinares). O conteúdo é atualizado conforme novas ameaças e habilidades exigidas. Diretrizes nacionais e internacionais são seguidas. Programas de estágio e aprendizado prático (apprenticeships) unem teoria e prática. Programas nacionais de pesquisa e formação estão na vanguarda da educação em cibersegurança.

Evidências

Ações educativas sobre privacidade e uso de dados pessoais.
Currículos formais de cibersegurança no ensino fundamental, médio e técnico.
Currículos universitários alinhados a padrões internacionais (por exemplo ACM/IEEE).
Indicadores de redução de incidentes de phishing e golpes digitais após campanhas educativas.
Oferta de cursos de pós-graduação lato sensu em cibersegurança para servidores públicos de órgãos reguladores e formuladores de políticas.
Oferta de cursos EAD certificados em temas específicos de segurança (cloud, OT, forense).
Programa nacional de formação em segurança de IA e proteção de dados.
Programas de bolsas para formação em áreas críticas.

Programas educacionais para comportamento online seguro em instituições de ensino fundamental, médio e técnico.

E3-Capacidades-1-B
Professores

Detalhamento:

Explora a existência de um número suficiente de professores e palestrantes qualificados.

Níveis de Maturidade:

Inicial:
Poucos ou nenhum educador em cibersegurança está disponível.

Fundamental:
Há um pequeno grupo de professores qualificados existente.

Básico:
Há um número insuficiente de professores qualificados existente.

Médio:
Há um número moderado de professores com formação específica.

Evoluído:
Há um número significativo de professores com formação específica.

Avançado:
Há ampla disponibilidade de professores com formação específica.

Evidências

Cursos universitários e pós-graduações específicas em cibersegurança.

Programas educacionais de cibersegurança voltados a professores do ensino fundamental, médio e técnico.

Programas nacionais de formação continuada em cibersegurança para professores.

E3-Capacidades-1-C
Desenvolvimento e aprimoramento de estruturas educacionais

Detalhamento:

Explora a coordenação e os recursos para o desenvolvimento e aprimoramento de estruturas de educação em cibersegurança, com orçamento e gastos alocados com base na demanda nacional.

Níveis de Maturidade:

Inicial:
A necessidade de aprimorar a educação nacional em cibersegurança ainda não é considerada. Não há rede de pontos de contato nacionais entre governo, reguladores, setores críticos e instituições educacionais. Discussões sobre gestão coordenada da educação em cibersegurança são inexistentes ou iniciais.

Fundamental:

A necessidade de fortalecer a educação em cibersegurança é reconhecida por atores líderes do governo, indústria e academia. Escolas, governo e setor privado colaboram de forma ad hoc para viabilizar recursos educacionais. Ainda não há orçamento nacional dedicado à educação em cibersegurança. Mecanismos e métricas para monitorar oferta e demanda de cursos são limitados.

Básico:
Consultas eventuais entre governo, setor privado, academia e sociedade civil orientam prioridades educacionais, refletidas na estratégia nacional de cibersegurança. Programas e competições são promovidos ocasionalmente para atrair novos talentos.

Médio:
Consultas amplas entre governo, setor privado, academia e sociedade civil orientam prioridades educacionais, refletidas na estratégia nacional de cibersegurança. Há orçamento nacional voltado à pesquisa e laboratórios de cibersegurança em universidades. Programas e competições são promovidos regularmente para atrair novos talentos.

Evoluído:
Processos de revisão e métricas orientadas a resultados são aplicados, com financiamento adequado. Métricas são usadas para direcionar investimentos e formar profissionais especializados em todos os setores. A gestão orçamentária da educação em cibersegurança é baseada na demanda nacional. Instituições acadêmicas líderes compartilham lições aprendidas nacional e internacionalmente.

Avançado:
Centros de excelência acadêmicos nacionais em cibersegurança são estabelecidos, com parcerias internacionais ("twinning programmes") com instituições de classe mundial. A cooperação entre todas as partes interessadas é rotineira e comprovada. Os conteúdo educacionais são alinhados a desafios práticos e empresariais, e há mecanismos para atualização contínua do currículo.

Evidências

Competições nacionais de estudantes em ciberdefesa (CTFs).

Inclusão de módulos de segurança em cursos superiores.

Mapeamento da distribuição regional de centros de excelência em cibersegurança.

Mapeamento nacional periódico de lacunas de capacidades em cibersegurança específicas para órgãos reguladores e SEICs.

Produção de estudos nacionais sobre lacunas de competências em cibersegurança.

Produção de materiais didáticos locais sobre cibersegurança.

E3-Capacidades-1-C

Programas de orientação de carreira em cibersegurança para estudantes do ensino médio e técnico.

E3-Capacidades-2

Qualificação Profissional em Cibersegurança

Detalhamento:

Aborda e analisa a disponibilidade, oferta, qualidade e continuidade de programas de qualificação profissional em cibersegurança a preços acessíveis, visando formar um quadro de profissionais da área.

Além disso, analisa a adesão ao treinamento em cibersegurança e a transferência horizontal e vertical de conhecimento e habilidades em cibersegurança dentro das organizações, e como essa transferência de habilidades se traduz em um aumento contínuo do número de profissionais de cibersegurança.

E3-Capacidades-2-A

Oferta de programas de qualificação

Detalhamento:

Examina o desenvolvimento, a disponibilidade e a oferta de programas de treinamento em cibersegurança para aprimorar habilidades e capacidades.

Níveis de Maturidade:

Inicial:
Existem poucos ou nenhum programa de treinamento em cibersegurança.

Fundamental:
A necessidade de capacitação de profissionais em cibersegurança foi documentada em nível nacional.
O treinamento para a equipe geral de TI em questões de cibersegurança é oferecido para que possam reagir a incidentes à medida que ocorrem, mas não existe treinamento específico para profissionais de segurança dedicados.
A certificação profissional em TIC é oferecida, com alguns módulos ou componentes de segurança.
Treinamentos e certificações de melhores práticas podem ser acessados por meio de fontes online internacionais (por exemplo: CISSP).
Cursos de treinamento pontuais, seminários e recursos online estão disponíveis para profissionais de cibersegurança por meio de fontes públicas ou privadas, com evidências limitadas de adesão.

Básico:
Existem programas isolados de treinamento em cibersegurança para desenvolver habilidades visando a formação de um quadro de profissionais específicos da área.
Estruturas vocacionais nacionais ou internacionais de cibersegurança e as melhores práticas internacionais são ocasionalmente levadas em consideração no desenvolvimento de cursos de treinamento profissional.
A certificação profissional em segurança é oferecida no país.
As necessidades são parcialmente compreendidas e uma lista de requisitos mínimos de treinamento está documentada.

Médio:
Existem programas estruturados de treinamento em cibersegurança para desenvolver habilidades visando a formação de um quadro de profissionais específicos da área.
Estruturas vocacionais nacionais ou internacionais de cibersegurança e as melhores práticas internacionais são levadas em consideração no desenvolvimento de cursos de treinamento profissional.
A certificação profissional em segurança é oferecida em diversos setores no país.
As necessidades da sociedade são bem compreendidas e uma lista de requisitos de treinamento está documentada.

Programas de treinamento para profissionais que não atuam na área de cibersegurança são reconhecidos e oferecidos.
Podem existir iniciativas governamentais para incentivar a permanência no país após a conclusão bem-sucedida de programas de treinamento em cibersegurança.

Evoluído:
Uma gama de cursos de formação em cibersegurança é adaptada para atender à demanda estratégica nacional e está alinhada com as boas práticas internacionais.
Os programas de formação descrevem as prioridades da estratégia nacional de cibersegurança.
Os programas de formação são oferecidos a profissionais de cibersegurança e focam-se nas competências necessárias para comunicar desafios tecnicamente complexos a públicos não técnicos, como a gestão e os funcionários em geral.
Métricas orientadas para resultados, extraídas de dados abrangentes de oferta e procura de profissionais de cibersegurança, estão a ser utilizadas para orientar os métodos, a sustentabilidade e os procedimentos dos futuros programas de formação.

Avançado:
Os setores público e privado colaboram para oferecer treinamento e se adaptam constantemente, buscando desenvolver habilidades provenientes de ambos os setores.
As ofertas de treinamento e os programas educacionais são coordenados para que a base estabelecida nas escolas possa viabilizar a formação de uma força de trabalho altamente qualificada.
Existem programas e estruturas de incentivo para garantir a retenção da força de trabalho treinada no país.

Evidências

Capacitação contínua de equipes de auditoria interna e controle externo em cibersegurança de contratos e concessões de infraestrutura.
Criação de trilhas de formação em segurança de sistemas industriais (OT/SCADA) para engenheiros e técnicos que atuam em SEICs.
Desenvolvimento de competências em análise de ameaças específicas contra SEICs.
Formação de especialistas em segurança de dados e sistemas de informação de SEICs.
Formação especializada em segurança de comunicações críticas.
Formação especializada em segurança de sistemas OT/ICS/SCADA.
Indicadores de quantidade de especialistas formados anualmente.
Laboratórios de treino em cenários de ataque (cyber ranges) disponíveis nacionalmente.

Parcerias com centros de excelência internacionais para treinamento avançado em proteção de SEICs.
Parcerias com organismos internacionais para cursos avançados de segurança.
Programas de capacitação digital para micro e pequenas empresas.
Programas de capacitação para analistas de risco de agências reguladoras em temas de cibersegurança e resiliência operacional.
Programas de estágio e trainee em cibersegurança no setor público e privado.
Programas de formação em proteção de dados pessoais para DPOs e encarregados.
Programas de formação em segurança para cientistas de dados e equipes de IA.
Programas de trilhas de carreira para especialistas em cibersegurança no serviço público.
Programas federais de capacitação em cibersegurança voltados a equipes técnicas de empresas estatais de SEICs.
Programas nacionais de capacitação de servidores públicos.
Programas para desenvolver competências em segurança de sistemas de transporte inteligentes (ITS), semáforos e logística urbana.
Programas para formação de gestores públicos em governança digital.
Promoção de dias nacionais ou semanas temáticas dedicadas à cibersegurança.
Treinamento especializado em análise de malware e resposta a incidentes.
E3-Capacidades-2-B Certificação de Conhecimento

Detalhamento:

Examina a adesão e a acessibilidade financeira de tais programas para formar um grupo de profissionais de cibersegurança certificados. As questões investigadas incluem iniciativas de inscrição nesses programas, iniciativas para permanência no país após a conclusão bem-sucedida, compartilhamento de conhecimento após a conclusão de um programa e a existência de um registro nacional de alunos aprovados e certificados.

Níveis de Maturidade:

Inicial:
A adesão ao treinamento por parte do pessoal de TI designado para responder a incidentes de cibersegurança é limitada ou inexistente.
Não há transferência de conhecimento de funcionários treinados em cibersegurança para funcionários não treinados.

Fundamental:
As métricas que avaliam a adesão a cursos de treinamento, seminários, recursos online e ofertas de certificação ad hoc têm escopo limitado ou são ad hoc.
A transferência de conhecimento de funcionários treinados em cibersegurança para funcionários não treinados, tanto no setor público quanto no privado, é ad hoc.

Básico:
Existe um quadro ocasional de funcionários certificados e treinados em questões, processos, planejamento e análise de cibersegurança.
Pode existir um registro nacional de alunos e profissionais certificados e bem-sucedidos.
Iniciativas de criação de empregos em cibersegurança dentro das organizações começam a ser estabelecidas e incentivam os empregadores a treinar alguns de seus funcionários para se tornarem profissionais de cibersegurança.

Médio:
Existe um quadro estabelecido de funcionários certificados e treinados em questões, processos, planejamento e análise de cibersegurança.
Existe um registro nacional de alunos e profissionais certificados e bem-sucedidos.
A transferência de conhecimento de funcionários treinados em cibersegurança para funcionários não treinados, tanto no setor público quanto no privado, está estabelecida.
Iniciativas de criação de empregos em cibersegurança dentro das organizações estão estabelecidas e incentivam os empregadores a treinar seus funcionários para se tornarem profissionais de cibersegurança.
Processos e métricas de revisão de programas estão em vigor para permitir que o progresso seja medido e para avaliar a oferta e a demanda por trabalhadores qualificados em cibersegurança, tanto no setor público quanto no privado.
Esses processos são adequadamente financiados.

Evoluído:
A adesão ao treinamento em cibersegurança é usada para orientar futuros programas de treinamento.
A coordenação do treinamento em todos os setores garante que a demanda nacional por profissionais seja atendida.

Avançado:
Os profissionais de cibersegurança não só cumprem os requisitos nacionais, como também consultam profissionais locais no estrangeiro para partilhar lições aprendidas e boas práticas.

Evidências

Certificação nacional de auditores de segurança.

Certificações profissionais nacionalmente reconhecidas.

Existência de programas de certificação nacional em segurança aplicados a fornecedores de tecnologia para SEICs.

Mecanismos de certificação nacional de competências em cibersegurança reconhecidos pelo mercado.

Programas de certificação técnica alinhados ao mercado de trabalho.

Programas de residência tecnológica em cibersegurança, alocando profissionais em órgãos reguladores e SEICs.

Programas formais de residência tecnológica em cibersegurança.

Programas nacionais de certificação em segurança para desenvolvedores de software.

E3-Capacidades-2-C
Disponibilidade de profissionais de cibersegurança

Detalhamento:

Examina o acompanhamento da disponibilidade de profissionais de cibersegurança do país.

Níveis de Maturidade:

Inicial:
Existem poucos ou nenhum programa de acompanhamento dos profissionais disponíveis no país.

Fundamental:
A disponibilidade de profissionais em cibersegurança foi documentada com base em alguns treinamentos específicos.

Básico:
A disponibilidade de profissionais em cibersegurança foi documentada com base em registro de treinamentos de nível superior.

Médio:
A disponibilidade de profissionais em cibersegurança foi documentada com base em registro de treinamentos de nível superior e exercícios nacionais.

Evoluído:
A disponibilidade de profissionais em cibersegurança foi documentada com base em registro de treinamentos de nível superior e exercícios nacionais e setoriais.

Avançado:

A disponibilidade de profissionais em cibersegurança foi documentada com base em registro de treinamentos de nível superior e médio e de exercícios nacionais e setoriais.

Evidências

Mapeamento da força de trabalho nacional em cibersegurança.

Métricas de disponibilidade e escassez de profissionais por perfil de competência.

Métricas nacionais sobre evasão e retenção de talentos em cibersegurança.

Política de retenção de talentos.

Programas de certificação para cidadãos em competências de cibersegurança.

Relatórios periódicos sobre evolução da massa crítica de especialistas no país.

E3-Capacidades-3

Pesquisa e Inovação em Cibersegurança

Detalhamento:

Aborda a ênfase dada à pesquisa e inovação em cibersegurança para enfrentar os desafios tecnológicos, sociais e empresariais e para promover a construção de conhecimento e capacidades em cibersegurança no país.

E3-Capacidades-3-A

Pesquisa e Desenvolvimento em Cibersegurança

Detalhamento:

Investiga a existência de uma cultura de pesquisa e inovação no país, relacionada a uma lista nacional de projetos em andamento e concluídos, apoio financeiro, incentivos e resultados de pesquisa utilizáveis.

Níveis de Maturidade:

Inicial:
Existem atividades limitadas ou inexistentes de pesquisa e desenvolvimento (PD&I) em cibersegurança no país. Não há acesso a atividades de PD&I em cibersegurança provenientes de outros países.

Fundamental:
Alguma integração de atividades de PD&I em cibersegurança ocorre no país ou com um parceiro que compreende como a PD&I cibernética se aplica ao contexto local. O país pode participar de redes de colaboração regional/internacional relevantes de pesquisa em cibersegurança. As métricas de desempenho de PD&I em cibersegurança são limitadas ou ad hoc.

Básico:

As atividades de PD&I em cibersegurança são mencionadas na estratégia nacional de cibersegurança. Uma estratégia específica de PD&I pode estar em desenvolvimento. Recursos e processos necessários para implementar as ações de PD&I foram identificados. Há registros ocasionais de colaboração ativa com práticas e desenvolvimentos internacionais.

Médio:
As atividades de PD&I em cibersegurança mencionadas na estratégia nacional de cibersegurança estão estabelecidas. Uma estratégia específica de PD&I está em desenvolvimento. Recursos e processos necessários para implementar as ações de PD&I foram identificados e estão em vigor, com financiamento adequado. Há colaboração ativa recorrente com práticas e desenvolvimentos internacionais.

Evoluído:
O país participa e contribui ativamente em redes regionais e internacionais de pesquisa em cibersegurança. Existem métricas formais para medir o desempenho da PD&I e aprimorar continuamente a capacidade nacional. Comunidades de interesse são formadas em torno de prioridades de pesquisa, e a estratégia de PD&I está implementada e em execução.

Avançado:
O país faz contribuições significativas para a pesquisa e inovação em cibersegurança, participando de consórcios e investimentos internacionais. Riscos emergentes são avaliados regularmente e utilizados para atualizar a estratégia nacional de cibersegurança e futuros programas de PD&I. A sinergia entre instituições acadêmicas e a indústria impulsiona o desenvolvimento de currículos e práticas aplicadas. O país é um ator líder em pesquisa e inovação cibernética, moldando debates internacionais e antecipando novas ameaças e tecnologias, contribuindo para as melhores práticas globais.

Evidências

Centros de pesquisa e laboratórios nacionais de cibersegurança.
Cooperação internacional em P&D.
Criação de redes de pesquisadores nacionais em cibersegurança e privacidade.
Editais específicos de P&D voltados à segurança de infraestruturas críticas.
Parcerias entre universidades federais e operadores de infraestrutura para pesquisa aplicada em ciber-resiliência.
Produção científica nacional referenciada internacionalmente.
Programas de bolsas e apoio para pesquisa em segurança de redes 5G, fibras ópticas e infraestrutura de backbone nacional.
Programas de pesquisa financiados com foco em ciberdefesa.

Programas nacionais de fomento a startups de segurança.

E3-Capacidades-4

Indústria Nacional de Cibersegurança

Detalhamento:

Avalia a existência de um ambiente econômico, político e social favorável que apoie o desenvolvimento da cibersegurança incentivando o crescimento de empresas relacionadas à cibersegurança no setor privado e impulsionando o crescimento de startups de cibersegurança e dos mercados associados de seguros cibernéticos.

E3-Capacidades-4-A

Ambiente adequado ao ecossistema da cibersegurança

Detalhamento:

Investiga a existência de um ambiente econômico, político e social favorável ao desenvolvimento da cibersegurança incentivando o crescimento de empresas relacionadas à cibersegurança no setor privado.

Níveis de Maturidade:

Inicial:
Não existe um ambiente econômico, político e social favorável ao desenvolvimento da cibersegurança.

Fundamental:
Existe um ambiente econômico, político e social parcialmente favorável ao desenvolvimento da cibersegurança.

Básico:
Existe um ambiente econômico, político e social favorável ao desenvolvimento da cibersegurança. Medidas específicas de fomento estão em desenvolvimento.

Médio:
Existe um ambiente econômico, político e social favorável ao desenvolvimento da cibersegurança. Medidas específicas de fomento estão disponíveis.

Evoluído:
Empresas fornecedoras de produtos e serviços com tecnologia desenvolvida no país são estimuladas a participar de parcerias e concorrências internacionais.

Avançado:
Empresas fornecedoras de produtos e serviços com tecnologia desenvolvida no país são apoiadas quando participam de parcerias e concorrências internacionais.

Evidências

Ambientes promotores de Inovação (Incubadoras e Parques tecnológicos) dedicados à cibersegurança.

Empresas inovadoras.

Financiamento continuado para desenvolvimento de tecnologias de hardening industrial.

Incorporação de requisitos de soberania tecnológica e redução de dependências críticas em documentos estratégicos de cibersegurança.

Instituições de Ciência e Tecnologia (ICTs).

Instituições de Ensino e Pesquisa.

E3-Capacidades-5

Mecanismos de Incentivo Governamental

Detalhamento:

Analisa a existência de incentivos governamentais para o desenvolvimento de capacidades na área de cibersegurança, seja por meio de benefícios fiscais, subsídios, financiamentos, empréstimos, alienação de facilidades e outros motivadores econômicos e financeiros, incluindo órgãos institucionais dedicados e reconhecidos nacionalmente que supervisionam atividades de fortalecimento de capacidades em cibersegurança.

E3-Capacidades-5-A

Incentivos governamentais

Detalhamento:

Investiga a existência de incentivos governamentais para o desenvolvimento de capacidades na área de cibersegurança.

Níveis de Maturidade:

Inicial:
Não existem incentivos governamentais para o desenvolvimento de capacidades na área de cibersegurança.

Fundamental:
Existem incentivos governamentais ocasionais para o desenvolvimento de capacidades na área de cibersegurança.

Básico:
Existem incentivos governamentais setoriais regulares para o desenvolvimento de capacidades na área de cibersegurança.

Médio:
Existem incentivos governamentais nacionais regulares para o desenvolvimento de capacidades na área de cibersegurança.

Evoluído:
Existem incentivos governamentais nacionais permanentes para o desenvolvimento de capacidades na área de cibersegurança.

Avançado:

Evidências

"Selo" de reconhecimento pelo engajamento em cibersegurança.

Divulgação de práticas ou iniciativas de destaque nacionais e setoriais em cibersegurança.

Incentivo fiscal para empresas que treinam profissionais em segurança.

E4-Regulação

Marcos Legais e Regulatórios

Detalhamento:

Examina a capacidade do País de desenvolver e atualizar a legislação nacional que se relaciona direta e indiretamente com a cibersegurança, com particular ênfase nos requisitos regulamentares para a cibersegurança, na legislação relacionada com o cibercrime e na legislação conexa. A capacidade de fazer cumprir essas leis é examinada através das capacidades das forças policiais, do Ministério Público, dos órgãos reguladores e do Poder Judiciário.

E4-Regulação-1

Disposições Legais e Regulamentares

Detalhamento:

Aborda as disposições legislativas e regulamentares relacionadas à cibersegurança, incluindo requisitos legais e regulamentares, legislação substantiva e processual sobre cibercrimes e avaliação do impacto sobre os direitos humanos.

E4-Regulação-1-A

Legislação Substantiva sobre cibercrimes

Detalhamento:

Analisa se a legislação existente criminaliza uma variedade de cibercrimes em legislação específica ou no direito penal geral.

Níveis de Maturidade:

Inicial:
Não existe legislação criminal substantiva específica sobre cibercrimes. Pode existir legislação penal geral, mas sua aplicação a cibercrimes é incerta.

Fundamental:
Existe legislação parcial que aborda alguns aspectos dos cibercrimes, ou disposições legais sobre o tema estão em desenvolvimento.

Básico:
Disposições legais básicas sobre cibercrimes estão contidas em legislação específica ou em código penal geral. O país pode ter ratificado instrumentos bilaterais sobre cibercrimes e busca implementar suas medidas no direito doméstico.

Médio:
Disposições legais substantivas sobre cibercrimes estão contidas em legislação específica ou em código penal geral. O país pode ter ratificado instrumentos regionais ou internacionais sobre cibercrimes e busca implementar suas medidas no direito doméstico.

Evoluído:
Medidas estão em vigor para ir além dos requisitos mínimos de tratados internacionais, quando apropriado. O país busca adaptar sua legislação substantiva sobre cibercrimes às tecnologias emergentes e seus usos.

Avançado:

A legislação substantiva sobre cibercrimes é construída de modo a abranger mudanças dinâmicas na tecnologia e no ambiente de ameaças, sem a necessidade de revisões substanciais ou demoradas. O país contribui ativamente para a promoção internacional de legislações eficazes sobre cibercrimes.

Evidências

Cibercrimes tipificados legalmente.

Direitos claros para vítimas de crimes digitais.

E4-Regulação-1-B
Requisitos legais e regulamentares para a cibersegurança

Detalhamento:

Analisa a existência de quadros legais e regulamentares em matéria de cibersegurança.

Níveis de Maturidade:

Inicial:
Existem requisitos limitados de cibersegurança estabelecidos em lei ou regulação.

Fundamental:
A necessidade de criar estruturas legais e regulatórias sobre cibersegurança foi reconhecida e pode ter resultado em uma análise de lacunas ("gap analysis").

Básico:
Partes interessadas de setores essenciais foram consultadas para apoiar a criação de estruturas legais e regulatórias. Projetos de lei e regulamentos podem existir, mas ainda não foram adotados e podem não cobrir todos os setores essenciais.

Médio:
Setores essenciais foram consultados para apoiar a criação de estruturas legais e regulatórias. Legislações e regulamentos existem, mas não cobrem todos os setores essenciais.

Evoluído:
Requisitos abrangentes de cibersegurança estão definidos em regulamentações e leis (incluindo exigências setoriais específicas, quando aplicável). Podem incluir padrões obrigatórios, notificações de violação e requisitos de divulgação de vulnerabilidades. Responsabilidades civis e criminais são claramente definidas e compreendidas. Órgãos competentes possuem poderes para aplicar tais requisitos.

Avançado:
A efetividade das leis e regulações em melhorar as práticas de cibersegurança é regularmente avaliada e utilizada para orientar seu desenvolvimento futuro. As regulamentações são atualizadas conforme o surgimento de novas tecnologias. Os marcos regulatórios são suficientemente flexíveis para lidar com mudanças rápidas no ambiente tecnológico e de ameaças. O país promove as melhores práticas legais e regulatórias internacionalmente e participa ativamente do desenvolvimento de acordos internacionais para harmonizar e reconhecer mutuamente as leis e regulações de cibersegurança.

Evidências

Coordenação formal entre LGPD, Marco Civil da Internet e normas setoriais em temas de ciberincidentes e proteção de dados em SEICs.

Definição clara de responsabilidades entre governo central e reguladores setoriais em ciberincidentes.
Marco legal de cibersegurança formal e vigente.
Marco legal para operações de ciberdefesa ativa.
Mecanismos de resolução de disputas digitais.
Mecanismos legais para suspensão ou restrição de serviços inseguros em SEICs.
Metas de ciber-resiliência de SEICs no Plano Plurianual (PPA) e em outras peças de planejamento orçamentário federal.
Normais sobre penalidades proporcionais ao impacto de ciberincidentes.
Normas antitruste aplicadas ao mercado de cibersegurança.
Normas específicas para segurança de sistemas de IA generativa.
Normas para avaliação de impacto em cibersegurança em projetos financiados com recursos públicos.
Normas para classificação e proteção de informações em sistemas de colaboração e nuvem.
Normas para due diligence em segurança para contratação de nuvem pública.
Normas para operadores de data centers que hospedam dados de SEICs.
Normas para responsabilização de executivos em negligência grave de segurança.
Normas para sancionamento de SEICs que descumpram obrigações de cibersegurança.

Normas que incentivem ou obriguem adoção de padrões internacionais de segurança em SEICs.
Normas setoriais de cibersegurança em SEICs.
Normas sobre avaliação de impacto em proteção de dados para projetos sensíveis.
Normas sobre cadeia de suprimentos cibernética para SEICs.
Normas sobre combate à desinformação e abuso de redes sociais.
Normas sobre governança de risco de terceiros e cadeia de suprimentos digitais.
Normas sobre notificação de incidentes às autoridades competentes em prazos definidos.
Normas sobre notificação de incidentes de segurança por parte de SEICs.
Normas sobre preservação de evidências digitais em incidentes de grande impacto.
Normas sobre requisitos técnicos para SEICs.
Normas sobre segurança em sistemas de telemetria, sensoriamento e Internet das Coisas usados em SEICs.
Normas sobre soberania tecnológica e proteção de dados estratégicos.
Normas sobre testes de cibersegurança em sistemas de SEICs.
Normas sobre transparência algorítmica para determinados sistemas.
Normas sobre transparência mínima ao público em incidentes que afetem continuidade ou qualidade de SEICs.

Política legal envolvendo biometria e identidade digital.

E4-Regulação-1-C
Legislação Processual sobre cibercrimes

Detalhamento:

Examina se a legislação processual penal abrangente – com poderes processuais para a investigação de cibercrimes e requisitos probatórios para dissuadir, responder e processar cibercrimes e crimes que envolvam provas eletrônicas – está sendo implementada.

Níveis de Maturidade:

Inicial:
Não existe legislação processual específica para cibercrimes. Não está claro como a legislação processual penal geral se aplica a investigações, persecuções e provas eletrônicas.

Fundamental:
O desenvolvimento de legislação processual específica para cibercrimes, ou a adaptação da legislação processual penal geral, foi iniciado.

Básico:
Leis processuais criminais contendo disposições sobre investigação de cibercrimes e requisitos probatórios estão em discussão. O país pode ter ratificado instrumentos bilaterais e busca incorporá-los ao direito interno.

Médio:
Leis processuais criminais abrangentes contendo disposições sobre investigação de cibercrimes e requisitos probatórios foram adotadas e estão em vigor. O país pode ter ratificado instrumentos regionais ou internacionais e busca incorporá-los ao direito interno.

Evoluído:
As leis processuais relacionadas a cibercrimes permitem o intercâmbio de informações e outras ações necessárias para apoiar investigações transnacionais. Medidas são implementadas para exceder os padrões mínimos de tratados internacionais, quando adequado.

Avançado:
A legislação processual é estruturada de forma a lidar com mudanças tecnológicas e de ameaças de forma dinâmica, sem necessidade de revisões prolongadas. O país contribui para o desenvolvimento e promoção de instrumentos que aprimorem investigações internacionais sobre cibercrimes.

Evidências

Normas para perícia digital e cadeia de custódia de evidências eletrônicas.

E4-Regulação-1-D
Avaliação do impacto sobre os direitos humanos

Detalhamento:

Examina se são realizadas avaliações do impacto sobre os direitos humanos da legislação substantiva e processual relativa ao cibercrime e dos regulamentos de cibersegurança.

Níveis de Maturidade:

Inicial:

As legislações substantiva e processual sobre cibercrimes e as regulações de cibersegurança podem estar em desenvolvimento, mas não há avaliações de impacto em direitos humanos.

Fundamental:
Avaliações de impacto em direitos humanos podem ter sido conduzidas, incluindo considerações sobre privacidade e liberdade de expressão, embora algumas questões permaneçam pendentes. Especialistas em direitos humanos foram consultados.

Básico:
Avaliações de impacto em direitos humanos foram iniciadas. A implementação das legislações é monitorada ocasionalmente quanto à conformidade com direitos humanos.

Médio:
Avaliações completas de impacto em direitos humanos foram realizadas, atendendo aos padrões internacionais. A implementação das legislações é monitorada regularmente quanto à conformidade com direitos humanos, com verificação independente.

Evoluído:
As avaliações de impacto em direitos humanos são revisadas regularmente para garantir compatibilidade com as normas e considerar o efeito de tecnologias emergentes. Considera-se também como a cibersegurança pode fortalecer a proteção de direitos humanos no país e internacionalmente.

Avançado:
O país contribui ativamente para o desenvolvimento e promoção de avaliações de impacto em direitos humanos relacionadas à cibersegurança.

Evidências

Normas sobre uso governamental de ferramentas de interceptação e vigilância.

E4-Regulação-2

Marcos Legislativos Relacionados

Detalhamento:

Aborda os marcos legislativos relacionados à cibersegurança, incluindo proteção de dados, proteção infantil, proteção do consumidor e propriedade intelectual.

E4-Regulação-2-A

Legislação de Proteção de Dados

Detalhamento:

Examina a existência e a implementação de uma legislação abrangente de proteção de dados.

Níveis de Maturidade:

Inicial:
A legislação de proteção de dados não existe.

Fundamental:
A legislação de proteção de dados está em desenvolvimento.

Básico:
Partes interessadas de setores relevantes foram consultadas no desenvolvimento dessa legislação.

Médio:
Setores relevantes participaram do desenvolvimento e adaptação dessa legislação.

Evoluído:

Uma legislação abrangente de proteção de dados, alinhada a padrões e melhores práticas internacionais, foi adotada e está sendo aplicada. Uma autoridade principal responsável pela proteção de dados foi designada.

Avançado:
A efetividade da legislação de proteção de dados é avaliada regularmente e usada para orientar seu desenvolvimento. O país busca adaptar suas leis de proteção de dados às tecnologias emergentes e seus usos. A legislação é construída de forma a acomodar mudanças dinâmicas na tecnologia e no ambiente de ameaças, sem necessidade de revisões longas. O país desenvolve e promove padrões internacionais e participa ativamente da elaboração de instrumentos jurídicos que favorecem a colaboração internacional.

Evidências

Legislação de proteção de dados pessoais.

E4-Regulação-2-B
Legislação de Proteção de Crianças e Adolescentes

Detalhamento:

Foca na proteção legislativa das crianças online, incluindo a proteção dos seus direitos online e a criminalização do abuso infantil online.

Níveis de Maturidade:

Inicial:
A legislação relacionada à proteção infantil é limitada e sua aplicação no ambiente online ainda não foi considerada.

Fundamental:
Existe legislação sobre proteção infantil e ela está sendo adaptada para refletir sua aplicação no ambiente online.

Básico:
Partes interessadas de setores relevantes foram consultadas no desenvolvimento dessa legislação.

Médio:
Setores relevantes participaram do desenvolvimento e adaptação dessa legislação.

Evoluído:
A aplicação da proteção infantil no ambiente online é compreendida e refletida na legislação relevante, que é implementada em conformidade com padrões e boas práticas internacionais.

Avançado:
A efetividade da legislação de proteção infantil online é avaliada regularmente e usada para seu aprimoramento. O país busca adaptar a legislação à evolução tecnológica e participa do desenvolvimento e promoção de padrões e instrumentos internacionais nessa área.

Evidências

Legislação de proteção de crianças e adolescentes.

E4-Regulação-2-C
Legislação de Proteção ao Consumidor

Detalhamento:

Aborda a existência e a implementação de legislação que protege os consumidores online contra fraudes e outras formas de práticas comerciais abusivas.

Níveis de Maturidade:

Inicial:
A legislação relacionada à proteção do consumidor é limitada e sua aplicação no ambiente online ainda não foi considerada.

Fundamental:
Existe legislação sobre proteção do consumidor e ela está sendo adaptada para refletir sua aplicação no ambiente online.

Básico:
Partes interessadas de setores relevantes foram consultadas no desenvolvimento dessa legislação.

Médio:
Setores relevantes participaram do desenvolvimento e adaptação dessa legislação.

Evoluído:
A aplicação da proteção do consumidor no ambiente online é compreendida e refletida na legislação relevante, que é implementada em conformidade com padrões e boas práticas internacionais.

Avançado:
A efetividade da legislação de proteção do consumidor online é avaliada regularmente e usada para orientar seu desenvolvimento. O país busca adaptar a legislação às novas tecnologias e promover padrões e instrumentos internacionais de proteção do consumidor.

Evidências

Legislação de proteção ao consumidor de serviços digitais.

E4-Regulação-2-D
Legislação de Propriedade Intelectual

Detalhamento:

Diz respeito à existência e implementação da legislação de propriedade intelectual online.

Níveis de Maturidade:

Inicial:
A legislação relacionada à proteção da propriedade intelectual é limitada e sua aplicação no ambiente online ainda não foi considerada.

Fundamental:
Existe legislação sobre propriedade intelectual e ela está sendo adaptada para refletir sua aplicação no ambiente online.

Básico:
Partes interessadas de setores relevantes foram consultadas no desenvolvimento dessa legislação.

Médio:
Setores relevantes participaram do desenvolvimento e adaptação dessa legislação.

Evoluído:
A aplicação da proteção de propriedade intelectual no ambiente online é compreendida e refletida na legislação relevante, que é implementada em conformidade com padrões e boas práticas internacionais.

Avançado:
A efetividade da legislação de propriedade intelectual online é avaliada regularmente e usada para orientar seu desenvolvimento. O país busca adaptar sua legislação a novas tecnologias, promovendo padrões e instrumentos internacionais para melhorar a colaboração global nessa área.

Evidências

Legislação de proteção de propriedade intelectual.

E4-Regulação-3

Capacidade e Competência Judiciária

Detalhamento:

Analisa a capacidade investigativa das autoridades policiais quanto a cibercrimes, a capacidade do Ministério Público de apresentar casos de cibercrimes e provas eletrônicas, e a capacidade dos tribunais de julgar casos de processos que envolvem provas eletrônicas.

E4-Regulação-3-A

Aplicação da lei

Detalhamento:

Examina se os agentes e agências de aplicação da lei receberam treinamento em investigação e gestão de casos de cibercrimes e casos que envolvem provas eletrônicas, e se existem recursos humanos, processuais e tecnológicos suficientes.

Níveis de Maturidade:

Inicial:
As forças policiais/agências de aplicação da lei não possuem capacidade suficiente para prevenir e combater cibercrimes e não recebem treinamento especializado em investigações cibernéticas. Medidas investigativas tradicionais são aplicadas, mas a capacidade digital é limitada.

Fundamental:
Policiais podem receber treinamentos sobre cibercrimes e evidências digitais, porém, de forma ad hoc e não institucionalizada.

Básico:
Existe uma capacidade institucional mínima, com recursos humanos, processuais e tecnológicos necessários para investigar casos de cibercrimes.

Médio:
Existe uma capacidade institucional abrangente, com recursos humanos, processuais e tecnológicos suficientes para investigar casos de cibercrimes. Cadeia de custódia digital e integridade das evidências são estabelecidas, incluindo papéis e responsabilidades formais.

Evoluído:
Padrões formais de treinamento sobre cibercrimes e evidências digitais são implementados. As responsabilidades entre forças nacionais e locais estão claramente definidas e há mecanismos de coordenação. Dados e estatísticas sobre cibercrimes são analisados para orientar estratégias e alocação de recursos.

Avançado:
As forças policiais desenvolvem e promovem novas abordagens para prevenção e interrupção de cibercrimes, colaborando internacionalmente e influenciando boas práticas globais.

Evidências

Capacitação de forças policiais em OSINT e investigação digital.

Treinamento para policiais em crimes digitais.

E4-Regulação-3-B
Processo penal

Detalhamento:

Examina se os procuradores receberam formação sobre como lidar com casos de cibercrimes e casos que envolvam provas eletrônicas, e se existem recursos humanos, processuais e tecnológicos suficientes.

Níveis de Maturidade:

Inicial:
Promotores não recebem treinamento ou recursos adequados para lidar com provas eletrônicas ou processar cibercrimes.

Fundamental:
Consultas iniciais podem ter sido realizadas para desenvolver essa capacidade no Ministério Público.

Básico:
Um número limitado de promotores possui capacidade para conduzir casos de cibercrimes e lidar com evidências eletrônicas, de forma ad hoc.

Médio:
Um número moderado de promotores possui capacidade para conduzir casos de cibercrimes e lidar com evidências eletrônicas, de forma procedimentada.

Evoluído:
Existe uma capacidade institucional abrangente, com recursos humanos e tecnológicos suficientes para processar casos de cibercrimes e evidências eletrônicas. Estruturas institucionais e mecanismos de troca de boas práticas entre promotores e juízes estão em vigor.

Avançado:
O país possui capacidade para processar casos complexos de cibercrimes, inclusive de natureza transnacional, e participa ativamente no desenvolvimento de boas práticas internacionais.

Evidências

Mecanismos legais de preservação e retenção de logs.

Normas processuais para prova digital.

Regras para requisição de dados digitais sob ordem judicial.

Treinamento para promotores em crimes digitais.

E4-Regulação-3-C
Tribunais

Detalhamento:

Examina se os tribunais possuem recursos e treinamento suficientes para garantir o processamento eficaz e eficiente de casos de cibercrimes e casos que envolvam provas eletrônicas.

Níveis de Maturidade:

Inicial:
Não há processo para capacitar juízes a presidir casos de cibercrimes ou lidar com provas eletrônicas.

Fundamental:
Consultas podem ter sido iniciadas para desenvolver essa capacidade no Judiciário.

Básico:
Alguns juízes possuem capacidade limitada para julgar casos de cibercrimes, e o treinamento sobre o tema é ad hoc.

Médio:
Alguns juízes possuem capacidade moderada para julgar casos de cibercrimes, e o treinamento sobre o tema é procedimentado, mas apenas básico.

Evoluído:
Recursos humanos e tecnológicos adequados estão disponíveis para garantir a eficiência de julgamentos de cibercrimes e casos com provas eletrônicas. Juízes recebem treinamento especializado.

Avançado:
A capacidade institucional do sistema judicial é periodicamente revisada e aprimorada. O país contribui para o desenvolvimento de boas práticas internacionais sobre o julgamento de cibercrimes.

Evidências

Treinamento para magistrados em crimes digitais.

E5-Tecnologias

Padrões e Tecnologias

Detalhamento:

Avalia a adoção generalizada de tecnologias em cibersegurança para a proteção e resiliência de indivíduos e organizações, especialmente de serviços essenciais e infraestruturas críticas, também considerando o incentivo ao desenvolvimento e a promoção do uso de tecnologias computacionais emergentes (TCEs) em cibersegurança, com estudo e monitoramento de seus impactos, riscos e oportunidades.

Também examina o fomento ao desenvolvimento e àa implementação de arcabouços (frameworks), padrões e boas práticas de cibersegurança, bem como de implantação de processos e controles para desenvolvimento de tecnologias e produtos para reduzir os riscos de cibersegurança, incluindo modelos de qualidade para o desenvolvimento e aquisição de software e a adequação do mercado de cibersegurança aos padrões e boas práticas nacionais e internacionais.

Adicionalmente, considera o monitoramento de tecnologias computacionais emergentes (TCEs) e sua cibersegurança, e seu impacto na cibersegurança de outras tecnologias, bem como a capacidade de implementação de sandboxes regulatórios para acompanhamento dessas TCEs.

E5-Tecnologias-1

Adesão a Padrões e Boas Práticas

Detalhamento:

Analisa a capacidade do país de contribuir para o desenvolvimento de padrões, frameworks e de boas práticas nacionais e internacionais, bem como de promover a adesão, avaliar a implementação e monitorar a sua adequação e conformidade.

E5-Tecnologias-1-A

Boas práticas em SEICs

Detalhamento:

Examina se os padrões e as boas práticas relacionados à cibersegurança estão sendo amplamente respeitados e implementados nas organizações provedoras de serviços essenciais ou operadoras de infraestruturas críticas.

Níveis de Maturidade:

Inicial:
Nenhum padrão ou boa prática foi identificado para uso na proteção de dados, tecnologias ou infraestruturas ligadas a SEICs.

Fundamental:
Alguns padrões e boas práticas adequadas foram identificados e há implementação pontual, mas sem esforço coordenado ou mensuração de impacto.

Básico:
Padrões mínimos de gestão de ciber-riscos foram identificados e há sinais iniciais de promoção e adoção em SEICs.

Médio:

Padrões de gestão de ciber-riscos foram identificados e há sinais de promoção e adoção em SEICs. Há evidências de implementação mensurável e uso de padrões internacionais.

Evoluído:
Uma base nacional acordada de padrões e boas práticas de cibersegurança foi amplamente implementada. Existe uma entidade governamental para avaliar o uso de padrões e esquemas para promover melhorias contínuas e monitorar conformidade.

Avançado:
A escolha e implementação de padrões são continuamente revisadas. Riscos emergentes são reavaliados periodicamente, e há debate ativo entre governo e partes interessadas. O país participa ativamente de organismos internacionais e decisões sobre conformidade são tomadas de forma colaborativa, conforme mudanças no ambiente de ameaças e recursos.

Evidências

Adoção de arquitetura de segurança em camadas para SEICs.
Adoção de padrões nacionais ou internacionais para segurança de medidores inteligentes e equipamentos de campo conectados.
Adoção de práticas de DevSecOps na evolução de sistemas críticos utilizados por estatais e grandes operadores de SEICs.
Adoção de soluções de gerenciamento centralizado de identidades e acessos para o governo.
Adoção obrigatória de padrões reconhecidos (ISO/NIST).
Aplicação de princípios de arquitetura Zero Trust em ambientes de redes que suportam SEICs.
Certificação obrigatória de hardware crítico utilizado em SEICs.
Exigência de autenticação forte e gestão de identidades para acesso a consoles de operação de SEICs.
Existência de políticas formais de hardening e gestão de patches para TO em uso em SEICs.
Implementação de controles de segurança e monitoramento contínuo em sistemas de TO em SEICs.
Implementação de monitoração de integridade de software e firmware em dispositivos-chave de SEICs.

Implementação de registro detalhado (logs) e trilhas de auditoria em sistemas de supervisão e controle de SEICs.

Implementação de separação de ambientes de teste, desenvolvimento e produção em SEICs.

Implementação de soluções de monitoramento de integridade em SEICs.

Padrões mínimos de segurança para APIs expostas em SEICs.

Política nacional para uso seguro de serviços de nuvem por SEICs.

Programa nacional de substituição de tecnologias legadas inseguras em SEICs, com critérios de risco e prioridade.

Requisitos de arquiteturas de rede segregadas para SEICs, com controles estritos de acesso remoto.

Requisitos mínimos para segurança em comunicações utilizadas por SEICs.

E5-Tecnologias-1-B Normas em Aquisições
Detalhamento: Aborda a implementação de normas e boas práticas para orientar os processos de aquisição, incluindo gestão de riscos, gestão do ciclo de vida, garantia de software e hardware, terceirização e utilização de serviços em nuvem.

Níveis de Maturidade:

Inicial: Nenhum padrão ou boa prática foi identificado para orientar os processos de aquisição. Caso existam, sua implementação é ad hoc e descoordenada.
Fundamental: Padrões e boas práticas de cibersegurança que orientam processos de aquisição (gestão de riscos, ciclo de vida, garantia de software e hardware, terceirização e uso de nuvem) foram identificados.
Básico: Há evidências de promoção e implementação de padrões e boas práticas de cibersegurança em processos de aquisição em algumas instituições.
Médio: Há evidências de promoção e implementação de padrões e boas práticas de cibersegurança em processos de aquisição.

Evoluído:
Os padrões e boas práticas em aquisição são amplamente seguidos. Conformidade e efetividade são medidas e avaliadas.

Avançado:
As organizações monitoram e ajustam o uso de padrões conforme necessário, com base em decisões de risco. Novos riscos de cibersegurança são avaliados regularmente para aprimorar padrões. O país participa do desenvolvimento internacional de padrões e promove melhoria contínua em competências e processos.

Evidências

Políticas nacionais de procurement seguro e exigências de segurança nas compras públicas.

Valorização de "selos de qualidade" em compras públicas, considerando a especificidade e criticidade do ente público.

E5-Tecnologias-1-C
Normas para o fornecimento de produtos e serviços

Detalhamento:

Aborda o uso de normas e boas práticas por fornecedores locais de bens e serviços, incluindo software, hardware, serviços gerenciados e serviços em nuvem.

Níveis de Maturidade:

Inicial:
Nenhum padrão ou boa prática foi identificado para uso na segurança de produtos e serviços (software, hardware, serviços gerenciados e nuvem).

Fundamental:
Atividades e metodologias para desenvolvimento seguro e gestão de ciclo de vida em software, hardware e serviços começam a ser discutidas.

Básico:
O governo promove padrões relevantes, de forma limitada.

Médio:
O governo promove padrões relevantes, mas sem evidência de adoção ampla.

Evoluído:
Há ampla implementação de padrões de desenvolvimento seguro, garantia de qualidade de hardware e segurança em nuvem em organizações públicas e privadas.

Avançado:
O governo mantém programas de promoção e monitoramento da adoção de padrões e assegura que técnicas de alta integridade em sistemas e software estejam incorporadas na formação educacional e profissional do país.

Evidências

Arquitetura Zero Trust.

Assinaturas digitais e identidade eletrônica.

Definição de padrões de segmentação de rede para ambientes de missão crítica.
Guia nacional para gestão de terceiros e fornecedores críticos em contratos públicos.
Mapa nacional de capacidades laboratoriais e centros de teste em cibersegurança.
Normas nacionais sobre segurança de APIs públicas.
Normas técnicas para ICS/SCADA.
Políticas de software seguro (SSDLC).
Políticas nacionais para proteção de dispositivos IoT utilizados em serviços públicos.
Programas nacionais de auditoria técnica.

E5-Tecnologias-1-D
Modelos oficiais de gestão de riscos

Detalhamento:

Afere a existência de referenciais de benchmarking nacionais ou setoriais oficiais para estratégias de avaliação de riscos.

Níveis de Maturidade:

Inicial:
Referenciais de benchmarking nacionais ou setoriais oficiais para estratégias de avaliação de riscos ainda não foram formulados.

Fundamental:
Referenciais de benchmarking nacionais ou setoriais oficiais para estratégias de avaliação de riscos estão sendo elaborados.

Básico:
Referenciais de benchmarking nacionais ou setoriais oficiais para estratégias de avaliação de riscos estão estabelecidos em alguns setores essenciais.

Médio:
Referenciais de benchmarking nacionais ou setoriais oficiais para estratégias de avaliação de riscos estão estabelecidos em todos os setores essenciais.

Evoluído:
Referenciais de benchmarking nacionais ou setoriais oficiais para estratégias de avaliação de riscos são constantemente revisados e aprimorados com base em lições aprendidas e riscos emergentes.

Avançado:

O entendimento dos controles tecnológicos implementados se estende ao impacto nas operações organizacionais e na segurança nacional. O país é referência internacional em referenciais de benchmarking nacionais ou setoriais oficiais para estratégias de avaliação de riscos, cuja implementação responde a ambiente de ameaças em constante evolução.

Evidências

Existência de política nacional de gestão de ciber-riscos alinhada a frameworks internacionais.

Frameworks de gestão de risco adotados.

Políticas para mitigação de vulnerabilidades zero-day em sistemas governamentais.

Programa de gestão de risco nacional baseado em padrões internacionais.

E5-Tecnologias-2

Controles de Segurança

Detalhamento:

Analisa o desenvolvimento e a implementação de processos e controles de segurança nos setores público e privado, bem como a adequação deles às boas práticas nacionais e internacionais.

E5-Tecnologias-2-A

Controles de segurança tecnológica por usuários

Detalhamento:

Explora em que medida os controles de segurança tecnológica atualizados, incluindo aplicação de patches e backups, são implementados pelos usuários.

Níveis de Maturidade:

Inicial:
Há pouca ou nenhuma compreensão ou implementação, pelos usuários, dos controles tecnológicos de segurança disponíveis no mercado. Provedores de serviços de Internet e outros provedores de tecnologia podem não oferecer controles preventivos (“upstream”) aos seus clientes.

Fundamental:
Controles tecnológicos de segurança são implantados ocasionalmente pelos usuários. A implementação de controles atualizados é promovida de maneira ad hoc, e todos os usuários são incentivados a adotá-los. Provedores de Internet e tecnologia podem oferecer serviços de segurança como parte de seus serviços, ainda que de forma irregular.

Básico:
Controles tecnológicos atualizados, incluindo correções (patching) e backups, são implementados por até 25% dos usuários.

Médio:
Controles tecnológicos atualizados, incluindo correções (patching) e backups, são implementados por até 50% dos usuários.

Evoluído:

Controles tecnológicos atualizados, incluindo correções (patching) e backups, são implementados por mais de 50% dos usuários.

Avançado:
Controles tecnológicos atualizados, incluindo correções (patching) e backups, são implementados por mais de 75% dos usuários.

Evidências

Estratégia nacional para interoperabilidade segura entre sistemas de diferentes órgãos e níveis de governo.

Guia nacional de configuração segura para sistemas operacionais e aplicações comuns.

Programa nacional de conformidade em cibersegurança baseado em frameworks reconhecidos.

Requisitos mínimos de configuração segura.

E5-Tecnologias-2-B
Controles de segurança tecnológica no setor público

Detalhamento:

Explora em que medida os controles de segurança tecnológica atualizados, incluindo aplicação de patches e backups, são implementados pelo setor público.

Níveis de Maturidade:

Inicial:
Há pouca ou nenhuma compreensão ou implementação, pelo setor público, dos controles tecnológicos de segurança disponíveis no mercado.

Fundamental:
Controles tecnológicos de segurança são implantados pelo setor público, porém, de forma inconsistente entre os setores. A implementação de controles atualizados é promovida de maneira ad hoc, com incentivos à sua adoção.

Básico:
Controles tecnológicos atualizados, incluindo correções (patching) e backups, são implementados em algumas instituições públicas. Controles físicos de segurança são ocasionalmente utilizados para prevenir o acesso não autorizado a instalações computacionais.

Médio:
Controles tecnológicos atualizados, incluindo correções (patching) e backups, são implementados na maioria do setor público. Controles físicos de segurança são utilizados para prevenir o acesso não autorizado a instalações computacionais.

Evoluído:
O conjunto de controles tecnológicos de cibersegurança reflete estruturas, padrões e boas práticas internacionalmente reconhecidas. A adoção generalizada de controles tecnológicos de segurança resulta em proteção efetiva do setor público, que tem capacidade para avaliar continuamente a eficácia e adequação dos controles implementados.

Avançado:

O entendimento dos controles tecnológicos implementados se estende ao impacto nas operações organizacionais e na alocação orçamentária. O setor público tem capacidade para avaliar criticamente e aprimorar controles de cibersegurança conforme sua adequação e riscos emergentes. Há ampla adoção de autenticação multifator para serviços online e contas privilegiadas. Autoridades certificadoras estão disponíveis e certificados digitais são amplamente utilizados. Provedores de Internet e tecnologia podem restringir acesso a sites não confiáveis conforme exigências regulatórias. O país é referência internacional na aplicação de controles tecnológicos avançados no setor público, cuja implementação responde a ambiente de ameaças em constante evolução.

Evidências

Autenticação forte em sistemas governamentais.

Controles de segurança para redes governamentais.

Estratégia de criptografia e PKI nacional.

Política nacional de segmentação de redes governamentais.

Requisitos de criptografia para dados em repouso e em trânsito em sistemas governamentais.

Requisitos mínimos de segurança para dispositivos móveis usados em atividades governamentais.

Requisitos técnicos de segurança para APIs expostas por serviços públicos.

Utilização de frameworks de segurança específicos para sistemas de controle industrial, como IEC 62443, em projetos nacionais.

E5-Tecnologias-2-C

Controles de segurança tecnológica no setor privado

Detalhamento:

Explora em que medida os controles de segurança tecnológica atualizados, incluindo aplicação de patches e backups, são implementados pelo setor privado.

Níveis de Maturidade:

Inicial:
Há pouca ou nenhuma compreensão ou implementação, pelo setor privado, dos controles tecnológicos de segurança disponíveis no mercado.

Fundamental:

Controles tecnológicos de segurança são implantados pelo setor privado, porém, de forma inconsistente entre os setores. A implementação de controles atualizados é promovida de maneira ad hoc, e todos os setores são incentivados a adotá-los. Provedores de Internet e tecnologia podem oferecer serviços de segurança como parte de seus serviços, ainda que de forma irregular.

Básico:
Controles tecnológicos atualizados, incluindo correções (patching) e backups, são implementados em alguns SEICs. Controles físicos de segurança são ocasionalmente utilizados para prevenir o acesso não autorizado a instalações computacionais. Provedores de Internet e tecnologia de grande porte estabelecem políticas internas para implantar controles de segurança técnica e gerenciar riscos identificados em produtos e serviços.

Médio:
Controles tecnológicos atualizados, incluindo correções (patching) e backups, são implementados em todos os SEICs. Controles físicos de segurança são utilizados para prevenir o acesso não autorizado a instalações computacionais. Provedores de Internet e tecnologia estabelecem políticas internas para implantar controles de segurança técnica e gerenciar riscos identificados em produtos e serviços.

Evoluído:
O conjunto de controles tecnológicos de cibersegurança reflete estruturas, padrões e boas práticas internacionalmente reconhecidas. A adoção generalizada de controles tecnológicos de segurança resulta em proteção efetiva de SEICs, que possuem capacidade para avaliar continuamente a eficácia e adequação dos controles implementados.

Avançado:
O entendimento dos controles tecnológicos implementados se estende ao impacto nas operações organizacionais e na alocação orçamentária. SEICs possuem capacidade para avaliar criticamente e aprimorar controles de cibersegurança conforme sua adequação e riscos emergentes. Há ampla adoção de autenticação multifator para serviços online e contas privilegiadas. Autoridades certificadoras estão disponíveis e certificados digitais são amplamente utilizados. Provedores de Internet e tecnologia podem restringir acesso a sites não confiáveis conforme exigências regulatórias. O país é referência internacional na aplicação de controles tecnológicos avançados, cuja implementação responde a ambiente de ameaças em constante evolução.

Evidências

Autenticação forte em sistemas críticos privados.
Controles de segurança para redes críticas privadas.
Estratégia de criptografia e PKI nacional.
Política nacional de segmentação de redes críticas privadas.
Requisitos de criptografia para dados em repouso e em trânsito em sistemas críticos privados.
Requisitos mínimos de segurança para dispositivos móveis usados em atividades privadas.

Requisitos técnicos de segurança para APIs expostas por serviços críticos privados.

Utilização de frameworks de segurança específicos para sistemas de controle industrial, como IEC 62443, em projetos nacionais.

E5-Tecnologias-2-D
Controles criptográficos pelo setor público

Detalhamento:

Analisa a implementação de técnicas criptográficas, pelo setor público, para a proteção de dados em repouso ou em trânsito, e em que medida esses controles criptográficos atendem aos padrões e diretrizes internacionais e são mantidos atualizados.

Níveis de Maturidade:

Inicial:
Técnicas criptográficas (por exemplo, criptografia e assinaturas digitais) para proteção de dados em repouso e em trânsito são consideradas importantes, mas ainda não são implantadas de forma significativa pelo setor público.

Fundamental:
Controles criptográficos para proteção de dados em repouso e em trânsito são reconhecidos e implantados de forma ad hoc por múltiplas partes interessadas do setor público. Ferramentas como TLS são aplicadas pontualmente por provedores de serviços para proteger comunicações entre servidores e usuários.

Básico:
Técnicas criptográficas estão disponíveis em algumas instituições, provendo proteção de dados em repouso e em trânsito. Há alguma compreensão sobre serviços de comunicação segura (por exemplo, e-mails criptografados ou assinados).

Médio:
Técnicas criptográficas estão disponíveis para todo o setor público, garantindo proteção de dados em repouso e em trânsito. Há ampla compreensão sobre serviços de comunicação segura (por exemplo, e-mails criptografados ou assinados). Controles criptográficos implantados atendem a padrões e diretrizes internacionais e são mantidos atualizados.

Evoluído:
O setor público avalia criticamente a implementação de controles criptográficos conforme seus objetivos e prioridades. Políticas de criptografia são adaptadas de acordo com avanços tecnológicos e mudanças no ambiente de ameaças. O país considera a implementação de gestão de identidades digitais e infraestrutura nacional de chaves públicas (PKI).

Avançado:
O setor público possui políticas de criptografia e controle criptográfico baseadas em avaliações anteriores, revisadas regularmente quanto à eficácia. O país participa ativamente do debate internacional sobre boas práticas em controles criptográficos. A implementação de controles criptográficos é adaptada conforme o cenário de ameaças evolui.

Evidências

Existência de procedimentos técnicos padronizados para desativação segura de equipamentos comprometidos em ambiente crítico.

Monitoramento nacional da adoção de protocolos seguros como DNSSEC e RPKI.

E5-Tecnologias-2-E
Controles criptográficos pelo setor privado

Detalhamento:

Analisa a implementação de técnicas criptográficas, por SEICs, para a proteção de dados em repouso ou em trânsito, e em que medida esses controles criptográficos atendem aos padrões e diretrizes internacionais e são mantidos atualizados.

Níveis de Maturidade:

Inicial:
Técnicas criptográficas (por exemplo, criptografia e assinaturas digitais) para proteção de dados em repouso e em trânsito são consideradas importantes, mas ainda não são implantadas de forma significativa pelo setor privado.

Fundamental:
Controles criptográficos para proteção de dados em repouso e em trânsito são reconhecidos e implantados de forma ad hoc por múltiplas partes interessadas do setor privado. Ferramentas como TLS são aplicadas pontualmente por provedores de serviços para proteger comunicações entre servidores e usuários.

Básico:
Técnicas criptográficas estão disponíveis em algumas instituições, provendo proteção de dados em repouso e em trânsito. Há alguma compreensão sobre serviços de comunicação segura (por exemplo, e-mails criptografados ou assinados).

Médio:
Técnicas criptográficas estão disponíveis para todos os SEICs, garantindo proteção de dados em repouso e em trânsito. Há ampla compreensão sobre serviços de comunicação segura (por exemplo, e-mails criptografados ou assinados). Controles criptográficos implantados atendem a padrões e diretrizes internacionais e são mantidos atualizados.

Evoluído:
SEICs avaliam criticamente a implementação de controles criptográficos conforme seus objetivos e prioridades. Políticas de criptografia são adaptadas de acordo com avanços tecnológicos e mudanças no ambiente de ameaças.

Avançado:
SEICs possuem políticas de criptografia e controle criptográfico baseadas em avaliações anteriores, revisadas regularmente quanto à eficácia. A implementação de controles criptográficos é adaptada conforme o cenário de ameaças evolui.

Evidências

Existência de procedimentos técnicos padronizados para desativação segura de equipamentos comprometidos em ambiente crítico.

Monitoramento nacional da adoção de protocolos seguros como DNSSEC e RPKI.

E5-Tecnologias-2-F
Controles criptográficos por usuários

Detalhamento:

Analisa a implementação de técnicas criptográficas, por usuários, para a proteção de dados em repouso ou em trânsito, e em que medida esses controles criptográficos atendem aos padrões e diretrizes internacionais e são mantidos atualizados.

Níveis de Maturidade:

Inicial:
Técnicas criptográficas (por exemplo, criptografia e assinaturas digitais) para proteção de dados em repouso e em trânsito são consideradas importantes, mas ainda não são implantadas de forma significativa pelos usuários comuns.

Fundamental:
Controles criptográficos para proteção de dados em repouso e em trânsito são reconhecidos e implantados de forma ad hoc por alguns usuários. Ferramentas como TLS são aplicadas pontualmente por provedores de serviços para proteger comunicações entre servidores e usuários.

Básico:
Técnicas criptográficas estão disponíveis para múltiplos usuários, provendo proteção de dados em repouso e em trânsito. Há alguma compreensão sobre serviços de comunicação segura (por exemplo, e-mails criptografados ou assinados).

Médio:
Técnicas criptográficas estão disponíveis para muitos usuários, garantindo proteção de dados em repouso e em trânsito. Há ampla compreensão sobre serviços de comunicação segura (por exemplo, e-mails criptografados ou assinados). Controles criptográficos implantados atendem a padrões e diretrizes internacionais e são mantidos atualizados.

Evoluído:
Um número significativo de usuários avalia criticamente a implementação de controles criptográficos conforme seus objetivos e prioridades.

Avançado:
A maioria dos usuários avalia criticamente a implementação de controles criptográficos conforme seus objetivos e prioridades.

Evidências

Existência de procedimentos técnicos padronizados para desativação segura de equipamentos comprometidos em ambiente crítico.

Monitoramento nacional da adoção de protocolos seguros como DNSSEC e RPKI.

E5-Tecnologias-3

Qualidade de Software

Detalhamento:

Examina a qualidade do desenvolvimento e da implantação de software e os requisitos funcionais nos setores público e privado. Além disso, analisa a existência e o aprimoramento de políticas e processos para atualização e manutenção de software com base em avaliações de risco e na criticidade dos serviços.

E5-Tecnologias-3-A

Qualidade e Garantia de Software

Detalhamento:

Examina a qualidade da implantação de software e os requisitos funcionais nos setores público e privado.

Níveis de Maturidade:

Inicial:
A qualidade e o desempenho do software utilizado no país são uma preocupação, mas os requisitos funcionais ainda não são totalmente monitorados. Não existe catálogo de plataformas e aplicações de software confiáveis nos setores público e privado.

Fundamental:
A qualidade e os requisitos funcionais de software nos setores público e privado são reconhecidos e identificados, mas não necessariamente de forma estratégica. Um catálogo de plataformas e aplicações de software confiáveis está em desenvolvimento. Evidências de deficiências na qualidade do software estão sendo coletadas e avaliadas quanto ao impacto na usabilidade e desempenho.

Básico:
A qualidade e os requisitos funcionais de software nos setores público e privado são minimamente reconhecidos e estabelecidos. Aplicações de software confiáveis, em conformidade com padrões e boas práticas internacionais, são eventualmente utilizadas nos setores público e privado.

Médio:
A qualidade e os requisitos funcionais de software nos setores público e privado são reconhecidos e estabelecidos. Aplicações de software confiáveis, em conformidade com padrões e boas práticas internacionais, são amplamente utilizadas nos setores público e privado.

Evoluído:
As aplicações de software são caracterizadas quanto à confiabilidade, usabilidade e desempenho em conformidade com padrões e boas práticas internacionais.

Avançado:
A gestão da qualidade de software é proativa e integrada à estratégia organizacional e nacional de cibersegurança. A avaliação de riscos, a engenharia de software segura e os processos de certificação são incorporados nos ciclos de desenvolvimento. O país contribui ativamente para o aprimoramento internacional de padrões e frameworks de garantia de software.

Evidências

Adoção de referências normativas nacionais para segurança em desenvolvimento de software.

Mecanismos de garantia de integridade e autenticidade de software (por exemplo SBOM).

Normas para segurança de containers, microsserviços e práticas de DevSecOps.

Programas de bug bounty.

Programas de verificação independente de segurança em código-fonte de sistemas críticos.

Testbeds para segurança e validação.

E5-Tecnologias-3-B
Políticas de atualização

Detalhamento:

Analisa a existência e o aprimoramento de políticas e processos para atualizações e manutenção de software com base em avaliações de risco e na criticidade dos serviços.

Níveis de Maturidade:

Inicial:
Políticas e processos relativos a atualizações e manutenção (incluindo gestão de patches) ainda não foram formulados.

Fundamental:
Políticas e processos de atualização e manutenção (incluindo gestão de patches) estão sendo elaborados.

Básico:
Políticas e processos de atualização e manutenção (incluindo gestão de patches) estão estabelecidos em alguns setores essenciais.

Médio:
Políticas e processos de atualização e manutenção (incluindo gestão de patches) estão estabelecidos em todos os setores essenciais.

Evoluído:
Processos de atualização e manutenção são constantemente revisados e aprimorados com base em lições aprendidas e riscos emergentes.

Avançado:
O entendimento dos controles tecnológicos implementados se estende ao impacto nas operações organizacionais e na segurança nacional.

Evidências

Estratégia nacional de atualização segura de firmware em dispositivos críticos.

Estratégia nacional para gerenciamento de vulnerabilidades em larga escala (patch management).

E5-Tecnologias-4
Mercado de Cibersegurança

Detalhamento:

Aborda a disponibilidade e o desenvolvimento de tecnologias de cibersegurança competitivas, certificação de produtos e serviços de cibersegurança, mercado de seguro cibernético, serviços e conhecimentos especializados em cibersegurança e as implicações de segurança da terceirização.

E5-Tecnologias-4-A
Tecnologias de cibersegurança

Detalhamento:

Examina se existe um mercado nacional para tecnologias de cibersegurança, se este é apoiado e se está alinhado com as necessidades nacionais.

Níveis de Maturidade:

Inicial:
Se existe produção doméstica de tecnologias de cibersegurança, ela não segue processos seguros. O país não considera as implicações de segurança do uso de tecnologias estrangeiras.

Fundamental:
Se há produção doméstica, reconhece-se a necessidade de processos seguros. Se há dependência de tecnologias estrangeiras, as implicações de segurança são consideradas.

Básico:
Se há produção doméstica, alguns processos seguros estão em vigor. Se há dependência de tecnologias estrangeiras, as implicações de segurança são ocasionalmente identificadas e mitigadas no contexto da cadeia internacional de suprimentos.

Médio:
Se há produção doméstica, processos seguros estão em vigor. Se há dependência de tecnologias estrangeiras, as implicações de segurança são identificadas e mitigadas no contexto da cadeia internacional de suprimentos.

Evoluído:
O desenvolvimento local de tecnologias de cibersegurança segue diretrizes de codificação segura, boas práticas e padrões internacionalmente aceitos. Avaliações de risco e incentivos de mercado orientam a priorização do desenvolvimento de produtos e a mitigação de riscos identificados.

Avançado:
As implicações de segurança no uso de tecnologias estrangeiras são rotineiramente analisadas e revisadas com base em ciber-riscos emergentes. Funções de segurança em software e configurações de sistemas são automatizadas no desenvolvimento e na implantação de tecnologias. Produtos nacionais de cibersegurança são exportados e considerados de alta qualidade. O país possui um órgão para assegurar a segurança de tecnologias estrangeiras (hardware e software) e cadeias de suprimento, ou certifica entidades que desempenham essa função.

Evidências

Disponibilidade de tecnologias desenvolvidas no país.

Número de centros de testes e validação tecnológica.

Participação de mercado de tecnologias desenvolvidas no país.

E5-Tecnologias-4-B
Serviços especializados em cibersegurança

Detalhamento:

Explora a disponibilidade de serviços de consultoria em cibersegurança para organizações privadas e públicas.

Níveis de Maturidade:

Inicial:
Serviços de consultoria em cibersegurança não estão amplamente disponíveis no país. Poucos, se algum, provedores possuem certificações profissionais.

Fundamental:

Há um número crescente de serviços de consultoria em cibersegurança disponíveis para organizações públicas e privadas. Um número crescente de provedores detalha suas certificações profissionais. Pode haver orientação limitada ou inexistente para auxiliar organizações na escolha de provedores.

Básico:
Serviços de consultoria em cibersegurança estão disponíveis para organizações públicas e privadas. Alguns provedores detalham suas certificações profissionais.

Médio:
Serviços de consultoria em cibersegurança estão amplamente disponíveis para organizações públicas e privadas. A maioria dos provedores detalha suas certificações profissionais.

Evoluído:
Um órgão nacional credencia provedores de serviços, auxiliando organizações na seleção de fornecedores. Organizações públicas e privadas rotineiramente buscam consultoria sobre riscos emergentes.

Avançado:
Há oferta adequada de profissionais de cibersegurança no país. O setor de serviços de cibersegurança contribui ativamente para moldar o mercado internacional.

Evidências

Número de empresas de consultoria disponíveis.

Participação de mercado de empresas nacionais.

E5-Tecnologias-4-C
Implicações de segurança da terceirização

Detalhamento:

Examina se são realizadas avaliações de risco para determinar como mitigar os riscos da terceirização de TI para terceiros ou serviços em nuvem.

Níveis de Maturidade:

Inicial:
Nenhuma avaliação de risco é conduzida para determinar como mitigar riscos de terceirização de TI a terceiros ou serviços em nuvem. Há falta de compreensão sobre as medidas de segurança aplicadas pelos provedores de serviços terceirizados.

Fundamental:
Algumas organizações e setores realizam avaliações de risco para mitigar riscos de terceirização de TI a terceiros ou serviços em nuvem. Pelo menos algumas organizações compreendem as medidas de segurança aplicadas por provedores terceirizados. Algumas desenvolveram processos de continuidade de negócios e recuperação de desastres.

Básico:
Uma parte das grandes organizações públicas e privadas realiza avaliações de risco para mitigar riscos de terceirização de TI. Há alguma compreensão sobre as garantias de segurança oferecidas pelos provedores terceirizados. Algumas possuem processos testados de continuidade e recuperação.

Médio:
A maioria das grandes organizações públicas e privadas realiza avaliações de risco para mitigar riscos de terceirização de TI. Há compreensão generalizada sobre as garantias de segurança oferecidas pelos provedores terceirizados. A maioria possui processos testados de continuidade e recuperação.

Evoluído:
As percepções obtidas a partir de avaliações de risco são rotineiramente analisadas para estabelecer e promover boas práticas de cibersegurança relacionadas à terceirização. Diferentes cenários de risco com provedores de TI são explorados e testados, incluindo riscos emergentes.

Avançado:
O país contribui para as melhores práticas internacionais sobre mitigação de riscos associados à terceirização de TI.

Evidências

Acompanhamento da maturidade dos terceirizados.

Estratégia de proteção de cadeia de suprimentos de software e hardware.

E5-Tecnologias-4-D
Seguro cibernético

Detalhamento:

Explora a existência de um mercado para seguros cibernéticos, sua cobertura e produtos adequados para diversas organizações.

Níveis de Maturidade:

Inicial:
A necessidade de um mercado de seguro cibernético pode ter sido identificada, mas produtos e serviços não estão amplamente disponíveis, seja internamente ou de provedores externos.

Fundamental:
A necessidade de um mercado de seguro cibernético é reconhecida por meio da avaliação de riscos financeiros para os setores público e privado, e a adequação das ofertas disponíveis está em discussão.

Básico:
Um mercado de seguro cibernético está em desenvolvimento e incentiva o compartilhamento de informações sobre ameaças entre os participantes.

Médio:
Um mercado de seguro cibernético está estabelecido e incentiva o compartilhamento de informações sobre ameaças entre os participantes. Produtos adequados para pequenas e médias empresas também são oferecidos.

Evoluído:
O mercado oferece diversas coberturas para mitigar perdas consequenciais. Organizações selecionam seguros com base em planejamento estratégico e riscos identificados.

Avançado:
O mercado de seguro cibernético é inovador e adaptável a riscos emergentes, padrões e práticas, cobrindo todo o escopo de danos cibernéticos. Reduções de prêmios são concedidas a comportamentos ciberseguros consistentes. As práticas nacionais influenciam o mercado internacional.

Evidências

Oferta de produtos de seguro cibernético para SEICs

Participação de mercado de emrpesas que contratam seguro cibernético.

E5-Tecnologias-4-E
Certificação de Produtos e Serviços

Detalhamento:

Explora a existência de certificação de produtos e serviços de cibersegurança.

Níveis de Maturidade:

Inicial:
Não se exige a certificação de produtos e serviços.

Fundamental:
A necessidade de certificação de produtos e serviços de cibersegurança é reconhecida, e sua adoção está em discussão.

Básico:
Um processo de exigência de certificação de produtos e serviços de cibersegurança é adotado em alguns setores de SEICs.

Médio:
Um processo de exigência de certificação de produtos e serviços de cibersegurança é adotado na maioria setores de SEICs.

Evoluído:
Um processo de exigência de certificação de produtos e serviços de cibersegurança é adotado em todos os setores de SEICs.

Avançado:
Um processo de exigência de certificação de produtos e serviços de cibersegurança é amplamente adotado nacionalmente.

Evidências

Centros nacionais de testes para 5G e outras redes críticas.

Certificação de produtos e serviços de cibersegurança.

Existência de laboratórios nacionais de teste para avaliar segurança de equipamentos utilizados em SEICs.

Programas de validação de segurança para soluções de inteligência artificial usadas pelo governo.

Regras nacionais sobre certificação de segurança de dispositivos de Internet das Coisas.

E5-Tecnologias-5

Cibersegurança e TCEs

Detalhamento:

Aborda o desenvolvimento e Implementação de programas de monitoramento de riscos, desafios e oportunidades trazidos pelas tecnologias computacionais emergentes para a cibersegurança e para assegurar que cibersegurança seja prioridade no desenvolvimento e aplicação de tecnologias computacionais emergentes no país, bem como a capacidade de implementação de sandboxes regulatórios para acompanhamento dessas tecnologias.

E5-Tecnologias-5-A

Desafios e oportunidades

Detalhamento:

Considera o monitoramento de desafios e oportunidades trazidos pelas tecnologias computacionais emergentes (TCEs).

Níveis de Maturidade:

Inicial:
Políticas e processos relativos ao monitoramento de desafios e oportunidades trazidos pelas TCEs ainda não foram formuladas.

Fundamental:
Políticas e processos de monitoramento de desafios e oportunidades trazidos pelas TCEs estão sendo elaboradas.

Básico:
Políticas e processos de monitoramento de desafios e oportunidades trazidos pelas TCEs estão estabelecidas em alguns setores essenciais.

Médio:
Políticas e processos de monitoramento de desafios e oportunidades trazidos pelas TCEs estão estabelecidas em todos os setores essenciais.

Evoluído:
Políticas e processos de monitoramento de desafios e oportunidades trazidos pelas TCEs são constantemente revisadas e aprimoradas com base em lições aprendidas e riscos emergentes.

Avançado:
O entendimento dos controles tecnológicos implementados se estende ao impacto nas operações organizacionais e na segurança nacional. O país é referência internacional em políticas e processos de monitoramento de desafios e oportunidades trazidos pelas TCEs, cuja implementação responde a ambiente de ameaças em constante evolução.

Evidências

Estratégia de segurança nacional para TCEs.

Monitoramento de ameaças emergentes.

Plano para adoção segura computação quântica.

Plano para adoção segura de 5G e 6G.

Plano para adoção segura de IA.

Políticas de preparação para criptografia pós-quântica.

Quadros legais para IA e tecnologias avançadas.

E5-Tecnologias-5-B
Priorização da cibersegurança no ciclo de vida

Detalhamento:

Explora a priorização da cibersegurança no desenvolvimento e aplicação de TCEs no país

Níveis de Maturidade:

Inicial:
Políticas e processos relativos à priorização da cibersegurança no desenvolvimento e aplicação de TCEs ainda não foram formuladas.

Fundamental:
Políticas e processos de priorização da cibersegurança no desenvolvimento e aplicação de TCEs estão sendo elaboradas.

Básico:
Políticas e processos de priorização da cibersegurança no desenvolvimento e aplicação de TCEs estão estabelecidas em alguns setores essenciais.

Médio:
Políticas e processos de priorização da cibersegurança no desenvolvimento e aplicação de TCEs estão estabelecidas em todos os setores essenciais.

Evoluído:
Políticas e processos de priorização da cibersegurança no desenvolvimento e aplicação de TCEs são constantemente revisadas e aprimoradas com base em lições aprendidas e riscos emergentes.

Avançado:
O entendimento dos controles tecnológicos implementados se estende ao impacto nas operações organizacionais e na segurança nacional. O país é referência internacional em políticas e processos de priorização da cibersegurança no desenvolvimento e aplicação de TCEs, cuja implementação responde a ambiente de ameaças em constante evolução.

Evidências

Existência de arcabouço institucional e normativo para o monitoramento da priorização da cibersegurança de TCEs no ciclo de vida.

Monitoramento, pelos reguladores, da preocupação com cibersegurança nas diferentes etapas do ciclo de vida de produtos baseados em TCEs.

E5-Tecnologias-5-C
Sandboxes regulatórios

Detalhamento:

Analisa a capacidade de implementação de sandboxes regulatórios para acompanhamento de TCEs.

Níveis de Maturidade:

Inicial:
Políticas e processos relativos à implementação de sandboxes regulatórias para acompanhamento de TCEs ainda não foram formuladas.

Fundamental:
Políticas e processos de capacidade de implementação de sandboxes regulatórias para acompanhamento de TCEs estão sendo elaboradas.

Básico:
Políticas e processos de implementação de sandboxes regulatórias para acompanhamento de TCEs estão estabelecidas em alguns setores essenciais.

Médio:
Políticas e processos de implementação de sandboxes regulatórias para acompanhamento de TCEs estão estabelecidas em todos os setores essenciais.

Evoluído:
Políticas e processos de implementação de sandboxes regulatórias para acompanhamento de TCEs são constantemente revisadas e aprimoradas com base em lições aprendidas e riscos emergentes.

Avançado:
O entendimento dos controles tecnológicos implementados se estende ao impacto nas operações organizacionais e na segurança nacional. O país é referência internacional em políticas e processos de capacidade de implementação de sandboxes regulatórios para acompanhamento de TCEs, cuja implementação responde a ambiente de ameaças em constante evolução.

Evidências

Existência de arcabouço institucional e normativo para a implementação de sanboxes regulatórios para o monitoramento da cibersegurança de TCEs.

Implementações de sandboxes regulatórios variados para o monitoramento da cibersegurança de TCEs.

Programas nacionais de sandboxing e análise automatizada de ameaças.

E6-Governança

Governança

Detalhamento:

Considera a existência de estruturas nacionais de governança da cibersegurança estabelecidas para implementação de políticas e/ou estratégias de cibersegurança, avaliar o sucesso ou fracasso de sua implementação e se adaptar a novas realidades e ameaças.

Considera também a ação dos reguladores setoriais em cibersegurança, e a capacidade de coordenação e harmonização da estrutura nacional com os órgãos setoriais.

Aborda ainda a existência de referenciais nacionais e setoriais para aferição da maturidade em cibersegurança.

E6-Governança-1

(Gestão) Autoridade Nacional Responsável

Detalhamento:

Considera a existência de uma Autoridade (Agência/Órgão) responsável para a Implementação da Política/Estratégia Nacional de Cibersegurança, podendo incluir comitês permanentes, grupos de trabalho oficiais, conselhos consultivos ou centros interdisciplinares. Tal órgão também pode ser exclusivamente responsável pelo CIRT, que é nacional.

E6-Governança-1-A

Conselho/Comitê consultivo da cibersegurança (nível político)

Detalhamento:

Considera a existência de um Conselho/Comitê responsável pela definição da Política/Estratégia Nacional de Cibersegurança.

Níveis de Maturidade:

Inicial:
Uma autoridade consultiva nacional política de cibersegurança, responsável pela proposição da estratégia, ainda não foi implantada.

Fundamental:
Uma autoridade consultiva nacional de cibersegurança, responsável pela proposição da estratégia, está em implantação.

Básico:
Uma autoridade consultiva nacional de cibersegurança, responsável pela proposição da estratégia, está em funcionamento e gradualmente amplia sua atuação aos diferentes setores essenciais.

Médio:
Uma autoridade consultiva nacional de cibersegurança, responsável pela proposição da estratégia, está em funcionamento e atua para harmonizar a regulamentação dos diferentes setores essenciais.

Evoluído:
Uma autoridade consultiva nacional de cibersegurança, responsável pela proposição da estratégia, está em funcionamento e atua junto a todos os setores essenciais.

Avançado:

A autoridade consultiva nacional de cibersegurança é referência internacional em políticas e estratégias de cibersegurança.

Evidências

Comitê consultivo multissetorial ativo (indústria, academia, sociedade civil).

E6-Governança-1-B
Órgão nacional de governança da cibersegurança (nível operacional)

Detalhamento:

Considera a existência de uma Autoridade (Agência/Órgão) responsável para a Implementação da Política/Estratégia Nacional de Cibersegurança.

Níveis de Maturidade:

Inicial:
Uma autoridade nacional de cibersegurança, responsável pela implementação da estratégia, ainda não foi implantada.

Fundamental:
Uma autoridade nacional de cibersegurança, responsável pela implementação da estratégia, está em implantação.

Básico:
Uma autoridade nacional de cibersegurança, responsável pela implementação da estratégia, está em funcionamento e gradualmente amplia sua atuação aos diferentes setores essenciais.

Médio:
Uma autoridade nacional de cibersegurança, responsável pela implementação da estratégia, está em funcionamento e atua para harmonizar a regulamentação dos diferentes setores essenciais.

Evoluído:
Uma autoridade nacional de cibersegurança, responsável pela implementação da estratégia, está em funcionamento e atua junto a todos os setores essenciais.

Avançado:
A autoridade nacional de cibersegurança é referência internacional na implementação de políticas e processos de cibersegurança.

Evidências

Adoção formal de princípios de governança internacional em ciberespaço.

Criação de um fórum permanente de coordenação em cibersegurança.

Existência de uma autoridade nacional claramente responsável pela coordenação estratégica.

Órgão de coordenação nacional definido.

Processo estruturado para atualizar políticas com base em lições aprendidas de incidentes reais.

E6-Governança-2

(Regulação) Capacidade e Competência Regulatória

Detalhamento:

Avalia a existência de órgãos reguladores setoriais e intersetoriais para elaborar regulamentações específicas de cibersegurança.

E6-Governança-2-A

Capacidade e Competência Regulatória Setorial

Detalhamento:

Avalia a existência de órgãos reguladores setoriais (ORSs) com capacidade de elaboração de regulações específicas de cibersegurança.

Níveis de Maturidade:

Inicial:
Não há ORSs ou esses ainda não definiram regulamentos setoriais de cibersegurança para os setores essenciais.

Fundamental:
ORSs definiram regulamentos setoriais de cibersegurança para alguns setores essenciais.

Básico:
ORSs definiram regulamentos setoriais de cibersegurança para todos os setores essenciais.

Médio:
ORSs atualizam rotineiramente os regulamentos setoriais de cibersegurança.

Evoluído:
ORSs atualizam rotineiramente os regulamentos setoriais de cibersegurança e geram métricas e dados para realimentar o processo de regulação.

Avançado:
ORSs são referências internacionais em políticas e regulamentos setoriais de cibersegurança.

Evidências

Implementação de monitoramento contínuo de segurança em SEICs.

Regras para compartilhamento de threat intelligence.

Requisitos legais mínimos de segurança.

E6-Governança-2-B

Diálogo com a Sociedade no Processo Regulatório

Detalhamento:

Avalia a existência de mecanismos de participação social na elaboração de regulações específicas de cibersegurança.

Níveis de Maturidade:

Inicial:

Não há mecanismos de participação social na elaboração de regulações setoriais de cibersegurança para os setores essenciais.

Fundamental:
Mecanismos de participação social na elaboração de regulações setoriais de cibersegurança são adotados em alguns setores essenciais.

Básico:
Mecanismos de participação social na elaboração de regulações setoriais de cibersegurança são adotados em todos os setores essenciais.

Médio:
Mecanismos de participação social na elaboração de regulações setoriais de cibersegurança são adotados rotineiramente.

Evoluído:
Mecanismos de participação social na elaboração de regulações setoriais de cibersegurança são adotados rotineiramente e geram métricas e dados para realimentar o processo de regulação.

Avançado:
ORSs são referências internacionais na utilização de mecanismos de participação social na elaboração de regulações setoriais de cibersegurança.

Evidências

Diretivas formais para avaliação de impacto regulatório em cibersegurança.

Processos de consulta pública para regulamentações de cibersegurança.

Requisitos obrigatórios de análise de impacto regulatório digital.

E6-Governança-2-C
Órgãos Reguladores Intersetoriais

Detalhamento:

Analisa a existência de órgãos reguladores intersetoriais para supervisionar o cumprimento de regulamentos específicos de cibersegurança.

Níveis de Maturidade:

Inicial:
Reguladores setoriais têm compreensão limitada do impacto cibernético sobre as entidades reguladas. Não há órgão regulador intersetorial para supervisionar requisitos específicos de cibersegurança.

Fundamental:
Os reguladores setoriais começam a definir papéis em cibersegurança e consideram a criação de órgãos intersetoriais.

Básico:
Alguns reguladores setoriais estão equipados com recursos e capacidades para supervisionar o cumprimento das exigências de cibersegurança em seus setores.

Médio:
Reguladores setoriais estão equipados com recursos e capacidades para supervisionar o cumprimento das exigências de cibersegurança em seus setores.

Evoluído:

Órgãos reguladores intersetoriais estabelecidos possuem capacidade e recursos adequados para supervisionar o cumprimento de regulamentos específicos de cibersegurança.

Avançado:
O impacto das ações regulatórias é avaliado regularmente, e os resultados são usados para aprimorar políticas, práticas de supervisão e desenvolvimento regulatório.

Evidências

Capacidade regulatória intersetorial.

E6-Governança-3

(Fiscalização) Capacidade e Competência Fiscalizatória

Detalhamento:

Avalia a existência de órgãos reguladores setoriais e intersetoriais para supervisionar o cumprimento de regulamentações específicas de cibersegurança.

E6-Governança-3-A

Fiscalização de Conformidade Regulatória

Detalhamento:

Avalia a existência de órgãos reguladores setoriais (ORSs) com capacidade de fiscalização de conformidade regulatória em cibersegurança.

Níveis de Maturidade:

Inicial:
Não há ORSs ou esses ainda não capacidade de fiscalização de conformidade regulatória em cibersegurança para os setores essenciais.

Fundamental:
ORSs dispõem de capacidade de fiscalização de conformidade regulatória em cibersegurança para alguns setores essenciais.

Básico:
Há ORSs com capacidade de fiscalização de conformidade regulatória em cibersegurança para todos os setores essenciais.

Médio:
ORSs ampliam rotineiramente sua capacidade de fiscalização de conformidade regulatória em cibersegurança.

Evoluído:
ORSs atualizam rotineiramente sua capacidade de fiscalização de conformidade regulatória em cibersegurança e geram métricas e dados para realimentar o processo de fiscalização.

Avançado:
ORSs são referências internacionais em capacidade de fiscalização de conformidade regulatória em cibersegurança.

Evidências

Fiscalização regulatória proativa.

Mecanismos de fiscalização de privacidade e cibersegurança.

Sanções legais por descumprimento de obrigações.

E6-Governança-3-B
Auditoria (de Conformidade ou Operacional)

Detalhamento:

Avalia a existência de órgãos com capacidade de auditoria de conformidade ou operacional em cibersegurança.

Níveis de Maturidade:

Inicial:
Não há ORSs ou esses ainda não capacidade de auditoria de conformidade ou operacional em cibersegurança para os setores essenciais.

Fundamental:
ORSs dispõem de capacidade de auditoria de conformidade ou operacional em cibersegurança para alguns setores essenciais.

Básico:
Há ORSs com capacidade de auditoria de conformidade ou operacional em cibersegurança para todos os setores essenciais.

Médio:
ORSs ampliam rotineiramente sua capacidade de auditoria de conformidade ou operacional em cibersegurança.

Evoluído:
ORSs atualizam rotineiramente sua capacidade de auditoria de conformidade ou operacional em cibersegurança e geram métricas e dados para realimentar o processo de fiscalização.

Avançado:
ORSs são referências internacionais em capacidade de auditoria de conformidade ou operacional em cibersegurança.

Evidências

Disponibilidade de meios adequados para a realização, pela autoridade nacional ou setorial, de auditorias de conformidade em cibersegurança.

Existência de instrumentos legais para a realização, pela autoridade nacional ou setorial, de auditorias de conformidade em cibersegurança.

Realização, pela autoridade nacional ou setorial, de auditorias de conformidade em cibersegurança.

Realização, pela autoridade nacional ou setorial, de auditorias operacionais em cibersegurança.

E6-Governança-4

(Coordenação) Capacidade e Competência de Coordenação

Detalhamento:

Avalia a existência de órgãos reguladores setoriais e intersetoriais para coordenar ações de cibersegurança.

E6-Governança-4-A
Coordenação de Ações de Cibersegurança

Detalhamento:

Avalia a existência de órgãos com capacidade de coordenação de ações de cibersegurança.

Níveis de Maturidade:

Inicial:
Não há ORSs ou esses ainda não capacidade de coordenação de ações de cibersegurança para os setores essenciais.

Fundamental:
ORSs dispõem de capacidade de coordenação de ações de cibersegurança para alguns setores essenciais.

Básico:
Há ORSs com capacidade de coordenação de ações de cibersegurança para todos os setores essenciais.

Médio:
ORSs ampliam rotineiramente sua capacidade de coordenação de ações de cibersegurança.

Evoluído:
ORSs atualizam rotineiramente sua capacidade de coordenação de ações de cibersegurança e geram métricas e dados para realimentar o processo de fiscalização.

Avançado:
ORSs são referências internacionais em capacidade de coordenação de ações de cibersegurança.

Evidências

Definição de critérios nacionais para priorização de SEICs em situações de escassez de recursos de resposta (equipes, equipamentos, conectividade).

Estrutura de governança específica para coordenação com governos subnacionais.

Guia nacional de elaboração de planos setoriais de cibersegurança.

Integração explícita entre a Estratégia Nacional de Cibersegurança e as políticas setoriais da ANEEL, ANP, ANA, ANS, ANATEL, BACEN e ANTT em temas de cibersegurança.

Normas e regulamentos intersetoriais elaborados conjuntamente por diferentes ORSs.

E6-Governança-5

(Controle) Capacidade e Competência de Controle Operacional

Detalhamento:

Avalia a existência de órgãos reguladores setoriais e intersetoriais para realizar o controle operacional da cibersegurança.

E6-Governança-5-A
Inventário de Ciberativos

Detalhamento:

Afere a existência de inventários nacionais ou setoriais oficiais de ciberativos.

Níveis de Maturidade:

Inicial:
Inventários nacionais ou setoriais de ciberativos ainda não foram elaborados.

Fundamental:
Inventários nacionais ou setoriais de ciberativos estão sendo elaborados.

Básico:
Inventários nacionais ou setoriais de ciberativos estão sendo elaborados em alguns setores essenciais.

Médio:
Inventários nacionais ou setoriais de ciberativos estão estabelecidos em todos os setores essenciais.

Evoluído:
Inventários nacionais ou setoriais de ciberativos são constantemente revisados e aprimorados com base em lições aprendidas e riscos emergentes.

Avançado:
Inventários nacionais ou setoriais de ciberativos estão estabelecidos e consolidados. O país é referência internacional em gestão de ciberativos críticos, e na resposta a um ambiente de ameaças em constante evolução.

Evidências

Inventário nacional de ciber-riscos.

Mapeamento das dependências internacionais de TIC estratégicas.

E6-Governança-5-B
Métricas de Desempenho

Detalhamento:

Afere a existência de referenciais de benchmarking nacionais, setoriais ou institucionais oficiais para medir o desempenho nacional em cibersegurança.

Níveis de Maturidade:

Inicial:
Referenciais de benchmarking nacionais ou setoriais oficiais para medir o desempenho em cibersegurança ainda não foram formulados.

Fundamental:
Referenciais de benchmarking nacionais ou setoriais oficiais para medir o desempenho em cibersegurança estão sendo elaborados.

Básico:

Referenciais de benchmarking nacionais ou setoriais oficiais para medir o desempenho em cibersegurança estão estabelecidos em alguns setores essenciais.

Médio:
Referenciais de benchmarking nacionais ou setoriais oficiais para medir o desempenho em cibersegurança estão estabelecidos em todos os setores essenciais.

Evoluído:
Referenciais de benchmarking nacionais ou setoriais oficiais para medir o desempenho em cibersegurança são constantemente revisados e aprimorados com base em lições aprendidas e riscos emergentes.

Avançado:
O entendimento dos controles tecnológicos implementados se estende ao impacto nas operações organizacionais e na segurança nacional. O país é referência internacional em referenciais de benchmarking nacionais ou setoriais oficiais para medir o desempenho em cibersegurança, cuja implementação responde a ambiente de ameaças em constante evolução.

Evidências

Estatísticas públicas sobre ciberincidentes e fraudes.

Existência de mecanismo oficial de medição e monitoramento da execução da política nacional de cibersegurança.

Existência de metas de cibersegurança integradas a indicadores de desempenho governamental.

Existência de uma política federal para avaliação periódica de ciber-riscos sistêmicos em SEICs.

Publicação periódica de relatório federal consolidado sobre riscos e ciberincidentes em SEICs, com recomendações estratégicas.

Relatórios públicos de tendências e novas ameaças.

E6-Governança-5-C
Métricas de Maturidade

Detalhamento:

Afere a existência de referenciais de benchmarking nacionais, setoriais ou institucionais oficiais para medir a maturidade institucional em cibersegurança.

Níveis de Maturidade:

Inicial:
Referenciais de benchmarking nacionais ou setoriais oficiais para medir a maturidade em cibersegurança ainda não foram formulados.

Fundamental:

Referenciais de benchmarking nacionais ou setoriais oficiais para medir a maturidade em cibersegurança estão sendo elaborados.

Básico:
Referenciais de benchmarking nacionais ou setoriais oficiais para medir a maturidade em cibersegurança estão estabelecidos em alguns setores essenciais.

Médio:
Referenciais de benchmarking nacionais ou setoriais oficiais para medir a maturidade em cibersegurança estão estabelecidos em todos os setores essenciais.

Evoluído:
Referenciais de benchmarking nacionais ou setoriais oficiais para medir a maturidade em cibersegurança são constantemente revisados e aprimorados com base em lições aprendidas e riscos emergentes.

Avançado:
O entendimento dos controles tecnológicos implementados se estende ao impacto nas operações organizacionais e na segurança nacional. O país é referência internacional em referenciais de benchmarking nacionais ou setoriais oficiais para medir a maturidade em cibersegurança, cuja implementação responde a ambiente de ameaças em constante evolução.

Evidências

Avaliação do nível de maturidade nacional a cada dois anos.

Ferramentas públicas de autoavaliação de cibersegurança para cidadãos e pequenos negócios.

Indicadores nacionais de ciber-risco reportados ao parlamento.

Publicação anual de relatório de situação e desempenho da estratégia de cibersegurança.

Relatórios anuais (ou extraordinários a qualquer tempo) ao parlamento sobre implementação da estratégia de cibersegurança.

E6-Governança-5-D
Comunicações de Emergência

Detalhamento:

Avalia a existência de órgãos com capacidade de efetuar comunicações de emergência com a população em emergências de cibersegurança.

Níveis de Maturidade:

Inicial:
Não há órgãos com capacidade de efetuar comunicações de emergência de cibersegurança.

Fundamental:
Há órgãos com capacidade de efetuar comunicações de emergência para alguns setores essenciais.

Básico:
Há órgãos com capacidade de efetuar comunicações de emergência para todos os setores essenciais.

Médio:
Órgãos com capacidade de efetuar comunicações de emergência ampliam rotineiramente sua capacidade de comunicação.

Evoluído:
Órgãos com capacidade de efetuar comunicações de emergência atualizam rotineiramente sua capacidade de comunicação e geram métricas e dados para realimentar o processo de fiscalização.

Avançado:
Órgãos com capacidade de efetuar comunicações de emergência são referências internacionais.

Evidências

Mecanismos oficiais de sinalização e alerta rápido para cidadãos.

E7-Cooperação

Cooperação

Detalhamento:

Avalia a capacidade de cooperação interagências, intersetorial e internacional, envolvendo governo, academia e setor privado na realização de iniciativas conjuntas, compartilhamento de informações, treinamentos e outras atividades que conectam profissionais, autoridades e outros atores em prol da cibersegurança.

E7-Cooperação-1

Acordos Internacionais de Cibersegurança

Detalhamento:

Analisa a existência de acordos e parcerias internacionais ou regionais (bilaterais ou multilaterais) oficialmente reconhecidos para compartilhamento de informações ou ativos de cibersegurança entre fronteiras pelo governo com outro governo estrangeiro e entidades regionais (ou seja, a cooperação ou intercâmbio de informação, expertise, tecnologia e outros recursos).

E7-Cooperação-1-A

Acordos e parcerias bilaterais nacionais ou setoriais

Detalhamento:

Avalia a existência de acordos e parcerias bilaterais (acordos um-para-um) nacionais ou setoriais para cooperação ou intercâmbio de informação, expertise, tecnologia e outros recursos.

Níveis de Maturidade:

Inicial:
Acordos e parcerias bilaterais ainda não foram formulados.

Fundamental:
Acordos e parcerias bilaterais estão sendo elaborados.

Básico:
Acordos e parcerias bilaterais estão estabelecidos em alguns setores essenciais.

Médio:
Acordos e parcerias bilaterais estão estabelecidos em todos os setores essenciais.

Evoluído:
Acordos e parcerias bilaterais são constantemente revisados e aprimorados com base em lições aprendidas e riscos emergentes.

Avançado:
O entendimento dos controles tecnológicos implementados se estende ao impacto nas operações organizacionais e na segurança nacional. O país é referência internacional em acordos e parcerias bilaterais, cuja implementação responde a ambiente de ameaças em constante evolução.

Evidências

Acordos de reconhecimento mútuo de testes, inspeções ou certificações.

Estrutura de cooperação internacional ativa em cibersegurança.

Programas de harmonização regulatória internacional (convergência com padrões internacionalmente aceitos).

Programas de intercâmbio internacionais para especialistas nacionais.

E7-Cooperação-1-B

Acordos e parcerias multilaterais nacionais ou setoriais

Detalhamento:

Avalia a existência de acordos e parcerias multilaterais nacionais ou setoriais para cooperação ou intercâmbio de informação, expertise, tecnologia e outros recursos.

Níveis de Maturidade:

Inicial:
Acordos e parcerias multilaterais nacionais ou setoriais ainda não foram formulados.

Fundamental:
Acordos e parcerias multilaterais nacionais ou setoriais estão sendo elaborados.

Básico:
Acordos e parcerias multilaterais nacionais ou setoriais estão estabelecidos em alguns setores essenciais.

Médio:
Acordos e parcerias multilaterais nacionais ou setoriais estão estabelecidos em todos os setores essenciais.

Evoluído:
Acordos e parcerias multilaterais nacionais ou setoriais são constantemente revisados e aprimorados com base em lições aprendidas e riscos emergentes.

Avançado:
O entendimento dos controles tecnológicos implementados se estende ao impacto nas operações organizacionais e na segurança nacional. O país é referência internacional em acordos e parcerias multilaterais nacionais ou setoriais, cuja implementação responde a ambiente de ameaças em constante evolução.

Evidências

Adesão formal a acordos internacionais.

E7-Cooperação-2

Acordos de Assistência Jurídica Mútua em Cibersegurança

Detalhamento:

Ratificação de acordos internacionais contendo cláusulas relacionadas à Assistência Jurídica Mútua e à cibersegurança.

E7-Cooperação-2-A

Acordos de assistência jurídica mútua

Detalhamento:

Avalia o número de acordos ratificados internacionais contendo cláusulas relacionadas à Assistência Jurídica Mútua e à cibersegurança.

Níveis de Maturidade:

Inicial:
Acordos de Assistência Jurídica Mútua ainda não foram formulados.

Fundamental:
Acordos de Assistência Jurídica Mútua estão sendo elaborados.

Básico:
Acordos de Assistência Jurídica Mútua estão estabelecidos em alguns setores essenciais.

Médio:
Acordos de Assistência Jurídica Mútua estão estabelecidos em todos os setores essenciais.

Evoluído:
Acordos de Assistência Jurídica Mútua são constantemente revisados e aprimorados com base em lições aprendidas e riscos emergentes.

Avançado:
O entendimento dos controles tecnológicos implementados se estende ao impacto nas operações organizacionais e na segurança nacional. O país é referência internacional em acordos de Assistência Jurídica Mútua, cuja implementação responde a ambiente de ameaças em constante evolução.

Evidências

Instrumentos legais que facilitem cooperação internacional em casos de cibercrime.

Mecanismos legais de cooperação com plataformas globais em remoção de conteúdo malicioso.

E7-Cooperação-3

Parcerias Público-Privadas

Detalhamento:

Afere o número de PPPs nacionais ou setoriais oficialmente reconhecidas para compartilhamento de informações e ativos de cibersegurança (pessoas, processos, ferramentas) entre o setor público e privado (ou seja, parcerias oficiais para cooperação ou troca de informações, expertise, tecnologia e/ou recursos), seja nacional ou internacionalmente.

E7-Cooperação-3-A

Parcerias Público-Privadas de troca de informações

Detalhamento:

Número de PPPs nacionais ou setoriais oficialmente reconhecidas para compartilhamento de informações e ativos de cibersegurança (pessoas, processos, ferramentas) entre o setor público e privado (ou seja, parcerias oficiais para cooperação ou troca de informações, expertise, tecnologia e/ou recursos), seja nacional ou internacionalmente.

Níveis de Maturidade:

Inicial:
Políticas e processos relativos a PPPs nacionais ou setoriais ainda não foram formulados.

Fundamental:

Políticas e processos de PPPs nacionais ou setoriais estão sendo elaborados.

Básico:
Políticas e processos de PPPs nacionais ou setoriais estão estabelecidos em alguns setores essenciais.

Médio:
Políticas e processos de PPPs nacionais ou setoriais estão estabelecidos em todos os setores essenciais.

Evoluído:
Políticas e processos de PPPs nacionais ou setoriais são constantemente revisados e aprimorados com base em lições aprendidas e riscos emergentes.

Avançado:
O entendimento dos controles tecnológicos implementados se estende ao impacto nas operações organizacionais e na segurança nacional. O país é referência internacional em políticas e processos de PPPs nacionais ou setoriais, cuja implementação responde a ambiente de ameaças em constante evolução.

Evidências

Existência de meios legais para a instituição de PPPs para troca de informações.

Existência de PPPs para troca de informações.

E7-Cooperação-4

Parcerias Interagências

Detalhamento:

Avalia a existência de parcerias formais entre o governo e agências do país (não se refere a parcerias internacionais, portanto). Isso pode designar parcerias para compartilhamento de informações ou ativos entre ministérios, departamentos, agências programas e outras instituições do setor público.

E7-Cooperação-4-A

Parcerias interagências formais

Detalhamento:

Existência de parcerias formais entre o governo e agências do país (não se refere a parcerias internacionais, portanto). Pode incluir parcerias para compartilhamento de informações ou ativos entre ministérios, departamentos, agências programas e outras instituições do setor público, ou ainda normas intersetoriais elaboradas conjuntamente por mais de um ORS [proposta FGV].

Níveis de Maturidade:

Inicial:
Parcerias formais entre o governo e agências ainda não foram formulados.

Fundamental:
Parcerias formais entre o governo e agências estão sendo elaborados.

Básico:
Parcerias formais entre o governo e agências estão estabelecidos em alguns setores essenciais.

Médio:
Parcerias formais entre o governo e agências estão estabelecidos em todos os setores essenciais.

Evoluído:

Parcerias formais entre o governo e agências são constantemente revisados e aprimorados com base em lições aprendidas e riscos emergentes.

Avançado:
O entendimento dos controles tecnológicos implementados se estende ao impacto nas operações organizacionais e na segurança nacional. O país é referência internacional em parcerias formais entre o governo e agências, cuja implementação responde a ambiente de ameaças em constante evolução.

Evidências

Cooperação formalizada entre reguladores setoriais e autoridade de cibersegurança para casos envolvendo ciberincidentes complexos.

Cooperação jurídica internacional estruturada.

Estruturas formais de coordenação interministerial.

Parcerias universidade-indústria-governo.

Previsão legal de cooperação entre autoridades de proteção de dados e de cibersegurança.

E7-Cooperação-5

Cooperação Formal e Informal

Detalhamento:

Aborda a existência e a função de mecanismos formais e informais que permitem a cooperação entre atores nacionais e internacionais para dissuadir e combater o cibercrime.

E7-Cooperação-5-A

Cooperação entre as forças policiais e o setor privado

Detalhamento:

Examina o mecanismo de troca de informações sobre cibercrimes entre os setores público e privado nacionais, incluindo a cooperação com provedores de serviços de internet e outros provedores de tecnologia.

Níveis de Maturidade:

Inicial:
A cooperação entre setores público e privado nacionais em matéria de cibercrime é limitada. Especificamente, a cooperação entre provedores de serviços de Internet e outros provedores de tecnologia e as forças de aplicação da lei não foi estabelecida.

Fundamental:
A troca de informações sobre cibercrime entre setores público e privado nacionais ocorre de forma ad hoc e sem regulação. Cooperação informal entre provedores de Internet e outros provedores de tecnologia e as forças de aplicação da lei existe, mas nem sempre é eficaz.

Básico:

Informações são trocadas ocasionalmente entre setores público e privado nacionais, com fundamento em legislação apropriada. Mecanismos de cooperação entre provedores de Internet, outros provedores de tecnologia e as forças de aplicação da lei são estabelecidos como parte de arranjos mais amplos de colaboração público-privada.

Médio:
Informações são trocadas regularmente entre setores público e privado nacionais, com ampara de legislação apropriada. Mecanismos eficazes de cooperação entre provedores de Internet, outros provedores de tecnologia e as forças de aplicação da lei foram estabelecidos como parte de arranjos mais amplos de colaboração público-privada.

Evoluído:
A eficácia da cooperação público-privada é avaliada regularmente e usada para aprimorar os processos colaborativos.

Avançado:
Os marcos de colaboração são continuamente adaptados para considerar novas tecnologias e formas emergentes de cibercrime. O país contribui ativamente para a promoção de parcerias público-privadas e para o desenvolvimento de plataformas internacionais de cooperação.

Evidências

Instrumentos de cooperação entre autoridades de proteção de dados e de cibersegurança.

Previsão legal de cooperação entre autoridades de proteção de dados e de cibersegurança.

E7-Cooperação-5-B
Cooperação com as autoridades policiais estrangeiras

Detalhamento:

Examina a existência de mecanismos formais de cooperação internacional em matéria de aplicação da lei.

Níveis de Maturidade:

Inicial:
Há poucas ou nenhuma forma de cooperação internacional para prevenir e combater o cibercrime.

Fundamental:
Mecanismos formais de cooperação internacional entre forças de aplicação da lei podem existir, mas sua aplicação ao cibercrime é pontual ou limitada a alguns casos. As forças nacionais não estão formalmente integradas a redes regionais ou internacionais de combate ao cibercrime.

Básico:
Mecanismos formais de cooperação internacional entre forças de aplicação da lei são estabelecidos para facilitar a detecção, investigação e persecução de cibercrimes. As agências nacionais de aplicação da lei estão se integrando a redes regionais e internacionais, como a Interpol.

Médio:
Mecanismos formais de cooperação internacional entre forças de aplicação da lei foram estabelecidos para facilitar a detecção, investigação e persecução de cibercrimes. Acordos e mecanismos de assistência jurídica mútua e extradição foram criados e aplicam-se a casos de cibercrime. As agências nacionais de aplicação da lei estão integradas a redes regionais e internacionais, como a Interpol ou redes 24/7.

Evoluído:

As forças de aplicação da lei trabalham em conjunto com contrapartes estrangeiras, possivelmente por meio de forças-tarefa conjuntas, resultando em investigações e processos transnacionais bem-sucedidos.

Avançado:
O país contribui ativamente para a promoção e o desenvolvimento de mecanismos internacionais de cooperação.

Evidências

Instrumentos de cooperação com autoridades policiais estrangeiras.

Previsão legal de mecanismos de cooperação com autoridades policiais estrangeiras.

E7-Cooperação-5-C
Colaboração entre o Governo e o Setor de Justiça Criminal

Detalhamento:

Analisa os canais formais de comunicação entre o governo e os atores do sistema de justiça criminal.

Níveis de Maturidade:

Inicial:
A interação entre governo e atores da justiça criminal é mínima.

Fundamental:
A troca de informações entre governo e atores da justiça criminal é limitada e ad hoc.

Básico:
Relações formais entre governo e atores da justiça criminal são estabelecidas, resultando em troca ocasional de informações sobre questões de cibercrime.

Médio:
Relações formais entre governo e atores da justiça criminal foram estabelecidas, resultando em troca regular de informações sobre questões de cibercrime.

Evoluído:
A relação entre governo, promotores, juízes e forças de aplicação da lei é regularmente avaliada e usada para aprimorar sua eficácia.

Avançado:
O país contribui para o desenvolvimento de boas práticas e modelos de colaboração entre o governo e o setor de justiça criminal, inclusive em nível internacional.

Evidências

Instrumentos de cooperação do Governo com a Justiça Criminal.

Previsão legal de mecanismos de cooperação do Governo com a Justiça Criminal.

E8-Resiliência

Resiliência e Gestão de Incidentes

Detalhamento:

Avalia os instrumentos de proteção e continuidade de Serviços Essenciais e Infraestruturas Críticas (SEICs).

Considera também a melhoria dos mecanismos de gestão de cibercrises, incidentes e vulnerabilidades disponibilizados no País.

E8-Resiliência-1

Resposta a Incidentes e Gestão de Crises

Detalhamento:

Aborda a capacidade do governo de identificar e determinar as características de incidentes em nível nacional de forma sistemática. Também analisa a capacidade do governo de organizar, coordenar e operacionalizar a resposta a incidentes e se a cibersegurança foi integrada à estrutura nacional de gerenciamento de crises.

E8-Resiliência-1-A

Identificação e categorização de incidentes

Detalhamento:

Identifica se existem mecanismos internos para identificar e categorizar incidentes.

Níveis de Maturidade:

Inicial:
Não há processo nacional para identificar ou classificar incidentes.

Fundamental:
Mecanismos iniciais existem, porém, fragmentados e sem escalonamento claro.

Básico:
Processo nacional em definição, com incidentes começando a ser registrados e categorizados.

Médio:
Processo nacional em definição, com incidentes registrados e categorizados.

Evoluído:
Classificação é revisada com base em inteligência e evolução de ameaças.

Avançado:
Processos adaptativos e antecipatórios; referência internacional.

Evidências

Procedimentos formais para notificação de violações significativas.

Procedimentos padronizados de classificação de incidentes por severidade.

Sistema nacional de reporte de incidentes para governo e setor privado.

E8-Resiliência-1-B
Governança

Detalhamento:

Aborda a existência de um órgão central mandatado para coletar informações sobre incidentes e sua relação com os setores público e privado para a resposta a incidentes em nível nacional.

Níveis de Maturidade:

Inicial:
Não há organismo nacional responsável.

Fundamental:
Organismo nacional em estabelecimento.

Básico:
Organismo existente, porém, com recursos limitados e coordenação ainda restrita.

Médio:
Organismo nacional estabelecido, com recursos, autoridade e protocolos.

Evoluído:
Coordenação madura entre setores e compartilhamento contínuo de inteligência.

Avançado:
Capacidade de resposta rápida, cooperação internacional ativa e exercícios regulares.

Evidências

Cursos especializados em resposta a incidentes para equipes de TI de SEICs.

Definição de papéis e responsabilidades para resposta a incidentes.

Definição formal, em documentos estratégicos, dos papéis do governo federal, estados, municípios e operadores privados na proteção de SEICs.

Estratégia nacional para detecção e resposta automatizada a incidentes (SOAR).

Exercícios nacionais de cibercrise (table-top, simulações técnicas).

Existência de plano de engajamento com setor privado em situações de crise cibernética.

Existência de um centro nacional de coordenação de crises cibernéticas com protocolos específicos para SEICs.

Política nacional de proteção contra-ataques de negação de serviço distribuídos.

Procedimentos de avaliação prévia de ciber-riscos em projetos de grandes obras federais de infraestrutura (rodovias, portos, aeroportos, hidrelétricas).

Procedimentos para que reguladores setoriais compartilhem, em tempo quase real, informações sobre incidentes relevantes com o governo federal.

Programa sistemático de lições aprendidas após crises e incidentes.

E8-Resiliência-1-C
Integração da Cibersegurança na Gestão Nacional de Crises

Detalhamento:

Explora em que medida a cibersegurança está integrada na estrutura nacional de gestão de crises.

Níveis de Maturidade:

Inicial:
Resposta a incidentes não integrada à gestão de crises.

Fundamental:
Reconhecimento inicial da relevância, com realização de exercícios limitados.

Básico:
Integração com estruturas de crise em desenvolvimento.

Médio:
Integração formal com estruturas de crise, com papéis definidos.

Evoluído:
Cenários cibernéticos incorporados em exercícios de crise nacionais.

Avançado:
Capacidade proativa, flexível e interoperável internacionalmente.

Evidências

Avaliação anual da prontidão de recursos humanos.

Centro nacional de resposta a incidentes (CSIRT/CERT nacional) operacional.

Estratégia de ciber-resiliência para continuidade do governo em crises.

Hackathons e desafios de segurança promovidos.

Plano nacional de comunicação estratégica em cibersegurança aprovado pelo alto escalão.

Procedimentos nacionais para resposta coordenada a cibercrises.

Procedimentos para ativação de estado de emergência cibernética ou equivalente.

Programas de qualificação recorrente em cibersegurança para equipes de resposta a desastres, integrando aspectos físicos e digitais.

E8-Resiliência-2

Proteção de Serviços Essenciais e Infraestruturas Críticas (SEICs)

Detalhamento:

Estuda a capacidade do governo de identificar ativos de SEIC, os requisitos regulatórios específicos para a cibersegurança de SEICs e a implementação de boas práticas de cibersegurança pelos provedores de Serviços Essenciais e operadores de Infraestruturas Críticas.

E8-Resiliência-2-A

Identificação

Detalhamento:

Aborda a existência de um inventário geral SEICS, seus ciberativos, provedores e operadores, bem como uma auditoria regular desses ativos.

Níveis de Maturidade:

Inicial:
Pode haver alguma compreensão do que constitui um ciberativo de SEIC, mas nenhuma categorização formal foi produzida.

Fundamental:
Um inventário de SEICs e seus ciberativos foi criada.

Básico:
O inventário de SEICs e seus ciberativos foi formalizado e inclui organizações públicas e privadas apropriadas.

Médio:
O inventário de SEICs e ciberativos foi formalizado e inclui organizações públicas e privadas apropriadas. Operadores específicos foram identificados e estão cientes de seu status.

Evoluído:
O inventário é mantido atualizado para refletir mudanças nas circunstâncias do país. Dependências transfronteiriças foram identificadas e são gerenciadas. As interdependências entre setores são administradas.

Avançado:
O inventário de SEICs é adaptável a mudanças estratégicas no ambiente técnico, social e econômico. O processo de identificação é flexível o suficiente para lidar com rápidas mudanças tecnológicas ou de ameaça. O país participa ativamente da identificação e priorização de ativos globais de SEICs. Dependências entre setores e fronteiras são mitigadas.

Evidências

Definição formal de níveis de criticidade para serviços públicos digitais.

Inventário nacional de SEICs e dependências sistêmicas.

Inventário nacional formal de SEICs.

Mapeamento formal de stakeholders públicos e privados.

Sistema nacional de classificação de ativos e dados críticos.

E8-Resiliência-2-B
Requisitos regulamentares

Detalhamento:

Aborda a existência de requisitos regulamentares específicos para a cibersegurança de SEICs.

Níveis de Maturidade:

Inicial:
Não existem requisitos regulatórios específicos para a cibersegurança de SEICs.

Fundamental:
Há reconhecimento da necessidade de padrões básicos para reger as SEICs, mas eles não são exigidos por regulamentação. Autoridades setoriais não avaliam rotineiramente o cumprimento pelos operadores de SEICs.

Básico:
Operadores de SEICs são obrigados por regulamentação setorial a adotar padrões adequados de cibersegurança.

Médio:
Operadores de SEICs são obrigados por regulamentação nacional a atender padrões adequados de cibersegurança. Existem requisitos formais de notificação de incidentes e vulnerabilidades.

Evoluído:
Processos formais avaliam a conformidade dos operadores de SEICs com normas regulatórias e requisitos de notificação. Estão sendo desenvolvidas abordagens inovadoras de supervisão para melhorar a cibersegurança sem comprometer a eficiência operacional.

Avançado:
O país promove as melhores práticas regulatórias em nível internacional. Estruturas regulatórias são flexíveis para responder rapidamente a mudanças tecnológicas e de ameaças. O país participa ativamente na formulação de abordagens regulatórias globais para a segurança de infraestruturas críticas.

Evidências

Adoção de padrões mínimos de segurança para centros de operação de SEICs, incluindo segmentação de redes OT/IT.

Definição, em ato normativo federal, dos setores que compõem a SEICs nacional e suas responsabilidades em cibersegurança.

Definição, em política nacional, de diretrizes para ciber-resiliência em projetos de PPPs e concessões de infraestrutura.
Existência de guias regulatórios para implementação de programas de gestão de risco de terceiros e cadeia de suprimentos em SEICs.
Existência de planos nacionais de continuidade de SEICs que incluam cenários de ciberataques em larga escala.
Inclusão de requisitos de cibersegurança em contratos públicos estratégicos.
Incorporação de requisitos de cibersegurança em políticas federais de universalização de SEICs.
Marco regulatório sobre certificação de SEICs.
Normas para resiliência física e lógica de data centers nacionais.
Normas que vinculem autorização de funcionamento de SEICs ao cumprimento de requisitos mínimos de cibersegurança.
Política nacional de backup e continuidade.
Prazos legais para retenção mínima e máxima de dados de log.
Processo oficial para coleta de requisitos de segurança dos setores críticos.
Regulação clara sobre responsabilidade de SEICs em incidentes de segurança.
Regulação específica para uso de criptografia forte por SEICs.
Regulação setorial obrigatória para SEICs.

Uso de criptografia adequada em canais de comunicação entre centros de controle e dispositivos remotos em campo.

E8-Resiliência-2-C
Prontidão e Aprestamento

Detalhamento:

Explora se gestores de SEICs implementam processos para melhoria da prontidão e aprestamento de suas equipes de prevenção e resposta a incidentes.

Níveis de Maturidade:

Inicial:
Alguns operadores de SEICs podem implementar boas práticas de cibersegurança, mas de forma inconsistente.

Fundamental:
Muitos operadores de SEICs implementam boas práticas de cibersegurança, com alguma autoavaliação em relação a padrões reconhecidos. Há arranjos informais de colaboração entre setores.

Básico:
Operadores de SEICs ocasionalmente implementam de padrões reconhecidos e avaliam a eficácia de seus controles de segurança.

Médio:
Operadores de SEICs implementam de forma consistente padrões reconhecidos e avaliam regularmente a eficácia de seus controles de segurança.

Evoluído:
Mecanismos estão em vigor para compartilhamento de informações sobre ameaças, vulnerabilidades e lições aprendidas. Operadores participam de exercícios nacionais de resposta a incidentes e gestão de crises. Autoridades públicas oferecem suporte prático antes e após incidentes.

Avançado:
Há colaboração extensa entre operadores e autoridades públicas para fortalecer a resiliência coletiva. A resiliência do ecossistema de SEICs é avaliada contra cenários diversos. O país e seus operadores participam do debate internacional sobre resiliência global. Especialistas nacionais são reconhecidos internacionalmente por sua contribuição à proteção de infraestruturas críticas.

Evidências

Estratégia nacional de proteção de endpoints em estações de trabalho governamentais.

Exercícios conjuntos civis-militares de resposta a incidentes.

Existência de estratégias setoriais de cibersegurança formalmente aprovadas para SEICs.

Implementação de mecanismos nacionais de detecção precoce de campanhas maliciosas em larga escala.

Incorporação de cenários de ciberameaças em planos de contingência de defesa civil para desastres que afetem SEICs.

Monitoramento centralizado de indicadores de cibersegurança provenientes de diferentes operadores de SEICs.

Política nacional para fortalecimento de logs e trilhas de auditoria em sistemas públicos.

Previsão legal de incentivos (regulatórios ou econômicos) para investimentos em cibersegurança (e ciber-resiliência) por SEICs.

Programa nacional de mitigação e resposta a ransomware.

Programa nacional de testes de penetração para SEICs.

Programas de varredura periódica de vulnerabilidades em redes que suportam operações de SEICs.

Programas permanentes de exercícios de cibercrise envolvendo simultaneamente múltiplos SEICs e diferentes níveis federativos.

Treinamentos conjuntos entre CSIRTs governamentais e equipes de segurança de SEICs.

E8-Resiliência-2-D Prática Operacional
Detalhamento: Explora se gestores de SEICs implementam padrões reconhecidos do setor e a existência de mecanismos de colaboração intra e intersetorial.

Níveis de Maturidade:

Inicial: Alguns operadores de SEICs podem implementar boas práticas de cibersegurança, mas de forma inconsistente.
Fundamental: Muitos operadores de SEICs implementam boas práticas de cibersegurança, com alguma autoavaliação em relação a padrões reconhecidos. Há arranjos informais de colaboração intersetorial.
Básico: Operadores de SEICs ocasionalmente implementam de padrões reconhecidos e avaliam a eficácia de seus controles de segurança.

Médio:
Operadores de SEICs implementam de forma consistente padrões reconhecidos e avaliam regularmente a eficácia de seus controles de segurança.

Evoluído:
Mecanismos estão em vigor para compartilhamento de informações sobre ameaças, vulnerabilidades e lições aprendidas. Operadores participam de exercícios nacionais de resposta a incidentes e gestão de crises. Autoridades públicas oferecem suporte prático antes e após incidentes.

Avançado:
Há colaboração extensa entre operadores e autoridades públicas para fortalecer a resiliência coletiva. A resiliência do ecossistema de SEICs é avaliada contra cenários diversos. O país e seus operadores participam do debate internacional sobre resiliência global. Especialistas nacionais são reconhecidos internacionalmente por sua contribuição à proteção de infraestruturas críticas.

Evidências

Definição de uma política nacional para tratamento de incidentes que afetem simultaneamente múltiplos SEICs (ataques sistêmicos).

Exigência de backup offline e imutável para dados de SEICs.

Implementação de mecanismos de redundância e failover em sistemas de controle de tráfego, energia e saneamento para suportar falhas cibernéticas.

Implementação de sistemas de detecção de intrusão específicos para ambientes industriais (IDS/IPS OT) em operadores de infraestrutura.

Instrumentos legais que permitam intervenção regulatória rápida em caso de risco iminente de falha cibernética em SEICs.

SOC nacional operacional.

Treinamento obrigatório para provedores ou operadores de SEICs.

Uso de soluções de backup e recuperação testadas regularmente para dados e sistemas de SEICs.

E8-Resiliência-3

Resiliência da Infraestrutura de Comunicações e Internet

Detalhamento:

Aborda a existência de serviços e infraestrutura de Internet confiáveis no país, bem como processos de segurança rigorosos nos setores público e privado. Além disso, analisa o controle que o governo

pode ter sobre sua infraestrutura de Internet e a extensão em que as redes e os sistemas são terceirizados.

E8-Resiliência-3-A
Confiabilidade da Infraestrutura da Internet

Detalhamento:

Examina a confiabilidade e a proteção dos serviços e da infraestrutura da Internet nos setores público e privado.

Níveis de Maturidade:

Inicial:
Serviços e infraestrutura de Internet acessíveis e confiáveis podem não ter sido estabelecidos no país; se existirem, as taxas de adoção desses serviços são uma preocupação. Há pouca ou nenhuma supervisão nacional da infraestrutura de rede. Se redes e sistemas forem terceirizados, a confiabilidade dos provedores externos pode não ter sido considerada. Medidas de redundância de rede podem ser cogitadas, mas não de forma sistemática ou abrangente.

Fundamental:
Serviços e infraestrutura de Internet limitados estão disponíveis, porém, com baixos níveis de adoção e problemas de confiabilidade. A capacidade da infraestrutura de Internet dos setores público e privado de resistir a incidentes com interrupções mínimas é discutida por múltiplas partes interessadas, mas pode não ter sido plenamente abordada. O suporte para proteger a infraestrutura de Internet pode depender de assistência regional.

Básico:
Serviços de Internet confiáveis estão ocasionalmente disponíveis e utilizados. Os serviços de Internet são relativamente confiáveis para condução de transações de e-commerce e negócios eletrônicos e processos mínimos de autenticação estão estabelecidos. A infraestrutura nacional é gerida informalmente, com processos, papéis e responsabilidades definidos ad hoc e redundância limitada.

Médio:
Serviços de Internet confiáveis estão amplamente disponíveis e utilizados. Os serviços de Internet são amplamente confiáveis para condução de transações de e-commerce e negócios eletrônicos; processos adequados de autenticação estão estabelecidos. A tecnologia implantada e os processos de gestão da infraestrutura de Internet seguem padrões internacionais e boas práticas. A infraestrutura nacional é formalmente gerida, com processos documentados, papéis e responsabilidades definidos e alguma redundância.

Evoluído:
Avaliações regulares são conduzidas sobre tecnologias, processos de conformidade com padrões internacionais e diretrizes que atendem às necessidades nacionais diante de riscos emergentes. Existe aquisição eficaz e controlada de tecnologias críticas, bem como planejamento estratégico e processos de continuidade de serviços gerenciados.

Avançado:
A aquisição de tecnologias de infraestrutura é controlada de forma eficaz, com flexibilidade incorporada conforme a dinâmica do mercado. Custos de tecnologias de infraestrutura são continuamente avaliados e otimizados. Capacidades científicas, técnicas, industriais e humanas são sistematicamente mantidas, aprimoradas e perpetuadas para assegurar a resiliência independente do país. Eficiência otimizada está em vigor para mediar interrupções prolongadas dos sistemas.

Evidências

Infraestrutura DNS resiliente e redundante.

Planejamento governamental para garantir comunicações seguras e resilientes entre autoridades durante cibercrises que afetem telecomunicações.

E8-Resiliência-3-B
Monitoramento e Resposta

Detalhamento:

Examina se existem mecanismos para realizar avaliações de risco e monitorar a resiliência da rede nos setores público e privado.

Níveis de Maturidade:

Inicial:
Nenhuma avaliação de risco é conduzida por proprietários de infraestrutura de Internet para identificar ativos vulneráveis e priorizar ações de proteção. Não há monitoramento para detectar ocorrências de incidentes. Nenhum plano de resposta a incidentes está em vigor.

Fundamental:
Processos para desenvolvimento de avaliações de risco pelos proprietários de infraestrutura de Internet foram iniciados. Há monitoramento ad hoc de partes da infraestrutura de Internet, mas pode não ser abrangente. Planos de resposta a incidentes estão em desenvolvimento em alguns setores.

Básico:
Mecanismos ad hoc são estabelecidos nos setores público e privado para conduzir avaliações de risco, monitorar e testar a resiliência da rede e responder a incidentes.

Médio:
Mecanismos formais estão estabelecidos nos setores público e privado para conduzir avaliações de risco, monitorar e testar a resiliência da rede e responder a incidentes. Planos de resposta a incidentes estão implementados em ambos os setores, são regularmente testados e revisados.

Evoluído:
Recursos apropriados são alocados para integração de hardware, testes de estresse tecnológico, treinamento de pessoal, monitoramento, resposta e exercícios para testar planos de resposta. Riscos relacionados a tecnologias emergentes e convergentes são regularmente avaliados por proprietários de infraestrutura e por agências reguladoras de comunicações eletrônicas, orientando decisões de financiamento e prioridades.

Avançado:
Ativos em nível nacional podem atuar em cooperação com a comunidade internacional em crises ou incidentes transnacionais. Lições aprendidas de colaborações internacionais são utilizadas para evoluir capacidades de monitoramento e resposta. Há evidências de desenvolvimento de capacidades soberanas e inovadoras de monitoramento e resposta em antecipação a ameaças emergentes.

Evidências

Eliminação de pontos únicos de falha da infraestrutura.

Existência de SOCs (ou SIEMs similares) para o monitoramento e acompanhamento da disponibilidade da infraestrutura.

E8-Resiliência-4

Divulgação Responsável

Detalhamento:

Explora o estabelecimento de uma estrutura de divulgação responsável para o recebimento e disseminação de informações sobre vulnerabilidades em todos os setores e se existe capacidade suficiente para revisar e atualizar continuamente essa estrutura.

E8-Resiliência-4-A

Compartilhamento de informações sobre vulnerabilidades

Detalhamento:

Explora os mecanismos ou canais de compartilhamento de informações existentes sobre os detalhes técnicos das vulnerabilidades entre as partes interessadas.

Níveis de Maturidade:

Inicial:
Não existe forma informal de compartilhamento de informações entre as partes interessadas sobre detalhes técnicos de vulnerabilidades. Provedores de software e serviços geralmente carecem de capacidade para tratar relatórios de bugs e vulnerabilidades.

Fundamental:
Detalhes técnicos de vulnerabilidades são compartilhados informalmente entre as partes interessadas, que podem redistribuir as informações de maneira mais ampla. Provedores de software e serviços são capazes de tratar relatórios de vulnerabilidades, mas protocolos formais podem não existir.

Básico:
Mecanismos ou canais informais de compartilhamento de informações são utilizados para compartilhamento de vulnerabilidades entre as partes interessadas.

Médio:
Mecanismos ou canais formais de compartilhamento de informações estão estabelecidos para distribuir detalhes técnicos de vulnerabilidades entre as partes interessadas. Uma proporção significativa de vulnerabilidades em produtos e serviços é corrigida dentro de prazos definidos após sua descoberta.

Evoluído:
Mecanismos de compartilhamento de informações sobre vulnerabilidades são continuamente revisados e atualizados conforme as necessidades das partes interessadas afetadas e à luz de riscos emergentes. Todos os produtos e serviços afetados são rotineiramente atualizados dentro dos prazos definidos.

Avançado:
Processos são implementados para revisar e reduzir prazos sempre que possível. O país contribui para o debate e o desenvolvimento de boas práticas internacionais sobre o compartilhamento de informações de vulnerabilidades.

Evidências

Existência de campanhas em favor do compartilhamento de informações sobre incidentes e vulnerabilidades.

Monitoramento de estimativas de subnotificação de ciberincidentes e vulnerabilidades.

E8-Resiliência-4-B

Políticas, processos e legislação para a divulgação responsável de falhas de segurança

Detalhamento:

Explora a existência de uma política ou estrutura de divulgação responsável em organizações dos setores público e privado e o direito à proteção legal para aqueles que divulgam falhas de segurança.

Níveis de Maturidade:

Inicial:
A necessidade de uma política de divulgação responsável em organizações públicas e privadas, bem como o direito a proteções legais para quem divulga falhas de segurança, ainda não são reconhecidos.

Fundamental:
A necessidade de uma política de divulgação responsável em organizações públicas e privadas é reconhecida, mas políticas ou processos ainda não estão em vigor, ou estão apenas em desenvolvimento. O direito a proteções legais para quem divulga falhas de segurança é reconhecido, mas a legislação pode não existir ou estar em elaboração.

Básico:
Política ou estruturas de divulgação responsável são estimuladas em organizações públicas e privadas. As organizações implementam processos para receber e disseminar informações de vulnerabilidades de maneira responsável.

Médio:
Provedores de software e serviços comprometem-se a não tomar ações legais contra quem divulga informações de forma responsável. Uma política ou estrutura de divulgação responsável está implementada em organizações públicas e privadas, incluindo prazos de divulgação, cronogramas de resolução e necessidade de reconhecimento formal. As organizações possuem processos para receber e disseminar informações de vulnerabilidades de maneira responsável. O direito a proteções legais para quem divulga falhas de segurança de forma responsável está assegurado.

Evoluído:
Políticas e processos de divulgação responsável são continuamente revisados e atualizados conforme as necessidades das partes interessadas afetadas e em resposta a riscos emergentes. Análises técnicas das vulnerabilidades são publicadas e informações de orientação são disseminadas conforme papéis e responsabilidades definidos.

Avançado:
O país contribui ativamente para o debate e o desenvolvimento de estruturas e legislações internacionais sobre divulgação responsável e proteção legal de quem divulga falhas de segurança de forma ética.

Evidências

Ações para orientar cidadãos sobre seus direitos em casos de ciberincidentes que afetem SEICs.

Proteção legal para denunciantes de incidentes e vulnerabilidades.

Proteção legal para divulgadores responsáveis.