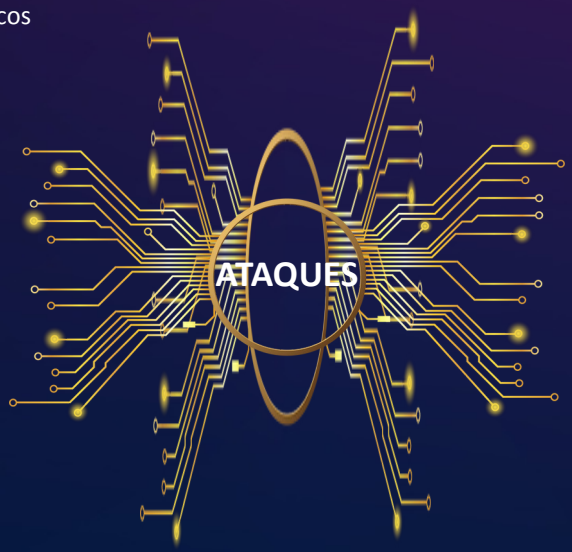
e-Ciber 2025-2028

Estatísticas de Ataques Cibernéticos no Brasil

- Tentativas de Ataques Cibernéticos:
  - Mais de 100 bilhões de tentativas de ataques cibernéticos registrados em 2022.
- Principais Tipos de Ataques:
  - Phishing e spear-phishing: 35%
  - Ransomware: 25%
  - DDoS (ataques de negação de serviço): 20%
  - Malware: 15%
  - Outros: 5%

Impactos Econômicos:

- Custo Global de Cibercrimes:
  - Estimado em 14% do PIB global.
- Prejuízo Estimado para o Brasil (2024):
  - Aproximadamente 1,5 trilhão de reais.
- Setores Mais Impactados:
  - Financeiro: Perdas significativas devido a fraudes e roubo de dados.
  - Saúde: Comprometimento de dados sensíveis e interrupções de serviços.
  - Infraestrutura Crítica: Energia, água, telecomunicações e transportes afetados.



Ameaças à Segurança:

- Cibercriminosos:
  - Individuais: Motivados por lucro, vingança ou diversão.
  - Organizados: Grupos que utilizam o ciberespaço para crimes financeiros e outros.
- Hacktivistas:
  - Ativistas que realizam ataques para promover causas específicas.
- Terroristas:
  - Usam o ciberespaço para angariar recursos, recrutar e espalhar propaganda.
- Nações-Estados:
  - Envolvidas em espionagem, projeção de poder e sabotagem.

ESTRATÉGIA NACIONAL DE CIBERSEGURANÇA (E-CIBER)

O objetivo geral da Estratégia Nacional de Cibersegurança (e-Ciber) 2025-2028 é fortalecer a cibersegurança do Brasil, promovendo a proteção da soberania nacional, garantindo os direitos fundamentais dos cidadãos, e assegurando a resiliência das infraestruturas críticas e serviços essenciais, por meio de ações coordenadas e integradas que envolvam o desenvolvimento tecnológico, a formação de profissionais, a pesquisa científica, e a cooperação internacional.

1 - Soberania e Interesses Nacionais

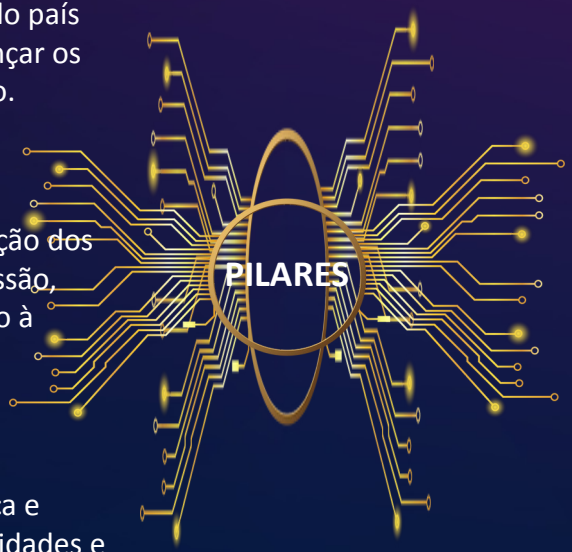
- Desenvolver capacidades tecnológicas e humanas nacionais para elevar o nível de cibersegurança do país de forma a proteger a soberania brasileira e avançar os interesses da sociedade brasileira no ciberespaço.

2 - Garantia de Direitos Fundamentais

- Alinhar a cibersegurança do país com a preservação dos direitos fundamentais, como liberdade de expressão, proteção de dados pessoais, privacidade e acesso à informação.

3- Defesa e Segurança Cibernética

- Estimular a adoção de medidas de cibersegurança e gestão de riscos para prevenir, mitigar vulnerabilidades e responder a ciberataques, bem como desenvolver mecanismos de governança, regulação, fiscalização e controle destinados a aprimorar a cibersegurança e a ciberresiliência.



4 – Cooperação e Atuação Internacional

- Desenvolver capacidades tecnológicas e humanas nacionais para elevar o nível de cibersegurança do país de forma a proteger a soberania brasileira e avançar os interesses da sociedade brasileira no ciberespaço.

5 – Cultura e Consciência em Cibersegurança

- Desenvolver a conscientização e a educação em cibersegurança na sociedade, criando uma mentalidade proativa, especialmente junto aos gestores públicos e privados, e incrementando a cooperação entre órgãos e entidades públicas e privadas em matéria de cibersegurança e combate ao cibercrime.

Pilar 1 – Soberania e Interesses Nacionais

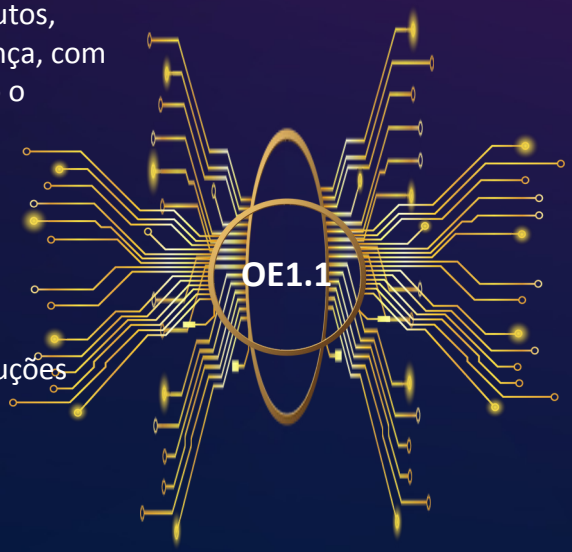
OE1.1: Promover o desenvolvimento de produtos, serviços e tecnologias nacionais destinados ao aprimoramento da cibersegurança e da ciberdefesa no país

AE1.1.1

- Desenvolver e ampliar programas de fomento e incentivo para o setor privado na oferta de produtos, serviços, tecnologias e inovação em cibersegurança, com atenção especial para PMEs e startups, incluindo o estabelecimento de PPPs.
- Responsável Principal: MDIC
- Responsáveis Adicionais: Sistema S e MCTI

AE1.1.2

- Priorizar a aquisição e o desenvolvimento de soluções tecnológicas nacionais.
- Responsável Principal: CC
- Responsáveis Adicionais: MGI



AE1.1.3

- Implementar sistema para troca segura de informações no âmbito da inteligência e da cibersegurança.
- Responsável Principal: CC

AE1.1.4

- Implementar capacidade para avaliação de conformidade em segurança de produtos, serviços e tecnologias de cibersegurança.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: GSI, ORSs, MD e MGI

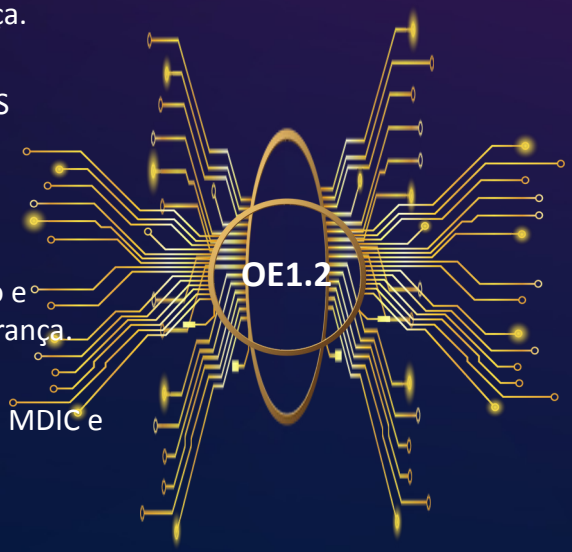
Pilar 1 – Soberania e Interesses Nacionais

OE1.2: Fomentar a formação e a capacitação técnico-profissional em cibersegurança em escala compatível com as necessidades nacionais.

AE1.2.1
- Fomentar programas de cursos técnico-profissionais, de graduação e de pós-graduação em cibersegurança.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: Sistema S, MEC e CAPES

AE1.2.2
- Desenvolver mecanismos de atração de talentos nacionais e internacionais, bem como a retenção e repatriação de pessoal qualificado em cibersegurança.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: MGI, MRE, ABIN, MCTI, MDIC e MTE

AE1.2.3
- Estabelecer parcerias com institutos brasileiros de pesquisa e desenvolvimento para ampliar as residências tecnológicas em cibersegurança.
- Responsável Principal: MCTI
- Responsáveis Adicionais: MDIC



AE1.2.4
- Fomentar a participação feminina e de populações subrepresentadas em cibersegurança.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: MCTI, MEC, Sistema S e RNP

AE1.2.5
- Ampliar a participação em fóruns, atividades acadêmicas e cursos, nacionais e internacionais, que permitam a difusão da mentalidade de cibersegurança.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: GSI, MEC, CAPES, MCTI, ORSs, MD, MGI e CGI/NIC

AE1.2.6
- Fomentar a concessão de bolsas de estudo e de intercâmbio, no Brasil e no exterior, para a formação de especialistas e professores em cibersegurança.
- Responsável Principal: CAPES
- Responsáveis Adicionais: FAPs

Pilar 1 – Soberania e Interesses Nacionais

OE1.3: Fomentar as atividades nacionais de pesquisa científica, de desenvolvimento tecnológico e de inovação sustentáveis relacionadas à cibersegurança.

AE1.3.1
- Fomentar linhas de pesquisa/projetos de pesquisa para graduação e pós-graduação stricto sensu relacionados à cibersegurança.
- Responsável Principal: MCTI
- Responsáveis Adicionais: CAPES

AE1.3.2
- Incluir a disciplina de cibersegurança no currículo dos cursos de graduação e pós-graduação.
- Responsável Principal: MEC/CNE

AE1.3.3
- Incrementar a base de conhecimento em cibersegurança no país.
- Responsável Principal: CGI/NIC
- Responsáveis Adicionais: GSI, MGI e ORSs

AE1.3.4
- Implantar Sistema de Gestão do Conhecimento nacional em cibersegurança.
- Responsável Principal: OGCiber

AE1.3.5
- Fomentar a realização de eventos e workshops para fortalecer a colaboração entre pesquisadores e profissionais da área de cibersegurança.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: Sociedades científicas, ORSs, MD, MGI, GSI, CGI/NIC e Associações de Empresas

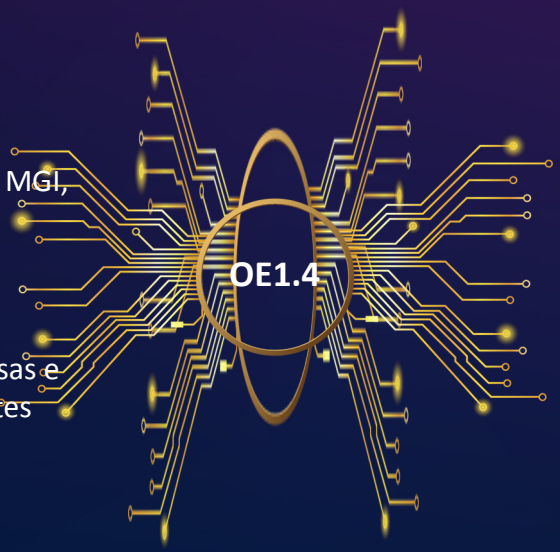
Pilar 1 – Soberania e Interesses Nacionais

OE1.4: Desenvolver capacidades relativas a tecnologias emergentes afetas à cibersegurança.

AE1.4.1
- Fomentar estudos continuados sobre o impacto/relação de tecnologias disruptivas e emergentes com a cibersegurança, bem como o desenvolvimento de capacidades considerando tais impactos.
- Responsável Principal: MCTI
- Responsáveis Adicionais: CGI/NIC, ORSs, MD, GSI, MGI, Sociedades científicas e ABIN

AE1.4.2
- Implementar programas de incentivo para empresas e profissionais envolvidos em tecnologias emergentes afetas à cibersegurança.
- Responsável Principal: MDIC
- Responsáveis Adicionais: MCTI

AE1.4.3
- Adotar algoritmo padronizado de criptografia quantum-resistant (pós-quânticos) no âmbito governamental.
- Responsável Principal: CC
- Responsáveis Adicionais: ABIN, GSI, MGI e MD



AE1.4.4
- Reduzir o débito tecnológico do país em tecnologias emergentes e disruptivas com ações governamentais afirmativas e incrementais relativas à cibersegurança.
- Responsável Principal: MCTI
- Responsáveis Adicionais: MDIC, Sistema S, CGI/NIC, ORSs, MD, MGI, GSI e FAPs

AE1.4.5
- Fomentar o desenvolvimento de propriedade intelectual e industrial centradas em tecnologias emergentes.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: MDIC e MCTI

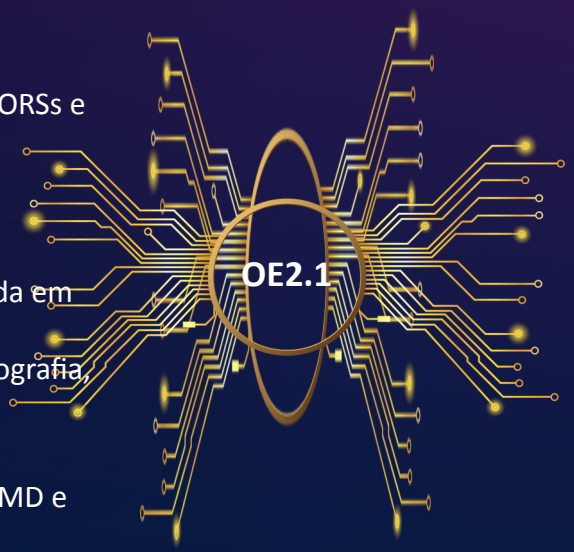
Pilar 2 – Garantia de Direitos Fundamentais

OE2.1: Garantir a confidencialidade, integridade, autenticidade e disponibilidade das soluções e dos dados utilizados para o processamento, armazenamento e transmissão eletrônica ou digital de informações.

AE2.1.1
- Estabelecer padrões mínimos de segurança de dados sensíveis para sistemas de informação.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: ANPD, GSI, ABIN, MGI, ORSs e MD

AE2.1.2
- Orientar a atuação segura no ciberespaço baseada em técnicas de vanguarda e nos padrões mínimos estipulados, tais como autenticação forte e criptografia, reforçando a proteção de dados sensíveis.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: ANPD, GSI, ABIN, MGI, MD e ORSs

AE2.1.3
- Expandir e aperfeiçoar processos, serviços e ferramentas disponibilizadas por meio de certificados digitais.
- Responsável Principal: MGI
- Responsáveis Adicionais: GSI, ORSs, MD e MGI



AE2.1.4
- Implementar mecanismos para garantir o sigilo na aquisição de sistemas, ferramentas e softwares relativos à cibersegurança e à ciberdefesa nacionais.
- Responsável Principal: MGI
- Responsáveis Adicionais: GSI, MD, AGU, CGU

AE2.1.5
- Ampliar a interoperabilidade e troca de informações entre os entes da comunidade de cibersegurança.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: MGI, GSI, CGI/NIC, ORSs e MD

Pilar 2 – Garantia de Direitos Fundamentais

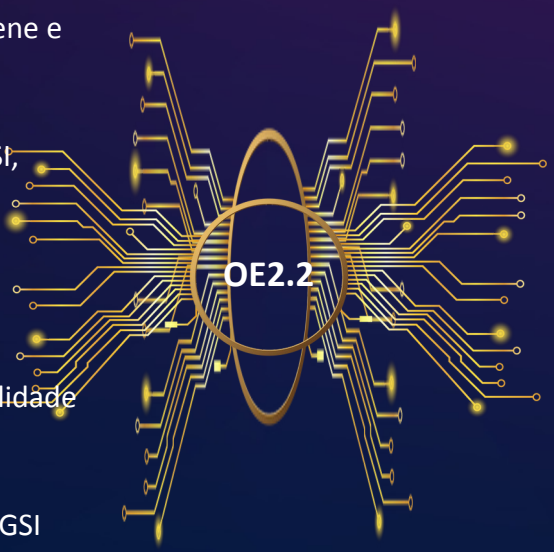
OE2.2: Promover a atuação consciente e a proteção do indivíduo no ciberespaço, especialmente de grupos mais vulneráveis, tais como crianças, adolescentes e idosos.

AE2.2.1

- Criação de campanhas de educação em ciber-higiene e privacidade para crianças, adolescentes e idosos.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: MEC, ORSs, MD, MGI, GSI, MJSP e CGI/NIC

AE2.2.2

- Ampliar a segurança de iniciativas de interoperabilidade de dados e de canais digitais unificados.
- Responsável Principal: MGI
- Responsáveis Adicionais: ANPD, ORSs, MD, MGI e GSI



AE2.2.3

- Implementar programa de letramento em privacidade e segurança da informação com uso de mídias sociais e recursos de comunicação de massa.
- Responsável Principal: CC
- Responsáveis Adicionais: SECOM, ANPD, CGI/NIC, ORSs, MGI, MD e GSI

AE2.2.4

- Incluir na Base Nacional Comum Curricular o eixo riscos no ambiente digital, práticas de ciber-higiene, cidadania digital, entre outros, desenvolvendo e disponibilizando materiais e treinamentos para professores e alunos.
- Responsável Principal: MEC/CNE

Pilar 2 – Garantia de Direitos Fundamentais

OE2.3: Contribuir para a prevenção e o combate ao cibercrime e às ações maliciosas no ciberespaço por meio da atuação multissetorial integrada e com pleno respeito ao estado de direito.

AE2.3.1

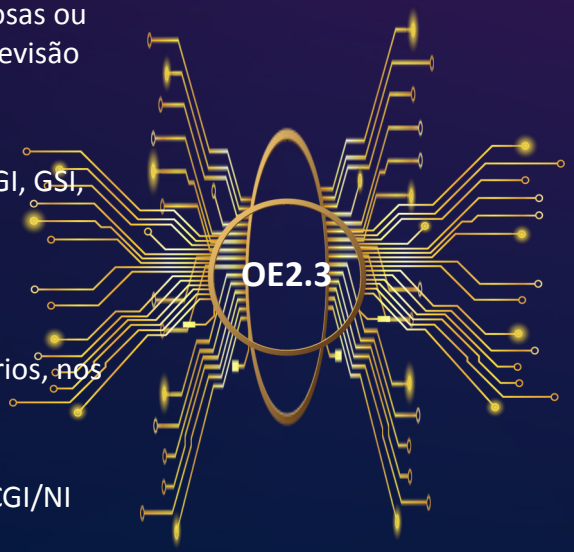
- Estimular a elaboração e acompanhar os anteprojetos de Lei necessários para definir as práticas maliciosas ou ilícitas ainda não tipificadas ou que demandem revisão da redação do tipo penal ou da pena.
- Responsável Principal: MJSP
- Responsáveis Adicionais: OGCiber, ORSs, MD, MGI, GSI, CGI/NIC e CNMP, CNJ

AE2.3.2

- Estimular a identificação e autenticação de usuários, nos termos da legislação vigente.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: GSI, ORSs, MGI, MD e CGI/NI

AE2.3.3

- Fomentar capacitação e alocação de recursos para as polícias judiciárias e outros órgãos de persecução penal e repressão ao cibercrime.
- Responsável Principal: MJSP
- Responsáveis Adicionais: GSI, OGCiber, CGI/NIC e Academias de Polícia Estaduais e MGI



AE2.3.4

- Estimular a criação e aprimoramento de delegacias específicas para tratar de cibercrimes, bem como de canais para sua notificação.
- Responsável Principal: MJSP
- Responsáveis Adicionais: GSI e Polícias Estaduais

AE2.3.5

- Fomentar a divulgação e a utilização dos mecanismos previstos nos instrumentos internacionais, em particular a Convenção de Budapeste.
- Responsável Principal: MJSP
- Responsáveis Adicionais: MRE

Pilar 2 – Garantia de Direitos Fundamentais

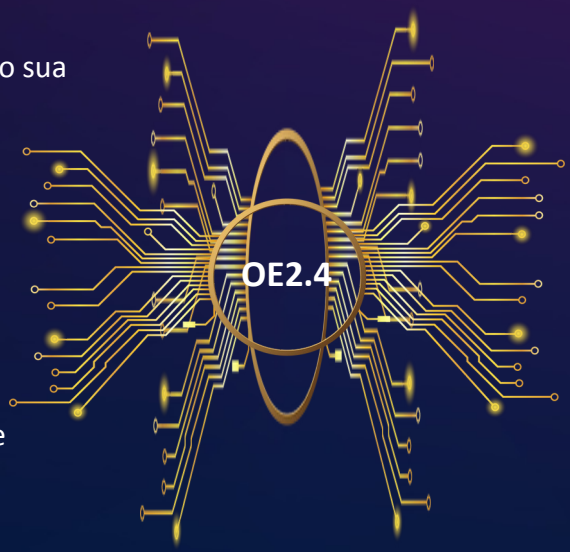
OE2.4: Nortear as atividades de cibersegurança para garantir um futuro resiliente, fortalecendo a cidadania e a prosperidade econômica do país.

AE2.4.1

- Atuar para aumentar a prioridade do tema cibersegurança na agenda nacional, considerando sua transversalidade.
- Responsável Principal: CNCiber
- Responsáveis Adicionais: OGCiber, Instituições participantes do CNCiber, ORSs, MGI, MD e GSI

AE2.4.2

- Criar um selo nacional de acreditação do nível de cibersegurança de ciberativos.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: ORSs, MGI, MD, GSI e MDIC/INMETRO



AE2.4.3

- Produzir um diagnóstico nacional sobre o funcionamento do ecossistema de comercialização e troca ilícita de dados e de vulnerabilidades a partir da articulação dos esforços existentes.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: ABIN, GSI, MGI, MJSP e MD

AE2.4.4

- Verificar a necessidade da exigência de seguro em proteção a ciberincidentes para provedores de serviços essenciais.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: ORSs, MGI, MD e GSI

Pilar 3 – Prevenção, Tratamento e Resposta a Ciberincidentes

OE3.1: Estimular a adoção de medidas de proteção cibernética e de gestão de riscos para prevenir, mitigar vulnerabilidades e responder a ciberincidentes e ciberataques.

AE3.1.1

- Fomentar a segurança e ciberresiliência de infraestruturas críticas e serviços essenciais.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: ORSs, MD, GSI, MGI e CGI/NIC

AE3.1.2

Estimular os entes com capacidade regulatória para promoverem, em coordenação com o órgão de governança da cibersegurança, a gestão de ciberriscos e adoção de medidas de ciberproteção e de resposta a incidentes nos seus respectivos setores.

- Responsável Principal: OGCiber
- Responsáveis Adicionais: ORSs, MD, GSI, MGI e CGI/NIC

AE3.1.3

Estabelecer um "Mecanismo Nacional de Notificação de Ciberincidentes" unificado que receba a comunicação e facilite a gestão de ciberincidentes.

- Responsável Principal: OGCiber
- Responsáveis Adicionais: ORSs, MD, GSI, MGI e CGI/NIC

AE3.1.4

- Estimular a discussão quanto à adoção de processos para Divulgação Coordenada de Vulnerabilidades (CVD).
- Responsável Principal: OGCiber
- Responsáveis Adicionais: ORSs, MD, GSI, MGI e CGI/NIC

Pilar 3 – Prevenção, Tratamento e Resposta a Ciberincidentes

OE3.2: Desenvolver mecanismos de governança, regulação, fiscalização e controle destinados a aprimorar a segurança e a resiliência cibernéticas de estruturas, produtos e serviços, com atenção especial às PMEs.

AE3.2.1

- Propor órgão de governança da cibersegurança nacional responsável pela coordenação, e pela criação de mecanismos de regulação, fiscalização e controle dessa atividade, contemplando a segurança de ICs e serviços essenciais e a gestão de cibercrises relevantes.
- Responsável Principal: CNCiber
- Responsáveis Adicionais: GSI, CC, MGI e MF

AE3.2.2

- Promover exercícios e simulações setoriais e multissetoriais regulares voltados ao aprimoramento da ciberresiliência de infraestruturas críticas e serviços essenciais de interesse nacional.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: ORSs, MD, GSI e MGI

AE3.2.3

- Atingir, ao menos, o nível mediano em todos os quesitos do diagnóstico modelo de maturidade em cibersegurança recomendados internacionalmente.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: ORSs, MD, GSI e MGI

AE3.2.4

- Propor modelo orçamentário sustentável e garantir recursos suficientes para a criação e continuidade do órgão de governança de cibersegurança nacional.
- Responsável Principal: CNCiber
- Responsáveis Adicionais: GSI, CC, MGI, MF e MPO

AE3.2.5

- Desenvolver iniciativas para apoiar as PMEs na gestão dos ciberriscos.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: ORSs, MD, MGI, GSI, MDIC, Sistema S

Pilar 3 – Prevenção, Tratamento e Resposta a Ciberincidentes

OE3.3: Incrementar a prontidão, a resiliência e a capacidade relacional das organizações públicas e privadas, fortalecendo a comunicação multissetorial, para o enfrentamento a ciberincidentes e ciberataques.

AE3.3.1

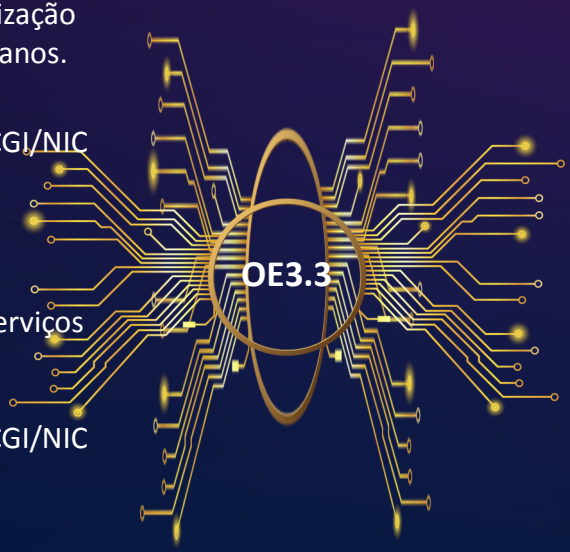
- Incentivar o desenvolvimento de planos de contingência institucionais, setoriais e multissetoriais, e a realização de testes e simulações para verificação desses planos.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: GSI, ORSs, MD, MGI e CGI/NIC

AE3.3.2

- Promover o desenvolvimento de CSIRT setoriais (governo e setores de infraestruturas críticas e serviços essenciais), inclusive por meio de ISACs.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: GSI, ORSs, MD, MGI e CGI/NIC

AE3.3.3

- Incentivar o compartilhamento de informações intrasetor, intersetor e interagência.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: GSI, ORSs, MD, MGI, MJSP e CGI/NIC



AE3.3.4

- Privilegiar iniciativas que incrementem a ciberresiliência e a continuidade das operações em infraestruturas críticas e serviços essenciais, em especial quanto à adoção de frameworks de cibersegurança em TO, além da TI.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: GSI, ORSs, MD, MGI e CGI/NIC

AE3.3.5

- Estimular a criação de equipes de resposta rápida a ciberincidentes e de laboratórios especializados, tanto a nível federal quanto estaduais, bem como setoriais.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: GSI, ORSs, MD, MGI, MJSP e CGI/NIC

Pilar 3 – Prevenção, Tratamento e Resposta a Ciberincidentes

OE3.4: Aprimorar continuamente a legislação e os normativos afetos à cibersegurança a partir de um melhor entendimento das ameaças decorrentes da evolução tecnológica.

AE3.4.1

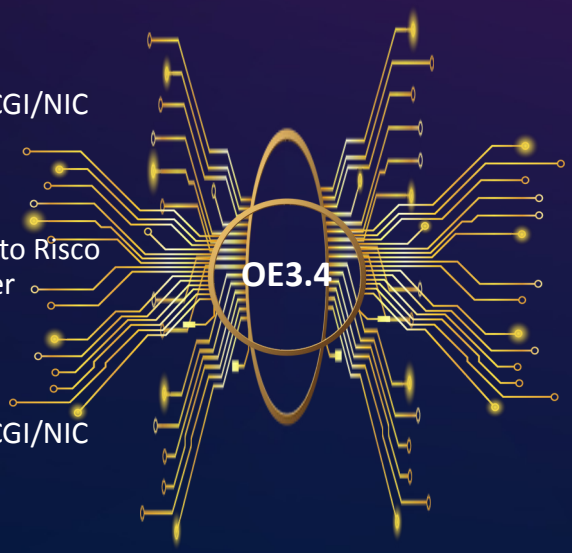
- Incentivar o desenvolvimento e a constante atualização de regulação setorial dedicada à cibersegurança.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: GSI, ORSs, MGI, MD e CGI/NIC

AE3.4.2

- Desenvolver e manter atualizada uma Lista de Alto Risco de Cibersegurança (alvos e vulnerabilidades) a ser utilizada como fundamentação para a gestão de ciberriscos setoriais.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: GSI, ORSs, MGI, MD e CGI/NIC

AE3.4.3

- Fomentar a estruturação das informações setoriais com o mapeamento dos macroprocessos cibernéticos, tanto técnicos quanto operacionais.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: GSI, ORSs, MGI, MD e CGI/NIC



AE3.4.4

- Estimular a criação e valorização de carreiras ou de especialidades nas carreiras de Estado voltadas à cibersegurança e tecnologia da informação, inclusive fomentando o intercâmbio entre o pessoal civil, militar e de segurança pública.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: CC, MGI, MD, MJSP e ORSs

AE3.4.5

- Harmonizar as diferentes regulações em cibersegurança.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: GSI, ORSs, MGI, MD e CGI/NIC

Pilar 4 – Cooperação e Atuação Internacional

OE4.1: Incrementar atividades de cooperação internacional para fortalecer a cibersegurança e a ciberresiliência brasileiras, além do combate ao cibercrime.

AE4.1.1

- Desenvolver cooperação no âmbito da aplicação de mecanismos de combate ao cibercrime de que o Brasil seja parte.
- Responsável Principal: MRE
- Responsáveis Adicionais: OGCiber e MJSP

AE4.1.2

- Mapear e coordenar continuamente a participação de instituições governamentais em iniciativas e mecanismos internacionais de interesse do Estado brasileiro voltados à ciberresiliência e ao combate ao cibercrime.
- Responsável Principal: MRE
- Responsáveis Adicionais: OGCiber, MJSP, MGI, MD, ORSs, GSI e CGI/NIC

AE4.1.3

- Defender a instituição e o fortalecimento de mecanismo permanente único no âmbito da AGNU para endereçar cibersegurança.
- Responsável Principal: MRE
- Responsáveis Adicionais: OGCiber, ORSs, MGI, GSI e CGI/NIC

AE4.1.4

- Fomentar o estabelecimento e a implementação de instrumentos intergovernamentais na área da cibersegurança que facilitem a cooperação e o intercâmbio de melhores práticas.
- Responsável Principal: MRE
- Responsáveis Adicionais: OGCiber, ORSs, MD, MGI, GSI e CGI/NIC

Pilar 4 – Cooperação e Atuação Internacional

OE4.2: Intensificar o intercâmbio de informações e promover a construção de capacidades em cibersegurança com parceiros internacionais.

AE4.2.1

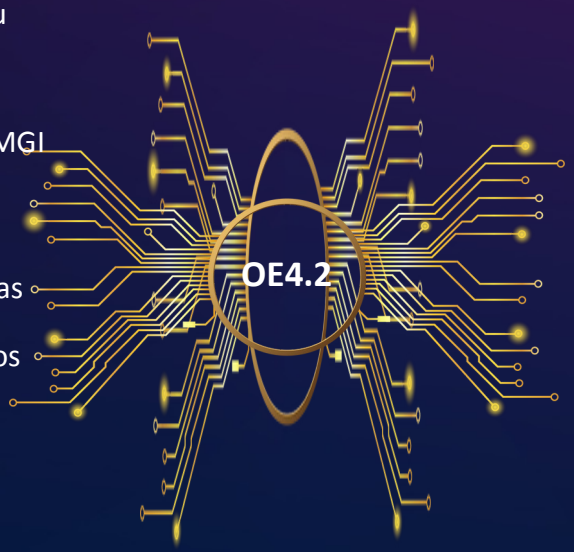
- Fortalecer a capacidade de cibersegurança de países do entorno regional, seja por iniciativas bilaterais ou multilaterais.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: MRE, ORSs, MD, GSI e MGI

AE4.2.2

- Ampliar e fomentar a cooperação e integração das agências brasileiras com suas contrapartes internacionais, no combate ao cibercrime e ilícitos cometidos no ciberespaço.
- Responsável Principal: MJSP
- Responsáveis Adicionais: MRE, GSI e OGCiber

AE4.2.3

- Ampliar e fomentar a capacidade de cooperação e integração das agências brasileiras com suas contrapartes internacionais.
- Responsável Principal: MRE
- Responsáveis Adicionais: OGCiber, ORSs, MD, GSI e MGI



AE4.2.4

- Promover a cooperação entre instituições acadêmicas nacionais e estrangeiras.
- Responsável Principal: MRE
- Responsáveis Adicionais: CAPES, CNPq e OGCiber

AE4.2.5

- Estabelecer atividades de capacitação em nível nacional com participação e apoio de organizações internacionais.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: CAPES, MCTI, MRE, MJSP, MGI, GSI e MD

Pilar 4 – Cooperação e Atuação Internacional

OE4.3: Ampliar a atuação coordenada brasileira nos debates regionais, plurilaterais, multilaterais e multissetoriais, com vistas a influenciar a formulação de padrões, normas, regras e princípios internacionais para o ciberespaço.

AE4.3.1

- Ampliar a participação ativa nas diversas organizações e fóruns que tratam de cibersegurança.
- Responsável Principal: MRE
- Responsáveis Adicionais: OGCiber, ORSs, MD, MGI, GSI e CGI/NIC

AE4.3.2

- Publicar uma Política Internacional para o ciberespaço.
- Responsável Principal: MRE
- Responsáveis Adicionais: GSI

AE4.3.3

- Promover e ampliar a participação multissetorial brasileira em reuniões e eventos multilaterais.
- Responsável Principal: MRE
- Responsáveis Adicionais: OGCiber, ORSs, GSI, MD, MGI, MCTI, MJSP e CGI/NIC

AE4.3.4

- Participar de adestramentos singulares, conjuntos e combinados, visando a colaboração técnica e operacional e a integração de dados e informações de interesse nacional.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: MRE, MD, MGI, GSI, CGI/NIC e ORSs

AE4.3.5

- Apoiar o fortalecimento da governança multilateral em cibersegurança e a construção gradual e cumulativa de normas e entendimentos comuns sobre cibersegurança.
- Responsável Principal: MRE
- Responsáveis Adicionais: OGCiber, ORSs, GSI, MD e MGI

Pilar 5 – Cultura e Conscientização em Cibersegurança

OE5.1: Desenvolver a conscientização e a educação em cibersegurança na sociedade.

AE5.1.1

- Expandir a conscientização da relevância do setor cibernético.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: ORSs, MD, MGI, GSI, MCTI, MEC e CGI/NIC

AE5.1.2

- Realizar campanhas nacionais para a conscientização em cibersegurança incluindo as necessidades de grupos vulneráveis.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: MEC, Sistema S, ORSs, MD, MGI, GSI e CGI/NIC

AE5.1.3

- Capacitar professores e formadores em cibersegurança, por meio de programas de treinamento específicos.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: MEC, Sistema S, ORSs, MD, MGI, GSI e CGI/NIC

AE5.1.4

- Criar iniciativas de capacitação técnica e profissionalizante voltada à formação de profissionais em cibersegurança.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: MEC, MCTI, Sistema S, ORSs, MD, MGI e CGI/NIC

Pilar 5 – Cultura e Conscientização em Cibersegurança

OE5.2: Desenvolver a mentalidade em cibersegurança junto aos gestores públicos e privados.

AE5.2.1

- Estimular a organização de fóruns, atividades acadêmicas e cursos voltados a gestores públicos e privados para a difusão da cultura da cibersegurança.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: Sistema S, MGI, GSI, ORSs, MD e CGI/NIC

AE5.2.2

- Incentivar a adoção de cláusulas com padrões mínimos de cibersegurança em contratos internacionais que envolvam aquisição ou oferta de produtos e serviços.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: MJSP, MRE, ORSs, GSI, MD, MGI e AGU

AE5.2.3

- Elaborar modelos de planos de conformidade em cibersegurança flexíveis (que permitam a adoção por organizações de diversos portes e sob a ameaça de diferentes riscos) para implementação por pessoas jurídicas públicas e privadas.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: ORSs, MD, MGI, GSI, MJSP e CGI/NIC

AE5.2.4

- Adotar uma cultura de “confiança-zero” para todos os serviços digitais do poder público.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: CC, ORSs, MGI, MD e GSI

Pilar 5 – Cultura e Conscientização em Cibersegurança

OE5.3: Incrementar a intensidade e a escala da cooperação entre órgãos e entidades, públicas e privadas, em matéria de cibersegurança e combate ao cibercrime.

AE5.3.1

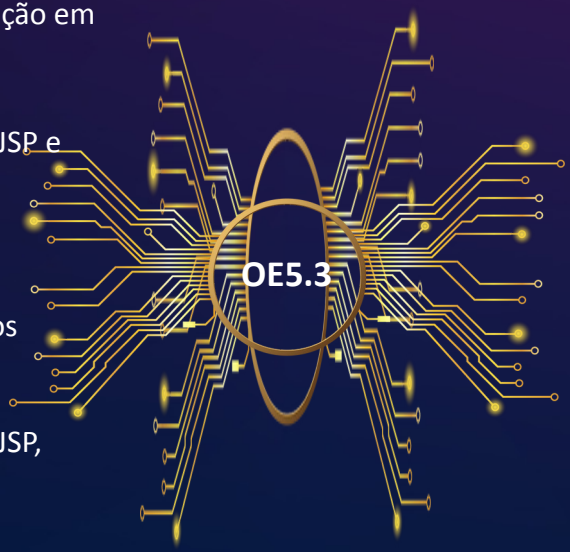
- Organizar atividades intersetoriais e interagências para promover a construção de confiança e a cooperação em matéria de cibersegurança.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: ORSs, MGI, MD, GSI, MJSP e CGI/NIC

AE5.3.2

- Expandir os serviços de apoio às vítimas de ilícitos praticados no ambiente cibernético.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: ORSs, MGI, MD, GSI, MJSP, AGU, Defensorias e CGI/NIC

AE5.3.3

- Estabelecer iniciativas governamentais ou federativas para prover orientação e apoio para pequenas e médias empresas em cibersegurança, inclusive com seguro contra ciberincidentes e apoio para a retomada das atividades.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: ORSs, MGI, MD, GSI, MJSP, AGU, SUSEP, Sistema S e CGI/NIC



AE5.3.4

- Desenvolver e ampliar estratégias interagências e multissetoriais para a prevenção e repressão de fraudes digitais.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: ORSs, MGI, MD, GSI, MJSP e CGI/NIC

AE5.3.5

- Estabelecer parcerias e integração multissetoriais para o desenvolvimento de ações de cibersegurança e ciberdefesa.
- Responsável Principal: OGCiber
- Responsáveis Adicionais: ORSs, MGI, MD, GSI, MJSP e CGI/NIC