5º Webinário para ETIRs da REGIC

Horário	Atividade
10:00	Boas-vindas e Abertura
10:05	REGIC Possibilidades Novidades
10:50	Intervalo
11:00	Perguntas e Respostas
11:25	Considerações Finais
11:30	Encerramento

5º Webinário para Equipes de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) dos órgãos e entidades participantes da Rede Federal de Gestão de Incidentes Cibernéticos (REGIC)

Brasília, 25 de Fevereiro de 2025

Secretaria de Segurança da Informação e Cibernética
Gabinete de Segurança Institucional da Presidência da República

Daniel Maier de Carvalho

Presidência da República
Gabinete de Segurança Institucional
Secretaria de Segurança da Informação e Cibernética
Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov)

Coordenador- Geral

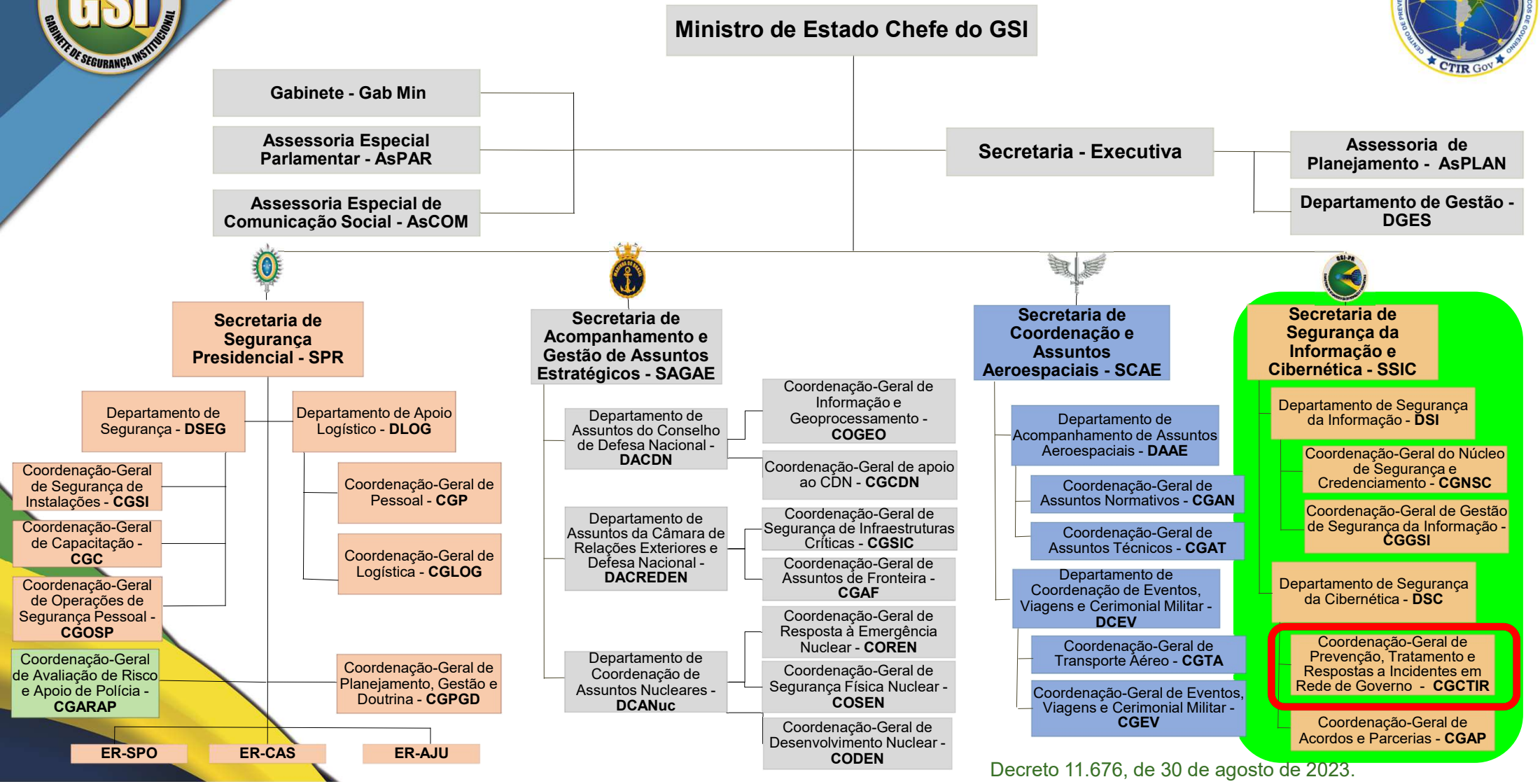
Agenda

1. Introdução
2. Desenvolvimento
   a. Apresentação do CTIR Gov
   b. Números de 2024
   c. Concepção operacional da REGIC
   d. Perspectivas 2025
3. Conclusão

Introdução

Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo – CTIR Gov

Estrutura Organizacional do GSI-PR



Decreto 11.676, de 30 de agosto de 2023.

ESTRUTURA DA SSIC

Decreto 11.676, de 30 de agosto de 2023.

CTIR Gov - Serviços

CSIRT de Responsabilidade Nacional de Governo (Coordenação)

- Gestão de Incidentes
- Gestão de Vulnerabilidades
  - Apoio SSIC/GSI
- Comunicação e Distribuição
  - Assessoramento Técnico
- Coordenação da REGIC
  - Cooperação Internacional
- Treinamento e Capacitação

Números – CTIR Gov - 2024

CTIR Gov – Resumo ações 2024

INCIDENTES
9490 Incidentes tratados

VULNERABILIDADES
5164
Vulnerabilidades notificadas

CAPACITAÇÃO
4 Webinários
TTX
Treinamento
Teórico-Prático

CONSCIENTIZAÇÃO
Ascender Defesas
CTIR em números

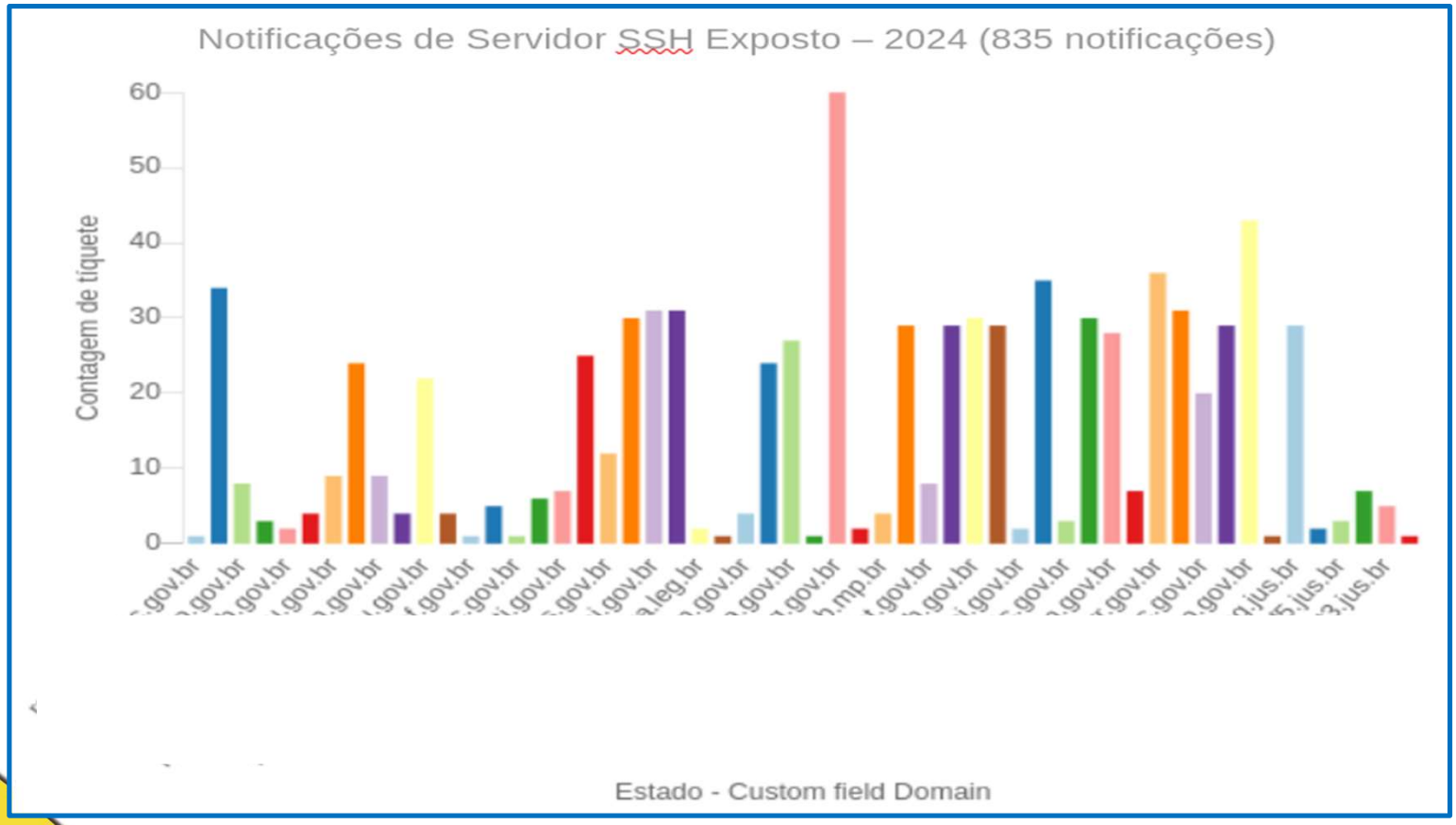
COORDENAÇÃO
Coordenação de incidentes graves

G20
272 notificações IC
10 visitas técnicas

www.ctir.gov.br

NOTIFICAÇÕES

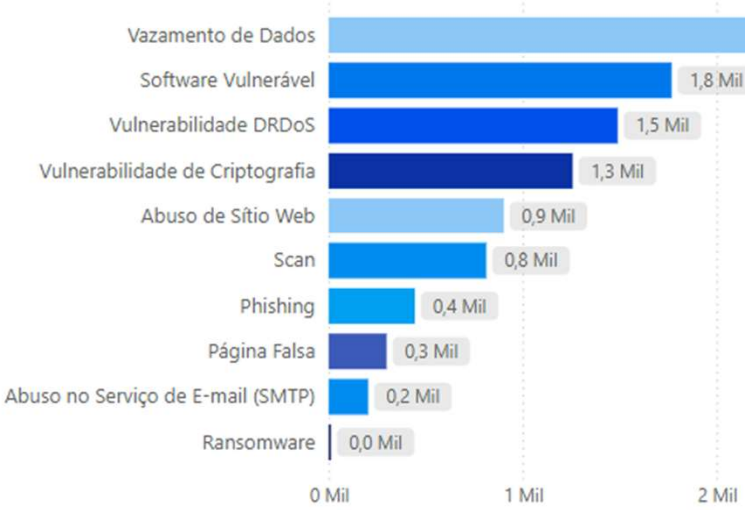
Notificações SSH exposto

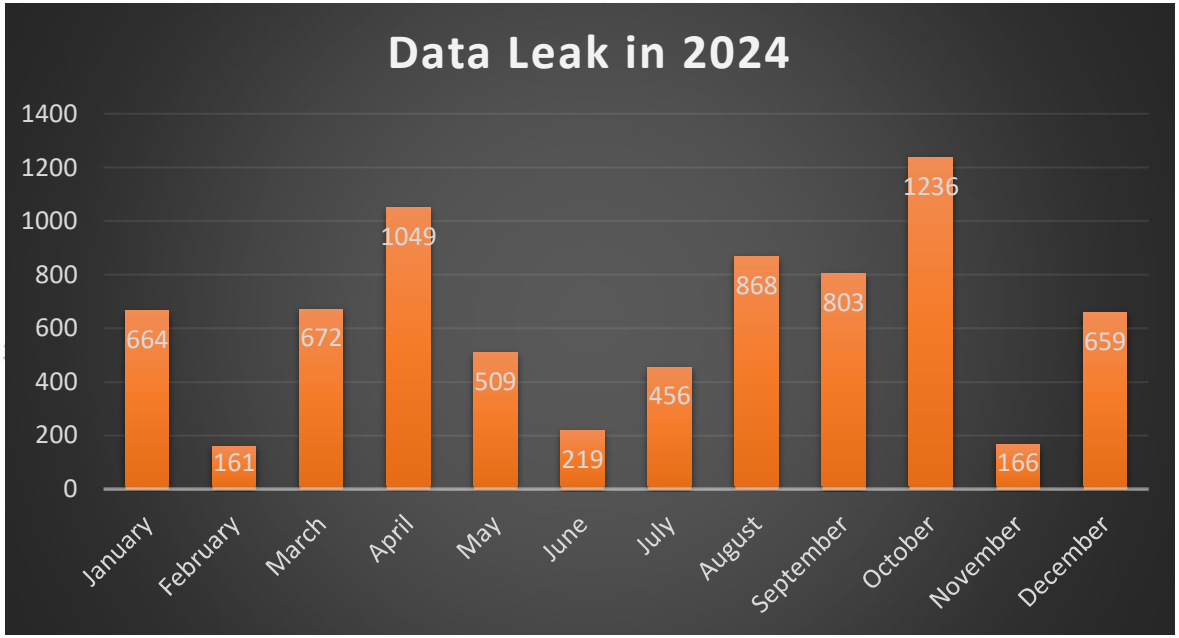


VAZAMENTO DE DADOS

CTIR GOV: vazamento de dados reportados

"as credenciais de administradores de rede e de alta gerência são as mais visadas"





"em 2024, os vazamentos de dados ultrapassaram os abusos de sites e os ataques de negação de serviço"

ABUSO DE SERVIDORES WEB

Reputação dos sites gov.br

Criminosos colocam links de apostas e abuso de menores em sites de governo

Hackers estariam utilizando domínios para aumentar a visibilidade de sites de apostas

Imagem: Nathana Rebouças/Unsplash

Home › Matérias › Internet

Bets ilegais se "escondem" em sites do governo para aparecer no Google

Por André Lourenti Magalhães • Editado por Bruno De Blasi | 25/11/2024 às 07:57 • Atualizado 26/11/2024 às 09:41

gov.br | Gabinete de Segurança Institucional da Presidência da República | Entrar com gov.br

CTIR Gov - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo

Assuntos > Alertas e Recomendações > Recomendações > 2024 > RECOMENDAÇÃO 08/2024

RECOMENDAÇÃO 08/2024

Abuso de servidores WEB para promoção de páginas em ferramentas de pesquisa

Compartilhe:

Publicado em 31/12/2024 12h06

[TLP:CLEAR]

1. Foi identificado um aumento no número de incidentes de cibersegurança envolvendo sítios governamentais, de estados e de municípios. Trata-se de promoção de termos e sítios alheios à administração pública em resultados de pesquisa das principais ferramentas de busca utilizadas na internet.

2. Esse comportamento malicioso emprega conceitos de otimização de ferramentas de busca, "*search engine optimization*" *(SEO)* para aumentar a visibilidade de sites e de termos de pesquisa, isto é, o "*search engine results pages*" *(SERP)*. Tal fato ocorre porque as ferramentas de busca atribuem maior valoração às informações oriundas de sítios institucionais ou governamentais.

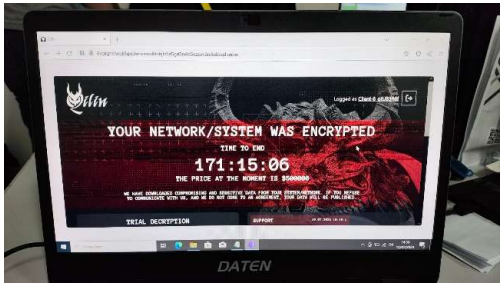
3. O ataque consiste na instalação de códigos maliciosos nos servidores com protocolos *HTTP/HTTPS*. Esses códigos são responsáveis por injetar dinamicamente os termos promovidos no conteúdo fornecido pelo servidor. Com isso as ferramentas de busca indexam o conteúdo da campanha relacionado ao site vitimado.

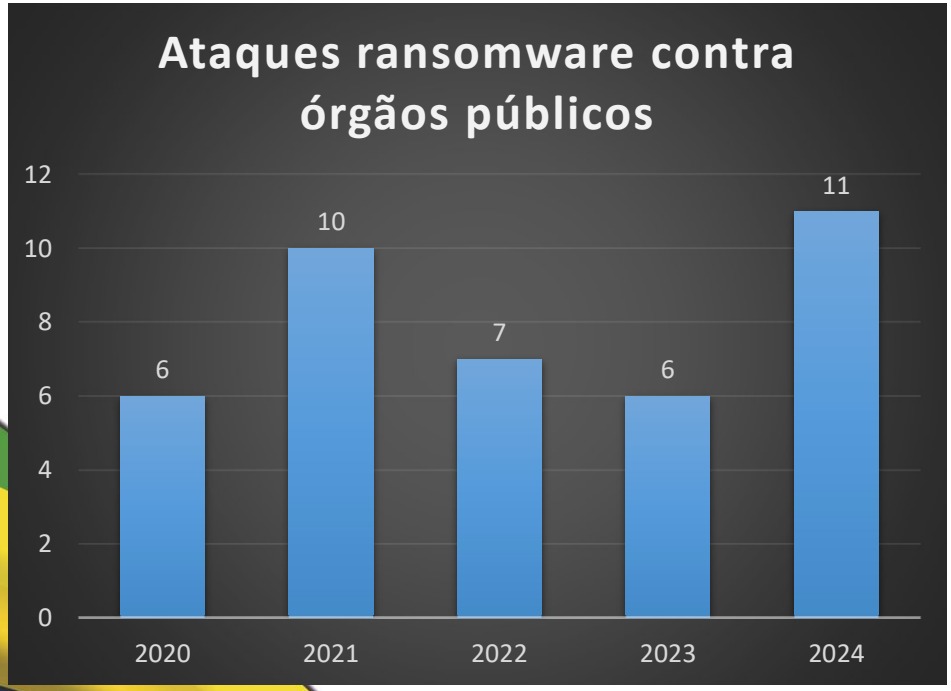
4. É importante ressaltar que as páginas disponibilizadas por esses servidores podem permanecer inalteradas no sistema de arquivos. O conteúdo é entregue dinamicamente pelo servidor comprometido e não há redirecionamento para outras páginas.

5. Esse abuso de páginas *WEB* pode levar o público em geral a associar, de forma equivocada, as informações de seu *site*/domínio com a promoção de atividades deletérias.

6. Neste sentido, o Centro de Tratamento e Resposta a Incidentes Cibernético de Governo - CTIR Gov recomenda que os integrantes da Rede Federal de Gestão de Incidentes Cibernéticos - ReGIC monitorem sistematicamente os resultados de ferramentas de pesquisa relacionados aos seus sítios *WEB*.

RANSOMWARE





Em 2024, o Brasil estava entre os 10 países mais atacados do mundo. Em setembro, era o 5º com 10 organizações afetadas.

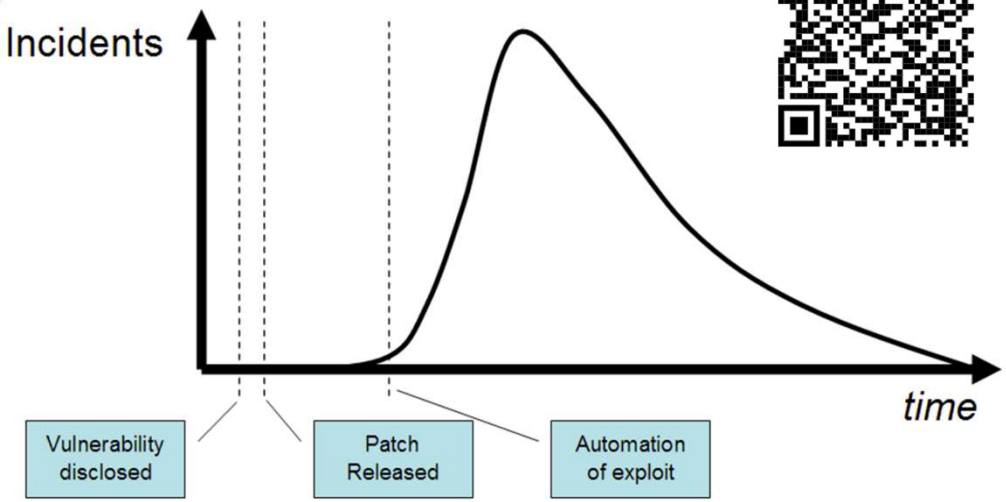
Diferentes setores afetados, o que indica a natureza abrangente da ameaça: Indústria, Tecnologia, Saúde, Governo, Finanças...

Há exploração de novos CVEs (horas após a publicação do POC) e antigos (CVE de 2017). Destaca-se engenharia social e phishing como vetor de ataque inicial.

Empresas com receitas anuais em torno de US$ 5 milhões são vítimas 2x mais frequentes do que 30-50 Mi (5x do que 100 Mi)

IMPORTÂNCIA DA PRESTEZA

Effectiveness of Proactive CSIRT Services



Coordinated vulnerability disclosure – CVD

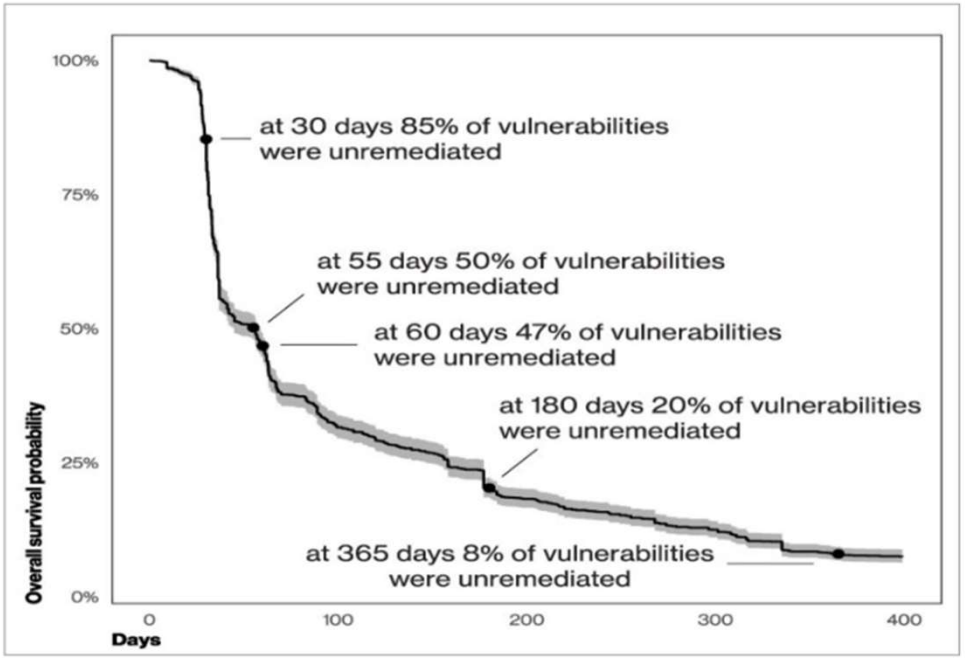
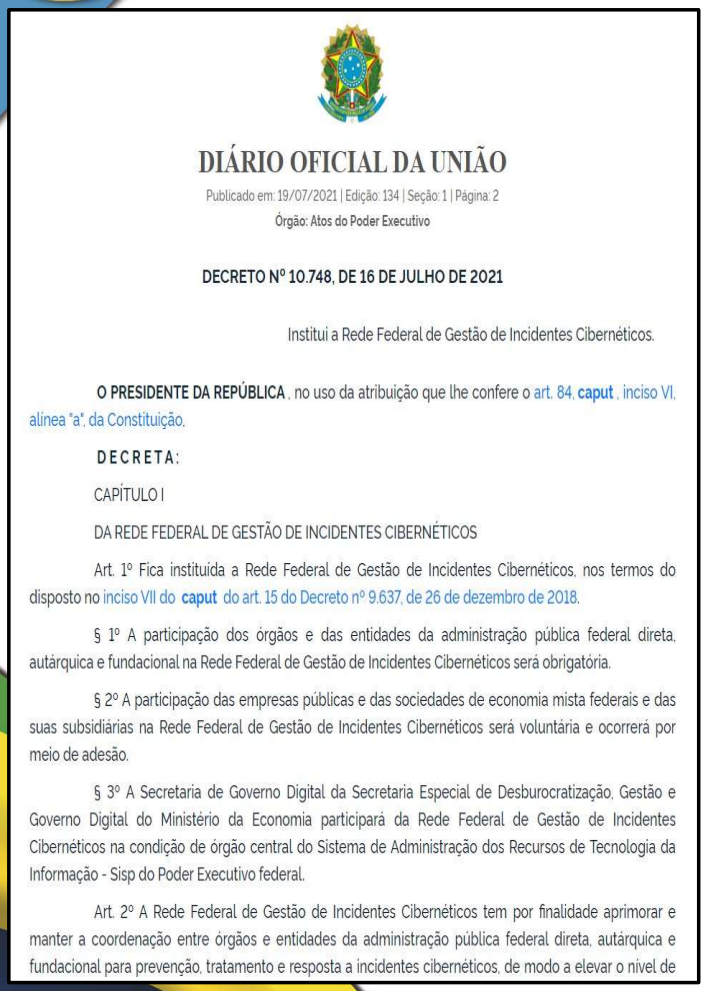


Figure 3. Timeliness of Remediation – Verizon 2024 DBIR

Rede Federal de Gestão de Incidentes Cibernéticos – REGIC (Dec. 10.748/21)

REDE FEDERAL DE GESTÃO DE INCIDENTES CIBERNÉTICOS (REGIC)



DIÁRIO OFICIAL DA UNIÃO

Publicado em: 19/07/2021 | Edição: 134 | Seção: 1 | Página: 2

Órgão: Atos do Poder Executivo

DECRETO Nº 10.748, DE 16 DE JULHO DE 2021

Institui a Rede Federal de Gestão de Incidentes Cibernéticos.

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 84, caput, inciso VI, alínea "a", da Constituição,

DECRETA:

CAPÍTULO I

DA REDE FEDERAL DE GESTÃO DE INCIDENTES CIBERNÉTICOS

Art. 1º Fica instituída a Rede Federal de Gestão de Incidentes Cibernéticos, nos termos do disposto no inciso VII do caput do art. 15 do Decreto nº 9.637, de 26 de dezembro de 2018.

§ 1º A participação dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional na Rede Federal de Gestão de Incidentes Cibernéticos será obrigatória.

§ 2º A participação das empresas públicas e das sociedades de economia mista federais e das suas subsidiárias na Rede Federal de Gestão de Incidentes Cibernéticos será voluntária e ocorrerá por meio de adesão.

§ 3º A Secretaria de Governo Digital da Secretaria Especial de Desburocratização, Gestão e Governo Digital do Ministério da Economia participará da Rede Federal de Gestão de Incidentes Cibernéticos na condição de órgão central do Sistema de Administração dos Recursos de Tecnologia da Informação - Sisp do Poder Executivo federal.

Art. 2º A Rede Federal de Gestão de Incidentes Cibernéticos tem por finalidade aprimorar e manter a coordenação entre órgãos e entidades da administração pública federal direta, autárquica e fundacional para prevenção, tratamento e resposta a incidentes cibernéticos, de modo a elevar o nível de

- ❑ **AMBIENTE COLABORATIVO baseado em troca de informações.**
- ❑ **ÓRGÃOS OBRIGATÓRIOS – APF direta, autárquica e fundacional.**
- ❑ **ÓRGÃOS VOLUNTÁRIOS – empresas públicas, sociedade de economia mista e suas subsidiárias.**
- ❑ **ÓRGÃOS CONVIDADOS – órgãos dos demais poderes e/ou entidades julgadas relevantes pelo GSI.**
- ❑ **ETIR - equipe de prevenção, tratamento e resposta a incidentes cibernéticos.**
- ❑ **ETIR de coordenação setorial - coordenar as atividades de cibersegurança e centralizar as notificações de incidentes.**

REGIC – OBJETIVOS

01 **Divulgar**
Medidas de prevenção

02 **Compartilhar**
Alertas, Recomendações

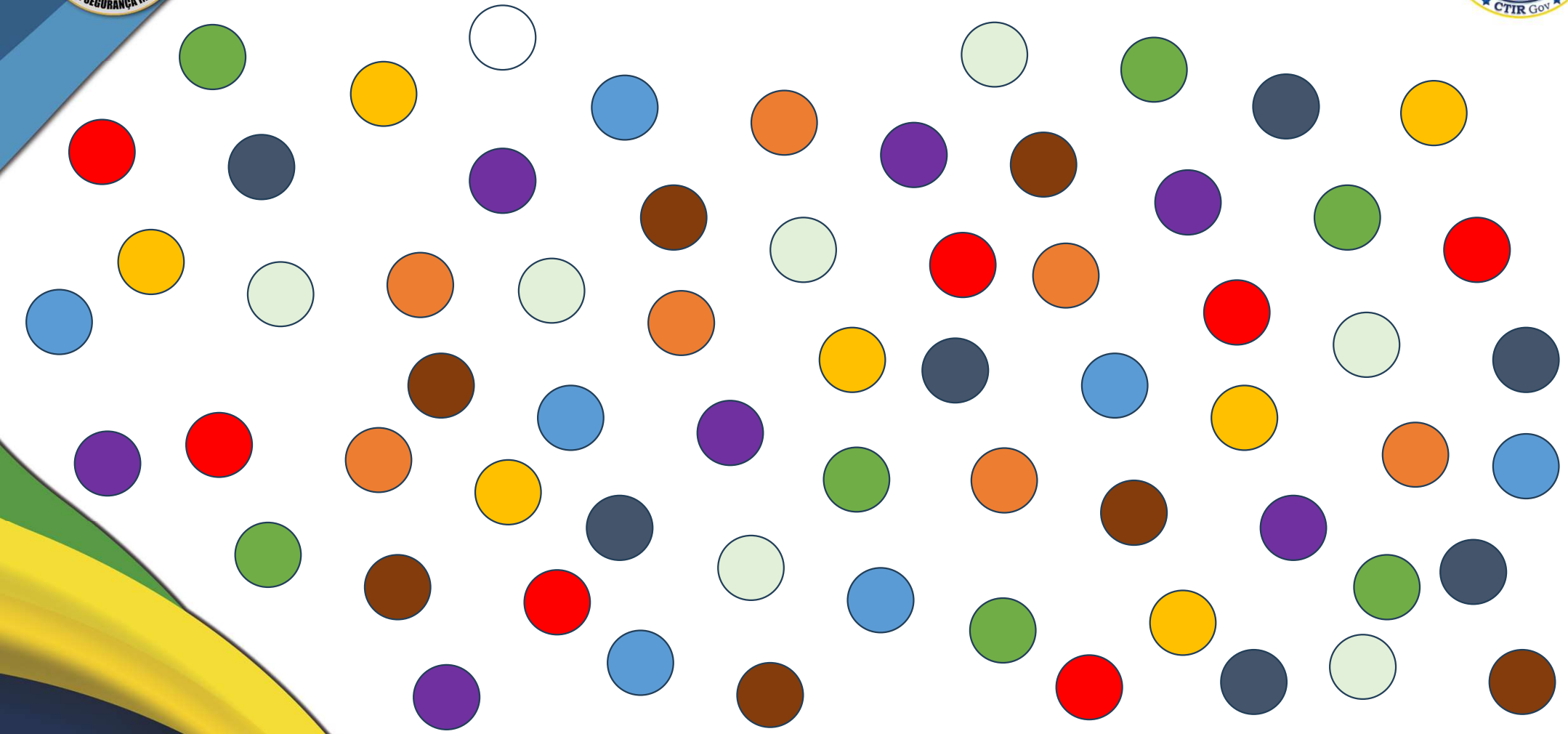
03 **Alertar**
Informações de ataques

04 **Incentivar**
Trabalho cooperativo

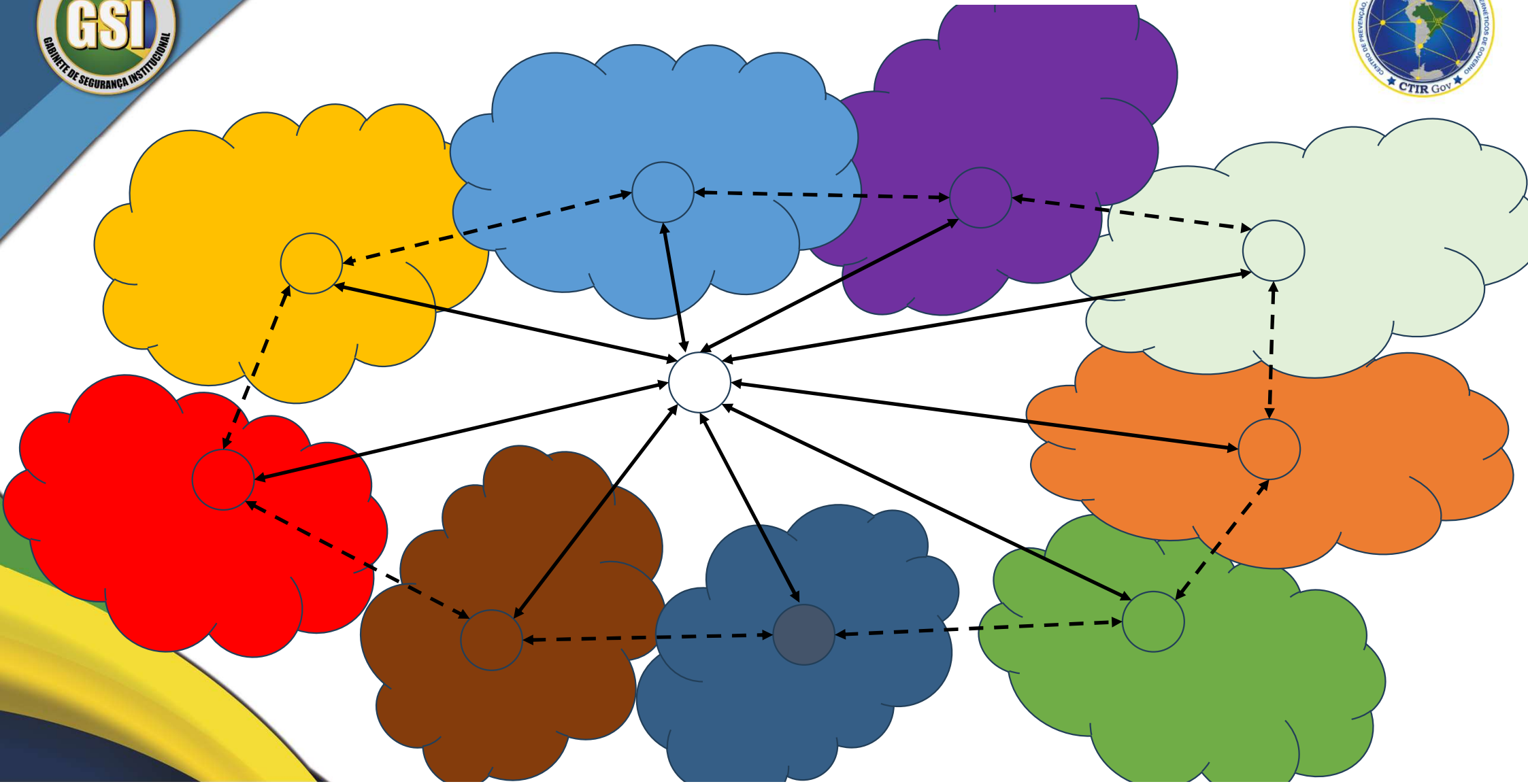
05 **Promover**
Celeridade e tempestividade

Elevar o nível de resiliência em Segurança Cibernética

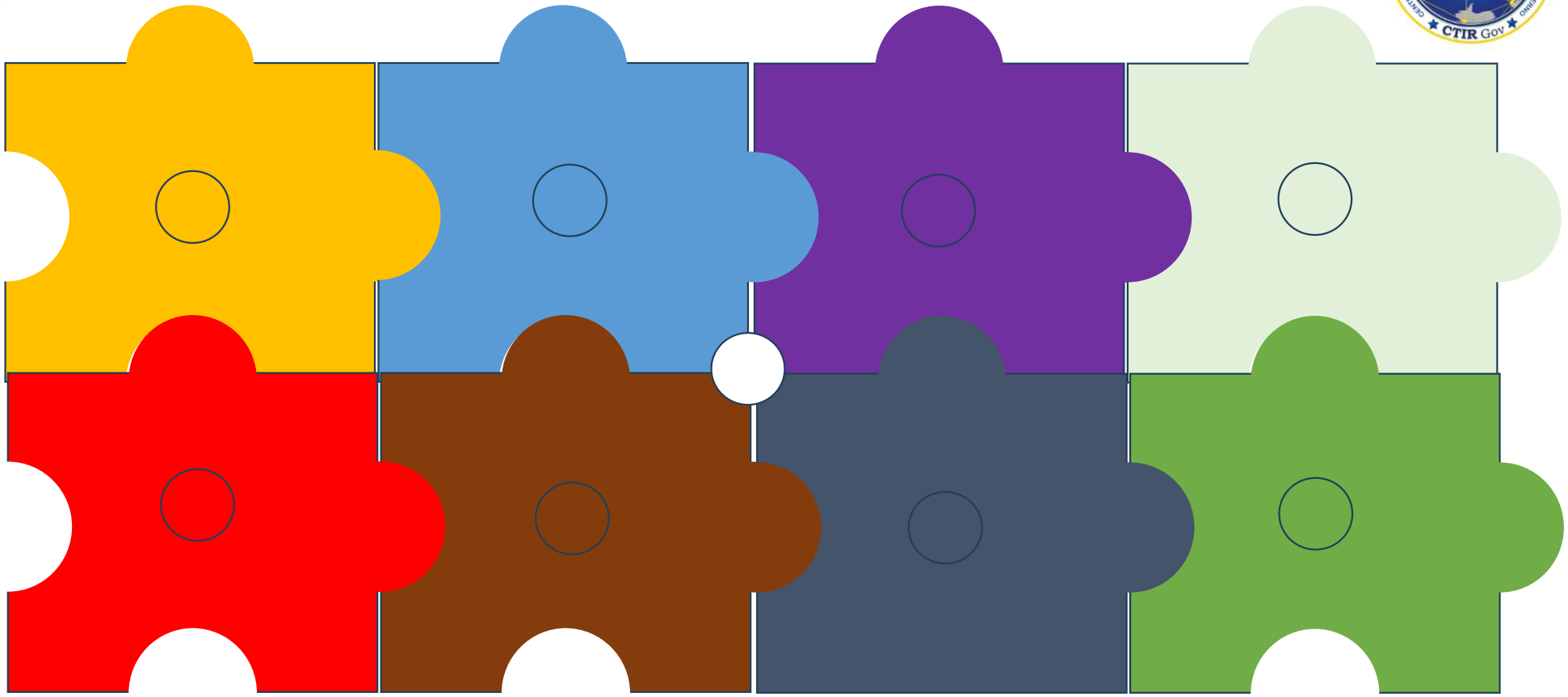
REGIC – Concepção operacional



REGIC – Concepção operacional



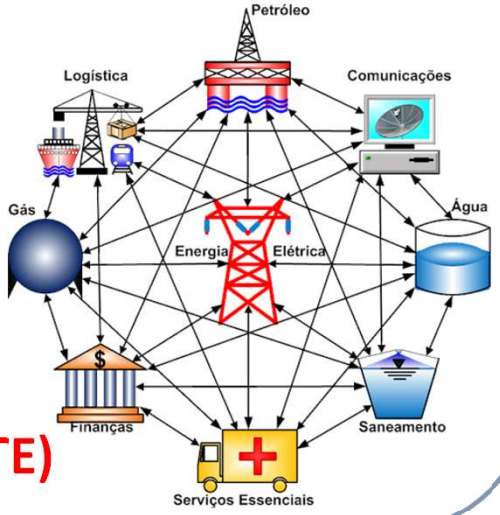
REGIC – Concepção operacional



REGIC - ARTICULAÇÃO

REGIC

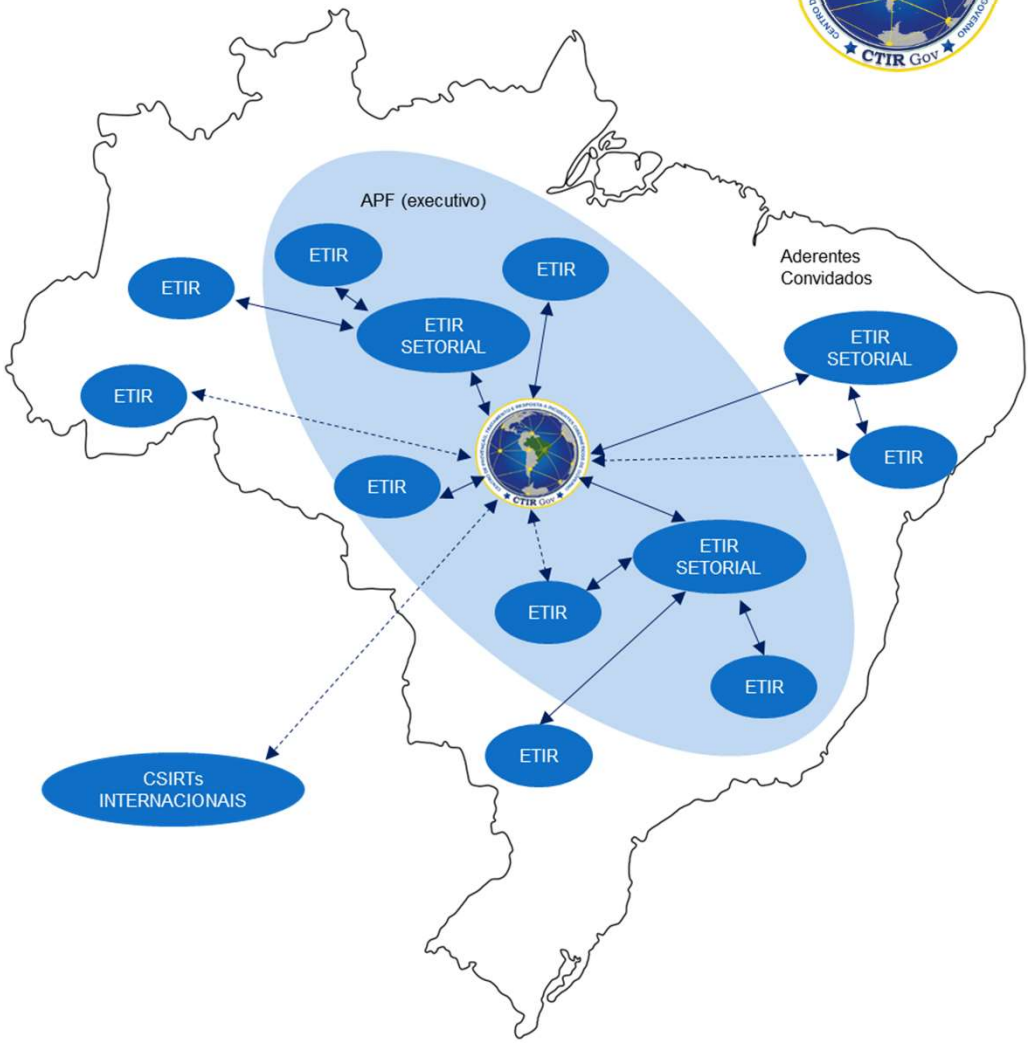
(COLABORATIVAMENTE)



REGIC - ORGANIZAÇÃO

155 Órgãos
88 adesões 2024
10 Estados
16 setoriais

Domínios de interesse
*.gov.br, *.mil.br, *.jus.br, *.leg.br, *.mp.br, *.def.br, *.tc.br, *.eb.br, *.mar.br, *.edu.br, Universidades, empresas públicas ou privadas participantes.



SETORIAIS

PALAVRA CHAVE: **COLABORAÇÃO**

AGÊNCIAS REGULADORAS

Agência Nacional de Águas e Saneamento Básico (ANA)
Agência Nacional de Aviação Civil (ANAC)
Agência Nacional de Energia Elétrica (ANEEL)
Agência Nacional de Mineração (ANM)
Agência Nacional de Telecomunicações (ANATEL)
Agência Nacional de Petróleo, Gás Natural e Biocombustíveis (ANP)
Agência Nacional de Saúde Suplementar (ANS)
Agência Nacional de Transportes Aquaviários (ANTAQ)
Agência Nacional de Transportes Terrestres (ANTT)
Agência Nacional de Vigilância Sanitária (ANVISA)
Agência Nacional do Cinema (ANCINE)
Banco Central do Brasil (BACEN)
Superintendência de Seguros Privados (SUSEP)

SETORES ESPECÍFICOS

Comissão Nacional de Energia Nuclear (CNEN)
Secretaria de Governo Digital (SGD)
Comando de Defesa Cibernética (ComDCiber)
Conselho Nacional de Justiça (CNJ)
Rede Nacional de Ensino e Pesquisa (RNP)

PRODs dos Estados

PRODs participantes da ReGIC

	SIGLA	ESTADO	NOME
1	ATI-TO		AGÊNCIA DE TECNOLOGIA DA INFORMAÇÃO DE TOCANTINS
2	PRODERJ		CENTRO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DO ESTADO DO RIO DE JANEIRO
3	PRODEB		COMPANHIA DE PROCESSAMENTO DE DADOS DA BAHIA
4	CODATA		COMPANHIA DE PROCESSAMENTO DE DADOS DA PARAÍBA
5	PRODEMGE		COMPANHIA DE TECNOLOGIA DA INFORMAÇÃO DO ESTADO DE MINAS GERAIS
6	PRODAM		PROCESSAMENTO DE DADOS AMAZONAS S.A.
7	SETDIG		SECRETARIA-EXECUTIVA DE TRANSFORMAÇÃO DIGITAL
8	ATI-PE		AGÊNCIA ESTADUAL DE TECNOLOGIA DA INFORMAÇÃO DE PERNAMBUCO
9	SETIC		SUPERINTENDÊNCIA ESTADUAL DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO
10	EMGETIS		EMPRESA SERGIPANA DE TECNOLOGIA DA INFORMAÇÃO

ISAC
(Information Sharing and Analysis Center)

Centros de Análise e Compartilhamento de Informações (Mensagem ao CN 2025)

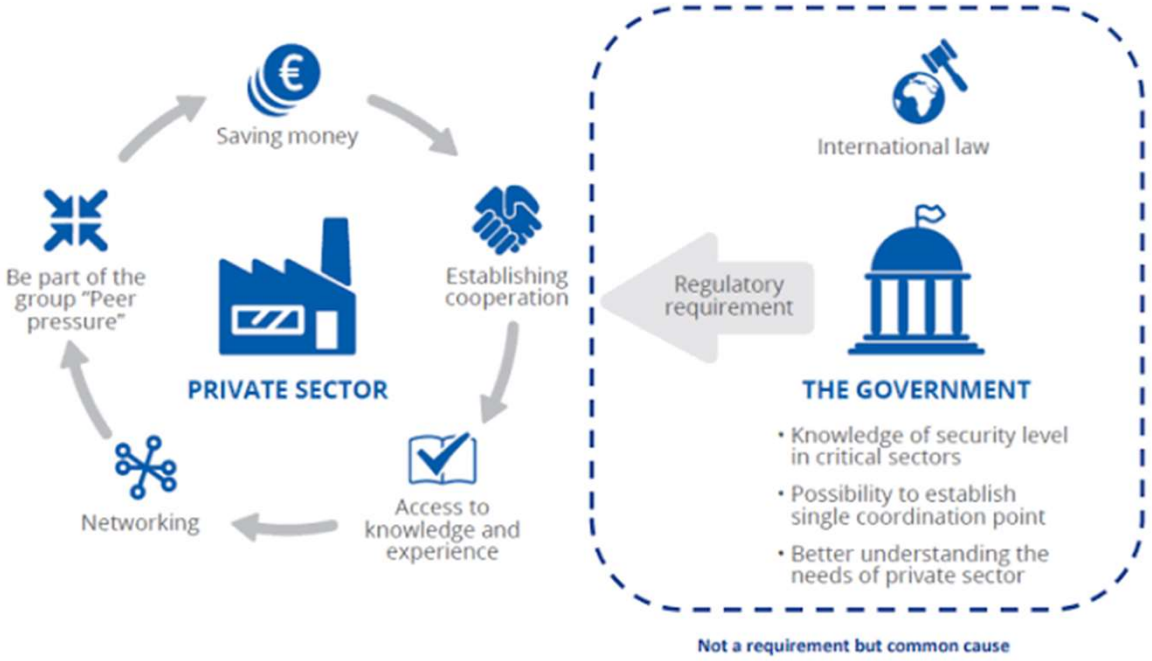


Figure 1: Reasons for the creation of ISACs

VALORES NO COMPARTILHAMENTO DE INFORMAÇÕES

- ✓ Código de Ética:
  - Garantir profissionalismo,
  - Exercer o cuidado,
  - Oferecer qualidade.

- ✓ Sem respeito e confiança do público alvo e comunidade é difícil atingir o sucesso.

- ✓ Independente das intenções, um CSIRT é visto pela impressão que ele deixa por suas palavras e ações.

- ✓ Membros de uma ETIR tem acesso a informações sensíveis sobre vulnerabilidades e sistemas.

PERSPECTIVAS 2025 e além

PERSPECTIVAS

✓TRILHA DE WEBINÁRIOS

TEMAS CANDIDATOS

- Organização de uma ETIR
- Monitoramento e Detecção
- Gestão de Vulnerabilidades
- Prevenção ao Ransomware
- Análise de Intrusão
- Gestão de Incidentes
- Apresentação do MISP
- Lições Aprendidas CTIR GOV
- Vazamento de Credenciais / Dados Pessoais

PERSPECTIVAS

✓Encontro de ETIRs Setoriais

02 de abril

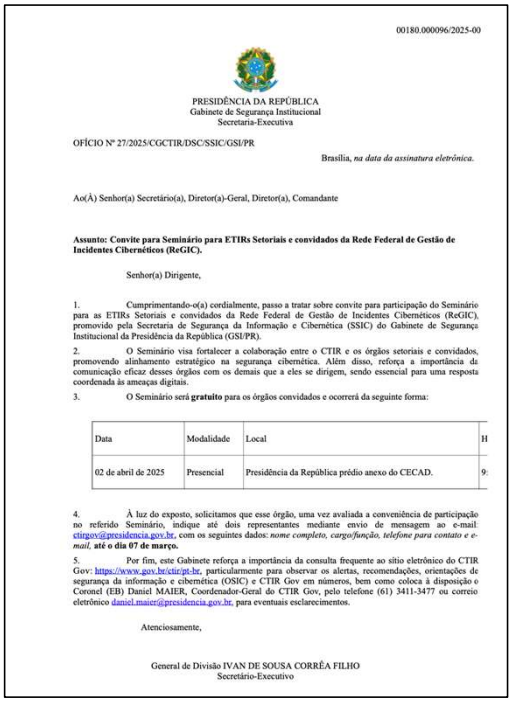
FINALIDADE

Troca de Experiências

Estratégias para a REGIC

Orientações para trabalho colaborativo

Normas de sistema



00180.000096/2025-00

PRESIDÊNCIA DA REPÚBLICA
Gabinete de Segurança Institucional
Secretaria-Executiva

OFÍCIO Nº 27/2025/CGCTIR/DSC/SSIC/GSI/PR

Brasília, *na data da assinatura eletrônica.*

Ao(À) Senhor(a) Secretário(a), Diretor(a)-Geral, Diretor(a), Comandante

Assunto: Convite para Seminário para ETIRs Setoriais e convidados da Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC).

Senhor(a) Dirigente,

1. Cumprimentando-o(a) cordialmente, passo a tratar sobre convite para participação do Seminário para as ETIRs Setoriais e convidados da Rede Federal de Gestão de Incidentes Cibernéticos (ReGIC), promovido pela Secretaria de Segurança da Informação e Cibernética (SSIC) do Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

2. O Seminário visa fortalecer a colaboração entre o CTIR e os órgãos setoriais e convidados, promovendo alinhamento estratégico na segurança cibernética. Além disso, reforça a importância da comunicação eficaz desses órgãos com os demais que a eles se dirigem, sendo essencial para uma resposta coordenada às ameaças digitais.

3. O Seminário será **gratuito** para os órgãos convidados e ocorrerá da seguinte forma:

Data	Modalidade	Local	H
02 de abril de 2025	Presencial	Presidência da República prédio anexo do CECAD.	9:

4. À luz do exposto, solicitamos que esse órgão, uma vez avaliada a conveniência de participação no referido Seminário, indique até dois representantes mediante envio de mensagem ao e-mail: ctirgov@presidencia.gov.br, com os seguintes dados: *nome completo, cargo/função, telefone para contato e e-mail*, **até o dia 07 de março.**

5. Por fim, este Gabinete reforça a importância da consulta frequente ao sítio eletrônico do CTIR Gov: https://www.gov.br/ctir/pt-br, particularmente para observar os alertas, recomendações, orientações de segurança da informação e cibernética (OSIC) e CTIR Gov em números, bem como coloca à disposição o Coronel (EB) Daniel MAIER, Coordenador-Geral do CTIR Gov, pelo telefone (61) 3411-3477 ou correio eletrônico daniel.maier@presidencia.gov.br, para eventuais esclarecimentos.

Atenciosamente,

General de Divisão IVAN DE SOUSA CORRÊA FILHO
Secretário-Executivo

Ofício nº27/2025/CGCTIR/DSC/SSIC/GSI/PR
Processo 00180.000096/2025-00

PERSPECTIVAS

✓Colóquio da REGIC

2ª quinzena de agosto

PERSPECTIVAS

✓TTX resposta à incidentes

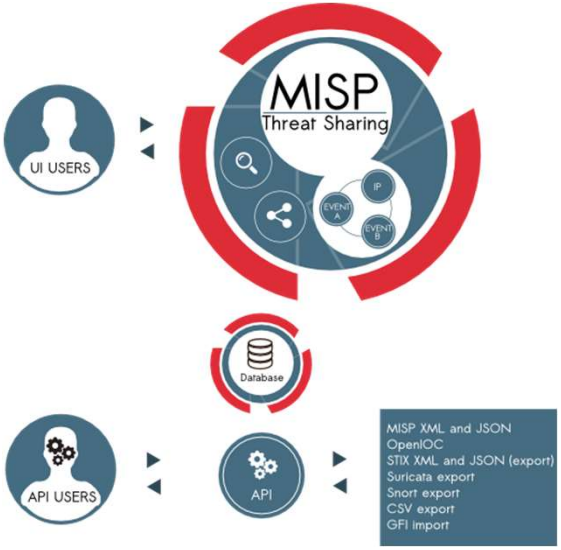
setembro

✓Treinamento Teórico-Prático

outubro

PERSPECTIVAS

✓Projeto MISP



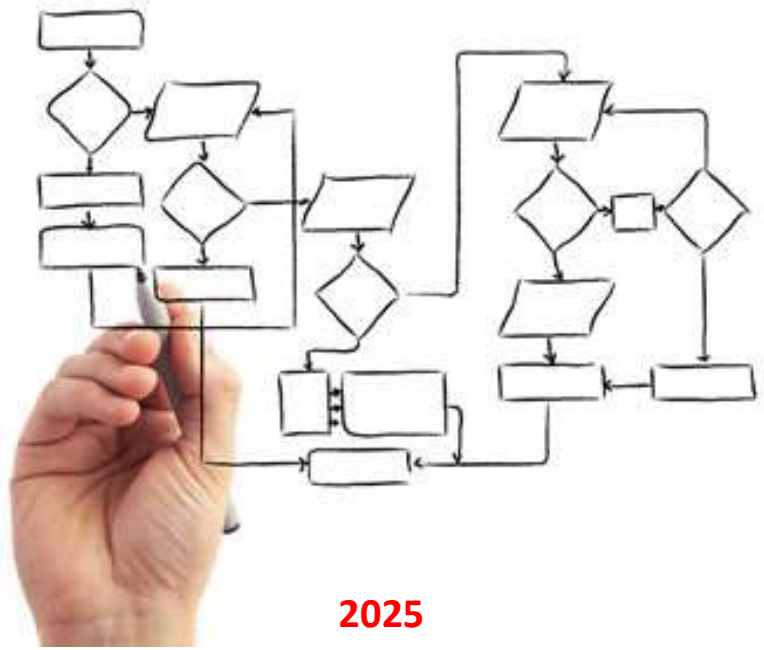
2025

✓Portal da REGIC

2025

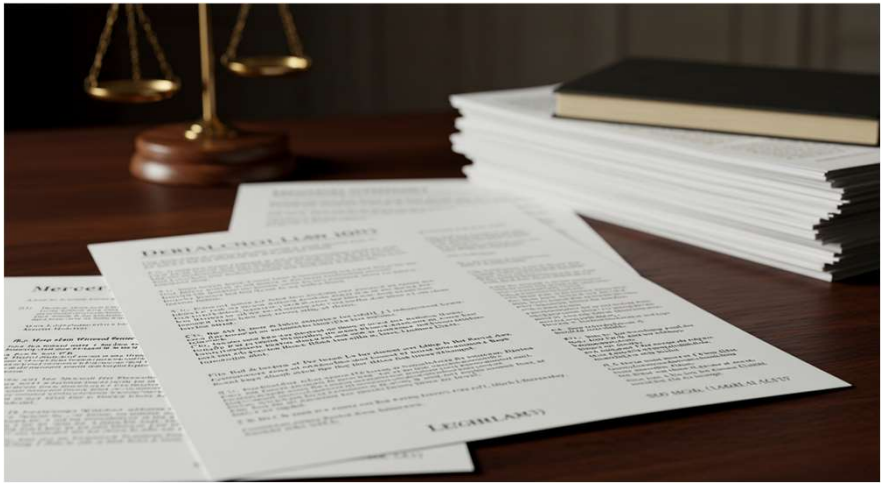
PERSPECTIVAS

✓Revisão Processos



2025

✓Revisão Normativos



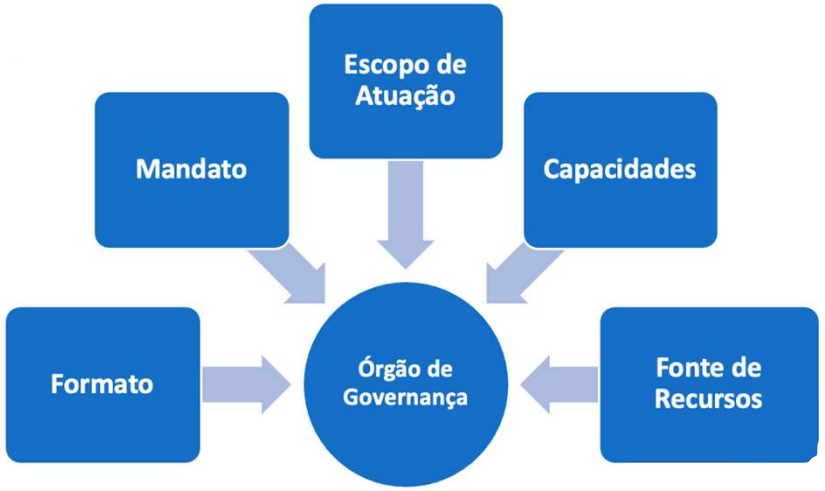
2025

EM BREVE

✓Estratégia Nacional de Cibersegurança

Primeiro semestre / 2025

✓Órgão de Governança da Cibersegurança



OBRIGADO

DANIEL MAIER DE CARVALHO
CTIR Gov/GSI-PR
ctirgov@presidencia.gov.br
www.ctir.gov.br

INTERVALO

PERGUNTAS