Fortalecendo a resiliência em Segurança Cibernética:

O poder do compartilhamento de informações entre os membros da REGIC – Desafios e Oportunidades.

Agenda

1. Introdução

   Um *Overview* da REGIC

2. Desenvolvimento

   a. Desafios para compartilhamento de informações na REGIC

   b. Contribuições do CTIR GOV para resiliência da REGIC

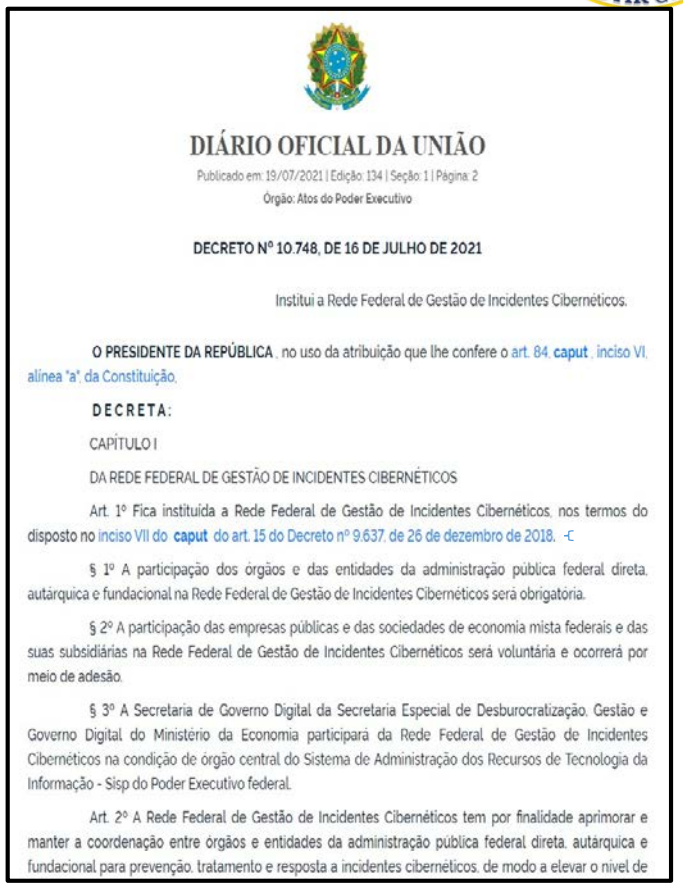
   c. Oportunidades na Detecção, Comunicação e Resposta na REGIC

3. Conclusão

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

REGIC - CRIAÇÃO

- **FINALIDADE – Aprimorar e manter a coordenação entre órgãos e entidades para o tratamento de incidentes de modo a elevar o nível de resiliência em segurança cibernética.**
- **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.**



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. -C

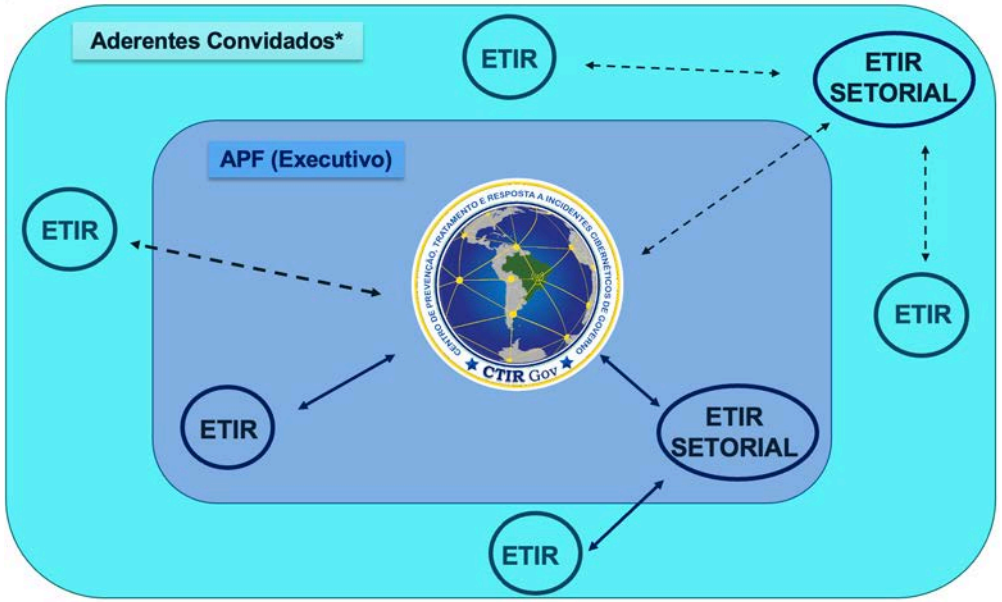
§ 1º A participação dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional na Rede Federal de Gestão de Incidentes Cibernéticos será obrigatória.

§ 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

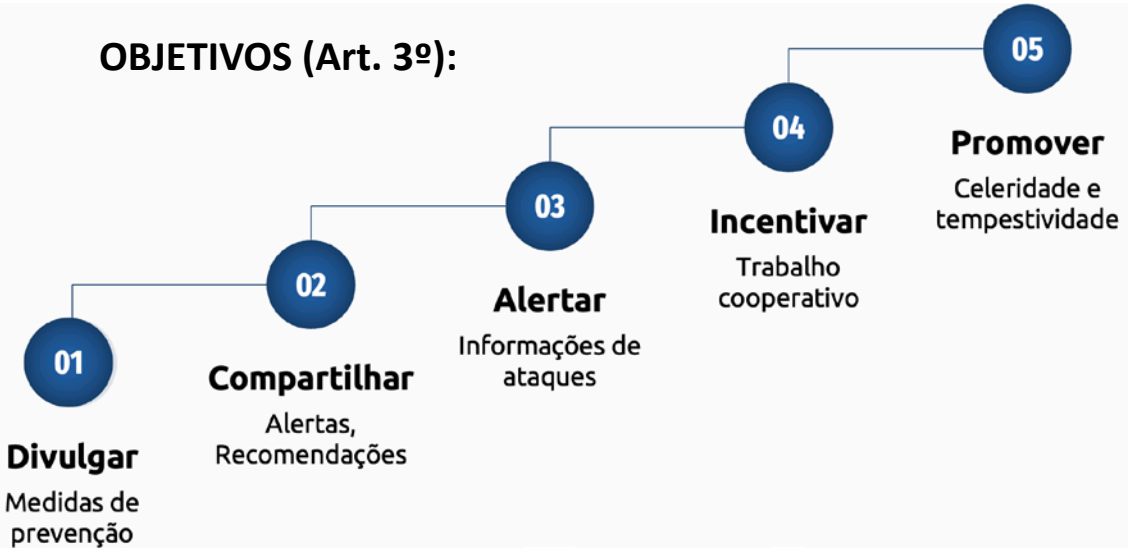
REGIC - CRIAÇÃO



Domínios de interesse

*.gov.br, *.mil.br, *.jus.br, *.leg.br, *.mp.br, *.def.br, *.tc.br, *.eb.br, *.mar.br, *.edu.br, Universidades federais, outros.

OBJETIVOS (Art. 3º):



Lista de Setoriais			
ANA	ANAC	ANATEL	ANCINE
ANEEL	ANM	ANP	ANS
ANTAQ	ANTT	ANVISA	BACEN
CNEN	CNJ	ComDCiber	SGD

REGIC - ADESÃO

42	127	41
Administração Direta	Organizações Governamentais	Fundações Públicas

210

Órgãos Públicos Federais

REGIC

(COLABORATIVAMENTE)

REGIC - PARTICIPAÇÃO

Para aderir à REGIC, sejam seguidos os seguintes passos:

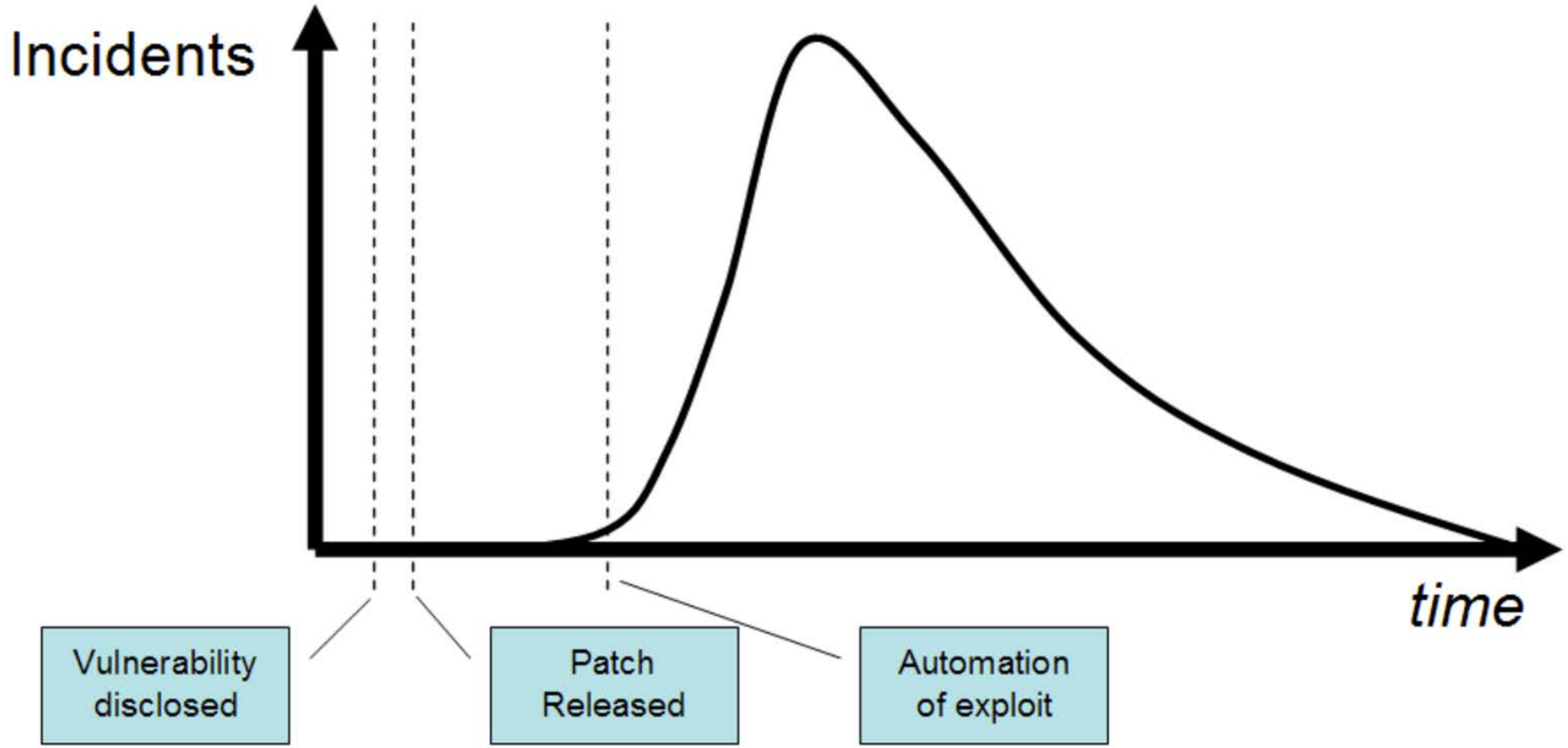
1. Possuir uma Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) formalmente instituída;

2. Enviar, por ofício, manifestação de interesse em ingressar a REGIC, assinado pelo dirigente máximo do órgão ou seu representante legal; e

3. Encaminhar o Termo de Adesão à Rede Federal de Gestão de Incidentes Cibernéticos.

https://www.gov.br/ctir/pt-br/assuntos/regic-decreto-no-10-748-de-16-de-julho-de-2021

REGIC - DESAFIOS



Effectiveness of Proactive CSIRT Services

REGIC - DESAFIOS

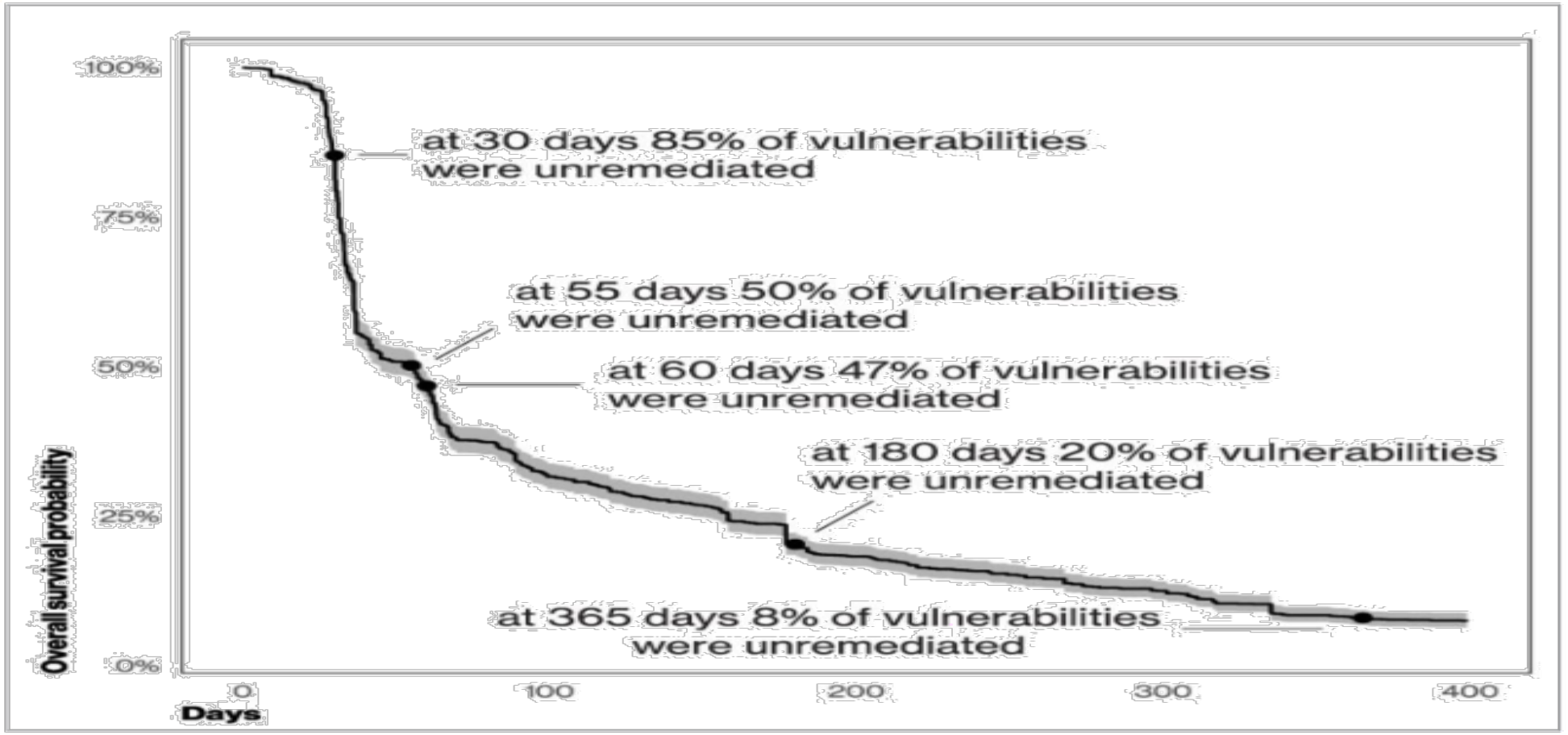
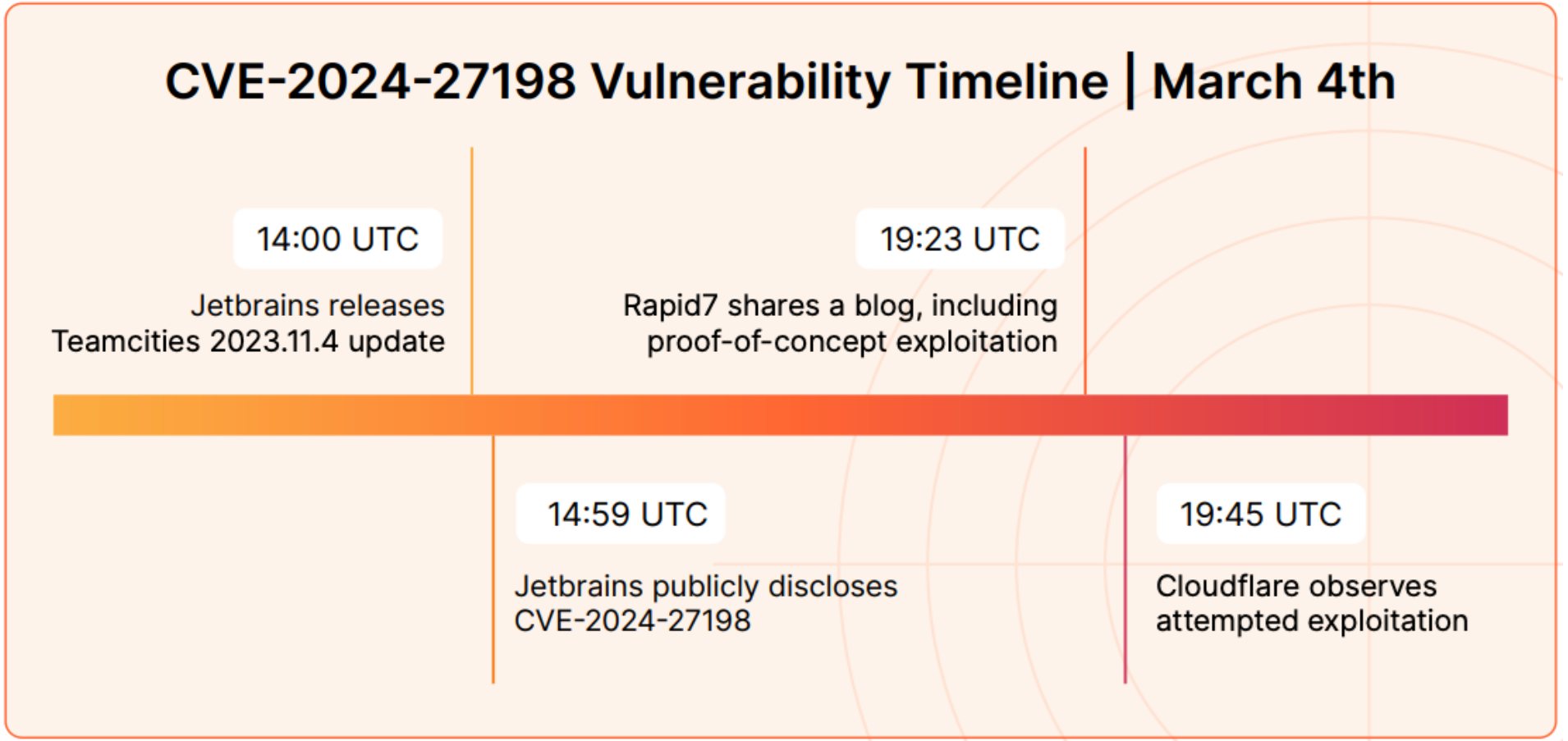


Figure 3. Timeliness of Remediation – Verizon 2024 DBIR

[2024-dbir-data-breach-investigations-report.pdf]

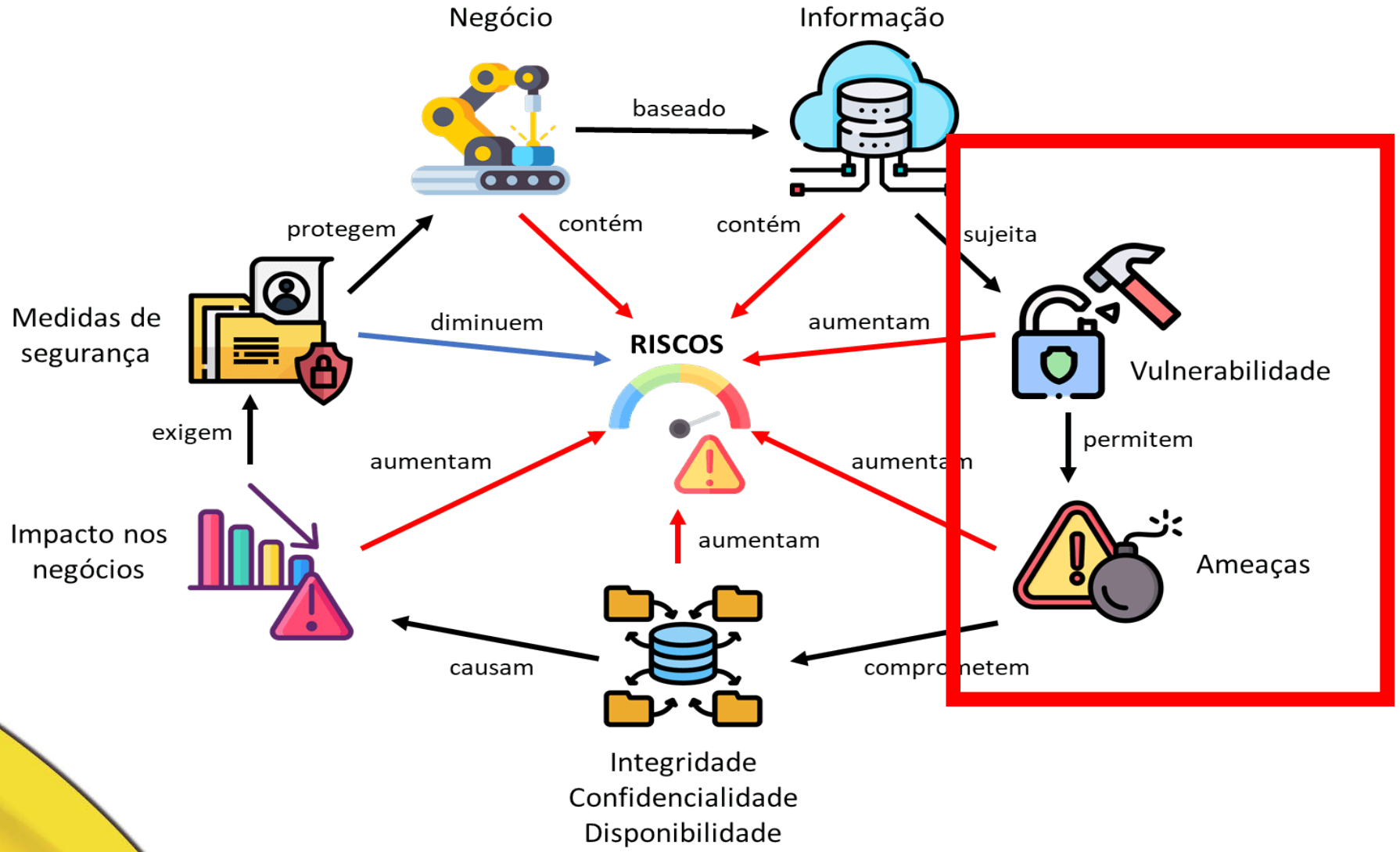
REGIC - DESAFIOS



[2024 Cloudflare Application Security Report]

REGIC - DESAFIOS

REGIC - DESAFIOS



DETECÇÃO

COMUNICAÇÃO

RESPOSTA

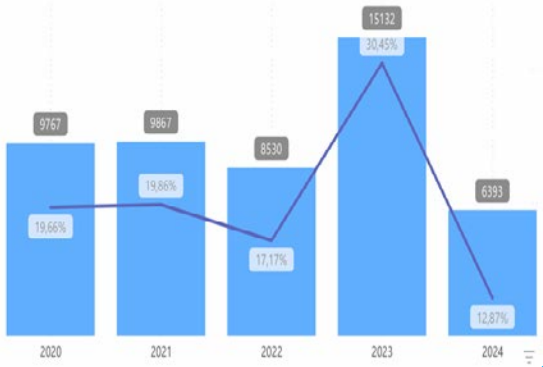
CTIR GOV - CAPACIDADES

1. Consciência situacional
2. Coordenação do tratamento de incidentes
3. Prevenção a incidentes
4. Apoio para a definição de normativos
5. Articulação CSIRTs de outros países

CTIR GOV - NÚMEROS

Notificações Reportadas pelo CTIR Gov - 2020 a 2024

INFORME: Os gráficos são dinâmicos, alterando a visualização de acordo com a escolha pretendida. *Clique e verifique!*



Ano	Vulnerabilidades	Incidentes	Total
2024	1821	4572	6393
2023	10220	4912	15132
2022	5128	3402	8530
2021	4964	4903	9867
2020	2540	7227	9767
Total	24673	25016	49689

Trimestre	Vulnerabilidades	Incidentes	Total
Trim 4	4581	4611	9192
Trim 3	7203	4355	11558
Trim 2			
Trim 1	4742	8199	12941
Total	24673	25016	49689

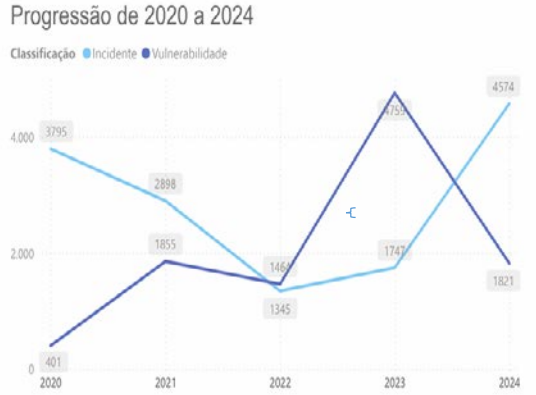
Notificações Reportadas pelo CTIR Gov

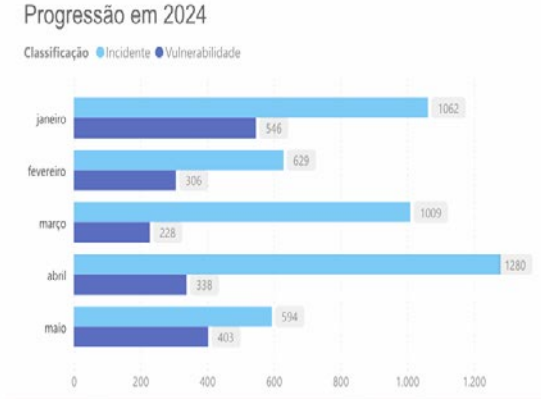
Mês	Vulnerabilidades	Incidentes	Total
janeiro	889		
fevereiro		2218	3690
março	1381	3177	4558
abril	2479	3512	5991
maio	3079	2646	5725
junho	2589	1693	4282
julho	3330	1555	4885
agosto	2345	1225	3570
setembro	1528	1575	3103
outubro	1764	1520	3284
novembro	1332	1461	2793
dezembro	1485	1630	3115
Total	24673	25016	49689

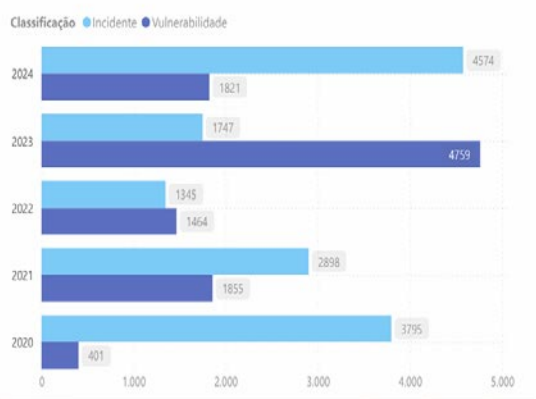
Estatísticas dos Incidentes e Vulnerabilidades - Progressão

INCIDENTES - O CTIR Gov define um incidente de segurança como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

VULNERABILIDADES - Notificações de caráter pre[illegible] responsável pelo ativo a respeito de fragilidades dos sistemas computacionais que possam ser alvo de exploração ou [illegible]







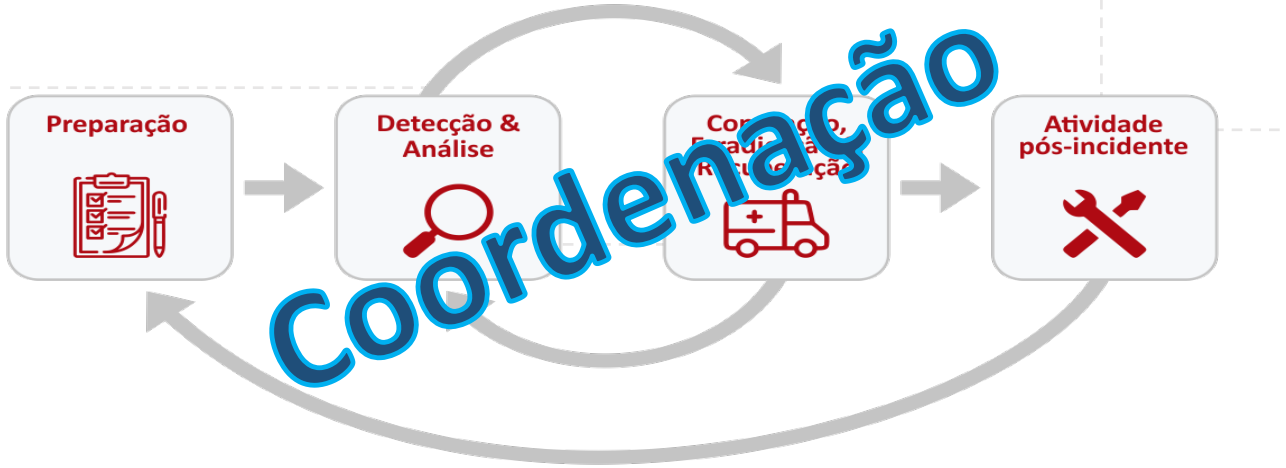
CTIR GOV - NOTIFICAÇÕES

QUEM?

COMO?

QUANDO?

PORQUE?



CTIR GOV - PREVENÇÃO

Alertas

Recomendações

Tempestividade

RECOMENDAÇÃO 01/2024 — última modificação 26/03/2024 17h42

Relatório sobre ataques de negação de serviço (DDoS)

RECOMENDAÇÃO 02/2024 — última modificação 20/06/2024 17h12

Informações sobre o Ransomware Black Basta

RECOMENDAÇÃO 03/2024 — última modificação 25/07/2024 09h23

Utilização da RFC 2350 por Equipes de Tratamento de Incidentes de Redes

RECOMENDAÇÃO 04/2024 — última modificação 25/07/2024 15h34

Configuração de controles recomendados pelas boas práticas para serviços Web, E-mail e DNS.

ALERTA 01/2024 — última modificação 12/01/2024 13h58

Vulnerabilidades críticas em produtos Volexity Ivanti

ALERTA 02/2024 — última modificação 02/02/2024 17h28

Atualizações sobre vulnerabilidades em produtos Volexity Ivanti

ALERTA 03/2024 — última modificação 08/03/2024 17h47

Vulnerabilidades críticas no software Jenkins

ALERTA 04/2024 — última modificação 16/03/2024 15h11

Aplicativos maliciosos com temática "IRPF"

ALERTA 05/2024 — última modificação 03/04/2024 09h10

Vulnerabilidade crítica na ferramenta XZ

ALERTA 06/2024 — última modificação 12/04/2024 11h21

Vulnerabilidade no Sistema Operacional Palo Alto Networks (PAN-OS)

ALERTA 07/2024 — última modificação 19/04/2024 19h52

Aumento de casos de vazamentos de credenciais de acesso a sistemas de governo

ALERTA 08/2024 — última modificação 04/06/2024 10h29

Vulnerabilidade no Check Point Security Gateway

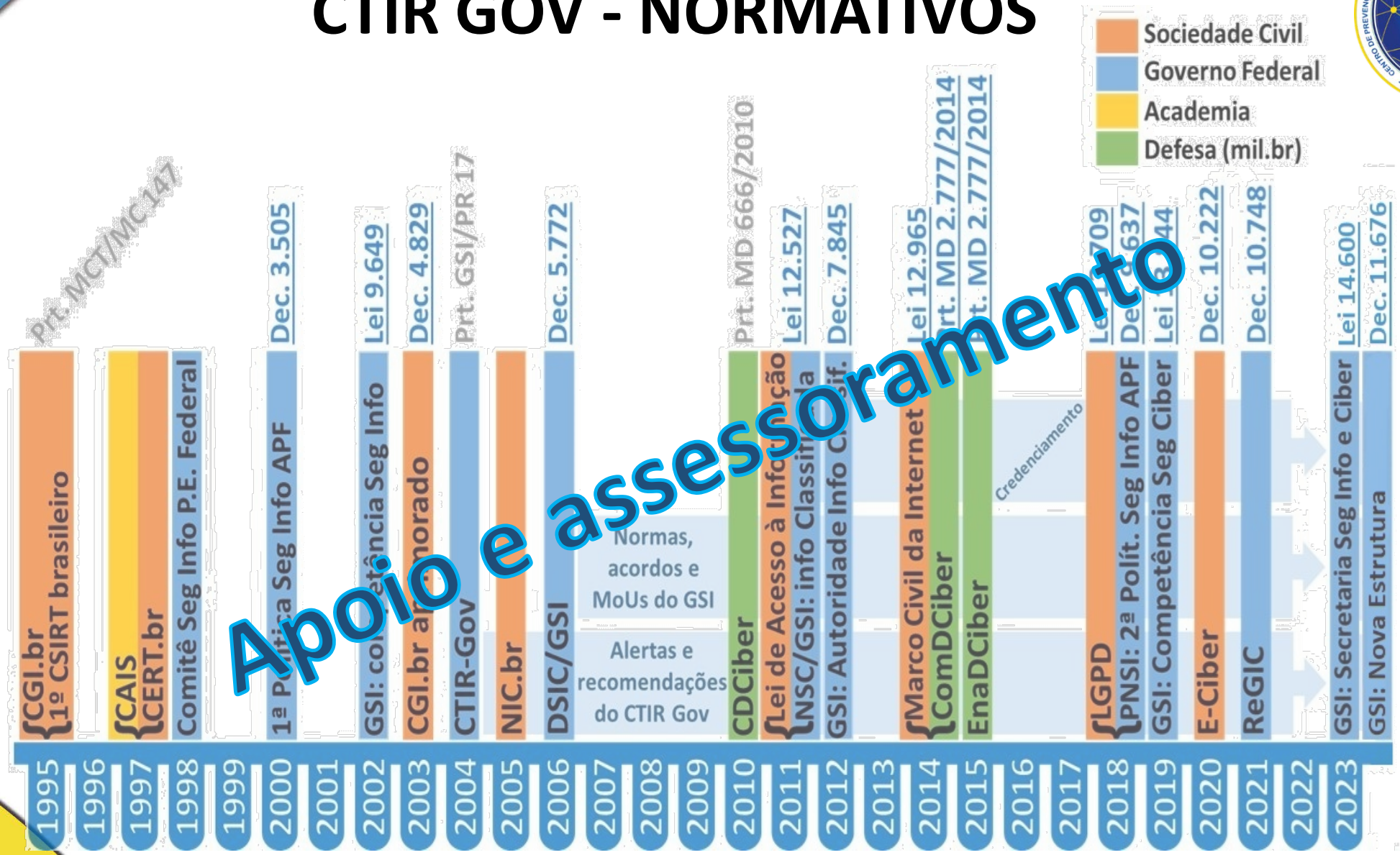
ALERTA 09/2024 — última modificação 01/07/2024 16h12

Vulnerabilidade crítica no OpenSSH

ALERTA 10/2024 — última modificação 25/07/2024 10h17

Falha em atualização de produto CrowdStrike

CTIR GOV - NORMATIVOS



Apoio e assessoramento

CTIR GOV - PARCERIAS

Articulação Nacional

cert.br

CISC gov.br

CAIS

ANATEL
Agência Nacional de Telecomunicações

SERPRO

DATAPREV

POLÍCIA FEDERAL

COM D CIBER

gov.br Ministério da Justiça e Segurança Pública

Órgãos do Governo

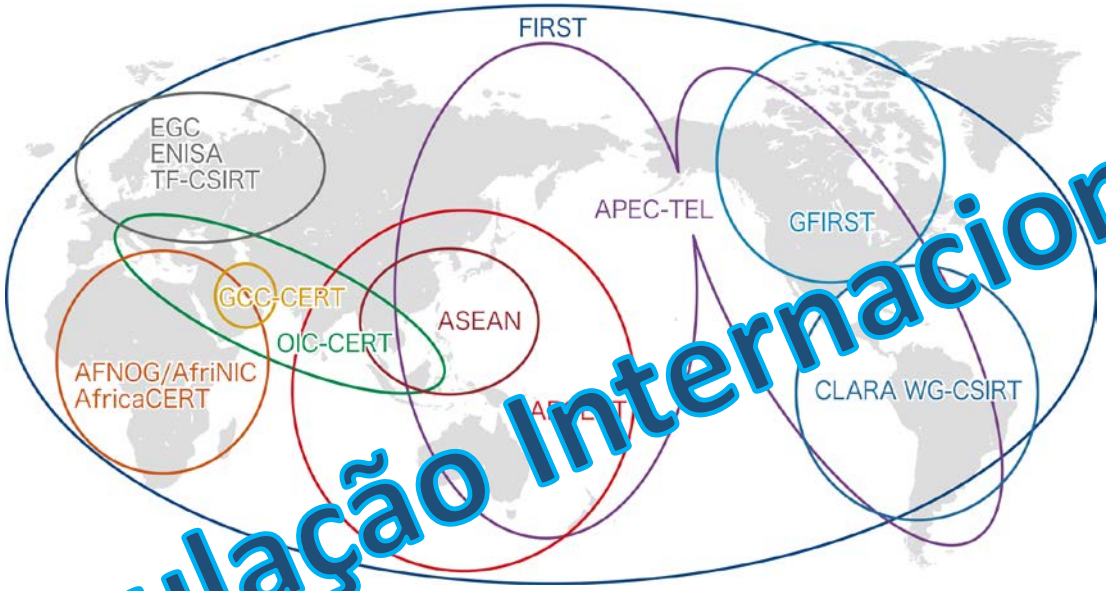
Acesso à Informação

Autoridade Nacional de Proteção de Dados

FIESP

FEBRABAN

CTIR GOV - PARCERIAS



Articulação Internacional

FIRST
Improving Security Together

SingCERT
Singapore Cyber Emergency Response Team

CERTCENTERCANADA

CSIRTAmericas
Network

certtn
Handling Computer Security Incidents

aws

SHADOWSERVER

US-CERT
United States
Computer Emergency Readiness Team

LAC4
Latin America and
Caribbean Cyber
Competence Centre

ONU

BID Banco Interamericano de Desenvolvimento

REGIC - OPORTUNIDADES

DETECÇÃO

(Amplitude nas Fontes de dados)

COMUNICAÇÃO

TLP:RED

TLP:AMBER

TLP:GREEN

TLP:CLEAR

(Processos e Ferramentas)

MISP
Threat Sharing

RESPOSTA

(ETIR – Amadurecimento e Capacitação)

CONCLUSÃO

CESAR MONTENEGRO JUSTO
Tenente Coronel (EB)
Assessor do CGCTIR/DSC/SSIC/GSI-PR
cesar.montenegro@presidencia.gov.br
ctirgov@presidência.gov.br