8º FÓRUM BRASILEIRO DE CSIRTs

PLANO NACIONAL DE TRATAMENTO E RESPOSTA A INCIDENTES COMPUTACIONAIS - PNTIR

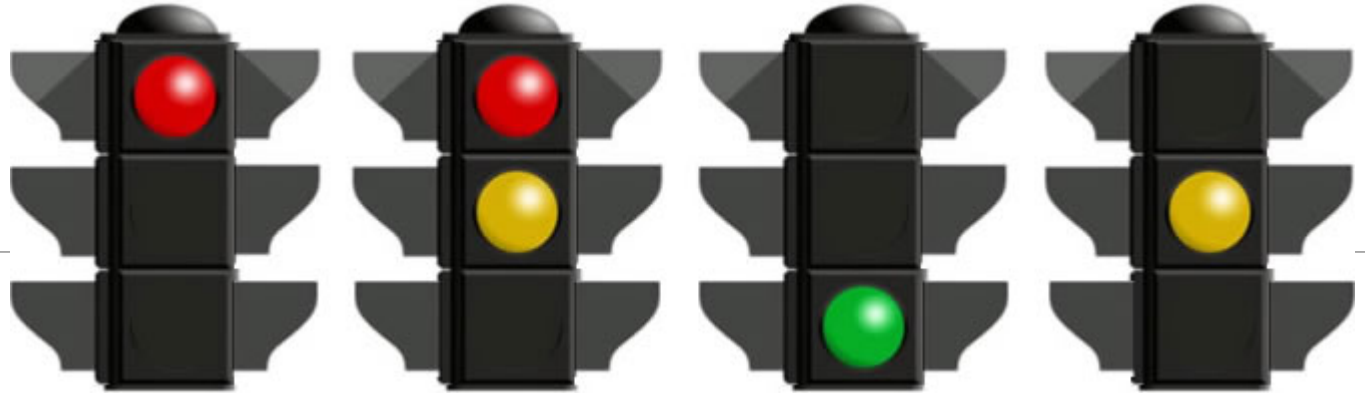
São Paulo, SP | 10 DE SETEMBRO DE 2019

15 Anos

Democlydes Carvalho – Coordenador-Geral

democlydes@ctir.gov.br
contato@ctir.gov.br

http://lattes.cnpq.br/7039080122100247



Dentro das trocas de informações entre CSIRTs, esta publicação está marcada como **TLP:WHITE***.

Sujeitas às regras padrão de direitos autorais, as informações do TLP: WHITE podem ser distribuídas sem restrições.

* *Traffic Light Protocol* (TLP), criado pelo *Forum of Incident Response and Security Teams* (**FIRST**)

Objetivo

Apresentar características do Plano Nacional de Tratamento e Resposta a Incidentes Computacionais - PNTIR, o processo de elaboração junto à Estratégia Nacional de Segurança Cibernética, suas metas e ações a serem desenvolvidas com sua publicação.

TLP:WHITE

Sumário

TLP:WHITE

O Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo

CTIR Gov

CTIR Gov

Criado em 2004

TLP:WHITE

http://www.gsi.gov.br/

http://dsic.planalto.gov.br/

https://ctir.gov.br/

MEDIDA PROVISÓRIA Nº 870, DE 1º DE JANEIRO DE 2019

(Estabelece a organização básica dos órgãos da Presidência da República e dos Ministérios)

GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA
(MEDIDA PROVISÓRIA Nº 870, DE 1º DE JANEIRO DE 2019)

Art. 10. Ao Gabinete de Segurança Institucional da Presidência da República compete:
I – (...);
II – (...);
III – (...);

IV - coordenar as atividades de segurança da informação e das comunicações no âmbito da administração pública federal;

V - planejar, coordenar e supervisionar a atividade de segurança da informação no âmbito da administração pública federal, nela incluídos a segurança cibernética, a gestão de incidentes computacionais, a proteção de dados, o credenciamento de segurança e o tratamento de informações sigilosas;

Competências (Decreto. 9.668, de 2 de janeiro de 2019)

- Coordenar e realizar ações destinadas à gestão de incidentes computacionais, no que se refere à prevenção, ao monitoramento, ao tratamento e à resposta a incidentes computacionais de responsabilidade nacional;

- Coordenar a rede de equipes de tratamento e resposta a incidentes computacionais - CSIRTs, formada pelos órgãos e pelas entidades governamentais;

Serviços

Em resumo, o conjunto de serviços providos pelo CTIR Gov pode ser dividido em: Notificação de Incidentes; Análise de Incidentes; Suporte à Resposta de Incidentes; Coordenação na Resposta a Incidentes, Distribuição de Alertas, Recomendações e Estatísticas; e Cooperação com outras Equipes de Tratamento de Incidentes.

Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov)

TLP:WHITE

Criado em 2004

Integração com outros atores:
- CERT.br/NIC.br
- CAIS/RNP
- SRCC/DPF/MJ
- CDCiber/MD
- SERPRO
- DATAPREV
- ABIN
- MRE

Atuação em Grandes Eventos
- Rio+20;
- Copa das Confederações;
- Jornada Mundial da Juventude;
- Copa do Mundo FIFA 2014;
- Jogos Olímpicos.

Público-Alvo

Comunidade

-Órgãos ou entidades de quaisquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios
- Forças Armadas
- Entidades vinculadas e estratégicas
- Infraestrutura Crítica

Domínios

*.gov.br, *.mil.br, *.jus.br, *.leg.br e *.mp.br

PROJETOS E ATIVIDADES

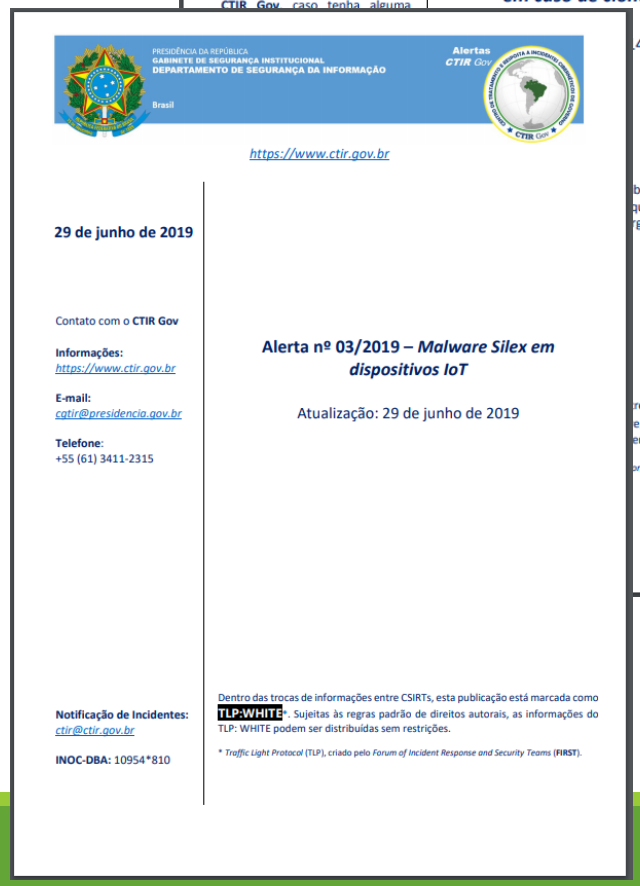

PRESIDÊNCIA DA REPÚBLICA
GABINETE DE SEGURANÇA INSTITUCIONAL
DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO
Brasil

Recomendações CTIR Gov

https://www.ctir.gov.br

14 de junho de 2019

Recomendação nº 05/2019 – *Como agir em caso de clonagem do celular*


PRESIDÊNCIA DA REPÚBLICA
GABINETE DE SEGURANÇA INSTITUCIONAL
DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO
Brasil

Alertas CTIR Gov

https://www.ctir.gov.br

29 de junho de 2019

Contato com o **CTIR Gov**

Informações:
https://www.ctir.gov.br

E-mail:
cgtir@presidencia.gov.br

Telefone:
+55 (61) 3411-2315

Alerta nº 03/2019 – *Malware Silex em dispositivos IoT*

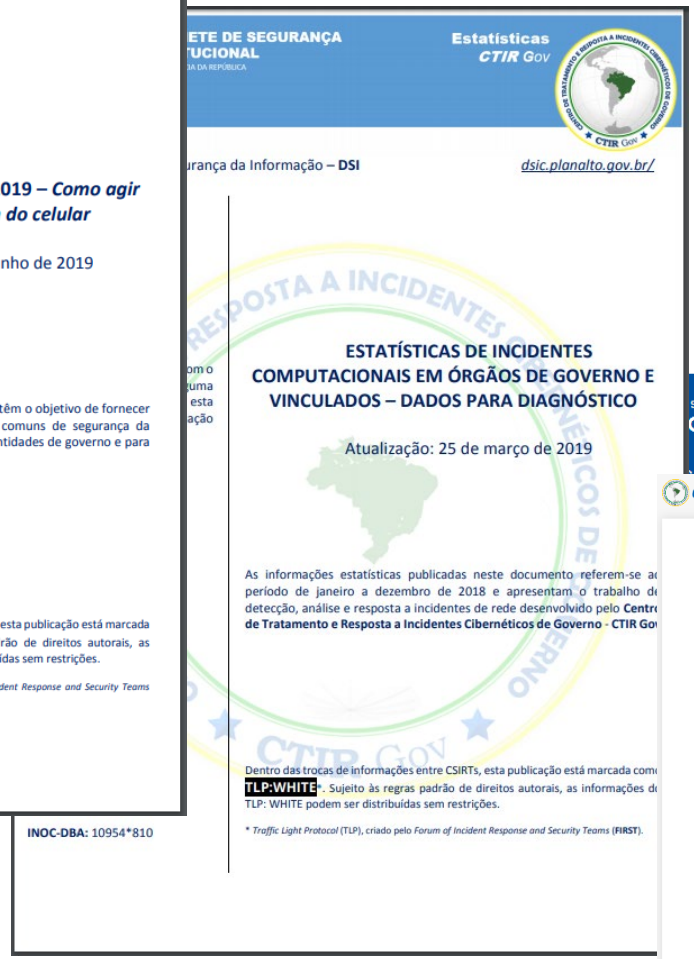
Atualização: 29 de junho de 2019

Notificação de Incidentes:
ctir@ctir.gov.br

INOC-DBA: 10954*810

Dentro das trocas de informações entre CSIRTs, esta publicação está marcada como **TLP:WHITE***. Sujeitas às regras padrão de direitos autorais, as informações do TLP: WHITE podem ser distribuídas sem restrições.

* *Traffic Light Protocol* (TLP), criado pelo *Forum of Incident Response and Security Teams* (**FIRST**).


Estatísticas CTIR Gov

dsic.planalto.gov.br/

ESTATÍSTICAS DE INCIDENTES COMPUTACIONAIS EM ÓRGÃOS DE GOVERNO E VINCULADOS – DADOS PARA DIAGNÓSTICO

Atualização: 25 de março de 2019

As informações estatísticas publicadas neste documento referem-se a período de janeiro a dezembro de 2018 e apresentam o trabalho d detecção, análise e resposta a incidentes de rede desenvolvido pelo **Centr de Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR Go**

Dentro das trocas de informações entre CSIRTs, esta publicação está marcada com **TLP:WHITE***. Sujeito às regras padrão de direitos autorais, as informações d TLP: WHITE podem ser distribuídas sem restrições.

* *Traffic Light Protocol* (TLP), criado pelo *Forum of Incident Response and Security Teams* (**FIRST**).

INOC-DBA: 10954*810


CENTRO DE TRATAMENTO E RESPOSTA A INCIDENTES CIBERNÉTICOS DE GOVERNO

INÍCIO | SOBRE O CTIR GOV | ALERTAS E RECOMENDAÇÕES | NOTÍCIAS | LEGISLAÇÃO | ESTATÍSTICAS | CONTATO

CTIR Gov

15 Anos

Gov comemora 15

CTIRGov Em Números

Visão Geral | Incidentes | Abuso de Sítio | Malwares

Detecção, Análise e Resposta

As informações estatísticas são o resultado do trabalho de detecção, triagem, análise e resposta a incidentes cibernéticos desenvolvido pelo Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo - CTIR Gov.

Conheça o Centro

Notificações Reportadas e Incidentes Confirmados pelo CTIR Gov ao longo do tempo

Variação dos Incidentes por Categoria ao longo do tempo

PROJETOS E ATIVIDADES

TLP:WHITE

- **PLANO NACIONAL DE TRATAMENTO E RESPOSTA A INCIDENTES COMPUTACIONAIS – PNTIR**
- **IMPLANTAÇÃO DA PLATAFORMA MISP (Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing) EM ÓRGÃOS DA ADMINISTRAÇÃO PÚBLICA.**
- **EXERCÍCIO GUARDIÃO CIBERNÉTICO**
- **COLÓQUIO TÉCNICO DE GESTÃO DE INCIDENTES COMPUTACIONAIS**
- **ATIVIDADES DE INTERAÇÃO ENTRE CSIRTs (FÓRUM BRASILEIRO DE CSIRTs, FIRST, LACNIC, OEA, BRICS, …)**

TLP:WHITE

POLÍTICA NACIONAL DE SEGURANÇA DA INFORMAÇÃO (PNSI)

DECRETO Nº 9637, DE 26 DE DEZEMBRO DE 2018

POLÍTICA NACIONAL DE SEGURANÇA DA INFORMAÇÃO (PNSI)

TLP:WHITE

DIÁRIO OFICIAL DA UNIÃO

Publicado em: 27/12/2018 | Edição: 248 | Seção: 1 | Página: 23
Órgão: Atos do Poder Executivo

DECRETO Nº 9.637, DE 26 DE DEZEMBRO DE 2018

Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, **caput** , inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional.

O PRESIDENTE DA REPÚBLICA , no uso da atribuição que lhe confere o art. 84, **caput** , inciso VI, alínea "a", da Constituição,
D E C R E T A :

CAPÍTULO I

DISPOSIÇÕES GERAIS

Art. 1º Fica instituída a Política Nacional de Segurança da Informação - PNSI, no âmbito da administração pública federal, com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação a nível nacional.

Art. 2º Para os fins do disposto neste Decreto, a segurança da informação abrange:

I - a segurança cibernética;

II - a defesa cibernética;

III - a segurança física e a proteção de dados organizacionais; e

IV - as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

CAPÍTULO IV

DOS INSTRUMENTOS

Art. 5º São instrumentos da PNSI:

I - a Estratégia Nacional de Segurança da Informação; e

II - os planos nacionais.

Art. 6º A Estratégia Nacional de Segurança da Informação conterá as ações estratégicas e os objetivos relacionados à segurança da informação, em consonância com as políticas públicas e os programas do Governo federal, e será dividida nos seguintes módulos, entre outros, a serem definidos no momento de sua publicação:

I - segurança cibernética;

II - defesa cibernética;

III - segurança das infraestruturas críticas;

IV - segurança da informação sigilosa; e

V - proteção contra vazamento de dados.

Parágrafo único. A construção da Estratégia Nacional de Segurança da Informação terá a ampla participação da sociedade e dos órgãos e das entidades do Poder Público.

Art. 7º Os planos nacionais de que trata o inciso II do **caput** do art. 5º conterão:

I - o detalhamento da execução das ações estratégicas e dos objetivos da Estratégia Nacional de Segurança da Informação;

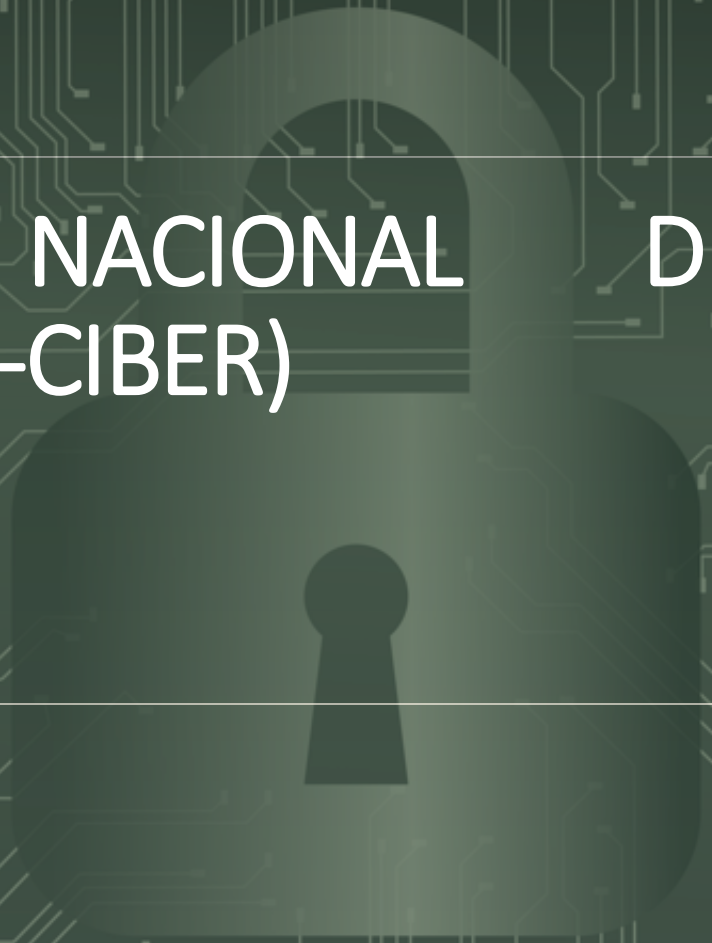
II - o planejamento, a organização, a coordenação das atividades e do uso de recursos para a execução das ações estratégicas e o alcance dos objetivos da Estratégia Nacional de Segurança da Informação; e

III - a atribuição de responsabilidades, a definição de cronogramas e a apresentação da análise de riscos e das ações de contingência que garantam o atingimento dos resultados esperados.

Parágrafo único. Os planos nacionais serão divididos em temas e designados a um órgão responsável, conforme estabelecido na Estratégia Nacional de Segurança da Informação.

Instrumentos da PNSI:

ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA (E-CIBER)



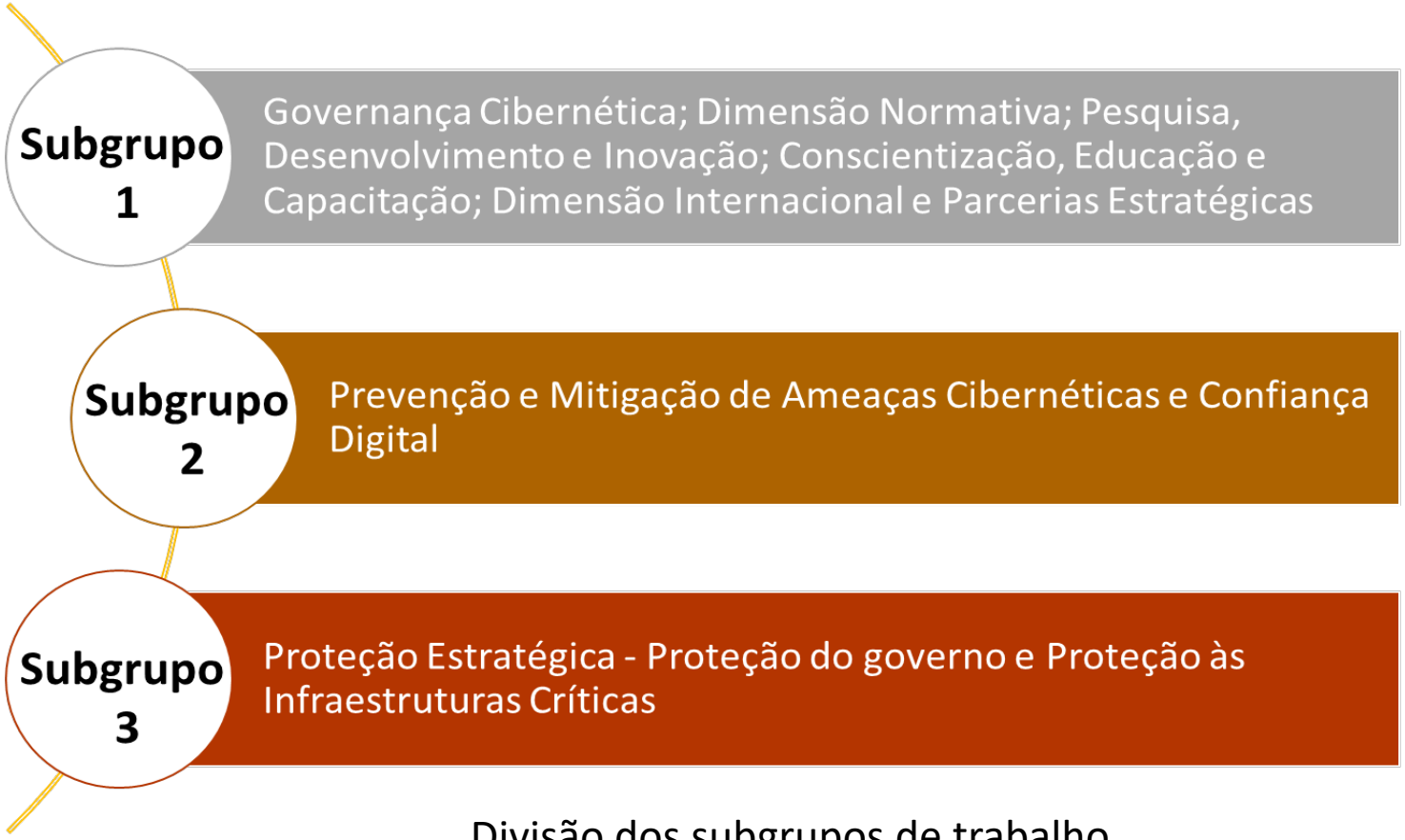
ESTRATÉGIA DE SEGURANÇA CIBERNÉTICA

TLP:WHITE

- **Revisão e integração da legislação**
- **Ampliação dos programas de capacitação e profissionalização**
- **Implantação do sistema nacional de segurança cibernética**
- **Expansão de programa de prospecções futuras**
- **Foco na proteção das crianças e adolescentes no ambiente digital**
- **Realização de campanhas educativas e de conscientização**
- **Atuação integrada na proteção das infraestruturas críticas**

METODOLOGIA ADOTADA

TLP:WHITE



Divisão dos subgrupos de trabalho

Resultado de trabalho realizado por representantes de órgãos públicos, de entidades privadas, e do meio acadêmico, que participaram de uma série de reuniões técnicas, para debater vários aspectos da Segurança Cibernética.

METODOLOGIA ADOTADA

TLP:WHITE

Etapas de elaboração da E-Ciber

31 reuniões dos subgrupos

- Participação efetiva de representantes de notório saber
- Intercâmbio de conhecimentos e de ideias
- Estabelecimento da concepção estratégica.

METODOLOGIA ADOTADA

TLP:WHITE

Eixos Temáticos da E-Ciber

Eixos de Proteção e Segurança

GOVERNANÇA DA SEGURANÇA CIBERNÉTICA NACIONAL

UNIVERSO CONECTADO E SEGURO: PREVENÇÃO E MITIGAÇÃO DE AMEAÇAS CIBERNÉTICAS

PROTEÇÃO ESTRATÉGICA

Eixos Transformadores

- **DIMENSÃO NORMATIVA**
- **DIMENSÃO INTERNACIONAL E PARCERIAS ESTRATÉGICAS**
- **PESQUISA, DESENVOLVIMENTO E INOVAÇÃO**
- **CONSCIENTIZAÇÃO, EDUCAÇÃO E CAPACITAÇÃO**

Foi considerado o Modelo de Maturidade da Capacidade em Segurança Cibernética (CMM)[3], que define as dimensões:

- Política e Estratégia de Segurança Cibernética;
- Cultura cibernética e sociedade;
- Educação, Treinamento e Habilidades em Segurança Cibernética;
- Marcos Legais e Regulatórios;
- Padrões, Organizações e Tecnologias.

TLP:WHITE

DIAGNÓSTICO E-CIBER / PNTIR

Base para Diagnóstico

TLP:WHITE

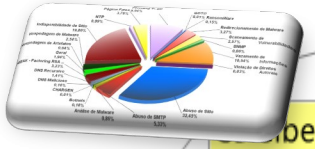
Base para diagnóstico

Colaboração

- Exemplos graves de incidentes
- Levantamento de legislação de Seg Ciber
- Fluxo de notificação e resposta

setores e órgãos diversos

Estatísticas



...ber e CAIS/RNP, CERT.br, CTIR.Gov

Relatórios Seg Ciber

OEA, ONU, OTAN e empresas privadas

Benchmarking internacional

- Políticas de Segurança Cibernética
- Estudos dos CERT's

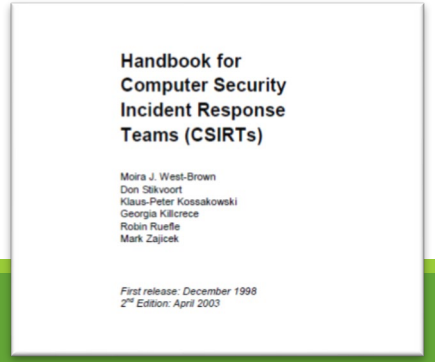
Argentina e Chile, Canadá, EUA, Holanda, Israel, Japão, México

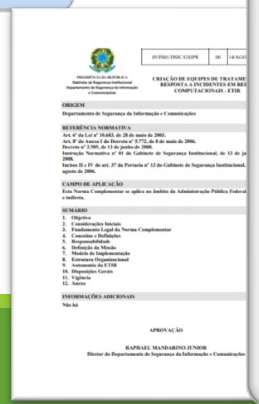
Exercício Guardião Cibernético

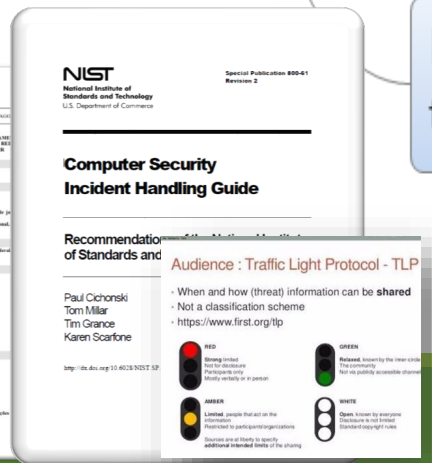
Relatório do grupo de estudos

Lacunas identificadas

ETIR







Mapeamento de processos de tratamento e resposta a incidentes

Alunos da UnB

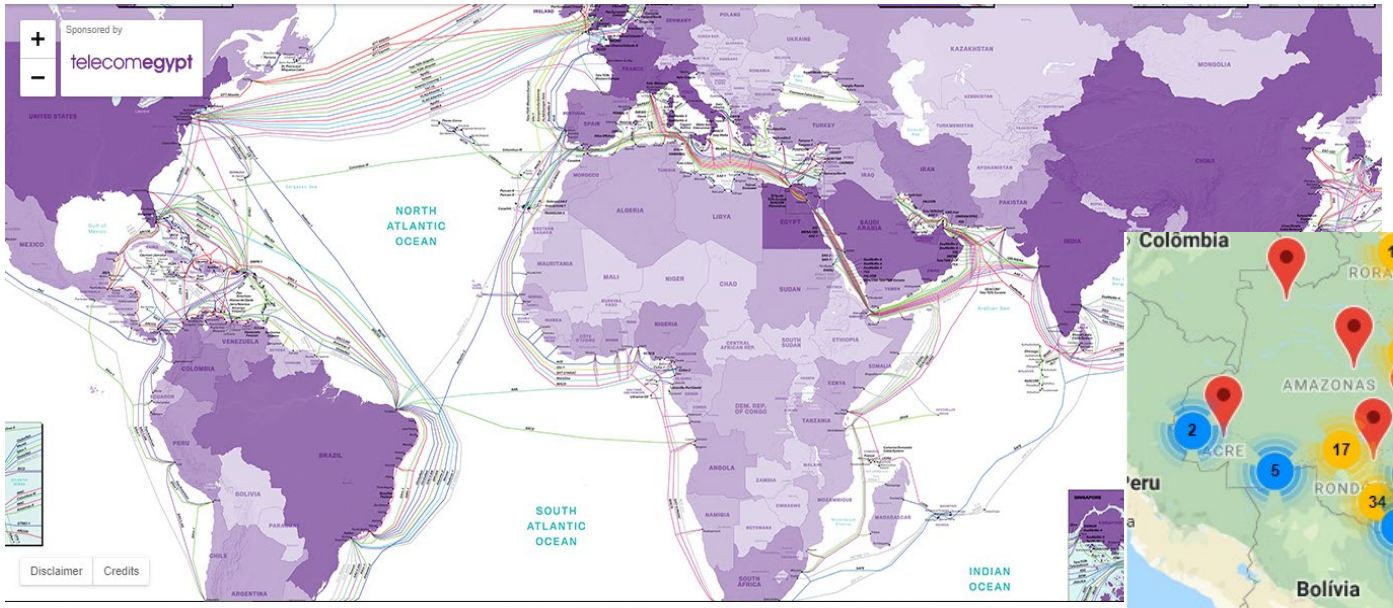
Características da Internet

TLP:WHITE

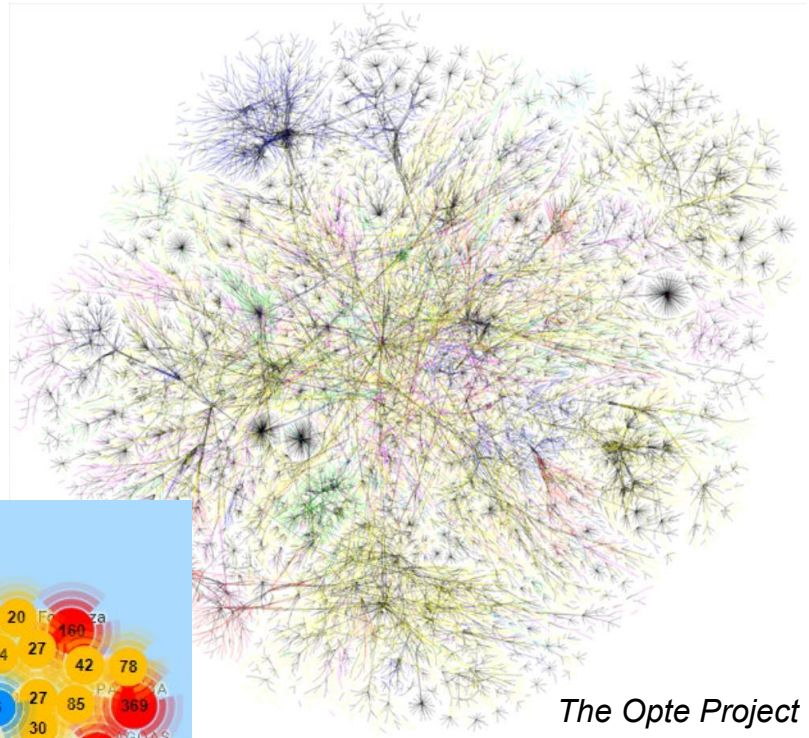
"Rede de redes"

- Sistema de **redes interconectadas**
- **Sem controle centralizado**

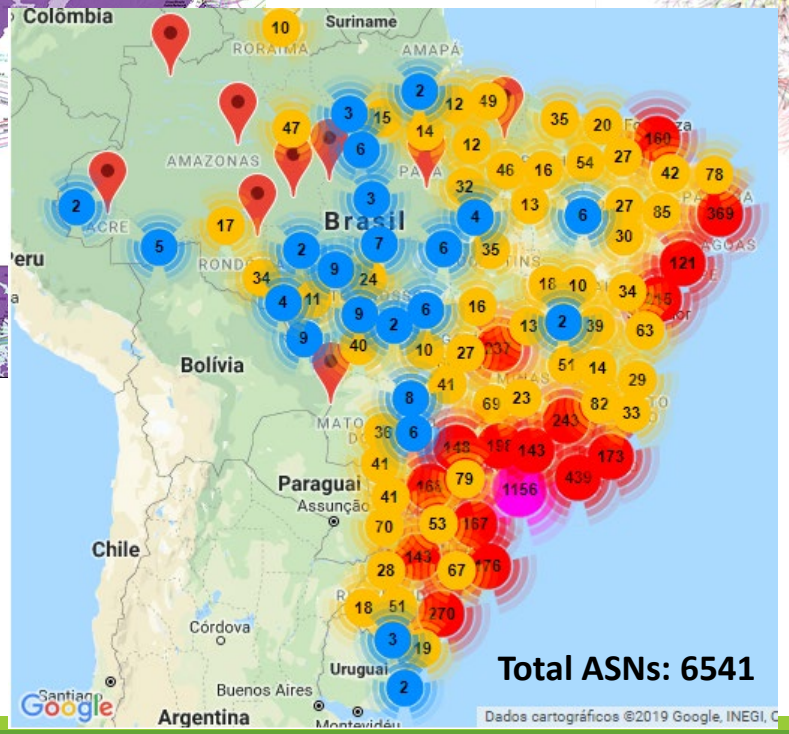
Fonte: CERT.br



https://submarine-cable-map-2019.telegeography.com/



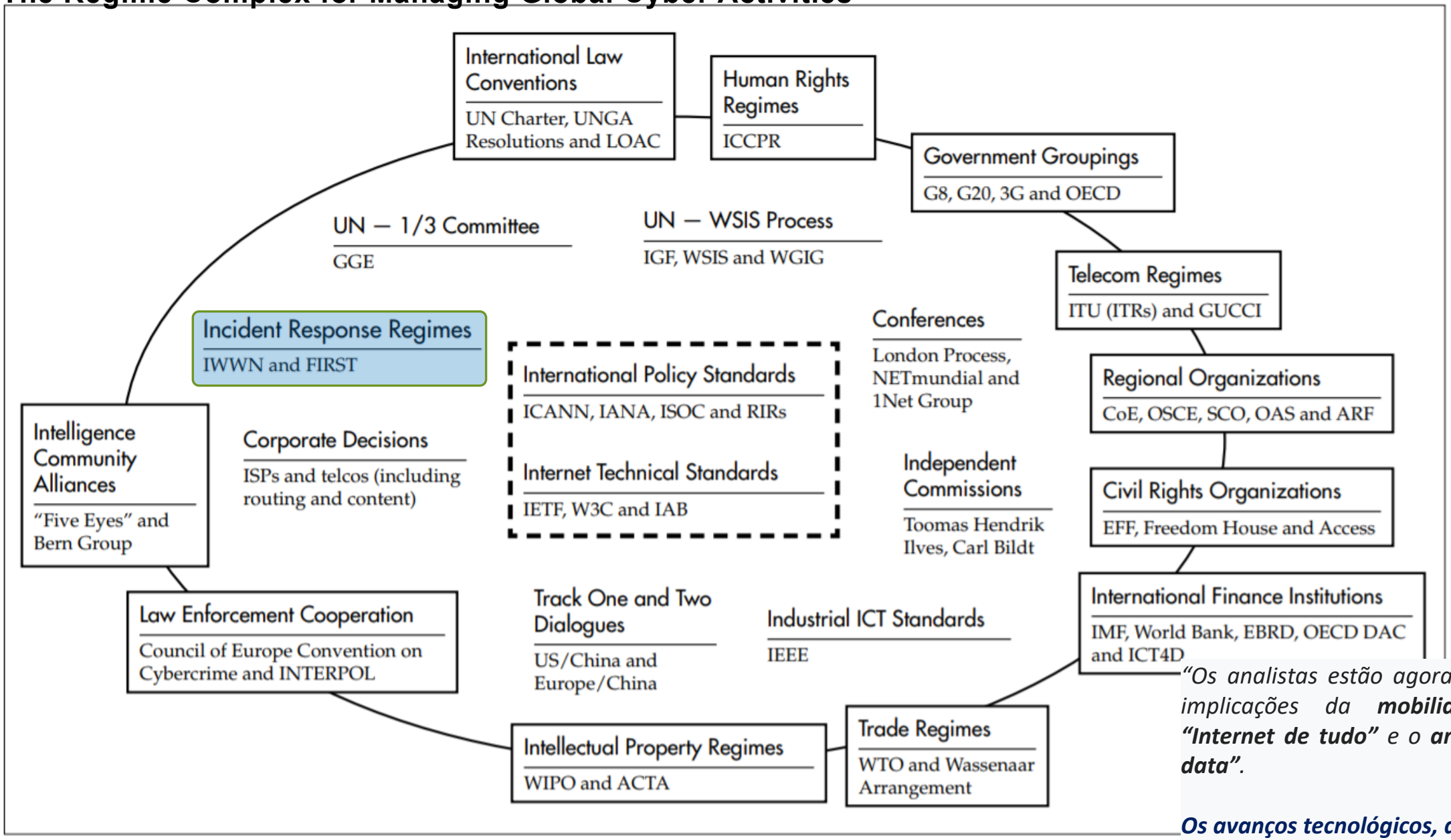
The Opte Project



Fonte: http://ix.br/localidades/brasmap

The Regime Complex for Managing Global Cyber Activities

TLP:WHITE



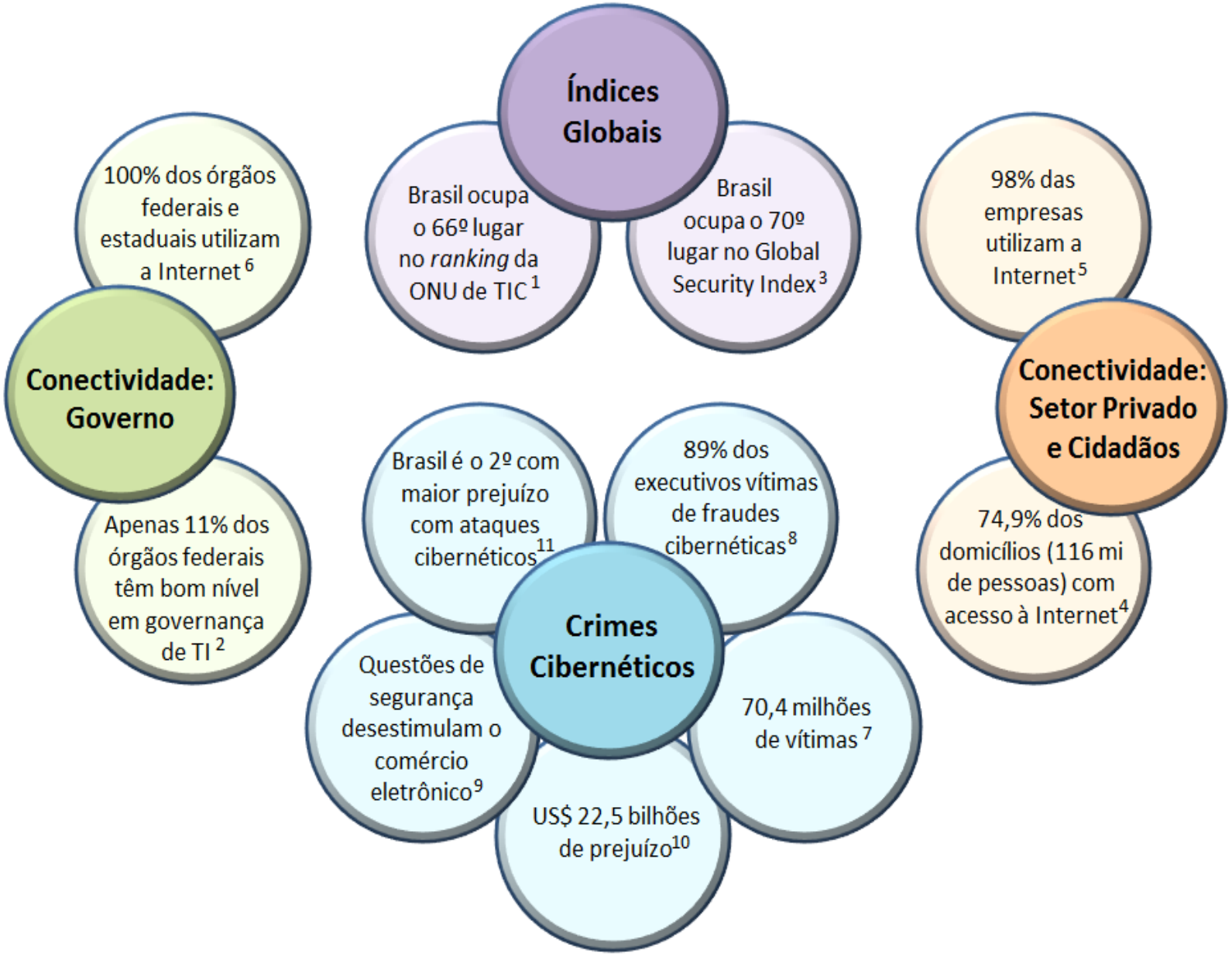
*"Os analistas estão agora tentando entender as implicações da **mobilidade onipresente**, a **"Internet de tudo"** e o **armazenamento de "big data"**.*

Os avanços tecnológicos, até agora, superaram a capacidade de resposta das instituições de governança."

Global Commission on Internet Governance Paper Series No. 1 May 20, 2014, Joseph S. Nye Jr.
https://www.cigionline.org/publications/regime-complex-managing-global-cyber-activities

Consolidação de dados estatísticos do Brasil em Segurança Cibernética

TLP:WHITE



(1) *MEASURING THE INFORMATION SOCIETY REPORT 2017.* ITU. Disponível em: <https://www.itu.int/en/ITUD/Statistics/Documents/publications/misr2017/MISR2017_Volume1.pdf>. Acesso em junho de 2019.

(2) BRASIL. Tribunal de Contas da União. Relatório de levantamento Governança de Tecnologia da Informação (TI) na Administração Pública Federal (APF). TC 008.127/2016-6. Disponível em: <https://portal.tcu.gov.br/fiscalizacao-de-tecnologia-da-informacao/atuacao/perfil-de-governanca-de-ti/>. Acesso em junho de 2019.

(3) *GLOBAL CYBERSECURITY INDEX 2018.* ITU. Disponível em: <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf>. Acesso em junho de 2019.

(4) *PNAD CONTÍNUA TIC 2017.* PNAD. Disponível em: <https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/23445-pnad-continua-tic-2017-internet-chega-a-tres-em-cada-quatro-domicilios-do-pais>. Acesso em junho de 2019.

(5) *PESQUISA TIC EMPRESAS 2017.* CETIC.BR. Disponível em: <https://www.cetic.br/publicacao/pesquisa-sobre-o-uso-das-tecnologias-de-informacao-e-comunicacao-nas-empresas-brasileiras-tic-empresas-2017/>. Acesso em junho de 2019.

(6) *PESQUISA TIC EMPRESAS 2017.* CETIC.BR. Disponível em: <https://cetic.br/tics/governo/2017/orgaos/>. Acesso em junho de 2019.

(7) *NORTON LIFELOCK CYBER SAFETY INSIGHTS REPORT 2018.* NORTON SECURITY. Disponível em: <2018 Norton LifeLock Cyber Safety Insights Report>. Acesso em junho de 2019.

(8) *8 A CADA 10 EXECUTIVOS JÁ ENFRENTARAM FRAUDES CIBERNÉTICAS.* IT FORUM 365. Disponível em: <https://itforum365.com.br/8-cada-10-executivos-ja-enfrentaram-fraudes-ciberneticas/> Acesso em junho de 2019.

(9) *PESQUISA TIC EMPRESAS 2017.* CETIC.BR. Disponível em: <https://www.cetic.br/media/docs/publicacoes/2/10522920190604-TIC-EMPRESAS-2017-ed-rev.pdf>. Acesso em junho de 2019.

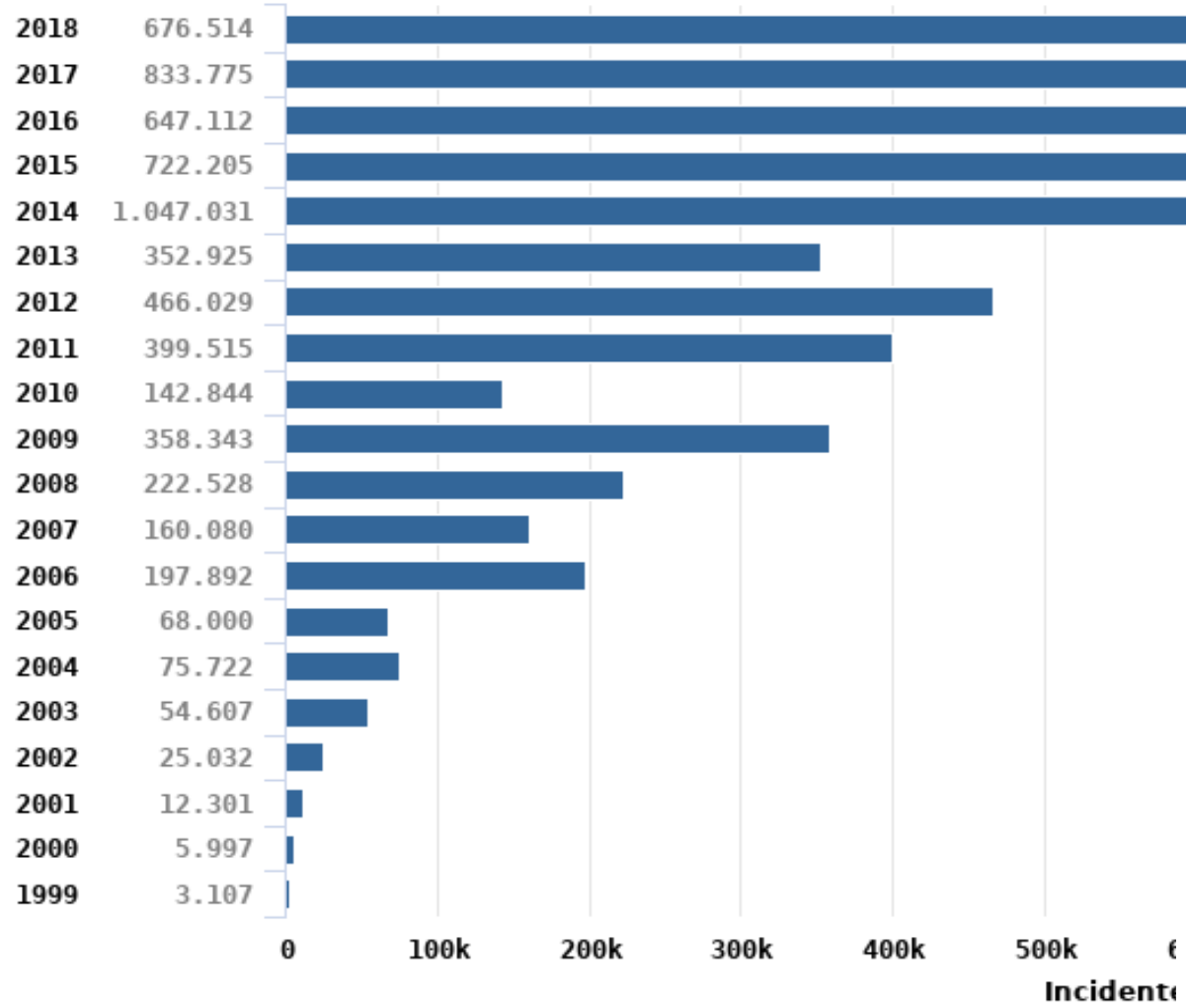
(10) *NORTON CYBER SAFETY INSIGHTS REPORT, 2017.* NORTON SECURITY. Disponível em: <https://us.norton.com/cyber-security-insights-2017> Acesso em junho de 2019.

(11) *NORTON CYBER SAFETY INSIGHTS REPORT, 2017.* NORTON SECURITY. Disponível em: <https://us.norton.com/cyber-security-insights-2017> Acesso em junho de 2019.

Números de notificações de incidentes

TLP:WHITE

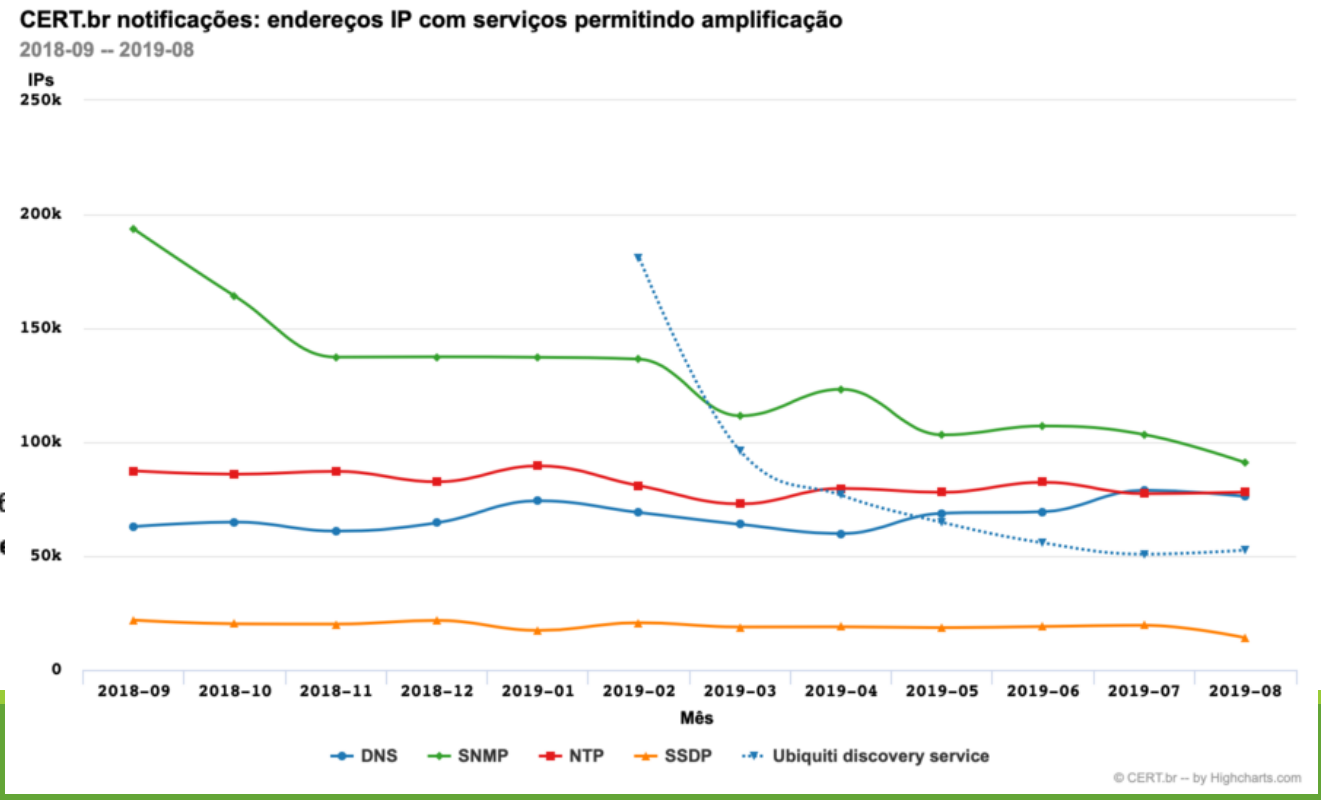
Ano	total
2018	676.514
2017	833.775
2016	647.112
2015	722.205
2014	1.047.031
2013	352.925
2012	466.029
2011	399.515
2010	142.844
2009	358.343
2008	222.528
2007	160.080
2006	197.892
2005	68.000
2004	75.722
2003	54.607
2002	25.032
2001	12.301
2000	5.997
1999	3.107



cert.br

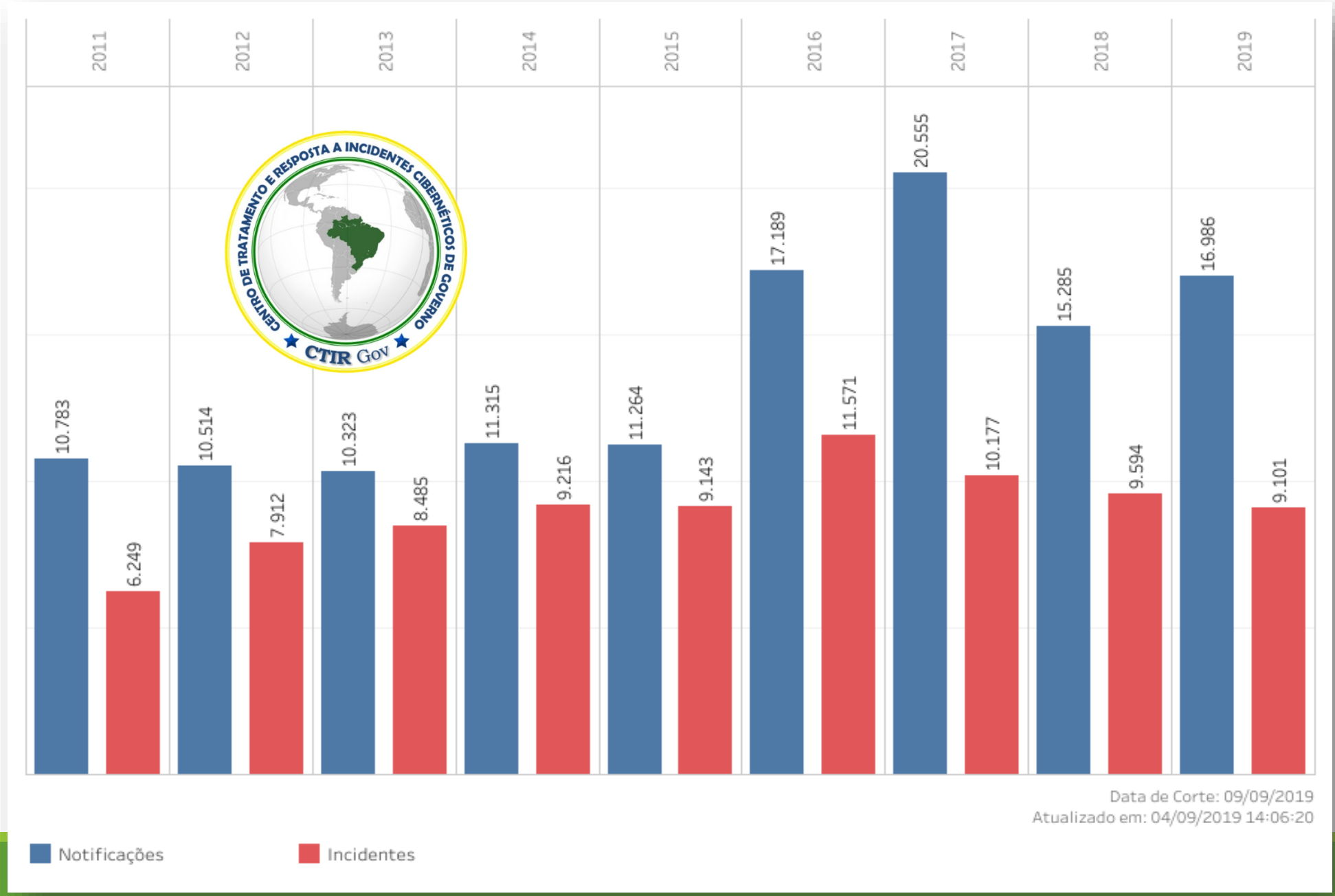
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

https://www.cert.br/



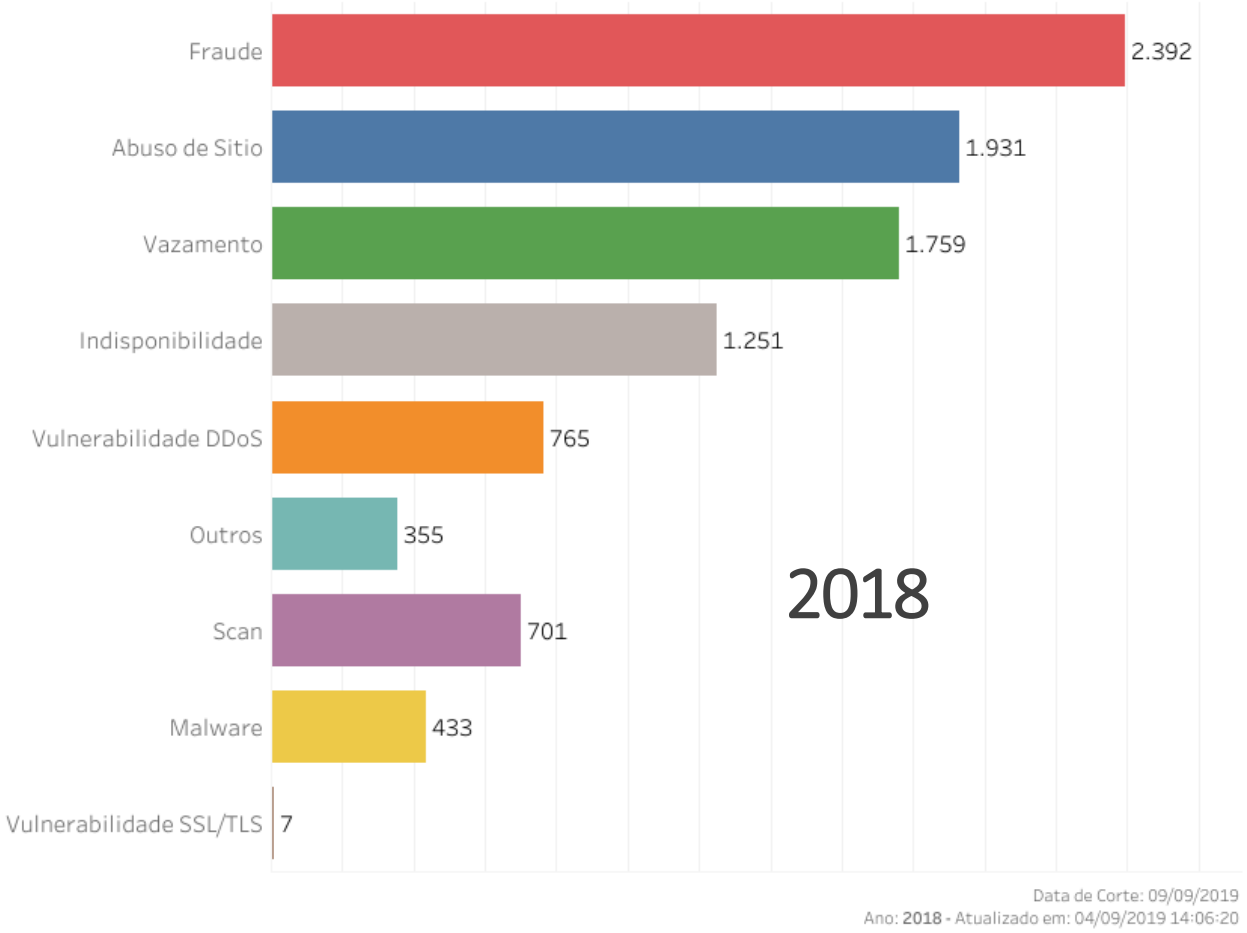
Números de notificações de incidentes

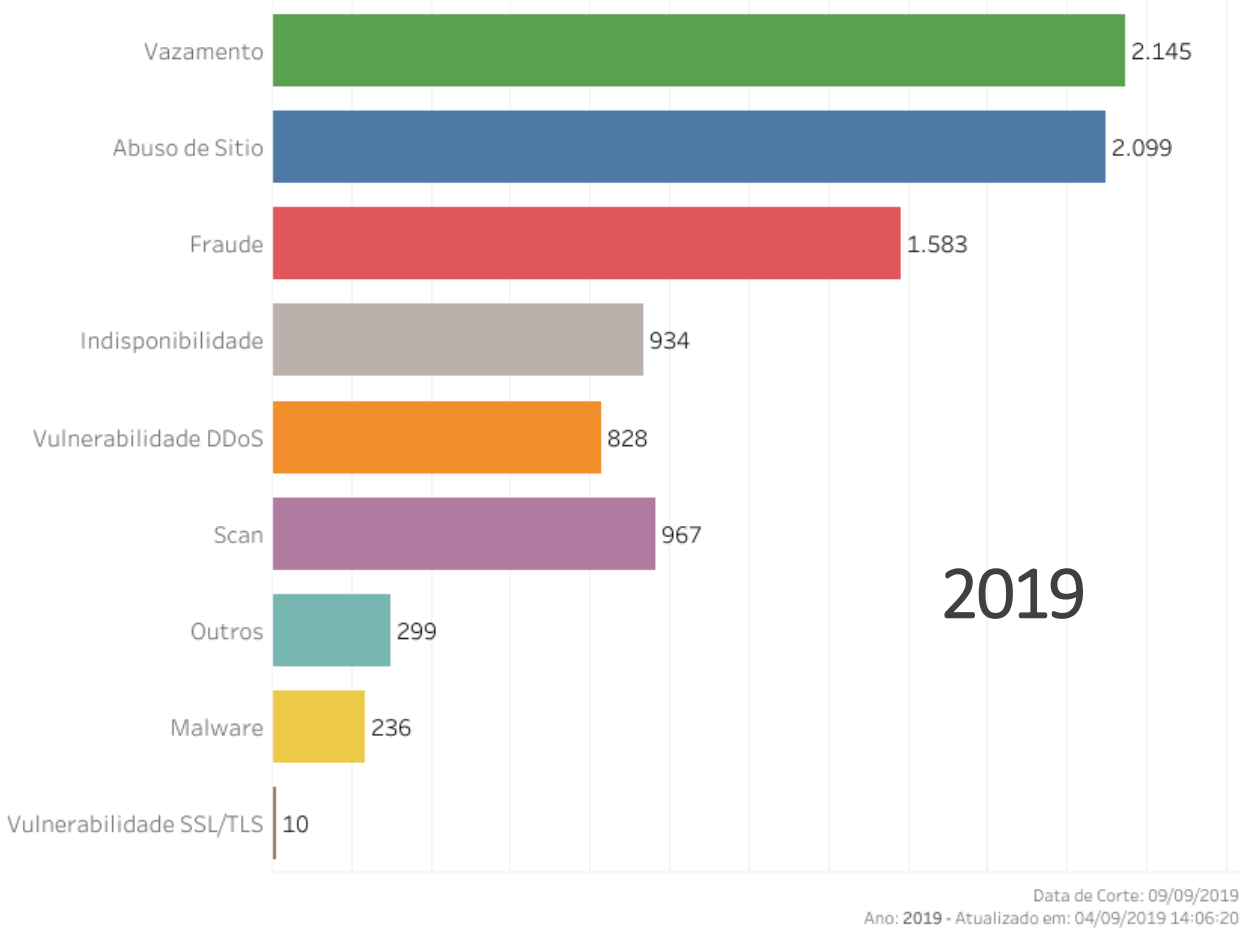
TLP:WHITE



Números de notificações de incidentes

TLP:WHITE





TLP:WHITE

PLANO NACIONAL DE TRATAMENTO E RESPOSTA A INCIDENTES COMPUTACIONAIS (PNTIR)

PARTE DA ESTRATÉGIA NACIONAL DE SEGURANÇA CIBERNÉTICA (E-CIBER)

PLANO NACIONAL DE TRATAMENTO E RESPOSTA DE INCIDENTES COMPUTACIONAIS (PNTIR)

TLP:WHITE

O **plano operacional** é o esquema que visa gerar **resultados a curto prazo** e descreve as tarefas a serem realizadas pelos colaboradores, indispensáveis para o alcance dos objetivos da instituição.

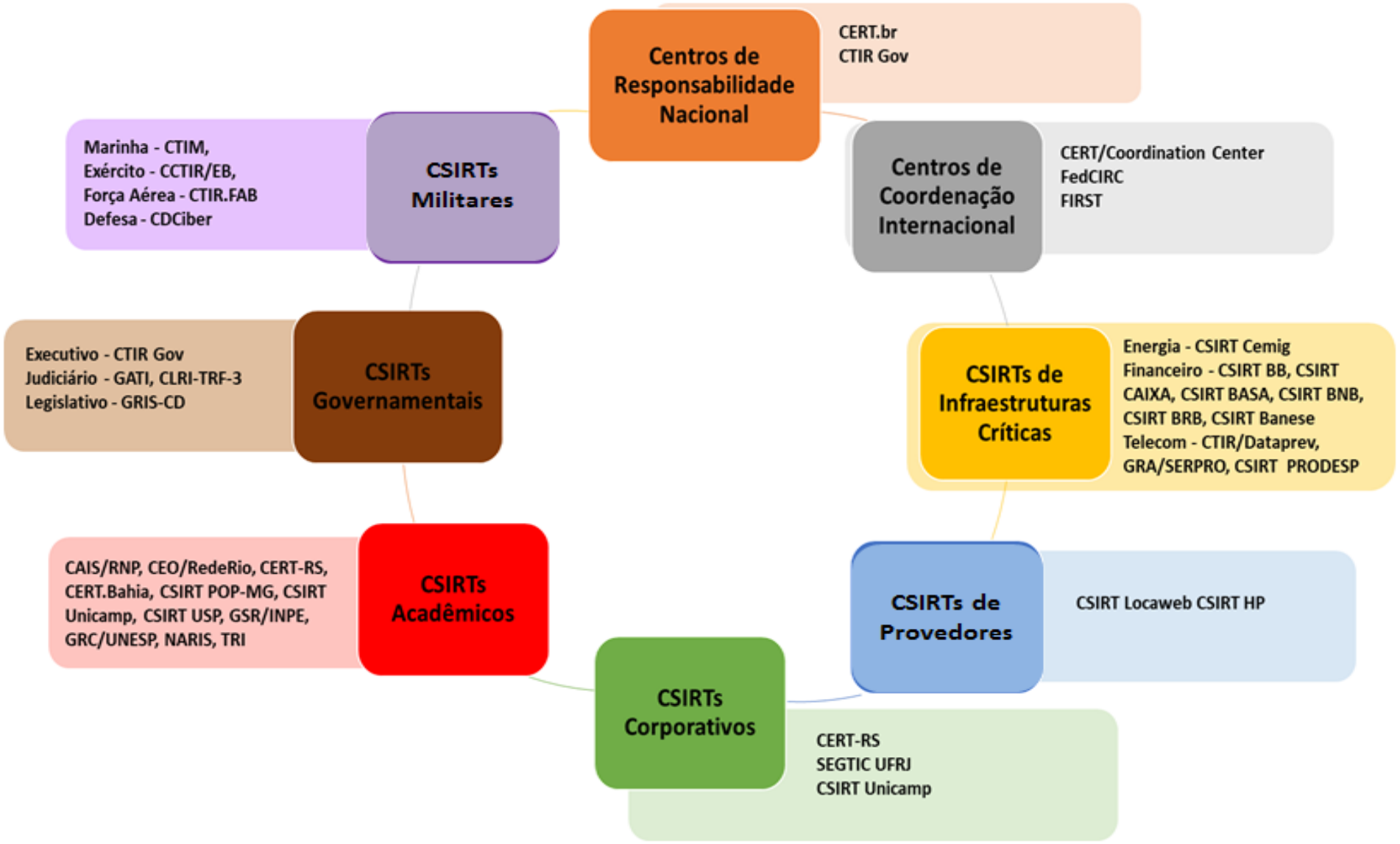
O PLANO é um verdadeiro guia sobre o que a instituição tem que fazer e como fazer, para o alcance de seus objetivos estratégicos.

O plano operacional cuida das **atividades de rotina** da instituição, garantindo que os colaboradores cumpram com suas responsabilidades de acordo com as políticas e conformidades.

*O plano operacional identifica **responsabilidades**, atividades, recursos, divide tarefas e define responsáveis.*

FOCO NA ATUAÇÃO DE CSIRTs

TLP:WHITE



PNTIR - ATUAÇÃO COLABORATIVA

PNTIR – 8 METAS BASEADAS NOS OBJETIVOS ESTRATÉGICOS DA E-CIBER

TLP:WHITE

ENTRE ELAS ....

- **Estimular o compartilhamento de informações de incidentes e vulnerabilidades cibernéticos, baseado na mútua confiança, tanto do setor público quanto do setor privado.**

- **Estimular a criação e atuação de equipes de tratamento e resposta de incidentes cibernéticos, tanto do setor público quanto do setor privado.**

- **Ampliar cooperação entre governo, academia e a iniciativa privada para soluções de segurança cibernética.**

- **Estabelecer treinamento regular para os integrantes das ETIRs/CSIRTs.**

PNTIR – AÇÕES NECESSÁRIAS AO CUMPRIMENTO DAS METAS ESTABELECIDAS

TLP:WHITE

O Plano Nacional de Tratamento de Incidentes apresenta um conjunto de ações estratégicas que deverão ser apoiadas ou implementadas pelo Departamento de Segurança da Informação (DSI), em conjunto com os diversos atores do setor de segurança cibernética, de modo a superar os desafios e atingir as metas estabelecidas.

- **Estabelecer mecanismos de cooperação nacional e internacional para evitar, detectar, tratar e responder às ameaças cibernéticas**
- **Elaborar guia de tratamento de incidentes cibernéticos para o setor público e privado**
- **Realizar parcerias com estados e municípios para estabelecer rotina de compartilhamento de informações sobre incidentes e vulnerabilidades cibernéticos**
- **Realizar ações que estabeleçam a transferência de conhecimento em segurança cibernética entre Estados, órgãos públicos, setor privado e a academia**
- **Promover e incentivar a realização de seminários em universidades sobre o tratamento e resposta a incidentes cibernéticos**

PNTIR - AÇÕES

TLP:WHITE

- **Desenvolver exercícios cibernéticos nacionais envolvendo múltiplos atores**
- **Participar de eventos e exercícios internacionais sobre segurança cibernética**
- **Criar ações de emissão de alertas de incidentes e vulnerabilidades cibernéticos**
- **Realizar reuniões de trabalho, conferências, seminários e outros foros de especialistas para compartilhar experiência e capacitar pessoas da área de segurança cibernética**
- **Criar guia prático para a criação de ETIR pelas agências reguladoras das IFC**
- **Criar treinamentos em técnicas de prevenção, detecção, resposta e resiliência**
- **Criar parcerias para incentivar o setor privado a investir em medidas de segurança**
- **Utilizar sistemas avançados baseados em tecnologias emergentes para atuação contra incidentes cibernéticos**

TLP:WHITE

CONSIDERAÇÕES FINAIS

Considerações Finais

TLP:WHITE

✓ **Implantação do Plano: Agenda Estratégica de Tratamento e Resposta a Incidentes Computacionais do Brasil e Documentos de execução**

- ✓ Como estratégia central para o alcance dos objetivos e das metas previstas neste documento, assim como para orientar as diversas atividades nele elencadas, estabeleceram-se dois caminhos integrados de planejamento e de implementação de políticas para a segurança cibernética brasileira:
  - (i) uma Agenda Estratégica da Segurança Cibernética Brasileira e
  - (ii) elaboração de documentos de caráter executivo.
- ✓ A cada edição do Plano Nacional, a Agenda será revista observando-se um horizonte de planejamento de 10 anos a partir da data de elaboração de cada PNTIR.

Considerações Finais

TLP:WHITE

- ✓ **Monitoramento e avaliação**
  - ✓ Indicadores, objetivos e ações devidamente monitorados e avaliados por meio da ampliação das ferramentas e dos sistemas de informações de segurança cibernética, que permitam o acompanhamento de seus resultados orçamentários e de suas vertentes de eficácia, eficiência e efetividade das políticas definidas.
  - ✓ A sistemática de monitoramento prevê a apresentação e a divulgação dos principais resultados obtidos em órgãos colegiados (entre eles a Câmara Técnica de Tratamento e Resposta a Incidentes Computacionais) que compõem o Sistema Nacional de Segurança da Informação, de acordo com os temas pertinentes e as competências regimentais de cada um dos colegiados.

Obrigado!

TLP:WHITE

Democlydes Carvalho – Coordenador Geral CTIR Gov

democlydes@ctir.gov.br

democlydes.carvalho@presidencia.gov.br

+55 61 3411-2315 | +55 61 98146-8989

https://www.ctir.gov.br/

ctir@ctir.gov.br (abuse)

@CtirGov

www.linkedin.com/company/ctirgov/