

Papel do CERT.br no Ecosystema Nacional de Tratamento de Incidentes

Dra. Cristine Hoepers

Gerente-Geral, CERT.br/NIC.br
cristine@cert.br

Exercício Guardião Cibernético 8.0
Brasília/DF – 21 de setembro de 2026

cert.br nic.br cgi.br

TLP:CLEAR



Missão do CERT.br

Aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil.

cert.br

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

Gestão de incidentes

- Ponto de contato nacional de último recurso
- Notificações e encaminhamentos
- Apoio técnico e coordenação

Consciência situacional

- Aquisição de dados
 - Sensores próprios
 - Dados de parceiros
- Compartilhamento
 - Eventos via MISP
 - Portal de estatísticas

Transferência de conhecimento

- Treinamento
- Conscientização
 - Cartilhas
 - Guias de boas práticas
- Fórum Brasileiro de CSIRTs
- Workshop MISP

Público Alvo (Constituency)

Redes que utilizam recursos administrados pelo NIC.br

- endereços IP ou ASNs alocados ao Brasil
- domínios sob o ccTLD .br

Governança

Mantido pelo NIC.br

- atividades custeadas pelo registro de domínios sob o ccTLD .br

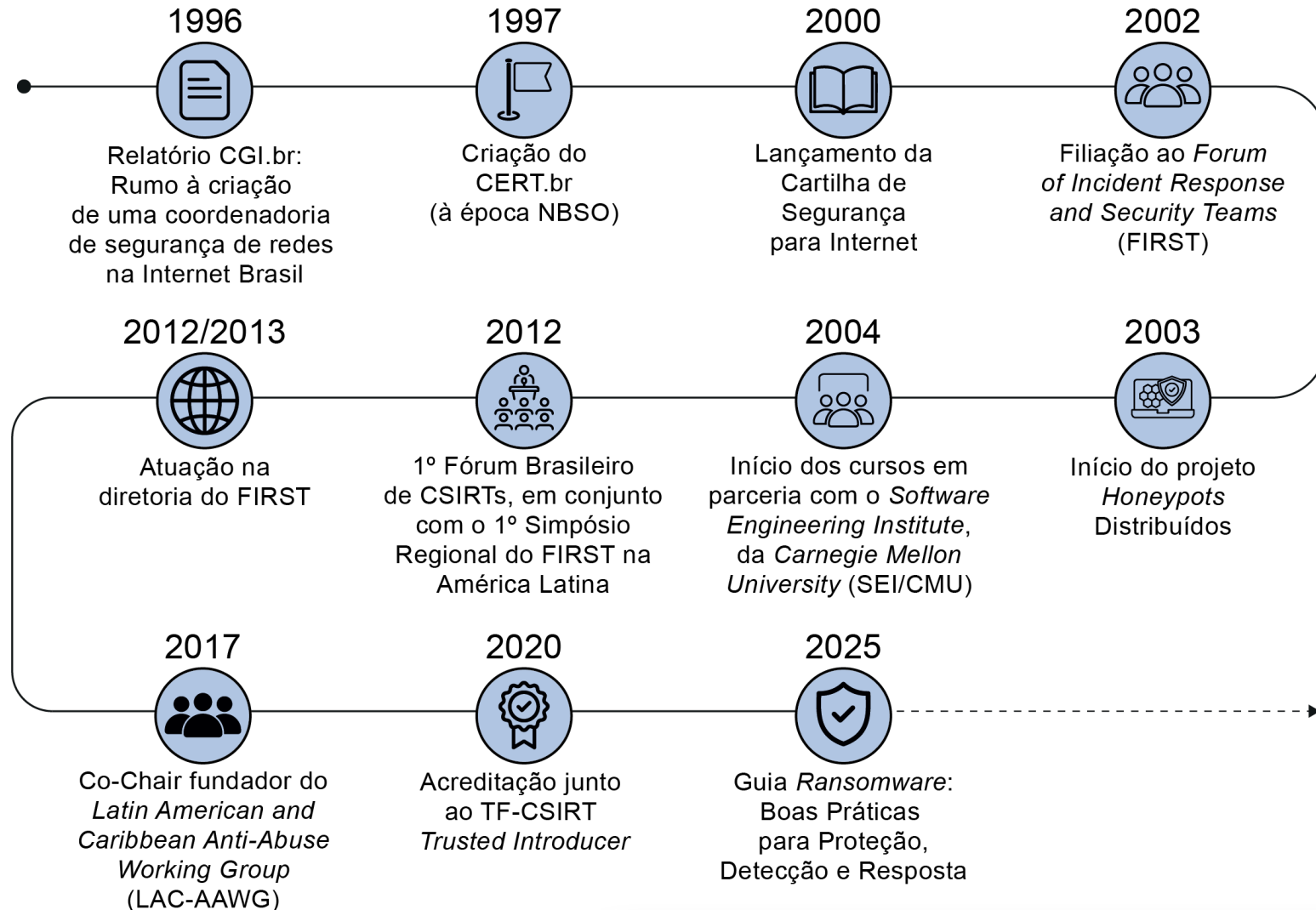
O NIC.br implementa as decisões e os projetos do CGI.br

- comitê responsável por coordenar e integrar as iniciativas e serviços da Internet no país.

<https://cert.br/sobre/>
<https://cert.br/sobre/filiacoes/>
<https://cert.br/sobre/reconhecimento/>

Estudo do Comitê Gestor da Internet no Brasil – CGI.br: Princípios que nortearam a criação e evolução do CERT.br

- Receber e registrar ocorrências
- Coletar e publicar estatísticas
- Orientar tecnicamente e intermediar o contato entre redes envolvidas em incidentes
- Fomentar treinamento e atualização em segurança
- Fomentar encontros e congressos de segurança
- Representar o Brasil como um dos órgãos de segurança em âmbito nacional e internacional



Fonte: Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil, CGI.br, 1996
<https://cert.br/sobre/estudo-cgibr-1996.html>

CERT.br 29 anos construindo pontes e comunidades para Aumentar a Capacidade Nacional de Tratamento de Incidentes

Nenhuma estrutura centralizada fará sozinha a segurança ou a resposta a incidentes

Comunidade Nacional

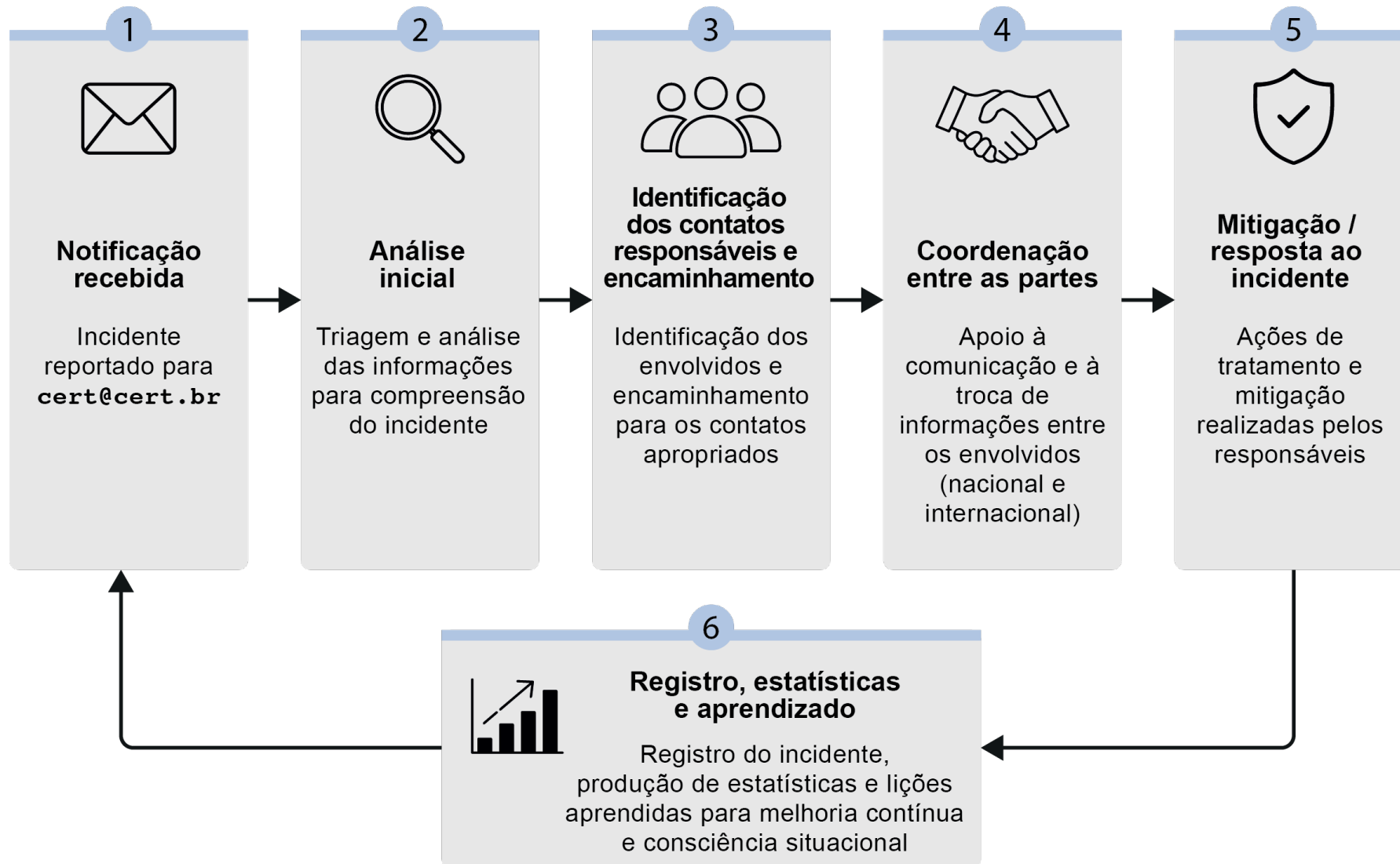
- Ajudar a criar e treinar Times de Tratamento de Incidentes de Segurança (CSIRTs/ETIRs)
 - mais times levam à cooperação e melhora na segurança das redes
- Compartilhar consciência situacional sobre tendências de ataques no Brasil

Comunidade Internacional

- Estabelecer relações de confiança
 - facilitar a comunicação
- Influenciar os padrões e certificações sendo construídos para CSIRTs
- Levar a visão nacional aos fóruns pertinentes



Papel do CERT.br no tratamento de um incidente

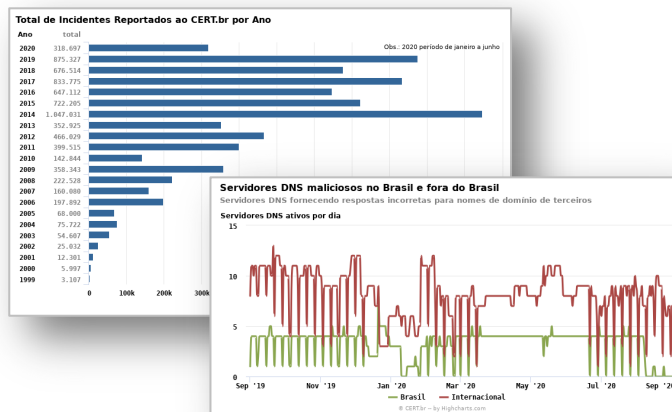


Consciência Situacional

Fontes dos Dados, Métricas e Compartilhamento

Notificações voluntárias de incidentes enviadas para:

cert@cert.br



Compartilhamento via MISP

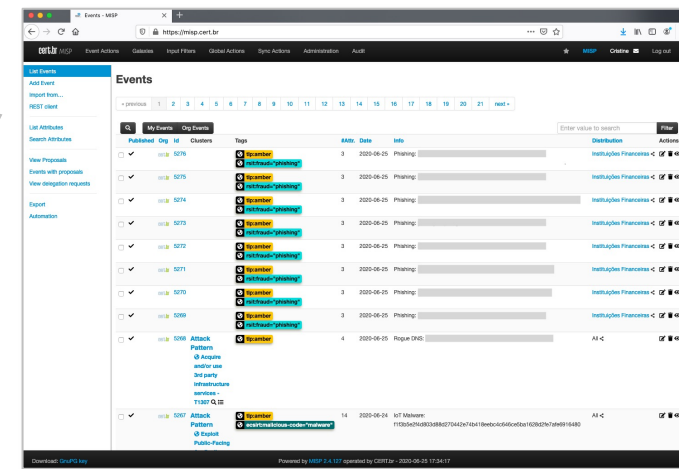
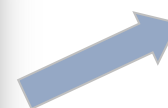
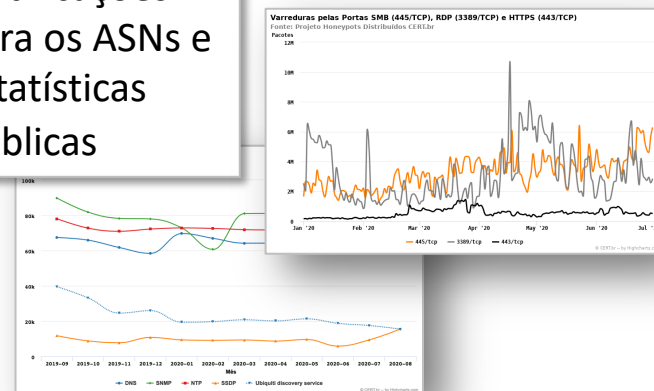
- Indicadores selecionados são compartilhados com parceiros
- Servidores DNS maliciosos
- *Phishing*
- Binários e Comando e Controle de *botnets* IoT
- Amplificadores usados em ataques DDoS
- URLs maliciosas

Threat feeds

- *Honeypots* Distribuídos do CERT.br
- Team Cymru
- ShadowServer
- SpamHaus
- Shodan
- Operações Anti-Botnet (Microsoft/FBI)



Notificações para os ASNs e estatísticas públicas



<https://stats.cert.br/>

<https://cert.br/misp/>

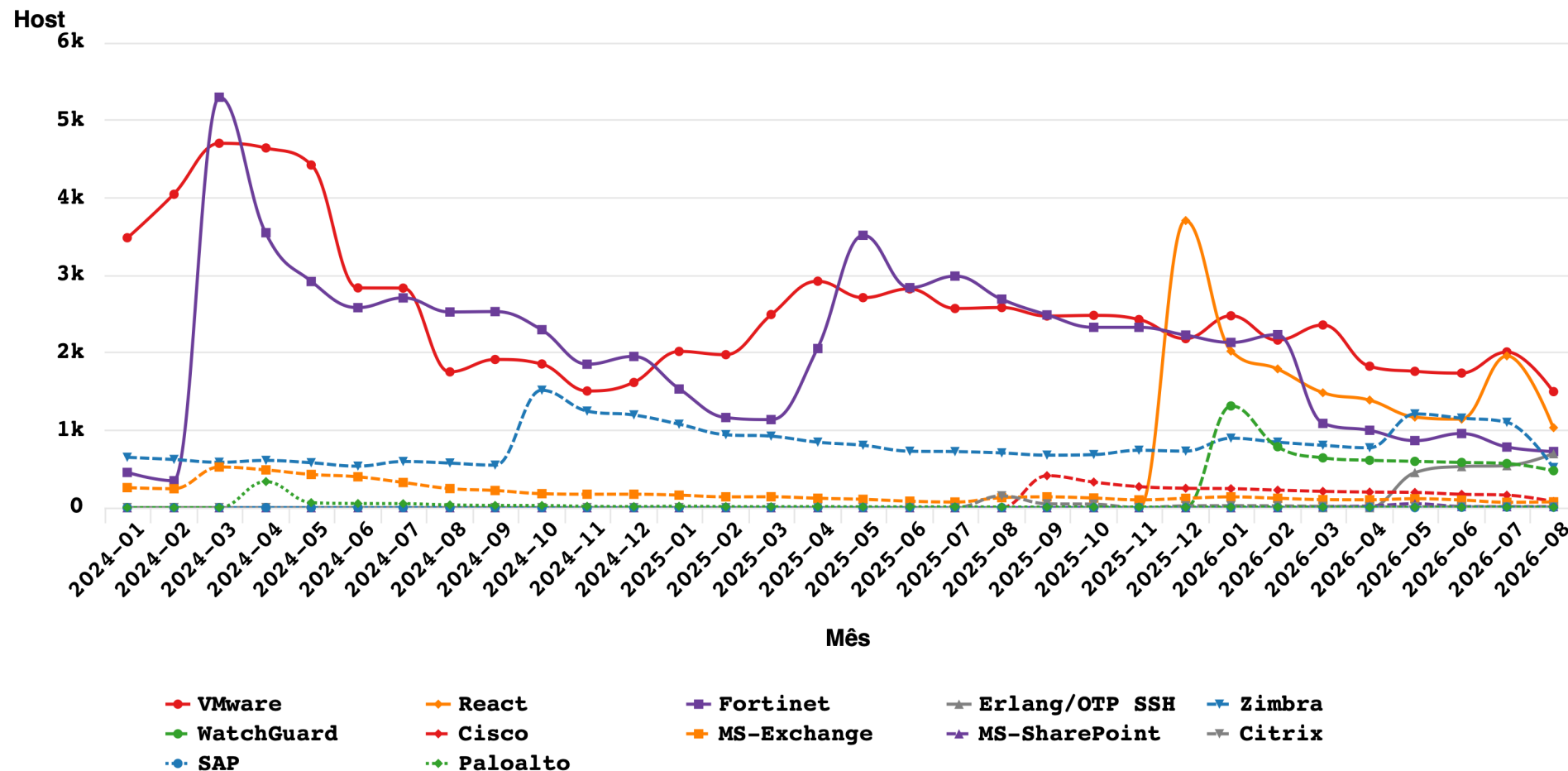
TLP:CLEAR

cert.br nic.br cgi.br

Notificações para Sistemas Autônomos CVEs CISA KEV ou usados por *Ransomware*

CERT.br notificações: hosts com serviços vulneráveis

2024-01 -- 2026-08



Fonte: CERT.br — <https://stats.cert.br/> — by Highcharts.com

<https://stats.cert.br/vulns/>

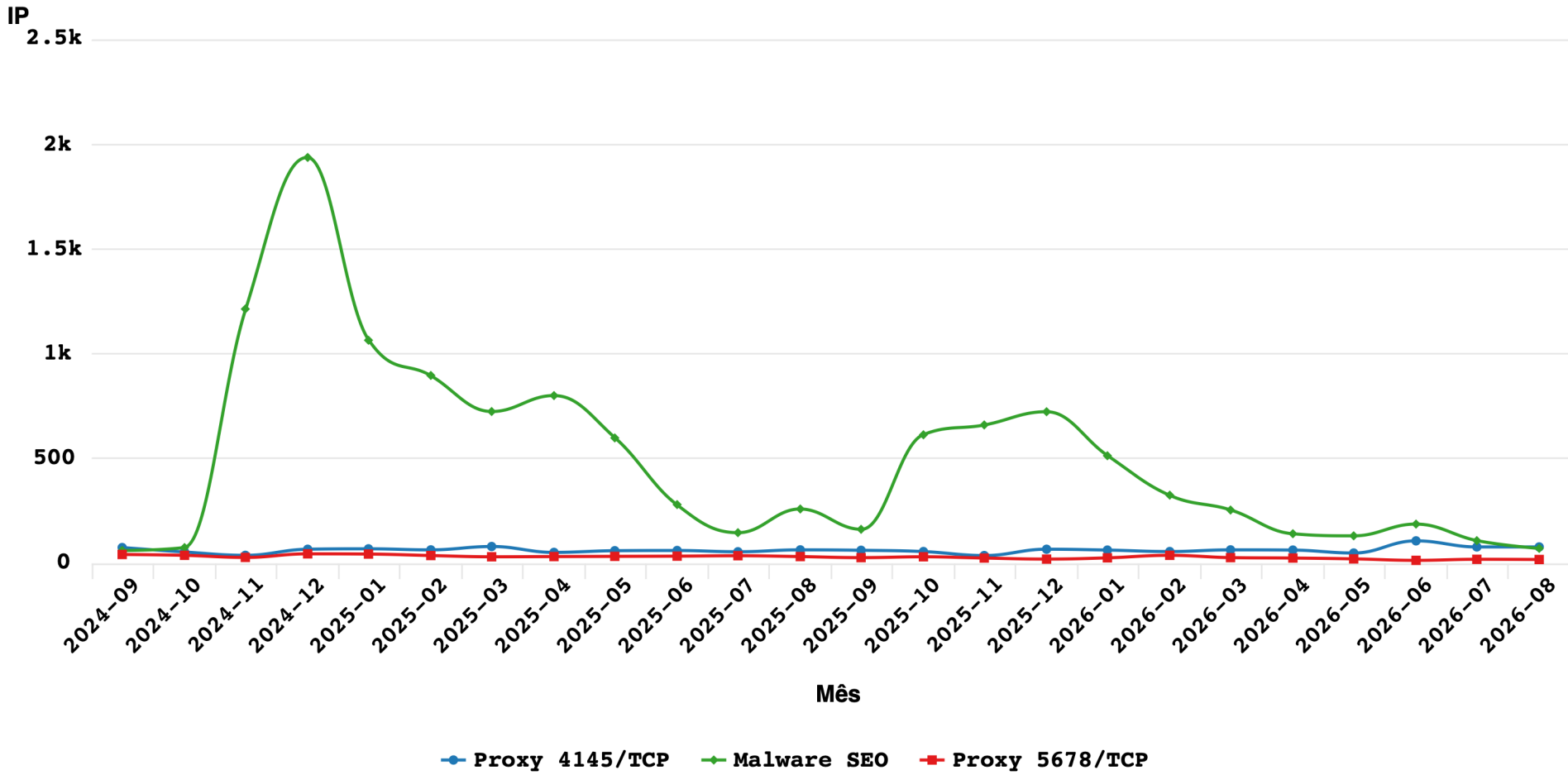
TLP:CLEAR

cert.br nic.br cgi.br

Notificações para Sistemas Autônomos

Indícios de Comprometimento

CERT.br notificações: endereços IP com indícios de comprometimento
Dispositivos com evidências de estarem comprometidos e sendo ativamente abusados



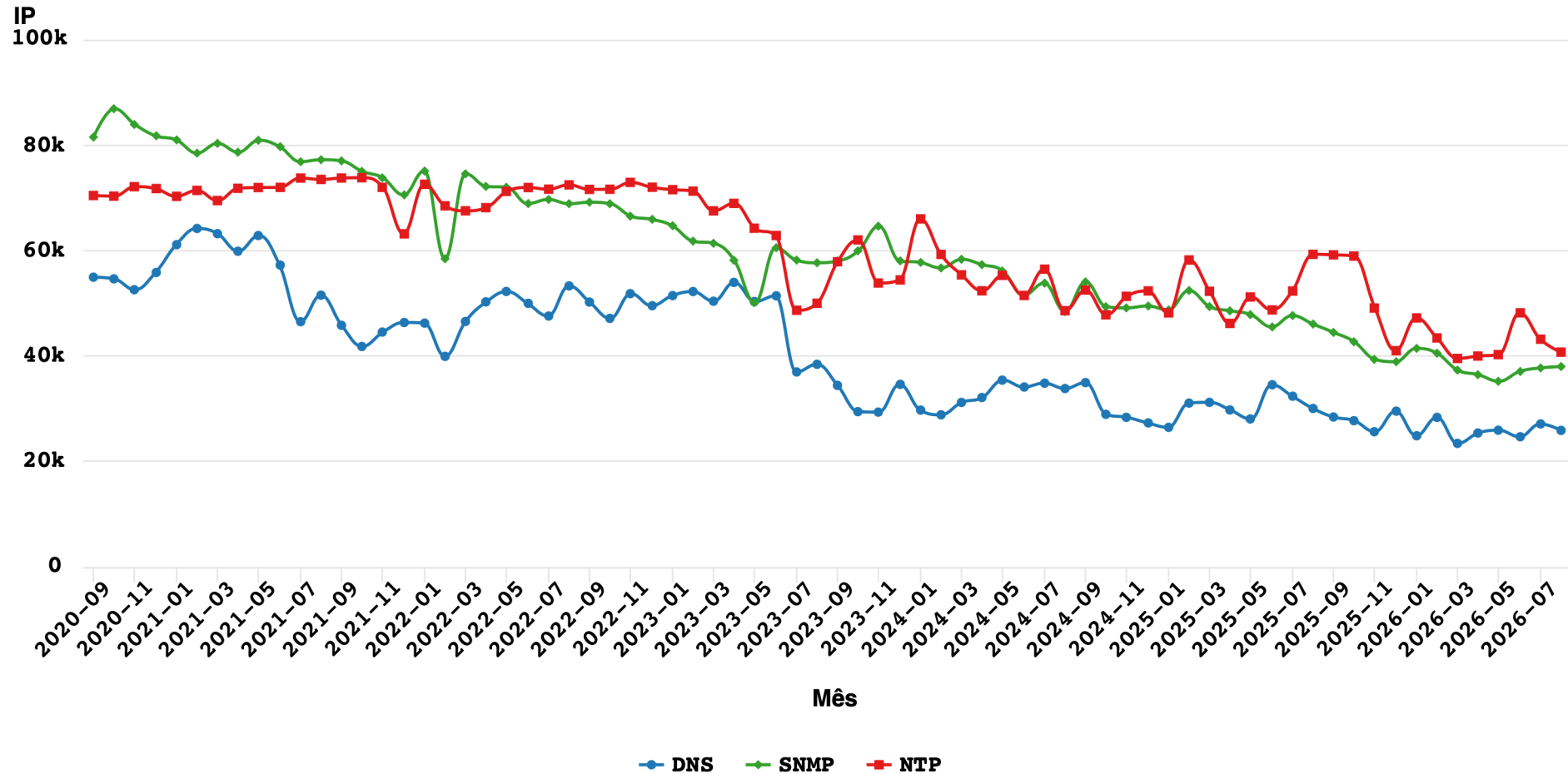
Fonte: CERT.br — <https://stats.cert.br/> — by Highcharts.com

<https://stats.cert.br/ioc/>

Notificações para Sistemas Autônomos Dispositivos Permitindo Amplificação

CERT.br notificações: endereços IP com serviços permitindo amplificação

2020-09 -- 2026-08



Fonte: CERT.br — <https://stats.cert.br/> — by Highcharts.com

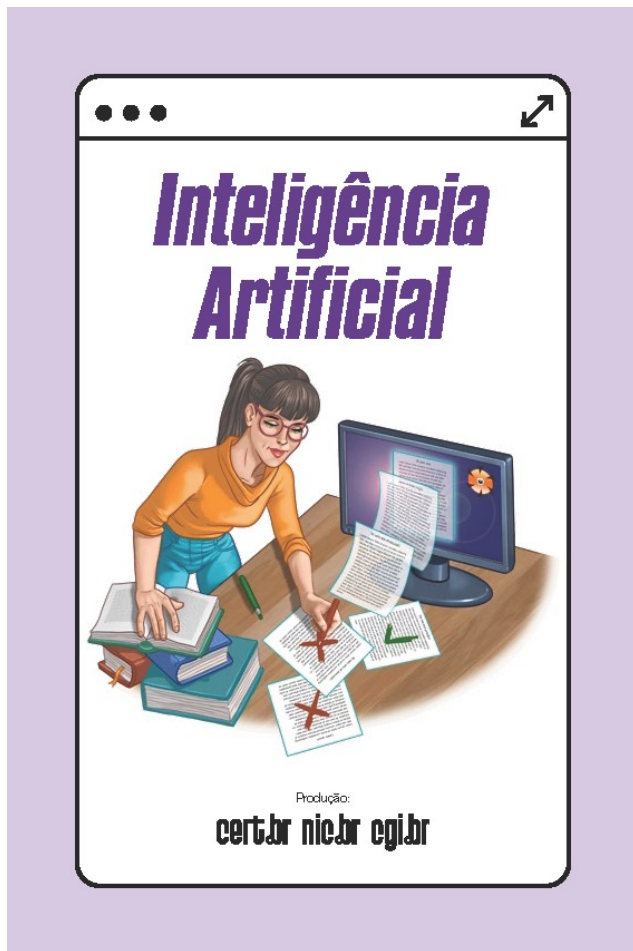
<https://stats.cert.br/amplificadores/>

TLP:CLEAR

cert.br nic.br cgi.br

Conscientização do Público em Geral

Cartilha de Segurança para Internet



<https://cartilha.cert.br/>

Boas Práticas para Público Técnico

Ransomware: Como se Proteger

cert.br

Sobre CSIRTs Cursos Publicações Palestras Estatísticas

Início > Publicações > Ransomware

Ransomware: Boas Práticas para Proteção, Detecção e Resposta

Nas 4 partes desse documento você encontra uma descrição de como acontece um ataque de ransomware e boas práticas para proteção, detecção e resposta a esses ataques.

Folheto "Ransomware: Como se Proteger"

Baixe o folheto com o resumo de todas as partes do documento.

 **Formato Digital e para Impressão Simples**

➔ [Baixe o PDF aqui](#)

➔ [Baixe o PDF em alta resolução aqui](#)

 **Formato para Impressão em Gráfica**

➔ [Baixe o PDF aqui](#)

Orientações para impressão em gráfica: Lâmina: 60x25cm total; Papel: Couché Fosco 300g; Impressão em CMYK; Saída em CTP; Laminado Fosco, frente e verso, faca especial e dobras paralelas (2 dobras).

Seja um Parceiro de Divulgação

 **Ministre Palestras**

Ajude a divulgar este material dando palestras sobre o tema.

➔ [Baixe os slides aqui](#)

 **Peça o Folheto com sua Logomarca**

Se tiver interesse no folheto personalizado com a logomarca da sua organização, envie a solicitação para o e-mail doc@cert.br. Ressaltamos que a impressão de materiais personalizados é responsabilidade do solicitante.

Infográficos completos em formato PNG e SVG

Ransomware: Como acontece		
Ransomware: Como proteger		
Ransomware: Como detectar		
Ransomware: Como responder		

 **Parte 1:**
Ransomware: Como Acontece

Entender como ataques de ransomware acontecem ajuda a determinar medidas de proteção, detecção e resposta a incidentes. Este documento explica o modelo de RaaS (Ransomware as a Service) e as fases do ataque.

➔ [Acesse aqui](#)

 **Parte 2:**
Ransomware: Como se Proteger

Este documento apresenta uma estratégia de defesa em camadas, com múltiplas medidas de segurança que se complementam. Assim, mesmo que não seja possível evitar totalmente o ataque, é possível adotar medidas para retardar o ataque, limitar o impacto e aumentar a resiliência operacional.

➔ [Acesse aqui](#)

 **Parte 3:**
Ransomware: Como Detectar

Este documento apresenta formas de detectar ataques de ransomware em diferentes fases, de distintas formas e com variados níveis de detalhamento. Quanto antes a detecção ocorrer, menores serão os impactos na empresa e, como resultado, os esforços da Resposta.

➔ [Acesse aqui](#)

 **Parte 4:**
Ransomware: Como Responder

Este documento apresenta os passos mínimos para a resposta a um ataque de ransomware, abordando como conter seu avanço, eliminar a presença do atacante, erradicar a causa raiz da invasão, restaurar o ambiente e retornar à operação normal.

➔ [Acesse aqui](#)

RANSOMWARE: COMO SE PROTEGER

Entenda como funciona o ataque, como proteger sua rede e instrumentá-la para detecção, e como responder caso seja vítima.

cert.br



<https://cert.br/docs/ransomware/>

TLP:CLEAR

cert.br nic.br cgi.br

Panorama Setorial da Internet

Atividades do NIC.br para uma Internet mais Segura

Panorama Setorial
da Internet

Número 2
Julho, 2026
Ano 18

Internet no Brasil: robustez, confiança e mais segurança

Construindo confiança no ambiente digital: o papel do NIC.br na promoção de uma Internet mais segura no Brasil¹

A disseminação da Internet e das tecnologias digitais tem impulsionado uma transformação digital cada vez mais acelerada em diversas dimensões da sociedade, nos âmbitos da vida social e econômica, ampliando sua centralidade nas atividades cotidianas de indivíduos, organizações e governos. Se, por um lado, a crescente incorporação dessas tecnologias está associada a importantes benefícios para o desenvolvimento econômico e o bem-estar social, a ampliação de sua presença nas atividades

cotidianas também introduz novos desafios. Entre eles, destacam-se a crescente exposição a riscos digitais e possíveis incidentes de segurança associados ao uso de dispositivos conectados à Internet, o que, em alguma medida, torna seus usuários mais vulneráveis no ambiente digital.

Desde sua concepção, a Internet foi desenvolvida em um contexto caracterizado por relações de confiança entre os participantes que se interligam na rede de computadores, composta inicialmente por um número limitado de instituições acadêmicas, governamentais e de pesquisa, com vínculos ou propósitos em comum. Nesse contexto, os protocolos fundamentais da rede foram projetados com foco na interoperabilidade e na troca de informações, sem incorporar mecanismos robustos de segurança como requisitos centrais de seu desenho. Com a expansão da rede e sua crescente utilização por diferentes segmentos da sociedade, essa premissa original de confiança mostrou-se insuficiente diante dos desafios contemporâneos de segurança digital.

¹ Este artigo foi redigido por Javiera F. Medina Macaya, pesquisadora no Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br), departamento do Núcleo de Informação e Coordenação do Ponto BR (NIC.br), a partir dos materiais institucionais de cada uma das iniciativas do NIC.br. Javiera é doutora em Administração de Empresas e mestre em Administração Pública e Governo pela Escola de Administração de Empresas de São Paulo da Fundação Getúlio Vargas (FGV EAESP), com graduação em Gestão de Políticas Públicas pela Universidade de São Paulo (USP). O artigo contou com a revisão de gestores envolvidos nessas iniciativas.

Segurança e tratamento de incidentes de segurança
no Brasil: história e papel do CERT.br

Artigo II

Segurança e tratamento de incidentes de segurança no Brasil: história e papel do CERT.br

Por Cristine Hoepers

O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) é um Grupo de Resposta a Incidentes de Segurança (Computer Security Incident Response Team (CSIRT)) de Responsabilidade Nacional de último recurso, mantido pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br), cuja missão é aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil.

Sua história começa a ser delineada em agosto de 1996, com a publicação do relatório *Rumo à criação de uma coordenação de segurança de redes na Internet Brasil* (Gomide et al., 1996), produzido pelo Subgrupo de Trabalho de Segurança do Grupo de Trabalho em Engenharia de Redes (GTER), do Comitê Gestor da Internet no Brasil (CGI.br). Esse relatório foi fruto de um ano de debates na comunidade Internet nacional, motivado pela necessidade de lidar com o crescimento no número de incidentes de segurança em computadores, que acompanhava o vigoroso crescimento da Internet no Brasil após sua abertura para exploração comercial, em 1995. O relatório apresentou um diagnóstico da situação do país naquele momento e apontou alguns caminhos a serem seguidos para a criação de uma estrutura que auxiliasse as organizações a melhor lidar com incidentes, considerando a complexidade e a escala do cenário nacional. Esse diagnóstico descrevia os objetivos e atribuições almejados pela comunidade para um centro de coordenação de temas relacionados à segurança digital no Brasil:

O objetivo da criação de uma organização encarregada de coordenar a segurança de redes não é que ela tome para si todas as tarefas que necessitam ser efetuadas. Esta organização deve possuir um conjunto básico de atribuições a partir dos quais ela possa atribuir ou fomentar a realização de tais tarefas por terceiros atuando apenas como coordenadora das atividades. Desta forma, é desejável que possua as seguintes atribuições:

- Receber e registrar ocorrências de violação de segurança de redes;
- Coletar estatísticas destas ocorrências e torná-las públicas;
- Orientar tecnicamente os que a ela recorrerem para sanar falhas de segurança;
- Intermediar o contato entre redes envolvidas em incidentes de segurança servindo como testemunha legal das ações destas;
- Fomentar a criação de programas de treinamento e atualização em segurança de redes através de interação estreita com o Grupo de Trabalho Formação de Recursos Humanos;



Cristine
Hoepers
Gerente do
CERT.br

Foto: Klaus Stading-Jessen

Cooperação e confiança na gestão de incidentes de cibersegurança

Entrevista II

Cooperação e confiança na gestão de incidentes de cibersegurança

Nesta entrevista, Olivier Caleff, *chair* do Conselho Diretor do FIRST²², especialista em CSIRT e resiliência Cibernética no CSIRT.FR²³, e auditor SIM3 na OpenCSIRT Foundation²⁴, reflete sobre os desafios da gestão de incidentes de cibersegurança no contexto da transformação tecnológica, destacando a importância da cooperação entre Grupos de Resposta a Incidentes de Segurança (Computer Security Incident Response Team (CSIRTs)) e CERTs, a construção de confiança nas comunidades de cibersegurança e o papel do Modelo de Maturidade de Gestão de Incidentes de Segurança (Security Incident Management Maturity Model (SIM3)) no reforço das capacidades de resposta a incidentes.

Panorama Setorial da Internet (P.S.I.). Em sua opinião, quais são os principais desafios para a gestão de incidentes de cibersegurança em um contexto de transformação tecnológica? Em que medida esses desafios se modificaram ao longo das últimas décadas?

Olivier Caleff (O.C.). Em primeiro lugar, o principal desafio é a divergência entre o ritmo das mudanças e a capacidade de as organizações adaptarem recursos de segurança e resposta a incidentes. Novas tecnologias, novas arquiteturas e novos processos de negócios são frequentemente implementados mais rapidamente do que a governança, os planos de resposta a incidentes e os procedimentos conseguem evoluir.

Um segundo grande desafio é a visibilidade e o controle. Uma gestão eficaz de incidentes exige uma compreensão clara do ambiente que está sendo protegido: ativos (que rapidamente se traduzem em "superfície de ataque"), dependências, processos de negócios e fluxos de dados. Durante transformações em larga escala, os inventários, a documentação e os mapeamentos arquitetônicos costumam estar incompletos ou desatualizados; como resultado, a superfície de ataque pode se expandir, enquanto os defensores podem perder a visibilidade sobre ativos e interconexões críticas.

A transformação também aumenta a complexidade técnica. Serviços em nuvem, plataformas de Software como Serviço (Software as a Service (SaaS)), sistemas baseados em Inteligência Artificial (IA), ambientes containerizados e integração de terceiros introduzem novas tecnologias, componentes e vetores de ataque. Os CSIRTs, juntamente com as equipes de cibersegurança ou de defesa cibernética, podem ainda não ter experiência suficiente com essas tecnologias. Como consequência, muitas vezes os processos de qualificação, avaliação de riscos e validação de segurança têm dificuldade para acompanhar o ritmo das mudanças.

²² Saiba mais: <https://first.org/>

²³ Saiba mais: <https://csirt.fr/>

²⁴ Saiba mais: <https://opencsirt.org/>



Olivier Caleff
Chair do Conselho
Diretor do FIRST,
especialista em
CSIRT e resiliência
Cibernética
no CSIRT.FR, e
auditor SIM3
na OpenCSIRT
Foundation

Foto: Caleff



<https://cetic.br/pt/publicacao/ano-xviii-n-2-internet-no-brasil-robustez-confianca-e-mais-seguranca/>

Mais Sobre o CERT.br

Cursos de Gestão de Incidentes

- <https://cursos.cert.br/>

Fórum Brasileiro de CSIRTs e Workshop MISP

- <https://forum.cert.br/>

Informações sobre MISP para compartilhamento de ameaças

- <https://cert.br/misp/>

Recomendações Técnicas e Boas Práticas

- <https://cert.br/docs/>

Feeds para Sistemas Autônomos

- Para receber dados de ataques saindo de suas redes contra nossos honeypots envie *e-mail* para [<feeds@cert.br>](mailto:feeds@cert.br)

Obrigada

@ Pedidos de *feeds*: feeds@cert.br

@ Materiais educativos: doc@cert.br

@ Notificações de Incidentes: cert@cert.br

X @certbr

<https://cert.br>

nic.br cgi.br

www.nic.br | www.cgi.br

TLP:CLEAR