

nic.br egi.br

cert.br

*Workshop CKN*

07 de dezembro de 2021

*Evento Online*

## Serviços Prestados à Comunidade

Gestão de Incidentes	Consciência Situacional	Transferência de Conhecimento
<ul style="list-style-type: none"> <li>▶ Coordenação</li> <li>▶ Análise Técnica</li> <li>▶ Suporte à Mitigação e Recuperação</li> </ul>	<ul style="list-style-type: none"> <li>▶ Aquisição de Dados               <ul style="list-style-type: none"> <li>▶ <i>Honeypots</i> Distribuídos</li> <li>▶ SpamPots</li> <li>▶ <i>Threat feeds</i></li> </ul> </li> <li>▶ Compartilhamento das Informações</li> </ul>	<ul style="list-style-type: none"> <li>▶ Conscientização               <ul style="list-style-type: none"> <li>▶ Desenvolvimento de Boas Práticas</li> <li>▶ Cooperação, Eventos e Reuniões (<i>Outreach</i>)</li> </ul> </li> <li>▶ Treinamento</li> <li>▶ Aconselhamento Técnico e Político</li> </ul>

### Filiações e Parcerias:



**Criação:**  
**Agosto/1996:** CGI.br publica o relatório “Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil”<sup>1</sup>  
**Junho/1997:** CGI.br cria o CERT.br (à época chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório<sup>2</sup>  
<sup>1</sup> <https://cert.br/sobre/estudo-cgibr-1996.html> | <sup>2</sup> <https://nic.br/pagina/gts/157>

## Missão

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

## 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** – Núcleo de Informação e Coordenação do .br

- todas as atividades são sustentadas pelo registro de domínios .br

O NIC.br é o **braço executivo do CGI.br** – Comitê Gestor da Internet no Brasil

- entidade multissetorial, coordenada pelo MCTI
- 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/about/rfc2350/>

# Uso do MISP pelo CERT.br

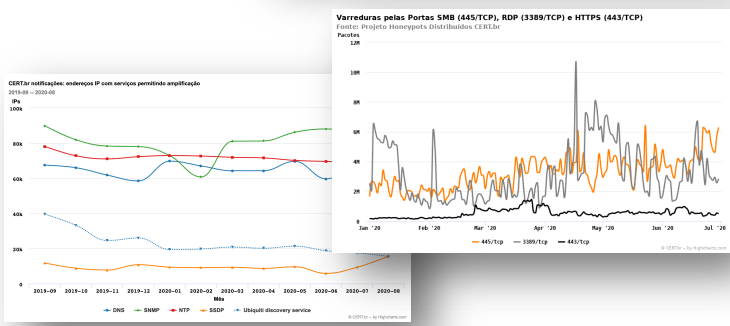
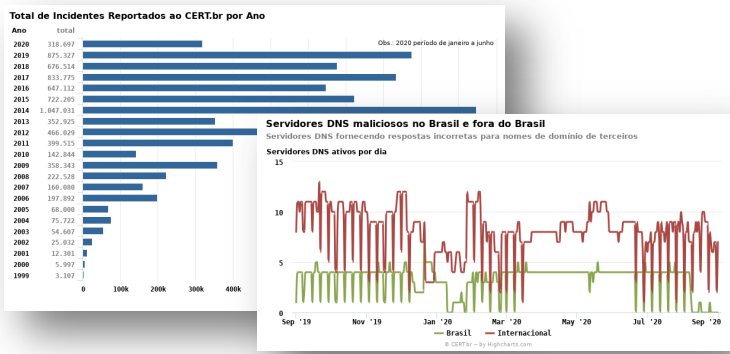
**Dr. Klaus Steding-Jessen**  
Gerente Técnico  
jessen@cert.br

cert.br nic.br egi.br





# Compartilhamento de Indicadores para Consciência Situacional

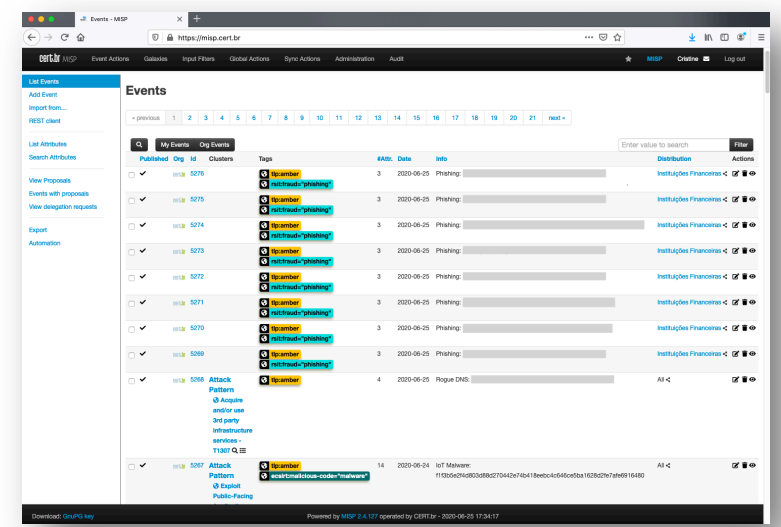


Estatísticas Públicas  
<https://cert.br/stats/>

Notificações de Incidentes

*Honeypots e Threat Feeds*

Notificações para os Sistemas Autônomos



Compartilhamento de indicadores via MISP  
<https://cert.br/misp/>

# Como sua Organização pode Usar os IoCs do CERT.br

## Todas as Comunidades

- Servidores DNS maliciosos

Fonte: notificações / *threat feeds* / *honeypots*

Uso:

- identificar usuários/clientes consultando esses servidores (via *netflow*)
- identificar *phishings* e solicitar *takedown*

- Binário, *hash*, IP de *download* e CnC de *botnets* IoT

Fonte: *threat feeds* / *honeypots*

Uso:

- identificar usuários/clientes infectados
  - acessando o IP/URL de *download* (via *netflow* ou *proxy*)
  - acessando o CnC (via *netflow*)
- procurar pelo *hash* em ferramentas/bases locais
- analisar o binário, se for de interesse

## Setor Financeiro

- *Phishings*

Fonte: notificações

Uso:

- identificar campanhas
- *takedown*

## Operadoras de Telecom

- Amplificadores

Fonte: *threat feeds*

Uso:

- identificar clientes afetados
- corrigir o problema

# https://cert.br/misp/ Referências em Português sobre MISP

- Lista de discussão <https://listas.cert.br/mailman/listinfo/misp-br>
- Passo-a-passo de instalação em um sistema Ubuntu <https://cert.br/misp/tutorial-ubuntu/>  
Incluindo:
  - Considerações de Segurança
    - Não Utilizar Imagens Baixadas da Internet para Instâncias em Produção
    - Cuidados com o Certificado Digital
    - Cuidados com Firewall, WAF e Anti-DDoS Corporativos
  - Instalação e Hardening Básicos do SO
  - Instalação do MariaDB, Apache, PHP e outras Dependências do MISP
  - Instalação do MISP
  - Configuração Inicial do MISP
    - Criar os arquivos de configuração e definir as credenciais de acesso
    - Definir as configurações iniciais do MISP

- Passo-a-passo de configuração e operação <https://cert.br/misp/certbr-passo-a-passo-misp-2021-08-19.pdf>  
Incluindo:
  - Primeiro login, criação e administração de usuários, atualização do MISP
  - Geração e uso de authkeys
  - Sincronização entre instâncias, Communities e Distribuição de Eventos
  - Automatização com curl e PyMISP

**Tipo de distribuição:**  
**This community only**

**PyMISP Exemplo de Código para Publicação de um Evento (1/2)**

```
#!/usr/bin/env python3
from pymisp import ExpandedPyMISP, MISPEvent, MISPAttribute
from keys import misp_url, misp_key, misp_verifycert

if __name__ == '__main__':
    # create misp instance
    misp = ExpandedPyMISP(misp_url, misp_key, misp_verifycert)

    # create event
    my_event = MISPEvent()

    my_event.info = 'Phishing: www.example.org'

    # threat IDs: 1 = High / 2 = Medium / 3 = Low / 4 = Undefined
    my_event.threat_level_id = 1
    # analysis IDs: 0 = Initial / 1 = Ongoing / 2 = Completed
    my_event.analysis = 1
    # distribution IDs:
    # 2 = Connected com
    my_event.distributio
    # add basic informat
    my_event = misp.add
```

**Sincronização: Push vs. Pull**

	Push	Pull
Direção	A envia eventos para B	B busca eventos em A
Propagação de eventos	Automática No momento da publicação do evento	Manual Via interface do MISP ou via cron
Dados para configuração de sincronia	A manda para B: - UUID e ORGNAME B manda para A: - URL, Authkey, UUID e ORGNAME	B manda para A: - UUID e ORGNAME A manda para B: - URL, Authkey, UUID e ORGNAME
Criação de contas e servidores para sincronia	B cria: - Org. local com os dados de A - Sync-user para A na Org. local criada A cria: - Servidor de sincronia, com a opção push marcada, com os dados de B	B cria: - Servidor de sincronia, com a opção pull marcada, com os dados de A A cria: - Org. local com os dados de B - Sync-user com 'authkey read only' para B na Org. local criada
Configuração de Rede	B precisa permitir conexões vindas de A na porta 443/TCP	A precisa permitir conexões vindas de B na porta 443/TCP

**Criando usuários (2/3)**

Na janela "Admin Add User", preencha os seguintes campos:

- **Email**
  - Endereço de e-mail do usuário
  - Marque o checkbox "Set password"
  - Digite e confirme a senha do usuário
- **Organisation**
  - Escolha a organização deste usuário
- **Role**
  - Escolha o papel do usuário
- **Authkey**
  - Gerada automaticamente pelo sistema
- **Nids Sid**
  - Utilizado pelo IDS

# Obrigado

✉ jessen@cert.br

✉ Notificações para: cert@cert.br

📧 @certbr

<https://cert.br/>

nic.br cgi.br

[www.nic.br](http://www.nic.br) | [www.cgi.br](http://www.cgi.br)