

nic.br egi.br

cert.br

ANBIMA
27 de maio de 2021
On-line

MISP para Compartilhamento de Informações e IoCs

cert.br nic.br egi.br

Introdução às Atividades do CERT.br

cert.br nic.br egi.br

Gestão de Incidentes

- ▶ Coordenação
- ▶ Análise Técnica
- ▶ Suporte à Mitigação e Recuperação

Consciência Situacional

- ▶ Aquisição de Dados
 - ▶ *Honeypots* Distribuídos
 - ▶ SpamPots
 - ▶ *Threat feeds*
- ▶ Compartilhamento das Informações

Transferência de Conhecimento

- ▶ Conscientização
 - ▶ Desenvolvimento de Boas Práticas
 - ▶ Cooperação, Eventos e Reuniões (*Outreach*)
- ▶ Treinamento
- ▶ Aconselhamento Técnico e Político

Filiações e Parcerias:



SEI
Partner
Network



Criação:

Agosto/1996: CGI.br publica o relatório “Rumo à Criação de uma Coordenadoria de Segurança de Redes na Internet Brasil”¹

Junho/1997: CGI.br cria o CERT.br (à época chamado NBSO – *NIC BR Security Office*), com base nas recomendações do relatório²

¹ <https://cert.br/sobre/estudo-cgibr-1996.html> | ² <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
- 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/>

Foco do CERT.br nestes 22 anos:

Aumentar a Capacidade Nacional de Tratamento de Incidentes

Nenhum grupo ou estrutura única conseguirá fazer sozinho a segurança ou a resposta a incidentes

Comunidade Nacional

- Auxiliar na análise técnica e facilitar o tratamento de incidentes por outros CSIRTs
- Ações junto a setores chave, para criação e treinamento de Grupos de Tratamento de Incidentes de Segurança (CSIRTs)
- Gerar massa crítica para possibilitar a cooperação e melhora na segurança das redes
- Ter uma visão sobre as principais tendências de ataques no Brasil

Comunidade Internacional

- Estabelecer relações de confiança
 - facilitar a comunicação em casos de incidentes
 - dar acesso a informações que ajudem a comunidade local
- Influenciar os padrões e certificações sendo construídos para CSIRTs
- Levar a visão nacional aos fóruns pertinentes

Cooperação Internacional: Construção de Confiança

FIRST

Fórum existe desde 1992

- membro desde 2002

É uma Rede Global de CSIRTs

- fomenta a cooperação
- acesso a times e especialistas do mundo todo

Destaques da Participação:

- Coordenação de conteúdo do padrão *FIRST CSIRT Services Framework*
- *Co-chair* do *Membership Committee* e do *Security Lounge SIG*
- *Chair* da Conferência 2020
- Viabilização da parceria entre o FIRST e o LACNIC
 - CERT.br é *co-host* dos TCs e Simpósios na região

Rede de CSIRTs Nacionais

Existe desde 2006

Fórum para discussão de assuntos específicos para grupos de responsabilidade nacional

- CERT.br e CTIR Gov são membros

Maiores parceiros do CERT.br:

CERT/CC	US-CERT	CERT.at
NCSC-NL	NCSC-FI	CERT.LV
JPCERT/CC	NISC JP	HKCERT
TWCERT/CC		

LAC-CSIRTs

Reunião de Grupos de Resposta a Incidentes de Segurança (CSIRTs) da região da América Latina e o Caribe – ocorre durante o LACNIC

Conscientização: Portal InternetSegura.br



The screenshot shows a web browser window with the URL `internetsegura.br`. The page header includes the `nic.br` logo, the `INTERNET SEGURA BR` logo, and navigation links for `Sobre`, `Outras iniciativas`, and `Como Pedir Ajuda`. The main heading reads: `Internet Segura – Faça sua parte e todos teremos uma Internet mais segura!`

Below the heading, there are six categories of target audiences, each with an illustration and a label:

- `para Crianças`: Illustration of two children.
- `para Adolescentes`: Illustration of two young people.
- `para Pais e Educadores`: Illustration of a woman and a man.
- `para 60+`: Illustration of an elderly couple.
- `para Técnicos`: Illustration of a person in a lab coat next to server racks.
- `para Interesse Geral`: Illustration of a diverse group of people.

Conscientização: Materiais sob Licença Creative Commons

Segurança na INTERNET

Faça sua parte e todos teremos uma Internet mais segura!

Já há muito tempo que segurança na Internet não é um assunto somente de interesse de um público especializado. Com a iniciativa InternetSegura.br, o NIC.br produz e disponibiliza gratuitamente uma série de materiais, em diversos formatos, que orientam diferentes públicos sobre o uso seguro da Internet. www.internetsegura.br

Catálogo de materiais e iniciativas do NIC.br

para Crianças

Guia Internet Segura

Apresenta conceitos de segurança na Internet de forma lúdica, com atividades para colorir, palavras cruzadas, desafios criados, dicas, complete a frase, caça-palavras, entre outros.

Desafios

Contém tanto os desafios do guia Internet Segura como materiais adicionais, atualizados periodicamente. internetsegura.br/desafios

para Adolescentes

Encarte #FikDik

Encarte do guia #Internet com Responsa - Cuidados e Responsabilidades no Uso da Internet, que apresenta os principais cuidados, riscos e consequências do uso inadequado da Internet de forma resumida.



Formato impresso, colorido e permite inclusão de logo de parceiros de impressão

para Pais e Educadores

Guia Internet Segura para seus filhos

Informações para pais e responsáveis sobre como proteger os filhos, seja zelando pela privacidade das crianças, ou utilizando tecnologias de controle parental.



Guia #Internet com Responsa - Cuidados e responsabilidades no uso da Internet

Orienta pais, responsáveis e educadores de adolescentes em temas sensíveis, como exposição excessiva na Internet, liberdade de expressão e danos à imagem e reputação, cyberbullying, danos e riscos da prática de nude, selfie, entre outros. Acompanha o encarte #FikDik



Guia #Internet com Responsa na sua Sala de Aula

Explica os desafios do uso da Internet a partir da exposição excessiva, dos direitos e possíveis danos à imagem dos professores e alunos, e dos limites da liberdade de expressão.



Slides: Fascículos da Cartilha de Segurança para Internet

Slides para a divulgação de boas práticas sobre o uso seguro da Internet. Há versões de apoio para professores, com notas explicativas. Disponíveis em formatos PowerPoint (.ppt), Libre-Office (.odp), PDF sem notas explicativas e PDF com notas explicativas. cartilha.cert.br/downloads



VEJA TAMBÉM

Curso de Formação de Professores Multiplicadores para o Uso Consciente e Responsável da Internet: cursointernetcomresponsa.nic.br

Materiais de referência:
TIC Kids Online Brasil
Indicadores com mapeamento de possíveis riscos e oportunidades on-line a partir dos usos que crianças e adolescentes de 9 a 17 anos fazem da Internet. Contém dados distintos para "crianças e adolescentes" e "pais e responsáveis". ctic.br/pesquisa/kids-online

TIC Educação
A pesquisa entrevistou alunos, professores, coordenadores pedagógicos e diretores para mapear o acesso, o uso e a apropriação das tecnologias de informação e comunicação (TIC) em escolas públicas e privadas de educação básica. ctic.br/pesquisa/educacao

Para quem tem 60 anos ou mais

#Internet com Responsa 60+: Cuidados e responsabilidades no uso da Internet

Apresenta cuidados específicos para essa faixa etária, pois esse ambiente repleto de informações e oportunidades também oferece alguns riscos para quem ingressou no uso das novas tecnologias recentemente.



para Técnicos

Portal BCP e Programa Por uma Internet Mais Segura

Reúne um conjunto de boas práticas operacionais para Sistemas Autônomos (ASs) conectados à Internet. São destacadas algumas práticas que, embora extremamente importantes, ainda não são adotadas amplamente pelos ASs brasileiros. O portal também disponibiliza conteúdos e iniciativas direcionadas à comunidade de operadores de redes e serviços que formam a Internet por meio do Programa por uma Internet Mais Segura. bcp.nic.br



VEJA TAMBÉM

Curso de Boas Práticas Operacionais para Sistemas Autônomos - Presencial: bcp.nic.br/curso-bcop

Curso "Fundamentals of Incident Handling": cert.br/cursos/fih/

Curso "Advanced Topics in Incident Handling": cert.br/cursos/atih/

Interesse geral

Cartilha de Segurança para Internet

Documento com recomendações e dicas sobre como o usuário de Internet deve se comportar para aumentar a sua segurança e se proteger de possíveis ameaças. Apresenta o significado de diversos termos e conceitos utilizados na Internet, aborda os riscos de uso desta tecnologia e fornece uma série de dicas e cuidados a serem tomados pelos usuários. Também disponível em cartilha.cert.br e em espanhol em cartilha.cert.br



Fascículos da Cartilha de Segurança para Internet

Aborda tópicos específicos contidos na Cartilha de Segurança para Internet e complementa conteúdos que não estavam disponíveis à época da última edição da Cartilha, como Boatos, cuidados atualizados para Redes Sociais e Códigos Maliciosos. Também disponíveis em cartilha.cert.br/fasciculos e em espanhol em cartilha.cert.br/fasciculos

Guia #Internet com Responsa Vai às Compras

Detalha os cuidados necessários para realizar compras na Internet de forma responsável, além de enfatizar a importância de exercer direitos previstos no Código de Defesa do Consumidor.



Portal Antispam.br

Fonte de referência imparcial e embasada tecnicamente sobre o spam. Contém desde informações para administradores de redes e usuários finais, incluindo vídeos que abordam de forma simples e divertida os perigos aos quais os usuários estão expostos, explicam o que é spam e dão dicas de como navegar com mais segurança na rede. antispam.br

VEJA TAMBÉM

Materiais de referência:

Caderno CGLbr "Combate ao spam na Internet no Brasil"

Histórico e reflexões sobre o combate ao spam e a gerência da porta 25 coordenados pelo Comitê Gestor da Internet no Brasil. cgi.br/publicacao/combate-ao-spam-na-internet-no-brasil

DISTRIBUIÇÃO DOS MATERIAIS

O NIC.br tem o compromisso de atender todos os interessados em seus materiais, da forma mais racional possível. Para que o máximo de interessados sejam atendidos, sem desperdício, limitamos o envio de materiais a lotes de 100 unidades. Caso sua instituição tenha interesse em distribuir uma quantidade maior, teremos o prazer em disponibilizar o conteúdo para que a impressão, com seu logotipo, seja realizada de acordo com sua capacidade.

SEJA UM PARCEIRO PARA A IMPRESSÃO DOS MATERIAIS!

Escreva para info@nic.br solicitando a inclusão do seu logotipo e especifique quais materiais você gostaria de imprimir.

LICENCIAMENTO

O objetivo primordial da produção dos nossos materiais é o compartilhamento de conteúdo, portanto a maioria destes está disponível gratuitamente para download e uso sob licenças Creative Commons. Sua instituição pode utilizá-los livremente, sem necessidade de autorização prévia, desde que a fonte seja mencionada, o uso do material não seja comercial (venda do material) e que o conteúdo não seja alterado. Para usos específicos fora do escopo da licença, escreva para info@nic.br.

Confira todas as nossas publicações e atividades em nic.br

nic.br cgi.br

CSIRTs no Brasil: Criação de Uma Comunidade Atuante

Foco

- Criar/aproximar CSIRTs (Grupos de Tratamento de Incidentes de Segurança) no Brasil
- Possuir profissionais preparados para resolver os problemas de segurança no país

Fórum Brasileiro de CSIRTs

- Evento anual para profissionais da área de Tratamento de Incidentes
- *Workshops* sobre assuntos específicos

Lista de CSIRTs Brasileiros

- <https://cert.br/csirts/brasil/>

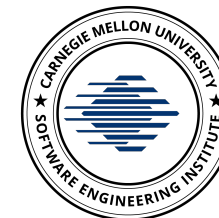
Fomento à adoção de MISP

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

Cursos de Gestão de Incidentes

Ministra os cursos do *CERT[®] Division*, do *SEI/Carnegie Mellon*, desde 2004:

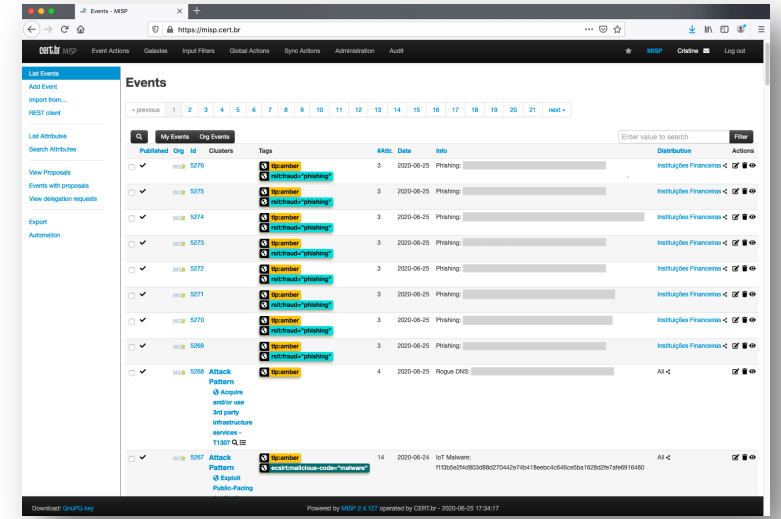
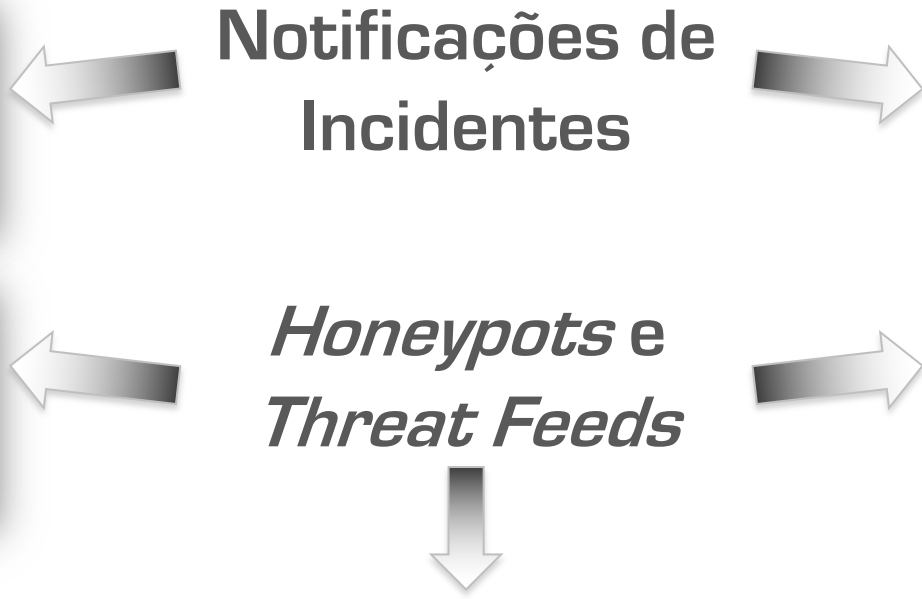
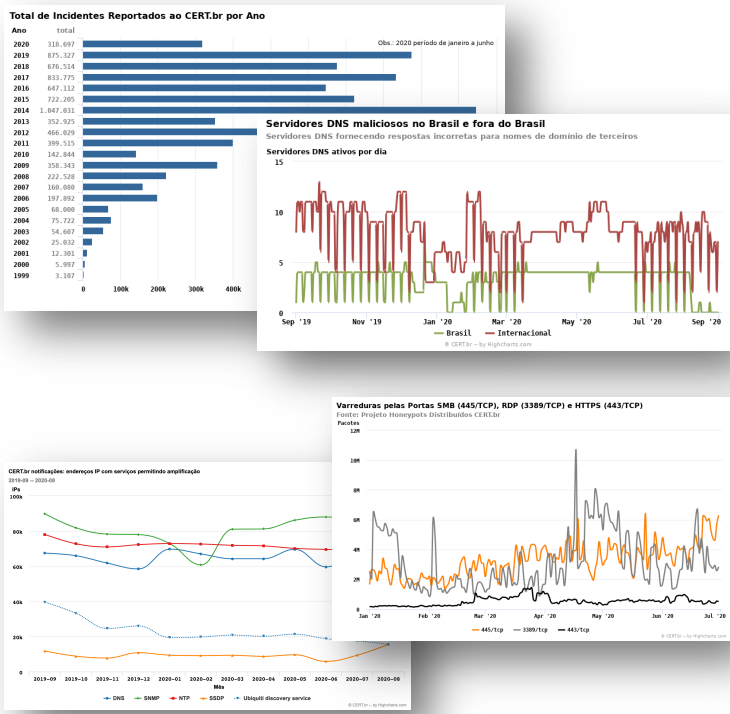
- 3 cursos, 1900+ alunos
- <https://cert.br/cursos/>



SEI
Partner
Network



Compartilhamento de Indicadores para Consciência Situacional



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

Notificações para os Sistemas Autônomos

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

MISP para Compartilhamento de Informações e IoCs

cert.br nic.br egi.br

MISP – Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing

TLP:WHITE

O que é o MISP

- uma plataforma de software livre para compartilhamento de dados de inteligência de ameaças

<https://www.misp-project.org/>

- um conjunto de padrões abertos para compartilhamento destas informações

<https://www.misp-standard.org>

Utilização de MISP ao redor do mundo em comunidades específicas

- *ENISA eCSIRT network*
- *TF-CSIRT Trusted Introducer*
- *FIRST – Forum of Incident Response and Security Teams*
- Redes setoriais de CSIRTs na Holanda e Sérvia
- Interpol

Uso de MISP no Brasil

Atividades promovidas pelo CERT.br

Treinamentos presenciais

- *Workshop* MISP, junto ao Fórum Brasileiro de CSIRTs em 2019 e 2020
- *Workshop* para a Febraban

Página dedicada ao MISP

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

- Passo-a-passo de instalação e operação na página do CERT.br

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

<https://cert.br/docs/palestras/certbr-workshop-misp2020.pdf>

- Lista de discussão

<https://listas.cert.br/mailman/listinfo/misp-br>

Setores utilizando MISP

- Acadêmico
- Energia
- Financeiro
- Governo
- Operadores de redes

O CERT.br compartilha os seguintes indicadores

- Servidores DNS maliciosos (todos)
- Binários e Comando e Controle de *botnets* IoT (todos)
- *Phishing* (setor financeiro)
- Amplificadores usados em ataques DDoS (operadores de redes)

Uso do MISP de maneira automatizada

cert.br nic.br egi.br

REST API

O MISP tem uma REST API que possibilita:

- gerenciar (adicionar, atualizar e remover) eventos
- gerenciar atributos
- gerenciar *tags*
- gerenciar organizações
- gerenciar usuários
- submeter *sightings*
- obter estatísticas de atributos/*tags*
- etc

Referências: <https://www.circl.lu/doc/misp/automation/>

Exemplo de consulta utilizando curl

Buscando eventos publicados no último dia:

```
curl \  
-d '{"returnFormat":"json","publish_timestamp":"1d"}' \  
-H "Authorization: authkey" \  
-H "Accept: application/json" \  
-H "Content-type: application/json" \  
-X POST https://<FQDN>/events/restSearch
```


PyMISP

O PyMISP é a biblioteca Python oficial utilizada para acessar o MISP através da sua REST API.

Com o PyMISP é possível:

- Adicionar, buscar, atualizar, publicar e apagar eventos
- Adicionar ou remover *tags*
- Adicionar atributos
- Fazer *upload/download* de binários
- Atualizar *sightings*
- Pesquisar por palavras chaves e por atributos

Referências:

<https://www.circl.lu/doc/misp/pymisp/>

<https://pymisp.readthedocs.io/en/latest/>

<https://www.misp-project.org/tools/#libraries-to-access-the-misp-api>

Obrigado

@ cristine@cert.br

@ jessen@cert.br

@ Notificações para: cert@cert.br

@ @certbr

www.cert.br

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

www.nic.br | www.cgi.br