

Conscientização: Desafios para Diferentes Públicos

Miriam von Zuben
Analista de Segurança
miriam@cert.br

Disciplina Literacia Digital Transformação Profissional - FEEC/Unicamp
10 de setembro de 2026, Campinas – SP

cert.br **nic.br** **egi.br**

Serviços Prestados à Comunidade

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 de Políticas

Filiações e Parcerias:



SEI
Partner
Network



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

Principais Atividades

- Facilitar a coordenação do tratamento de incidentes entre as partes
 - Ponto de contato nacional de último recurso
 - Trabalho colaborativo com outras entidades
 - Auxílio na análise técnica e compreensão de ataques e ameaças
- Aumentar a detecção, correlação de eventos e determinação de tendências
- Transferir o conhecimento através de cursos, boas práticas e conscientização

Membros e ex-membros do CGI.br
(somente os atuais membros tem direito a voto)



Assembleia Geral

7 membros eleitos
pela Assembleia Geral



Conselho de Administração



Conselho Fiscal

- Administração
- Jurídico
- Comunicação
- Assessorias:
CGI.br, Políticas Públicas Digitais e Presidência
- Desenvolvimento de
Sistemas Web



Diretoria Executiva

1. Diretor presidente
2. Diretor administrativo e financeiro
3. Diretor de serviços e tecnologia
4. Diretor de projetos especiais e de desenvolvimento
5. Diretor de assessoria às atividades do CGI.br

registro.br

Domínios

cert.br

Segurança

cetic.br

Indicadores

ceptro.br

Redes e
Operações

ceweb.br

Tecnologias
Web

ix.br

Troca de
Tráfego



Observatório
de IA

ceregi.br

Centro de
Referência

A Importância da Conscientização

cert.br nic.br cgi.br

“Conscientização é ajudar as pessoas a reconhecer riscos e situações de segurança e a agir de forma adequada diante deles.”

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-50r1.pdf>

ENISA Threat Landscape – 2024



https://www.enisa.europa.eu/sites/default/files/2024-11/ENISA%20Threat%20Landscape%202024_0.pdf

Riscos de Sistemas na Internet

- invasão de contas
- indisponibilidade de serviços
- perda de privacidade
- furto de dados
- perdas financeiras
- danos à imagem
- perda de confiança na tecnologia

**Sistemas
na Internet**

Riscos

Atacantes

- criminosos
- espionagem industrial
- governos
- vândalos

Vulnerabilidades

- projeto sem levar em conta segurança
- defeitos de *software*
- falhas de configuração
- uso inadequado
- fraquezas advindas da complexidade dos sistemas



Diferentes Riscos, Diferentes Danos

- O que faz com que uma mesma ameaça represente riscos diferentes para pessoas diferentes?
- **Depende da pessoa, do contexto e da situação**
- Não basta conhecer a ameaça:
 - é preciso considerar quem está exposto e em que circunstâncias
- Exemplo: Uma pessoa recebe um *e-mail* se passando pelo Banco X
- Pessoa:
 - tem conta naquele banco?
 - está esperando uma transferência?
 - precisa fazer um pagamento urgente?
 - está distraída ou com pressa?
- Mensagem:
 - vem de uma conta genérica?
 - tenta se passar pelo gerente da conta?
 - usa dados pessoais?

Children Online: Research and Evidence (CO:RE)

Classificação de Riscos Online para Crianças e Adolescentes

	Conteúdo (criança se envolve ou é exposta a conteúdos potencialmente danosos)	Contato (criança vivencia ou é alvo de contatos potencialmente danosos de ou por adultos)	Conduta (criança testemunha, participa ou é vítima de condutas potencialmente danosas entre pares)	Contrato (criança é parte ou é explorada por um contrato potencialmente danoso)
Agressivo	Violento, sangrento, racista, odioso ou informação e comunicação extremista	Assédio, perseguição (<i>stalking</i>), ataques de ódio, vigilância indesejada ou excessiva	<i>Cyberbullying</i> , comunicação ou atividade de ódio ou hostil entre pares (ex: trollagem, exclusão, ato com o intuito de causar constrangimento público)	Roubo de identidade, fraude, <i>phishing</i> , golpe, invasão e roubo de dados, chantagem, riscos envolvendo segurança
Sexual	Pornografia (danosa ou ilegal), cultura da sexualização, normas opressivas para a imagem corporal	Assédio sexual, aliciamento sexual, sextorsão, produção ou compartilhamento de imagens de abuso sexual infantil	Assédio sexual, troca não consensual de mensagens sexuais, pressões sexuais adversas	Tráfico para fins de exploração sexual, transmissão de conteúdo pago de abuso sexual infantil
Valores	Informação incorreta/desinformação, publicidade imprópria para idade ou conteúdo gerado pelos usuários	Persuasão ou manipulação ideológica, radicalização e recrutamento extremista	Comunidades de usuários potencialmente danosas (ex: automutilição, antivacinação, pressões entre pares adversas)	Jogos de azar, filtro bolha (filtro de seleção de conteúdos por semelhanças), microsegmentação, padrões ocultos de design (<i>dark patterns design</i>) modelando a persuasão ou a compra
Transversais	Violações de privacidade (interpessoal, institucional e comercial) Riscos para a saúde física e mental (ex: sedentarismo, estilo de vida, uso excessivo das telas, isolamento, ansiedade) Desigualdade e discriminação (inclusão/exclusão, exploração de vulnerabilidades, viés dos algoritmos/análise preditiva)			

<https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-da-internet-por-criancas-e-adolescentes-no-brasil-tic-kids-online-brasil-2021/>

Riscos de Conteúdo

Criança se envolve ou é exposta a conteúdos potencialmente danosos	
Natureza do risco	Exemplos
Agressivo	Violento, sangrento, racista, odioso ou informação e comunicação extremista
Sexual	Pornografia (danosa ou ilegal), cultura da sexualização, normas opressivas para a imagem corporal
Valores	Informação incorreta/desinformação, publicidade imprópria para idade ou conteúdo gerado pelos usuários

<https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-da-internet-por-criancas-e-adolescentes-no-brasil-tic-kids-online-brasil-2021/>

Riscos de Contato

Criança vivencia ou é alvo de contatos potencialmente danosos de ou por adultos	
Natureza do risco	Exemplos
Agressivo	Assédio, perseguição (<i>stalking</i>), ataques de ódio, vigilância indesejada ou excessiva
Sexual	Assédio sexual, aliciamento sexual, sextorsão, produção ou compartilhamento de imagens de abuso sexual infantil
Valores	Persuasão ou manipulação ideológica, radicalização e recrutamento extremista

<https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-da-internet-por-criancas-e-adolescentes-no-brasil-tic-kids-online-brasil-2021/>

Riscos de Conduta

Criança testemunha, participa ou é vítima de condutas potencialmente danosas entre pares

Natureza do risco	Exemplos
Agressivo	<i>Cyberbullying</i> , comunicação ou atividade de ódio ou hostil entre pares (ex: trollagem, exclusão, ato com o intuito de causar constrangimento público)
Sexual	Assédio sexual, troca não consensual de mensagens sexuais, pressões sexuais adversas
Valores	Comunidades de usuários potencialmente danosas (ex: automutilação, antivacinação, pressões entre pares adversas)

<https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-da-internet-por-criancas-e-adolescentes-no-brasil-tic-kids-online-brasil-2021/>

Riscos de Contrato

Criança é parte ou é explorada por um contrato potencialmente danoso	
Natureza do risco	Exemplos
Agressivo	<u>Roubo de identidade, fraude, <i>phishing</i>, golpe, invasão e roubo de dados, chantagem, riscos envolvendo segurança</u>
Sexual	Tráfico para fins de exploração sexual, transmissão de conteúdo pago de abuso sexual infantil
Valores	Jogos de azar, filtro bolha (filtro de seleção de conteúdos por semelhanças), microsegmentação, padrões ocultos de design (<i>dark patterns design</i>) modelando a persuasão ou a compra

<https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-da-internet-por-criancas-e-adolescentes-no-brasil-tic-kids-online-brasil-2021/>

Riscos Transversais

Conteúdo, Contato, Conduta e Contrato	
	Exemplos
Transversais	Violações de privacidade (interpessoal, institucional e comercial) Riscos para a saúde física e mental (ex: sedentarismo, estilo de vida, uso excessivo das telas, isolamento, ansiedade) Desigualdade e discriminação (inclusão/exclusão, exploração de vulnerabilidades, viés dos algoritmos/análise preditiva)

<https://cetic.br/pt/publicacao/pesquisa-sobre-o-uso-da-internet-por-criancas-e-adolescentes-no-brasil-tic-kids-online-brasil-2021/>

Conscientização

Importante Considerar as Características de Cada Público

- Se os riscos e os impactos podem variar, **a forma de comunicar e orientar também precisa se adaptar**
- Não é apenas uma questão de linguagem
- É importante considerar:
 - quem é o público
 - conhecimento prévio
 - autonomia
 - experiência
 - contexto de uso da Internet
 - possíveis consequências de um problema de segurança

Crianças

– Desenvolvimento em curso

- capacidade de julgamento e autorregulação ainda em formação
- compreensão limitada das consequências de suas ações
- autonomia crescente, mas ainda dependente de adultos

– Diversidade de contextos

- idade e estágio de desenvolvimento
- escolarização e letramento digital
- contexto familiar e rede de apoio
- diferentes níveis de acesso e uso da Internet

– Fatores que podem aumentar a vulnerabilidade

- busca por aceitação e influência dos pares
- impulsividade e dificuldade de avaliar riscos
- maior dificuldade para reconhecer manipulação
- receio de contar o que aconteceu ou pedir ajuda

– Particularidades

- menor capacidade de consentir e compreender implicações do compartilhamento de dados
- maior dependência de adultos para prevenção e proteção

Adolescentes

– Autonomia em expansão

- maior independência no uso da Internet
- tomada de decisões cada vez mais autônoma
- capacidade de julgamento e autorregulação ainda em desenvolvimento

– Influência social

- busca por pertencimento e aceitação
- influência de pares e pressão social
- maior importância da reputação e da exposição *online*

– Maior exposição

- uso intenso e diversificado de plataformas
- relacionamentos e interações com pessoas desconhecidas
- maior produção e compartilhamento de conteúdos pessoais

– Particularidades

- dificuldade em reconhecer manipulação e situações de risco
- impulsividade e busca por novas experiências
- receio de pedir ajuda ou relatar situações constrangedoras
- conflitos entre autonomia, privacidade e supervisão dos responsáveis

Público geral

– Diversidade de perfis e contextos

- diferentes níveis de conhecimento e letramento digital
- experiências e hábitos de uso distintos
- diferentes condições de acesso e suporte

– Fatores que podem aumentar a vulnerabilidade

- desatenção, pressa ou excesso de confiança
- desconhecimento sobre ameaças e formas de proteção
- situações de estresse, urgência ou fragilidade emocional

– Desafios para a proteção

- excesso de informações e recomendações
- mudanças rápidas nas tecnologias e nos golpes
- dificuldade de saber em quem confiar
- desconhecimento sobre como agir e onde buscar ajuda

60+

– Diversidade de perfis e trajetórias

- diferentes níveis de escolarização e letramento digital
- experiências e hábitos de uso distintos
- diferentes condições de acesso e redes de apoio

– Autonomia e adaptação

- tecnologias e serviços digitais em constante mudança
- necessidade de aprender novas formas de realizar tarefas cotidianas
- diferentes níveis de familiaridade e confiança com a tecnologia

– Fatores que podem aumentar a vulnerabilidade

- isolamento ou menor rede de apoio
- medo de errar ou de sofrer golpes
- excesso de confiança em interações
- limitações motoras, cognitivas ou sensoriais

– Desafios para a proteção

- dificuldade de reconhecer algumas formas de manipulação
- vergonha ou receio de relatar uma situação
- desconhecimento sobre como denunciar ou buscar ajuda
- **idadismo e autoidadismo**, que podem afetar a confiança para usar tecnologias e pedir ajuda

Materiais como Ferramentas de Apoio

- Resultado depende de como, quando e com quem são usados
- O mesmo material pode cumprir funções diferentes
 - apoio para uma aula ou palestra
 - material de consulta ou referência
 - recurso para treinamentos e oficinas
 - material de apoio para campanhas de conscientização
 - ponto de partida para conversas, debates ou atividades
 - complemento a outros materiais ou conteúdos

Algumas Dicas do que Temos Feito

- Adotar linguagem clara e direta
- Explicar o porquê das recomendações
- Evitar termos desnecessariamente técnicos
- Usar exemplos práticos e situações cotidianas
- Não culpabilizar nem infantilizar

Conscientização de Todos é Essencial: Portal InternetSegura.br



[Sobre](#) | [Outras iniciativas](#) | [Siga-nos no Instagram](#) | [Como Pedir Ajuda](#)

Internet Segura – Faça sua parte e todos teremos uma Internet mais segura!



para Crianças



para Adolescentes



para Pais e Educadores



para 60+



para Técnicos



para Interesse Geral

<https://internetsegura.br/>

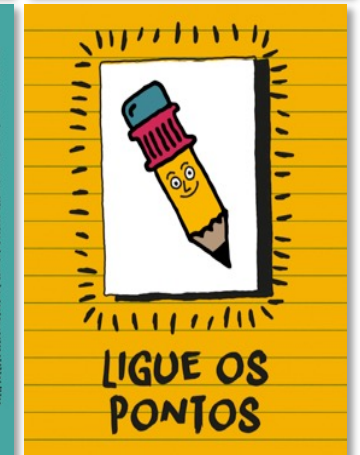
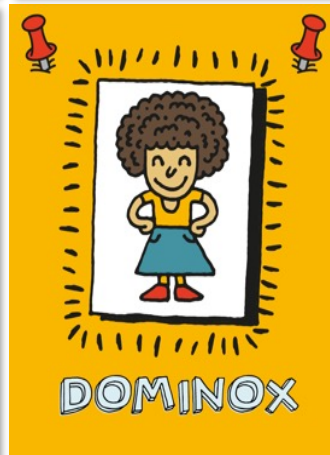
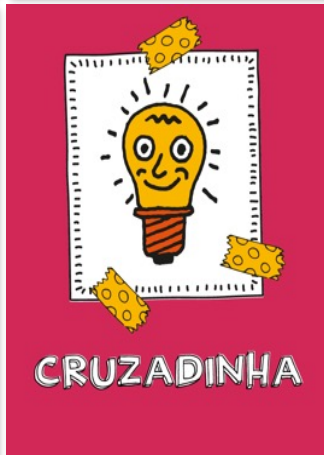
Portal Internet Segura

Guias Internet Segura



<https://internetsegura.br/>

Portal Internet Segura Passatempos



<https://internetsegura.br/passatempo/>

Portal Internet Segura Personagens para Montar

internetsegura.br

Sobre | Outras iniciativas | Como Pedir Ajuda

Personagens para montar

Monte os bonecos de papel tridimensionais da turma do bem e da turma do mal e crie suas próprias histórias! É só baixar os arquivos, imprimir e começar a brincar!



ANTIVÍRUS

Antivírus: ajuda a turma do bem a detectar, anular e eliminar vírus e outros tipos de códigos maliciosos do computador.



AUTENTICAÇÃO

Autenticação: o segurança da turma. Confirma se quem está ali é mesmo o dono do dispositivo. Pede senhas e outros códigos de verificação, checka tudo antes de liberar a entrada.



BACKUP

Backup: salva todas as informações do seu computador em outro dispositivo e não perde nada.



FIREWALL

Firewall: é o dispositivo de segurança usado para dividir e controlar o acesso entre redes de computadores.



SPYWARE

Spyware: espião da turma. Observa o que você faz no seu dispositivo e conta para o invasor.



TROJAN

Trojan: também chamado de Cavalo de Tróia. Além de fazer o que você espera que ele faça, também faz outras coisas, normalmente maliciosas, sem que você saiba.



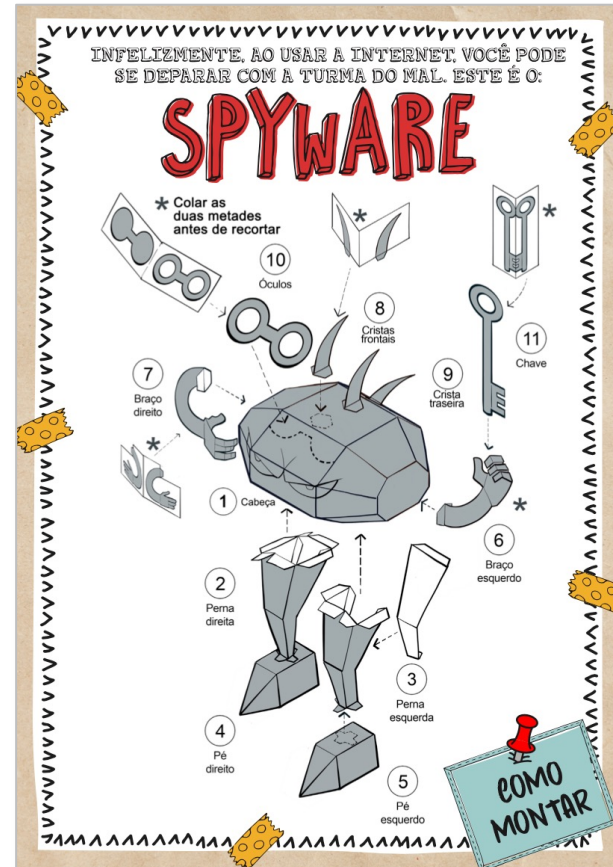
VÍRUS

Vírus: espalha-se pela rede inserindo cópias dele mesmo e se tornando parte de outros programas e arquivos.



ZUMBI

Zumbi: esse é o nome do computador que foi infectado por um bot. Nesse caso, a máquina pode ser controlada remotamente, sem que você saiba.



<https://internetsegura.br/personagensparamontar/>

Portal Internet Segura Jogos de Tabuleiro



Comportamento Seguro



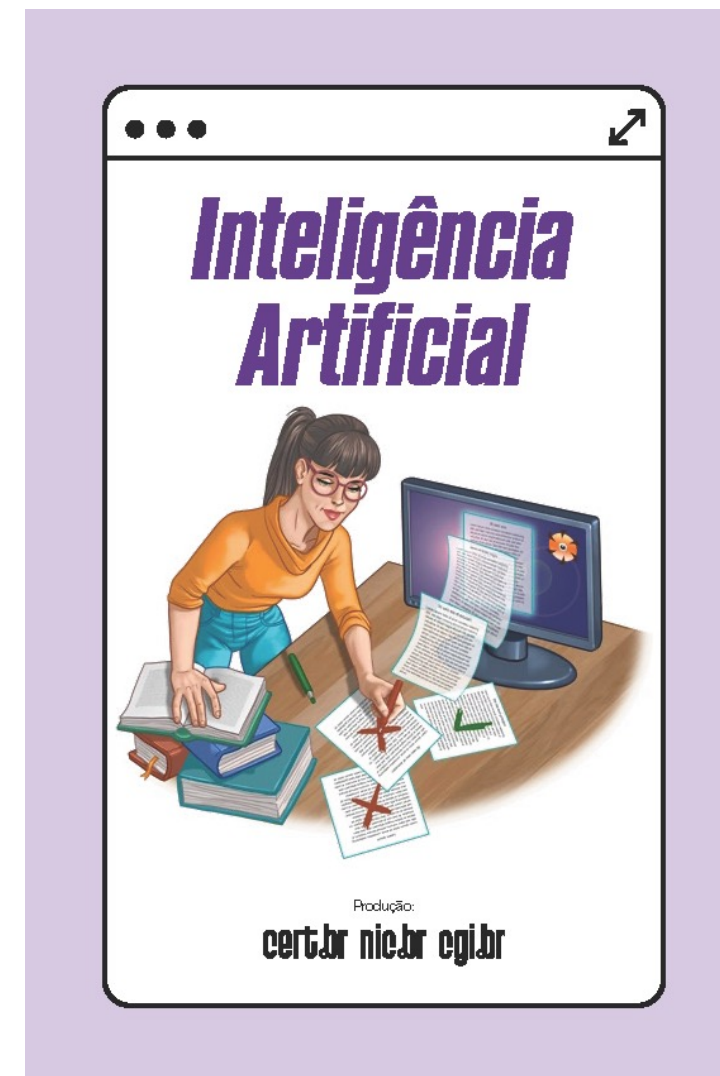
Segurança Online

<https://internetsegura.br/tabuleiro/>

Cartilha de Segurança para Internet

Fascículos – Versões Digital e Impressão

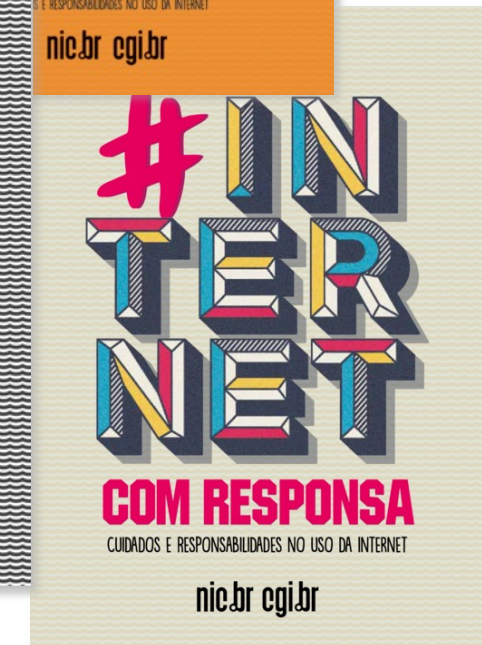
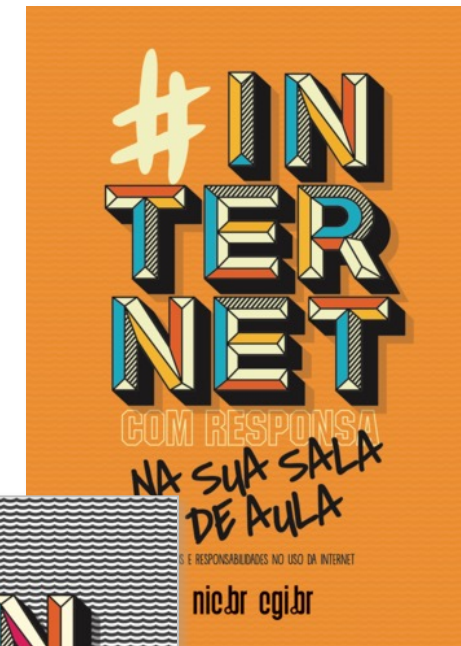
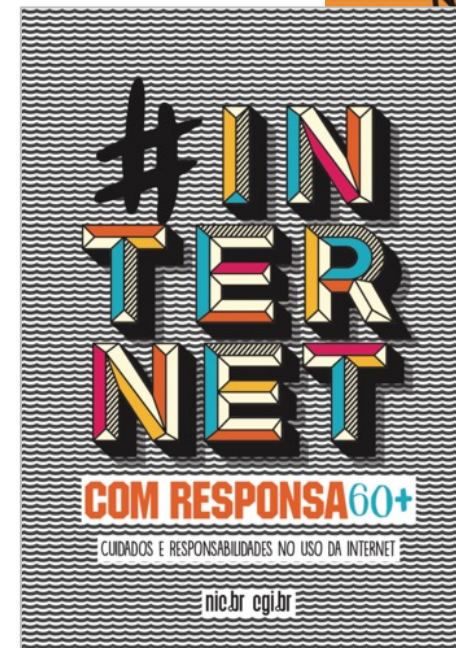
Cartilha de Segurança
para Internet



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

Portal Internet Segura

Guias #InternetComResponsa



<https://internetsegura.br/>

Projeto Cidadão na Rede

Vídeos curtos de diversos temas



Cidadão na
REDE



<https://cidadaonarede.nic.br/>

Redes Sociais

Perfil @InternetSeguraBR



<https://instagram.com/InternetSeguraBR/>

Leitura Recomendada

Documento Completo e Folheto Resumido

CERT.br - Ransomware: Boas Práticas para Proteção, Detecção e Resposta

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

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: Couchê Fosco 300g; Impressão em CMYK; Saída em CTP; Laminação Fosca, 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/>

Comunicar sobre segurança não é apenas dizer quais são os riscos. É ajudar diferentes pessoas a reconhecê-los, compreender suas possíveis consequências e saber como agir.

“Managing human risk requires a human approach.”

Lance Spitzner

Obrigada

@ miriam@cert.br

@ Notificações para: cert@cert.br

X @certbr

<https://cert.br/>

nic.br **cgi.br**

www.nic.br | www.cgi.br