

Painel 3: Iniciativas do setor privado para implementação do ECA Digital

Miriam von Zuben
Analista de Segurança
CERT.br/NIC.br

SID - 10 de fevereiro de 2026
São Paulo - SP

cert.br nic.br cgi.br

The background of the slide features a dark gray, textured surface with white circuit-like lines and patterns. In the top right corner, there is a partial view of a circular gauge or dial with a needle. The central text is set against a lighter gray rectangular background.

Como ficam as PME neste cenário?

cert.br nic.br cgi.br

Desafios de implementação do ECA Digital para PME

Custos de implementação

- Necessidade de adaptar sistemas
 - inclusive legados

Complexidade técnica

- Necessidade de pessoal especializado
 - nem sempre disponível internamente

Dependência de terceiros

- Aumento da área de risco
 - diferentes requisitos de segurança
 - falha em uma solução pode expor vários clientes ao mesmo tempo

Proteção de dados e privacidade

- Aumento na coleta e armazenamento de dados sensíveis
- **Criação de bases de dados centralizadas**
 - podem se tornar alvo de atacantes
 - invasão, exploração de vulnerabilidades, *insider threats*
- **Dados vazados usados para:**
 - golpes
 - invasões
 - extorsão
 - furto de identidade

Is age verification on social media becoming a gold mine for data hackers?

Age verification checks for the UK were brought in by Discord in order to comply with the Online Safety Act

Mark Tsagas The Conversation

Thursday 13 November 2025 22:41 GMT



Comments



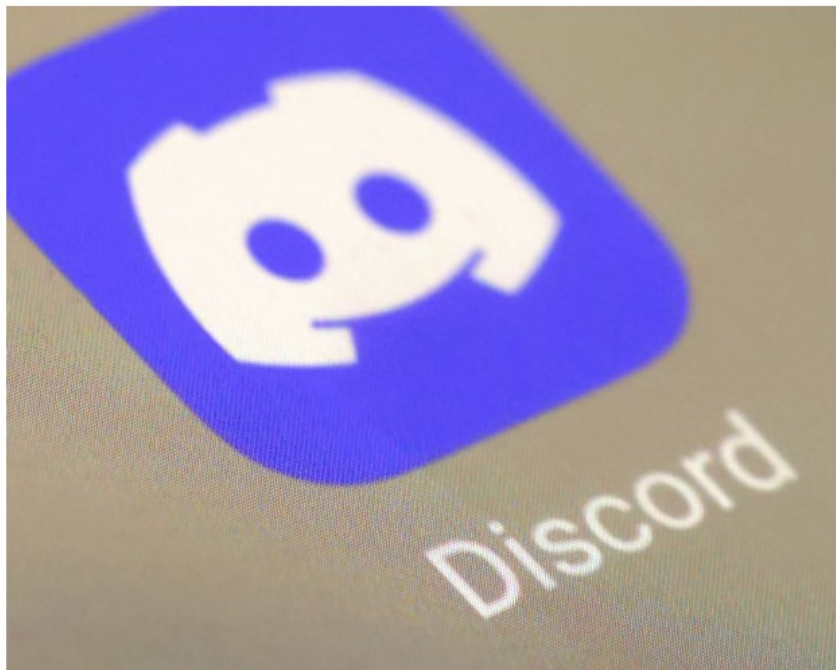
Online age checking is creating a treasure trove of data for hackers

Publicado: 11 novembro 2025 14:19 -03

Fonte: <https://www.independent.co.uk/tech/age-verification-social-media-checking-data-hackers-b2864996.html>
<https://theconversation.com/online-age-checking-is-creating-a-treasure-trove-of-data-for-hackers-268586>

Hack of age verification firm may have exposed 70,000 Discord users' ID photos

Names, email addresses and other contact details of users from around the world could also have been taken



📷 The photos in question were provided by users making age-related appeals in cases where they may have been locked out of the platform.
Photograph: Dado Ruvic/Reuters

CULTURE

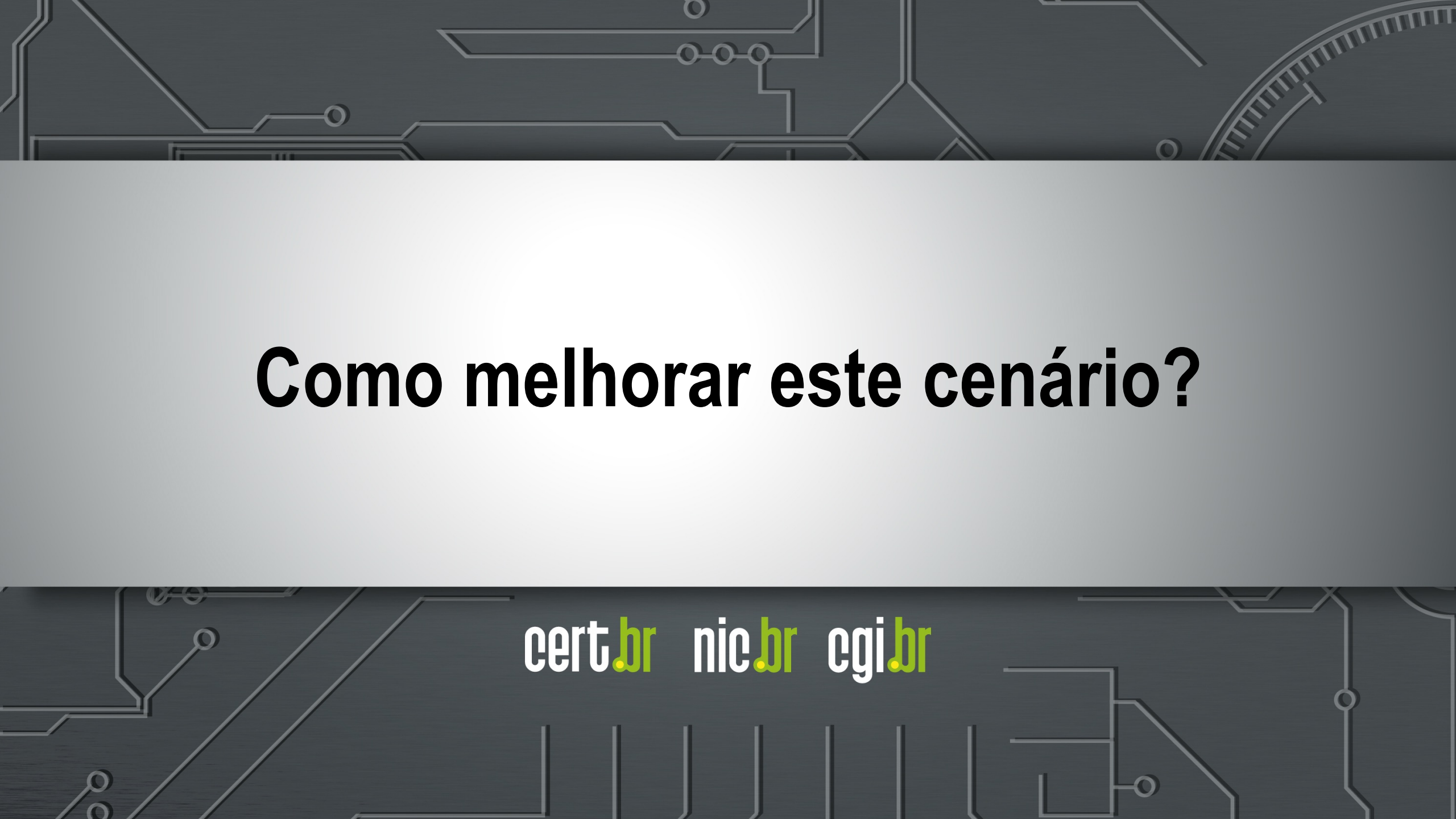
Tea encouraged its users to spill. Then the app's data got leaked

AUGUST 2, 2025 · 1:57 PM ET

By Alana Wise



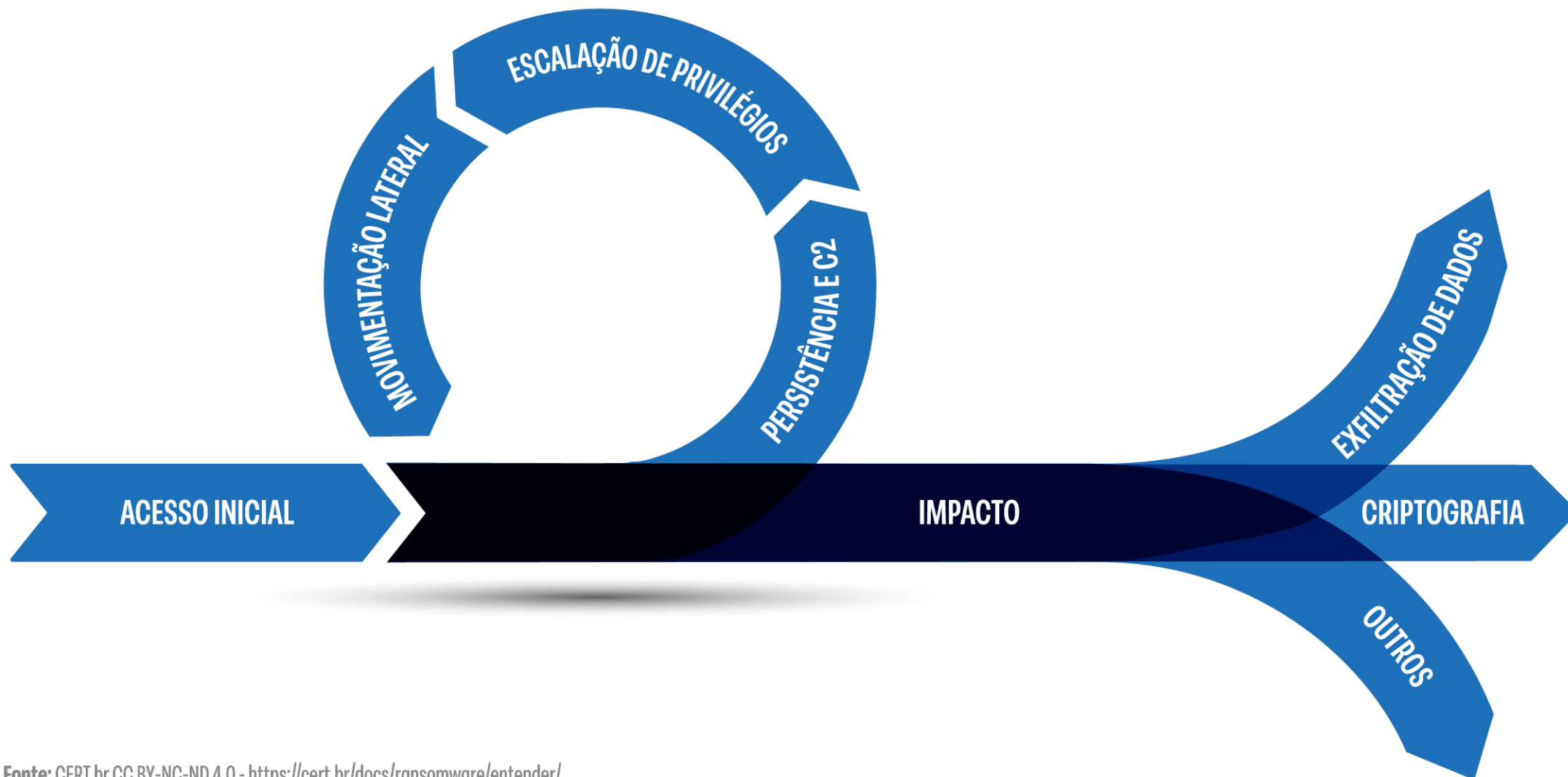
Fonte: <https://www.theguardian.com/media/2025/oct/09/hack-age-verification-firm-discord-users-id-photos>
<https://www.npr.org/2025/08/02/nx-s1-5483886/tea-app-breach-hacked-whisper-networks>

The background of the slide features a dark gray, textured surface with white circuit-like lines and patterns. In the top right corner, there is a partial view of a circular gauge or dial with a needle. The central part of the slide is a light gray rectangular area containing the main text.

Como melhorar este cenário?

cert.br nic.br egi.br

Ciclo de Vida Geral de um Ataque



Fonte: CERT.br CC BY-NC-ND 4.0 - <https://cert.br/docs/ransomware/entender/>

Proteção

Controles Básicos Que Podem Fazer a Diferença

A maior parte dos ataques poderia ser evitada com **controles básicos**.

Um mesmo controle pode ser **usado** em **fases distintas** do ataque.

Mesmo que não impeçam todas as fases, podem **retardar o ataque**, **limitar o impacto** e **aumentar a resiliência** operacional da empresa.



1. Usar Autenticação Multifator (MFA)



2. Fazer Gestão de Vulnerabilidades



3. Conscientizar Funcionários



4. Usar Ferramentas de Proteção



5. Fazer e Proteger *Backups*



6. Reduzir a Superfície de Ataque



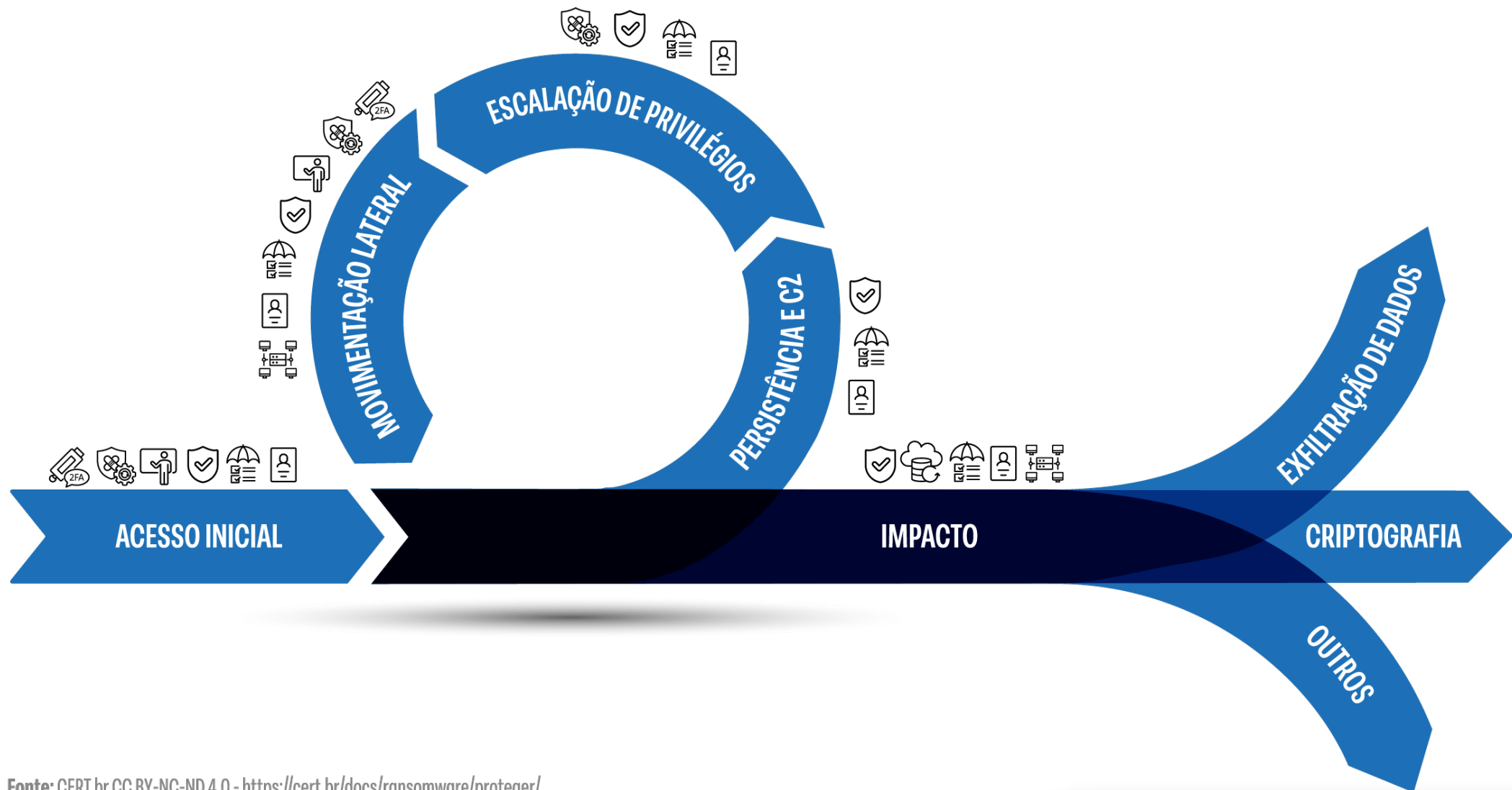
7. Gerenciar Identidades e Acessos



8. Segmentar a Rede

Proteção

Um único Mecanismo Pode ser Usado para Múltiplas Defesas



Fonte: CERT.br CC BY-NC-ND 4.0 - <https://cert.br/docs/ransomware/proteger/>

Deteção

Detectar o Quanto Antes para Minimizar ou até Evitar o Impacto

A **deteção** pode ocorrer nas **diferentes fases e de distintas formas**.

Quanto antes detectar, **menores** serão os **impactos**.

É necessário **preparar o ambiente** para **monitorar e detectar** as atividades dos atacantes.



1. Habilitar e Analisar *Logs*



2. Monitorar o Tráfego de Rede



3. Observar Alertas de Ferramentas de Proteção



4. Monitorar Contas de Usuários e Administradores



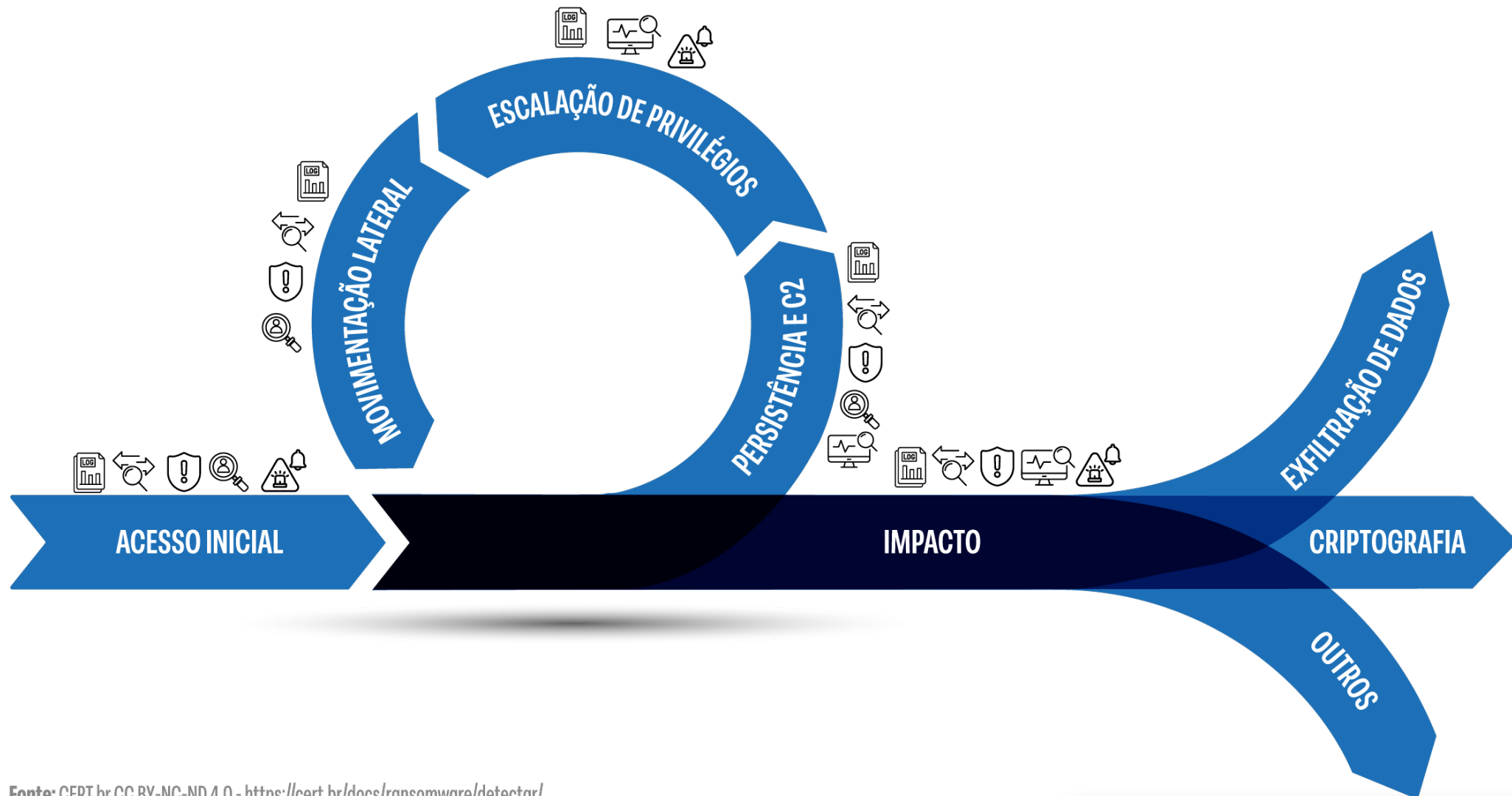
5. Monitorar o Uso dos Sistemas



6. Estabelecer um Canal para Receber Notificações de Segurança

Detecção

Detectar o Quanto Antes para Minimizar ou até Evitar o Impacto



Fonte: CERT.br CC BY-NC-ND 4.0 - <https://cert.br/docs/ransomware/detectar/>

Detalhes sobre Proteção e Detecção

Documento de Proteção contra *Ransomware*

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/>

Obrigada!

✉ para materiais de conscientização: doc@cert.br

✉ notificações para: cert@cert.br

✂ @certbr

<https://cert.br/>

nic.br **cgi.br**

www.nic.br | www.cgi.br