

# Cyber Academy

FEBRABAN  
/CYBER LAB



Laboratório de Segurança Cibernética - 01/07/2025

# A importância da Segurança da Informação

FEBRABAN  
/ CYBER LAB

 GoHacking



# WHOAMI



- ✓ Graduado em Engenharia de Computação pelo Instituto Militar de Engenharia (**IME**)
- ✓ Cofundador e Instrutor da **GoHacking**
- ✓ Foi instrutor do **SANS Institute**
- ✓ Certificações em SegInfo: **CISSP**, **GSE #291**, **OSED**, **OSCP**, **OSWP**, **OSCE**, GSP, GX-PT, GX-CS, GX-IA, GX-IH, GSEC, GCED, GCIA, GCIH, GCWN, GCFA, GNFA, GWAPT, GPEN, GPYC, GMOB, GDAT, GAWN, GRID, GREM, GXPN (<https://www.credly.com/users/laios-barbosa>)
- ✓ Mais de 15 anos de experiência em Administração de Redes/Sistemas e Segurança da Informação
- ✓ Participação ativa nos **Grandes Eventos** – Gerência e Proteção dos Sistemas de Comando e Controle do Ministério da Defesa: Rio +20, Copa das Confederações 2013, Jornada Mundial da Juventude, Copa do Mundo 2014, Jogos Olímpicos 2016
- ✓ “Um pouco viciado em **CTF** ... 😊”
- ✓ **SANS NetWars Champion (and Champion of Champions)**
- ✓ Pai, Marido e Surfista 



**CERT**  
Incident Response Process Professional  
Certificate Holder

# WHOAMI



@laios\_barbosa



Laios Barbosa



laios\_barbosa



# Agenda

1. Objetivo
2. Cenário Atual
3. Conceitos
4. A importância da Seg Info
5. Tendências
6. Recomendações

# Objetivo

FEBRABAN  
/ CYBER LAB



# Objetivo

Entender a importância da Segurança da Informação para as pessoas, empresas e para a sociedade.

# Cenário Atual

FEBRABAN  
/CYBER LAB



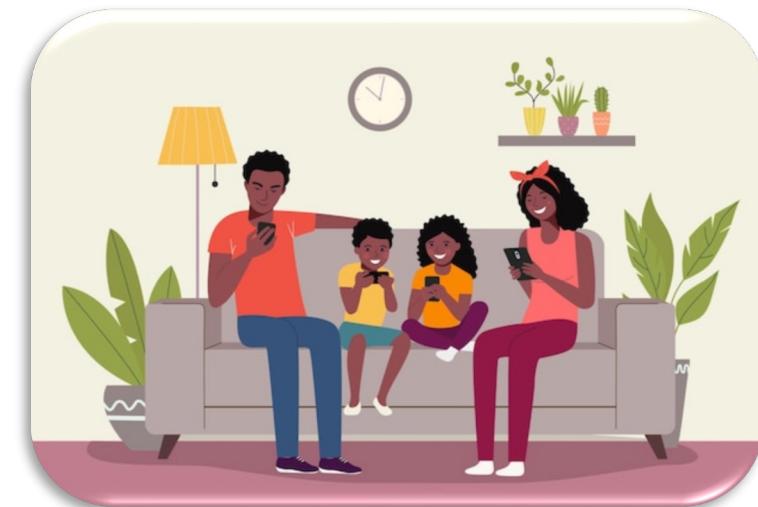
## Cenário Atual

- O mundo está cada vez **mais conectado** e mais dependente de tecnologias.
- A Tecnologia da Informação (TI) já faz **parte da vida de qualquer pessoa**: crianças, jovens, adolescentes, adultos e idosos.
- A TI já é **parte fundamental** para o sucesso de qualquer negócio, de qualquer empresa de qualquer tamanho.
- As redes de computadores e a Internet revolucionaram a sociedade moderna, mudaram a forma do relacionamento entre as pessoas e como os negócios, de maneira geral, são feitos, e com isso introduziram **riscos novos e substanciais**.



## Cenário Atual

- A tecnologia está fortemente presente na **vida pessoal e profissional** de qualquer ser humano da era moderna.
- Amigos, família e parentes se relacionam por computadores, celulares, tablets, **dispositivos que estão conectados na Internet**.
- Compartilhamos **informações** e aspectos da **nossa vida** nas diversas redes sociais.
- **Informações** pessoais (nome, endereço, telefone, outros) são **trafegadas** em redes, **processadas** e **armazenadas** em sistemas computacionais.



## Cenário Atual

- Em nosso trabalho, utilizamos algum **dispositivo tecnológico** para executar as tarefas: computador, laptop, celular, tablet.
- As empresas **precisam estar conectadas** em rede para que as **informações** possam ser distribuídas e acessadas.
- **Dados críticos para o negócio** são trafegados, processados e armazenados nas redes de computadores.
- As organizações podem ter seu próprio centro de dados (*Datacenters*) ou utilizar os serviços de Nuvem (*Cloud*).



## Cenário Atual

- Nesse novo mundo digital surgiram novas **ameaças**.
- **Indivíduos e grupos** que exploraram e utilizam a tecnologia para executar atividades criminosas: enganar pessoas, fraudar, roubar dinheiro, sabotar sistemas, “raptar” dados, extorquir empresas, entre outras.
- Os **ataques cibernéticos** já fazem parte do cotidiano das pessoas e das organizações do mundo todo.



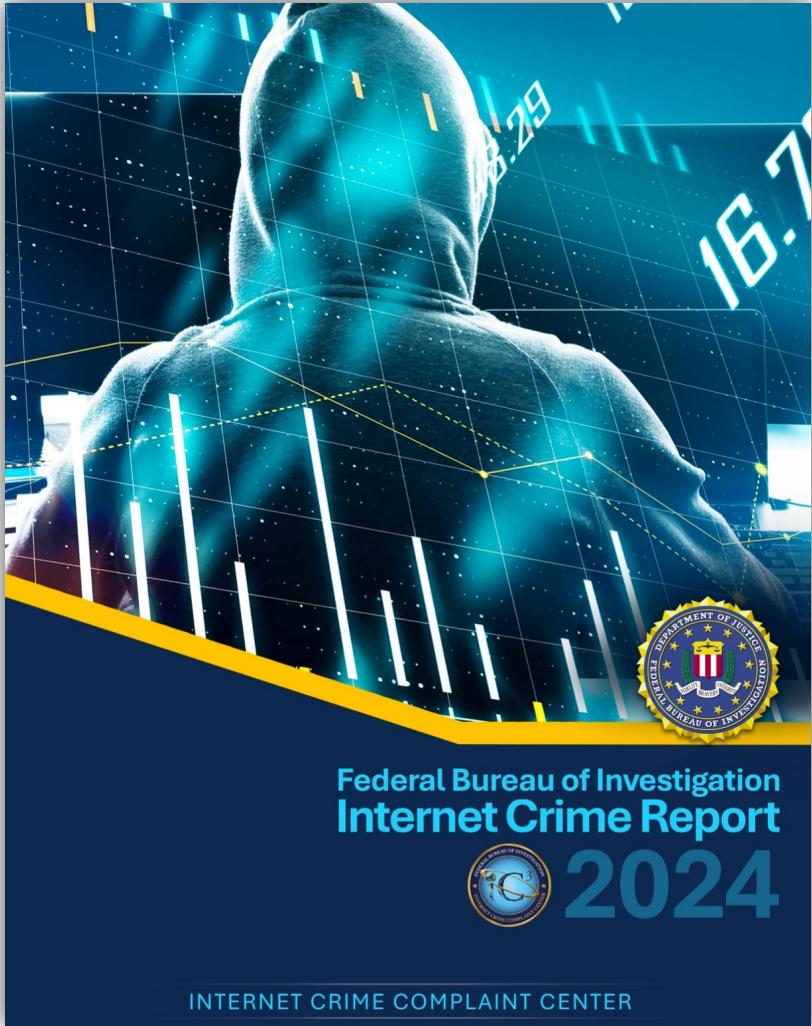
## Cenário Atual

**Ataques** a redes de computadores e sistemas digitais podem levar a graves perdas:

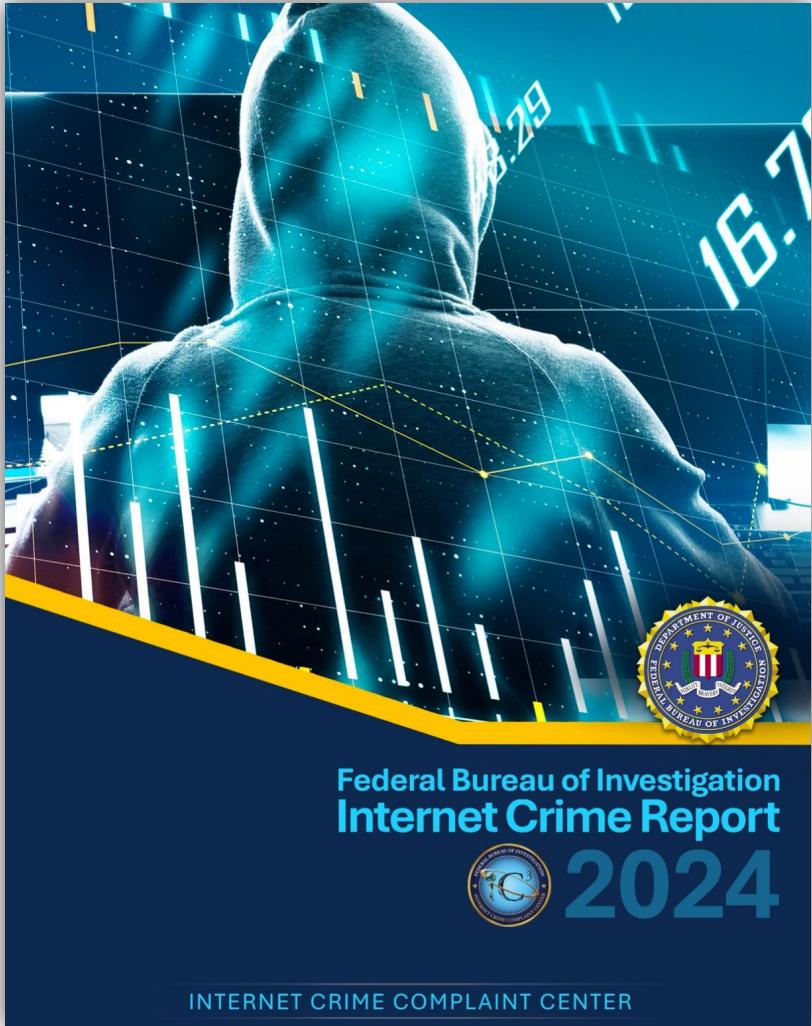
- ✓ Vidas
- ✓ Financeira
- ✓ Imagem
- ✓ Reputação
- ✓ Dados pessoais
- ✓ Propriedade intelectual



# Cenário Atual



[https://www.ic3.gov/AnnualReport/Reports/2024\\_IC3Report.pdf](https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf)

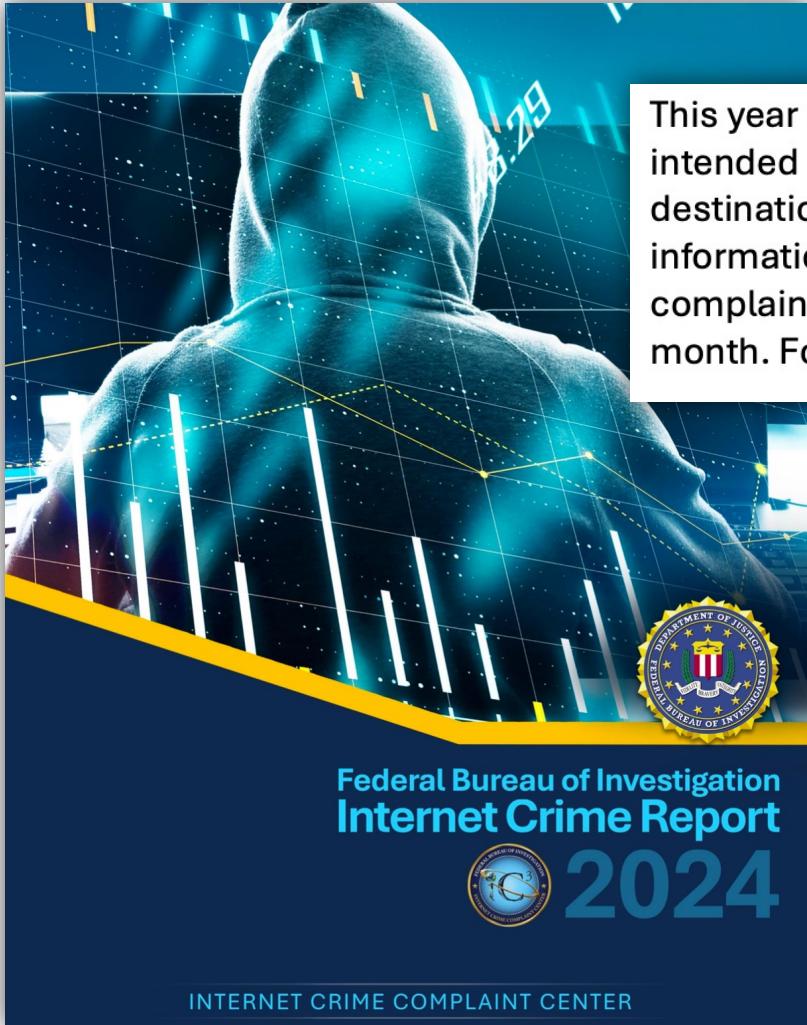


**FBI**

**Centro de Reclamações de Crimes na Internet**  
***Internet Crime Complaint Center (IC3)***

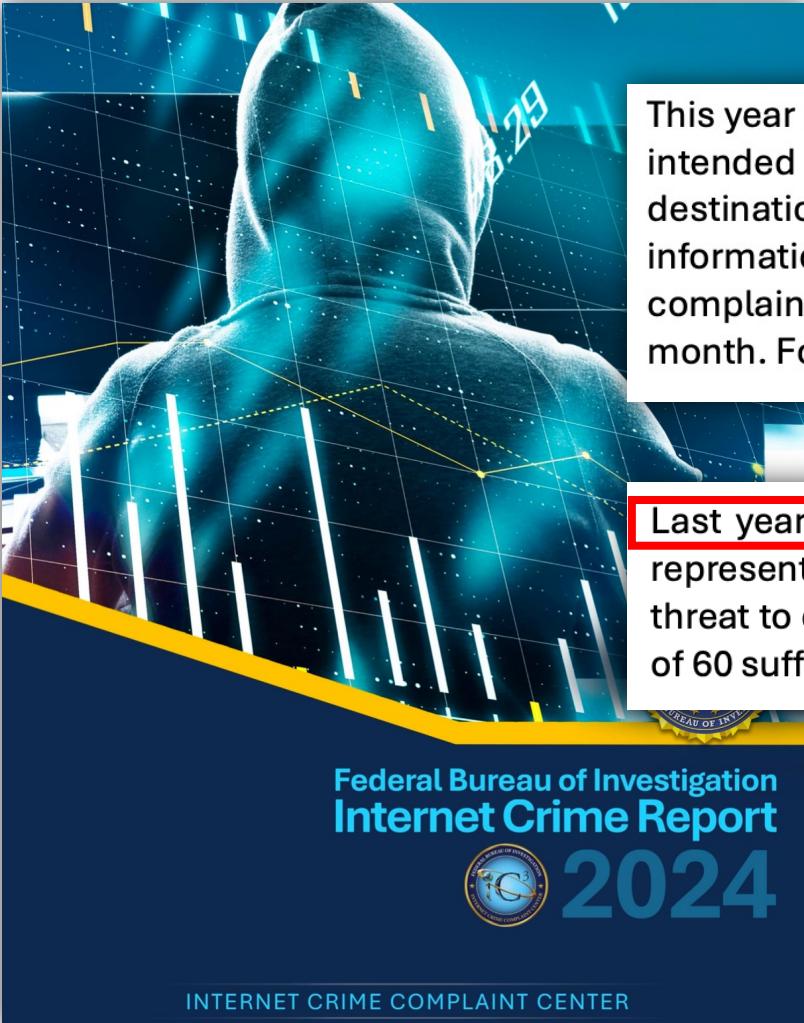
**Relatório Anual de Crimes na Internet**

# Cenário Atual



This year marks the 25<sup>th</sup> anniversary of the FBI's Internet Crime Complaint Center, or IC3. Originally intended to serve the law enforcement community, IC3 has evolved to become the primary destination for the public to **report cyber-enabled crime and fraud**, as well as a key source for information on scams and cyber threats. Since its founding, IC3 has received over 9 million complaints of malicious activity. During its infancy, IC3 received roughly 2,000 complaints every month. For the past five years, **IC3 has averaged more than 2,000 complaints every day.**

# Cenário Atual



This year marks the 25<sup>th</sup> anniversary of the FBI's Internet Crime Complaint Center, or IC3. Originally intended to serve the law enforcement community, IC3 has evolved to become the primary destination for the public to report cyber-enabled crime and fraud as well as a key source for information on scams and cyber threats. Since its founding, IC3 has received over 9 million complaints of malicious activity. During its infancy, IC3 received roughly 2,000 complaints every month. For the past five years, IC3 has averaged more than 2,000 complaints every day.

Last year saw a new record for losses reported to IC3, totaling a staggering \$16.6 billion. Fraud represented the bulk of reported losses in 2024, and ransomware was again the most pervasive threat to critical infrastructure, with complaints rising 9% from 2023. As a group, those over the age of 60 suffered the most losses and submitted the most complaints.



abes ▾ associados ▾ dados do setor serviços ▾ publicações ▾

## Brasil é o segundo país mais vulnerável a ataques cibernéticos, segundo relatório da Trend Micro

06/10/2023



## Instituto Brasileiro de Segurança, Proteção e Privacidade de Dados

[Início](#) [Eventos IBRASPD](#) [Mensagem da Diretoria](#) [Categoria de Associados](#) [Nossos Par](#)

# Incidentes Relevantes

Nesta pagina temos como objetivo apresentar os principais incidentes relevantes ocorridos no mercado e que vem sendo acompanhado pelo IBRASPD.

# Cenário Nacional

## **Contexto Atual – Incidentes de segurança com repercussão na mídia (Brasil)\***



- Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade



# Cenário Nacional



## Prefeitura de Munhoz de Mello confirma incidente cibernético com prejuízo de R\$ 298 mil

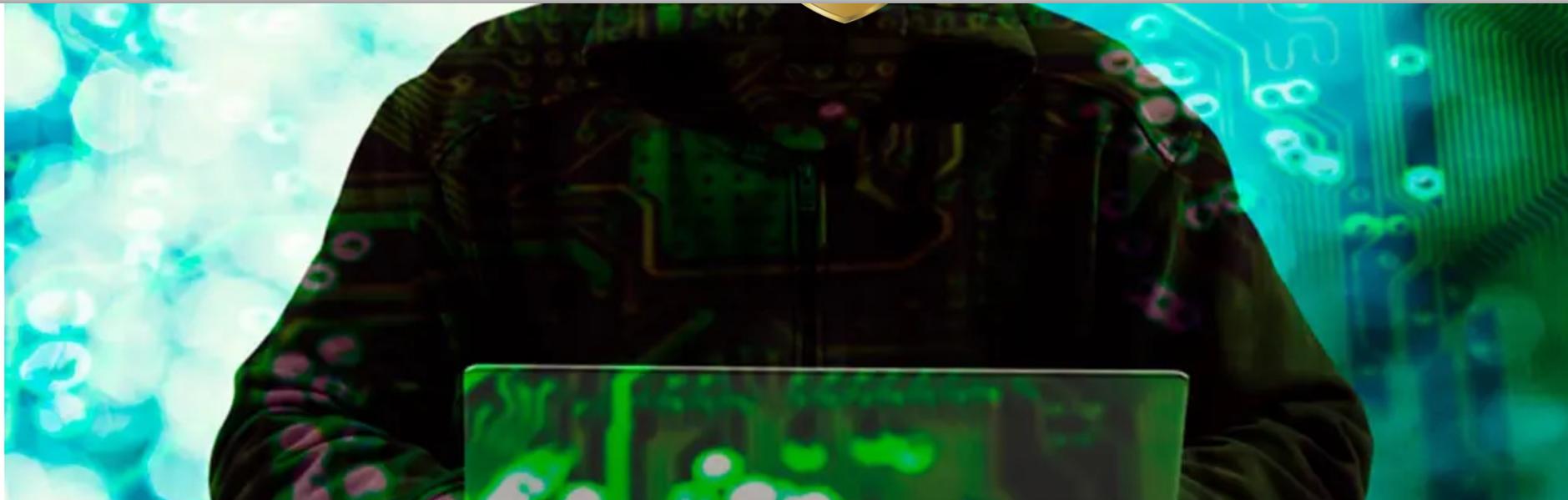
Segundo informações colhidas pelo boletim de ocorrência, a Secretaria de Finanças da cidade foi orientada por um falso gerente de banco a acessar um link malicioso que causou o desvio dos recursos. Em nota, a prefeitura informa que tomou providências adicionais de Segurança

Por: Matheus Bracco

janeiro 28, 2025

Destaques

# Cenário Nacional



## Grupo Sabin é atingido por incidente cibernético

Companhia de Diagnósticos de Saúde confirmou, por meio de nota, que um ciberataque impactou suas operações na loja online no início de janeiro. De acordo com a clínica, o incidente foi solucionado, e já está em contato com as autoridades e os clientes atingidos

Por: Matheus Bracco | fevereiro 7, 2025 | Destaques



## Dataprev investiga suposto comprometimento de dados no INSS

Nesta semana, circularam nas redes informação de que o sistema de Comunicação de Acidente de Trabalho (CAT), ligado ao instituto de segurança, teria sido alvo de um ataque hacker, comprometendo informações pessoais de 39 milhões de pessoas. Em nota, a Dataprev informa não ter detectado nenhum indicativo de vazamento, mas que segue investigando junto ao INSS

Por: Matheus Bracco

fevereiro 7, 2025

Destaques



## Banco Central comunica vazamento de chaves Pix

Falha em sistema da QI SCD S.A. expôs dados cadastrais de chaves Pix; o Banco Central garante que informações sensíveis não foram comprometidas; Esse é o primeiro vazamento de dados pessoais vinculados ao Pix em 2025.



Por: Mariana Nalessó Pó



março 17, 2025



Destaques

# Conceitos

FEBRABAN  
/ CYBER LAB



# Segurança da Informação



# Segurança da Informação



# Segurança da Informação



Presidência da República Órgãos do Governo Acesso à Informação Legislação Acessibilidade



Entrar com gov.br

≡ Gabinete de Segurança Institucional

O que você procura?



[Home](#) > Segurança da Informação e Cibernetica > Glossário de Segurança da Informação

## Glossário de Segurança da Informação

Publicado em 26/11/2021 14h21 | Atualizado em 28/02/2025 08h46

Compartilhe: [f](#) [X](#) [m](#) [in](#) [o](#)

A B C D E F G H I J K L M N O P Q R S T U >

PORTARIA GSI/PR Nº 93, DE 18 DE OUTUBRO DE 2021

# Segurança da Informação

- **CONFIDENCIALIDADE** - propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não **autorizados** nem credenciados.
- **INTEGRIDADE** - propriedade pela qual se assegura que a informação **não foi modificada** ou destruída de maneira não autorizada ou acidental.
- **DISPONIBILIDADE** - propriedade pela qual se assegura que a informação **esteja acessível e utilizável**, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados.

The screenshot shows a white header with the gov.br logo and links for Presidência da República, Órgãos do Governo, Acesso à Informação, and Legislação. Below the header, a blue navigation bar includes a menu icon, the text 'Gabinete de Segurança Institucional', and a breadcrumb trail: Home > Segurança da Informação e Cibernetica > Glossário de Segurança da Informação. The main content area has a blue header 'Glossário de Segurança da Informação'. At the bottom of the page, there is a small note: 'Publicado em 26/11/2021 14h21 | Atualizado em 28/02/2025 08h46'.

# Confidencialidade

- **Manter segredo**
- Só quem tem permissão pode acessar a informação.
- Imagine que você envia uma mensagem no WhatsApp para um amigo. A confidencialidade garante que só ele possa ler, e não outras pessoas no caminho (como hackers, provedores ou terceiros).
- Senhas, criptografia e controle de acesso.



# Integridade

- **Nada foi alterado**
- A informação chega do jeito que foi enviada, sem alterações.
- Você transfere R\$100 pelo aplicativo do banco. A integridade garante que o valor não seja alterado para R\$1.000 durante o processo.
- A integridade é garantida por mecanismos que verificam se os dados não foram corrompidos ou modificados indevidamente.



# Disponibilidade

- **Estar acessível quando necessário**
- A informação ou sistema precisa estar funcionando quando for preciso.
- Você quer pagar uma conta pelo app do banco e ele está fora do ar. Isso é um problema de disponibilidade.
- Backups, servidores redundantes (extras) e proteção contra ataques ajudam a manter a disponibilidade.



# A importância da Segurança da Informação

FEBRABAN  
/CYBER LAB



# A importância da Seg Info para as pessoas

- A **Segurança da Informação** é fundamental para qualquer pessoa, pois **protege os dados pessoais, a privacidade e até a integridade financeira e física do indivíduo.**
- Em um mundo cada vez mais digital, negligenciar a segurança da informação pode **expor alguém a sérios riscos**.



- **Proteção da privacidade**
  - ✓ Informações pessoais como CPF, endereço, dados bancários, conversas privadas e localização são **extremamente sensíveis**.
  - ✓ Vazamentos podem causar **constrangimentos, invasões de privacidade ou uso indevido da identidade**.
- **Prevenção contra fraudes e golpes**
  - ✓ Cibercriminosos usam **dados vazados** para aplicar golpes financeiros, roubo de identidade e clonagem de cartões.
  - ✓ Um simples descuido, como **usar a mesma senha em vários sites**, pode permitir acesso a contas bancárias e redes sociais.

# A importância da Seg Info para as pessoas

- **Preservação da reputação**
  - ✓ Fotos, mensagens ou opiniões expostas sem controle podem prejudicar a imagem pessoal ou profissional.
  - ✓ Isso é especialmente relevante em redes sociais e ambientes de trabalho.
- **Segurança física**
  - ✓ Informações vazadas, como rotinas diárias ou localização em tempo real, podem expor o indivíduo a riscos como sequestros, assaltos ou perseguições.
- **Controle da própria identidade digital**
  - ✓ Uma identidade digital bem protegida evita que terceiros se passem por você (*phishing*, contas falsas, *deepfakes*).
  - ✓ Ajudar a manter a autenticidade das interações online.

- **Usar senhas fracas ou repetidas:** aumenta o risco de invasão de contas.
- **Responder a e-mails falsos (*phishing*):** pode levar a perda de dados ou dinheiro.
- **Publicar localização em tempo real:** pode informar criminosos sobre sua ausência de casa.



# A importância da Seg Info para as pessoas

- Deve-se ter um cuidado especial com os mais vulneráveis.
- **Crianças e idosos** são alvos constantes de cibercriminosos.



## Crianças – Roblox

### Roblox: 'Achava que era um jogo inocente, mas meu filho estava sendo assediado por pedófilos'

A britânica Sarah (nome fictício) tomou precauções quando seu filho pré-adolescente começou a usar o Roblox, plataforma de games online voltada a jovens, em que jogadores podem criar seus próprios jogos e conectar-se com os demais 90 milhões de usuários espalhados pelo mundo.

Sarah acionou os dispositivos de controle parental, para proteger a privacidade de seu filho online e impedir que ele conseguisse enviar mensagens para terceiros.



Plataforma Roblox permite que se criem jogos e compartilhem-nos em comunidade online; uma mãe conta, porém, que seu filho foi induzido a mandar fotos de si mesmo sem roupa

## Crianças – Roblox

# O polêmico conselho do CEO da Roblox para os pais de jogadores



Graham Fraser

Repórter de tecnologia

22 março 2025

"Se você não se sente confortável, não deixe seus filhos jogarem Roblox." Com esse conselho, dado em uma entrevista exclusiva à BBC, o CEO da popular plataforma de jogos, Dave Baszucki, desencadeou um intenso debate entre os pais.

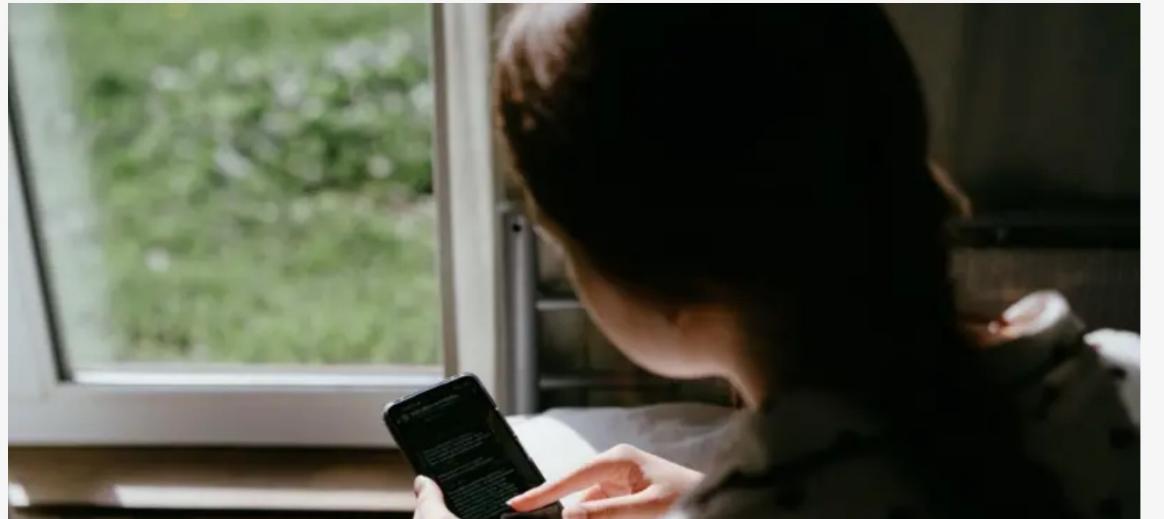
## Crianças – Roblox

O polêmico conselho do CEO da Roblox para os pais de jogadores



GETTY IMAGES

**'Minha filha de 9 anos foi aliciada no Roblox'**



# A importância da Seg Info para as organizações

A **Segurança da Informação** é vital para empresas e organizações porque protege ativos essenciais, como dados estratégicos, financeiros, operacionais e pessoais, além de garantir a continuidade do negócio, a conformidade legal e a confiança do mercado.



- **Proteção de dados sensíveis**
  - ✓ Informações como propriedade intelectual, dados de clientes, contratos, planos estratégicos e dados financeiros são **ativos críticos**.
  - ✓ Vazamentos ou perdas podem causar **prejuízos operacionais, financeiros e reputacionais**.
- **Continuidade do negócio**
  - ✓ Ataques cibernéticos (sequestro/criptografia de dados – *ransomware*) ou falhas de segurança **podem paralisar sistemas**, impedir vendas, interromper serviços e gerar grandes prejuízos.
  - ✓ A segurança da informação apoia **planos de continuidade e recuperação de desastres**.

# A importância da Seg Info para as organizações

- **Conformidade legal e regulatória**
  - ✓ Empresas precisam cumprir leis.
  - ✓ LGPD (Brasil) – proteção de dados pessoais;
  - ✓ PCI-DSS – segurança em transações com cartões de crédito;
  - ✓ SOX, HIPAA, GDPR, entre outras (a depender do setor).
  - ✓ A não conformidade pode **gerar multas milionárias**, sanções e ações judiciais.
- **Reputação e confiança do mercado**
  - ✓ Uma falha de segurança pode **abalar a confiança de clientes**, parceiros e investidores.
  - ✓ A **imagem institucional** é um ativo intangível precioso, difícil de reconstruir após uma violação.

- **Vantagem competitiva**
  - ✓ Empresas que tratam a segurança com seriedade demonstram **maturidade corporativa**, o que pode atrair novos negócios, especialmente em setores regulados (bancos, saúde, governo, tecnologia).
  - ✓ Boas práticas de segurança são um **diferencial competitivo**.
- **Redução de riscos e custos**
  - ✓ **Prevenção custa menos do que lidar com as consequências** de um incidente (investigações, multas, perdas financeiras, tempo de recuperação).
  - ✓ Segurança bem aplicada reduz o risco de fraudes internas, sabotagem, espionagem industrial.

# A importância da Seg Info para as organizações

- Quando um ataque cibernético é bem sucedido, uma empresa pode:
  - ✓ Ficar dias ou semanas sem operar.
  - ✓ Perder milhões em receita e resgate.
  - ✓ Ver sua base de clientes migrar para concorrentes.
  - ✓ Ser processada por não proteger dados pessoais.
  - ✓ Ter sua reputação destruída na mídia.



# Tendências

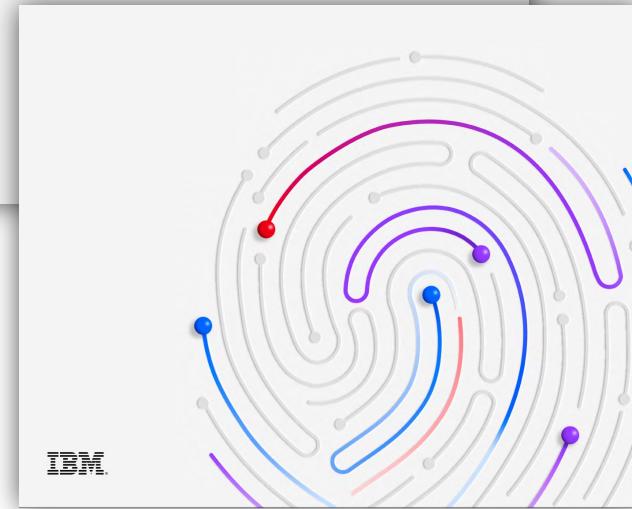
FEBRABAN  
/ CYBER LAB



# Tendências

## X-Force Threat Intelligence Index 2024

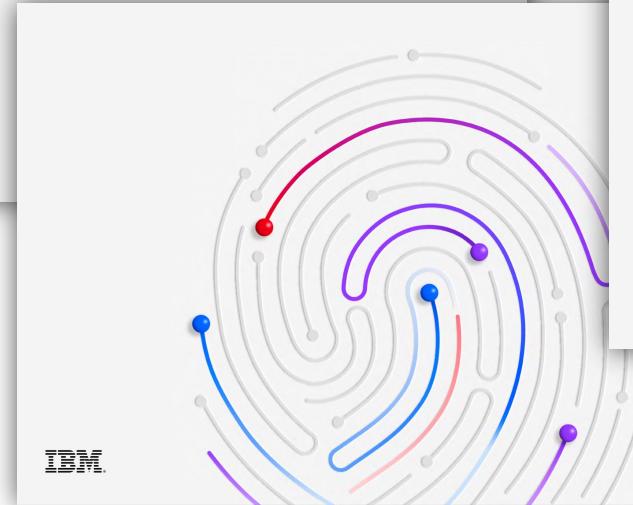
Resumo executivo



# Tendências

## X-Force Threat Intelligence Index 2024

Resumo executivo



71%

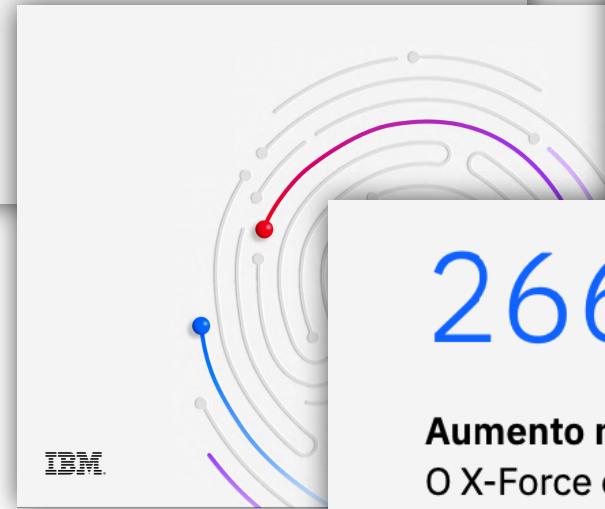
**Aumento ano após ano no volume de ataques usando credenciais válidas**

Pela primeira vez na história, a utilização de contas válidas tornou-se o ponto de entrada mais comum dos cibercriminosos nos ambientes das vítimas. Isso representou 30% de todos os incidentes aos quais o X-Force respondeu em 2023.

# Tendências

## X-Force Threat Intelligence Index 2024

Resumo executivo



71%

### Aumento ano após ano no volume de ataques usando credenciais válidas

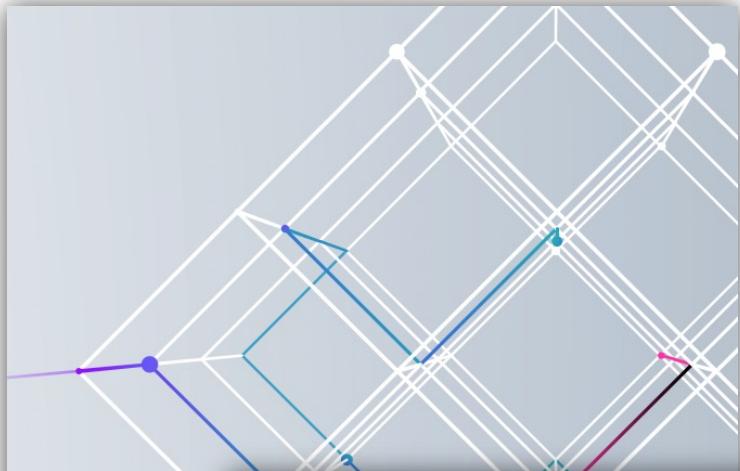
Pela primeira vez na história, a utilização de contas válidas tornou-se o ponto de entrada mais comum dos cibercriminosos nos ambientes das vítimas. Isso representou 30% de todos os

266%

### Aumento no uso de infostealers

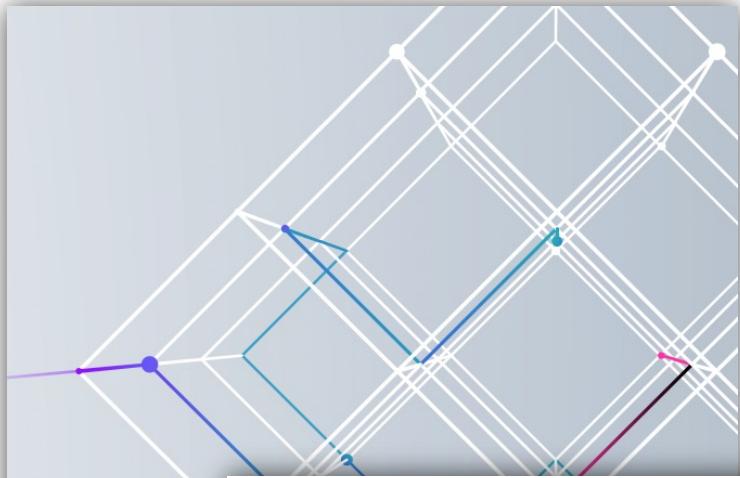
O X-Force observou que grupos de ameaças que anteriormente eram especialistas em ransomware demonstraram interesse crescente em infostealers. Uma série de novos infostealers proeminentes surgiram recentemente e demonstraram um aumento de atividade em 2023, como Rhadamanthys, LummaC2 e StrelaStealer.

# Tendências



IBM X-Force  
2025 Threat  
Intelligence Index

# Tendências



## IBM X-Force 2025 Threat Intelligence Index

### Threat actors add AI to their toolboxes.

Our analysts have documented that threat actors are using AI to build web sites and incorporate deepfakes in phishing attacks. We have also observed threat actors applying gen AI to create phishing emails and write malicious code.<sup>2</sup>

**AI – Artificial Intelligence**  
**IA – Inteligência Artificial**

# Uso de IA por Atacantes

Threat Intelligence

## Adversarial Misuse of Generative AI

January 29, 2025

Google Threat Intelligence Group

Rapid advancements in artificial intelligence (AI) are unlocking new possibilities for the way we work and accelerating innovation in [science](#), [technology](#), and beyond. In cybersecurity, AI is poised to transform digital defense, [empowering defenders and enhancing our collective security](#). Large language models (LLMs) open new possibilities for defenders, from sifting through complex telemetry to [secure coding](#), [vulnerability discovery](#), and streamlining operations. However, some of these same AI capabilities are also available to attackers, leading to understandable anxieties about the potential for AI to be misused for malicious purposes.



# Uso de IA por Atacantes – Deepfakes



<https://blog.wellsins.com/corporate-case-study-25-million-deepfake-scam-sends-a-wake-up-call-to-corporate-cybersecurity>

# Uso de IA por Atacantes – Deepfakes

According to Hong Kong police, the finance employee initially received an email from an account claiming to be Arup's chief financial officer (CFO) and requesting the deployment of multiple confidential transactions. The employee suspected the email was a phishing scam, but he reportedly felt more at ease after joining a video call with individuals who looked and sounded like the CFO and several of his colleagues.



# Recomendações

FEBRABAN  
/ CYBER LAB



## Recomendações

**“A segurança é tão forte quanto o elo mais fraco.”**



# Boas práticas de segurança para pessoas

- Usar senhas fortes e únicas com autenticação de dois fatores.
- Atualizar sistemas e aplicativos com frequência.
- Cuidar do que compartilha nas redes sociais.
- Desconfiar de mensagens, e-mails e links suspeitos.
- Usar antivírus e redes seguras (evitar Wi-Fi público sem proteção).



# Boas práticas de segurança para empresas

- Políticas de segurança claras e bem definidas.
- Gestão de acesso baseado no princípio do menor privilégio.
- Treinamento e conscientização de usuários.
- *Backups* regulares e planos de recuperação.
- Monitoramento e capacidade de resposta a incidentes.



# Cartilha de Segurança para a Internet

## Conheça Todos os Fascículos

Os materiais contém recomendações e dicas para aumentar a sua segurança e se proteger de possíveis ameaças.

Aqui você vai encontrar

- > **Fascículos** - livretos em formato PDF, com dicas sobre assuntos específicos
- > **Fascículos para impressão** - arquivos com resolução adequada para impressão, incluindo uma versão com marcas de corte para impressão em gráfica

Gostaria de uma versão com o logotipo de sua organização?

Entre em contato!

[» Saiba mais](#)



# Cartilha de Segurança para a Internet

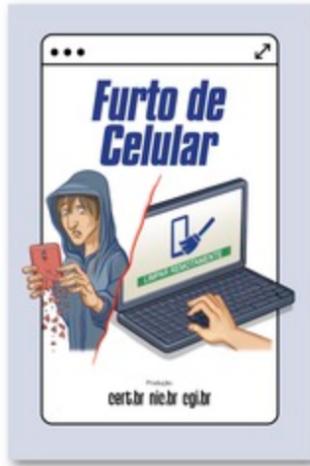
## Fascículos

A Cartilha de Segurança para Internet é organizada em Fascículos com temas específicos, acompanhados por *slides* para ministrar palestras ou complementar conteúdos de aulas.

Início / [Fascículos](#)



# Cartilha de Segurança para a Internet



## Furto de Celular

[BAIXE AQUI O PDF](#)

SEU CELULAR É SUA CARTEIRA: CUIDE DA SUA VIDA DIGITAL.  
Toda praticidade que o celular traz pode rapidamente se tornar um pesadelo se ele cair nas mãos erradas.

O [Fascículo Furto de Celular](#) mostra como se preparar antecipadamente para reduzir os danos e o que fazer se um furto ocorrer.



Assista aos vídeos do Cidadão na Rede com dicas sobre o assunto deste fascículo:

[Apagando os dados do celular remotamente](#)

[Localização remota do celular](#)

[Proteja o seu chip SIM](#)

[O que é IMEI?](#)

### Download

Fascículo Furto de Celular:

[PDF](#)

Versões em alta resolução, para impressão:

[PDF em alta resolução](#)

[PDF com marcas de corte](#)

[Acesse aqui para mais detalhes sobre tamanho e formato de impressão.](#)

**FIM**  
**Muito obrigado**

**FEBRABAN**  
/ CYBER LAB

