SEGURANÇA DA INFORMAÇÃO

Introdução

ROTEIRO

- Conceitos Fundamentais
- A importância da Informação
- O que é Segurança da Informação
- Pilares da Segurança da Informação
- Vulnerabilidades e Ameaças
- Ataques
- Incidentes mais frequentes

CONCEITOS FUNDAMENTAIS

A importância da informação?

A informação abarca diversos atributos no cotidiano do ser humano:

Adquirimos cidadania, cultura, desenvolvimento profissional, pessoal e social

Aprendemos a ser competitivos

Sinalização para influência e poder

CONCEITOS FUNDAMENTAIS

Proteger a informação é fundamental em várias vertentes:

Organizacional:
informações comerciais, patentes, direitos, etc.

Legal:
direito de propriedade, responsabilidade por atos praticados

Pessoal:
anonimato e privacidade

Política/ Administrativa:
transparência, informações estratégicas de um país ou empresa

CONCEITOS FUNDAMENTAIS

É muito complexo lidar com informação no contexto atual, pois envolve:

Quantidade, disponibilidade, múltiplas fontes (locais remotos, públicas e privadas, por exemplo)

Meios de acesso: diversos dispositivos, diversas tecnologias, diversos meios físicos (ar, cabos)

- Ao mesmo tempo em que a internet potencializa o acesso à informação, ela também potencializa vulnerabilidades e novas ameaças à segurança
- Inúmeras são as ferramentas à disposição de usuários mal-intencionados

CONCEITOS FUNDAMENTAIS

O que é segurança da informação?

Termo utilizado com o objetivo de assegurar que uma organização alcance suas metas, desenvolvendo sistemas que considere os riscos da tecnologia da informação para a própria organização, usuários e parceiros

Deve auxiliar para que informações sigilosas sejam acessadas somente por pessoas autorizadas

Também permite construir políticas e métodos que são empregados na troca de dados confidenciais

É responsável por se preocupar com o uso dos sistemas que possam colocar em risco os requisitos de segurança

CONCEITOS FUNDAMENTAIS

Pilares da segurança da informação

Basicamente envolve 3 fundamentos:

- **Disponibilidade** (dados e sistema)
- **Integridade** (dados e sistema)
- **Confidencialidade** (dados e informações dos sistemas)

Fonte: 1

CONCEITOS FUNDAMENTAIS

Pilares da segurança da informação

Confidencialidade → Trata-se do sigilo da informação. Muitos dados devem ser mantidos em segredo, em especial os privados e os que não devem ser divulgados para usuários não autorizados.

Exemplo: Dados no prontuário de um paciente, dados de controle de sistema de proteção (senhas e chaves criptográficas).

CONCEITOS FUNDAMENTAIS

Pilares da segurança da informação

Integridade → Dados

- Dados não podem ser alterados sem autorização

- **Quando um dado pode ser alterado?**
  No transporte, no armazenamento e no processamento

CONCEITOS FUNDAMENTAIS

Pilares da segurança da informação

Integridade → Sistemas

- Devem se comportar conforme seus requisitos e precisam estar livres de manipulações sem autorização

- **Exemplo:** Um sistema de processamento de folha de pagamento de um sistema bancário não pode ser sabotado.

CONCEITOS FUNDAMENTAIS

Pilares da segurança da informação

Disponibilidade

- Qualquer serviço prestado deve estar disponível de forma apropriada para os usuários que têm autorização em acessá-lo.
- Protege contra tentativas de deletar dados e impede o uso do sistema em ocasião de ataque de negação de serviço (DoS).
- Ataques do tipo DoS sobrecarregam os serviços disponíveis em servidores e na rede e impedem o uso dos mesmos pelos usuários.

VULNERABILIDADES

Tratam-se de fraquezas que são inerentes aos elementos de um sistema

Pontos fracos que podem ser explorados

Origens das vulnerabilidades:

Projeto de sistema deficiente

Implementação deficiente de uma aplicação/ sistema

Gerenciamento não realizado ou insuficiente

VULNERABILIDADES

Exemplos associados aos sistemas e dados

Física: proteção mal feita de equipamentos computacionais (servidores em locais inapropriados, sem ventilação adequada etc.)

Software: Bibliotecas com brechas, bugs

Canal de comunicação: grampo, interceptação de sinais, monitoramento do tráfego

→ Tudo que é conectado é vulnerável ←
A questão é como diminuir as vulnerabilidades!

AMEAÇAS

- Algo que possa atingir ou afetar o funcionamento, disponibilidade, operação, integridade das comunicações ou do sistema/servidor

ATAQUES

- **Técnicas específicas utilizadas para explorar vulnerabilidades.**

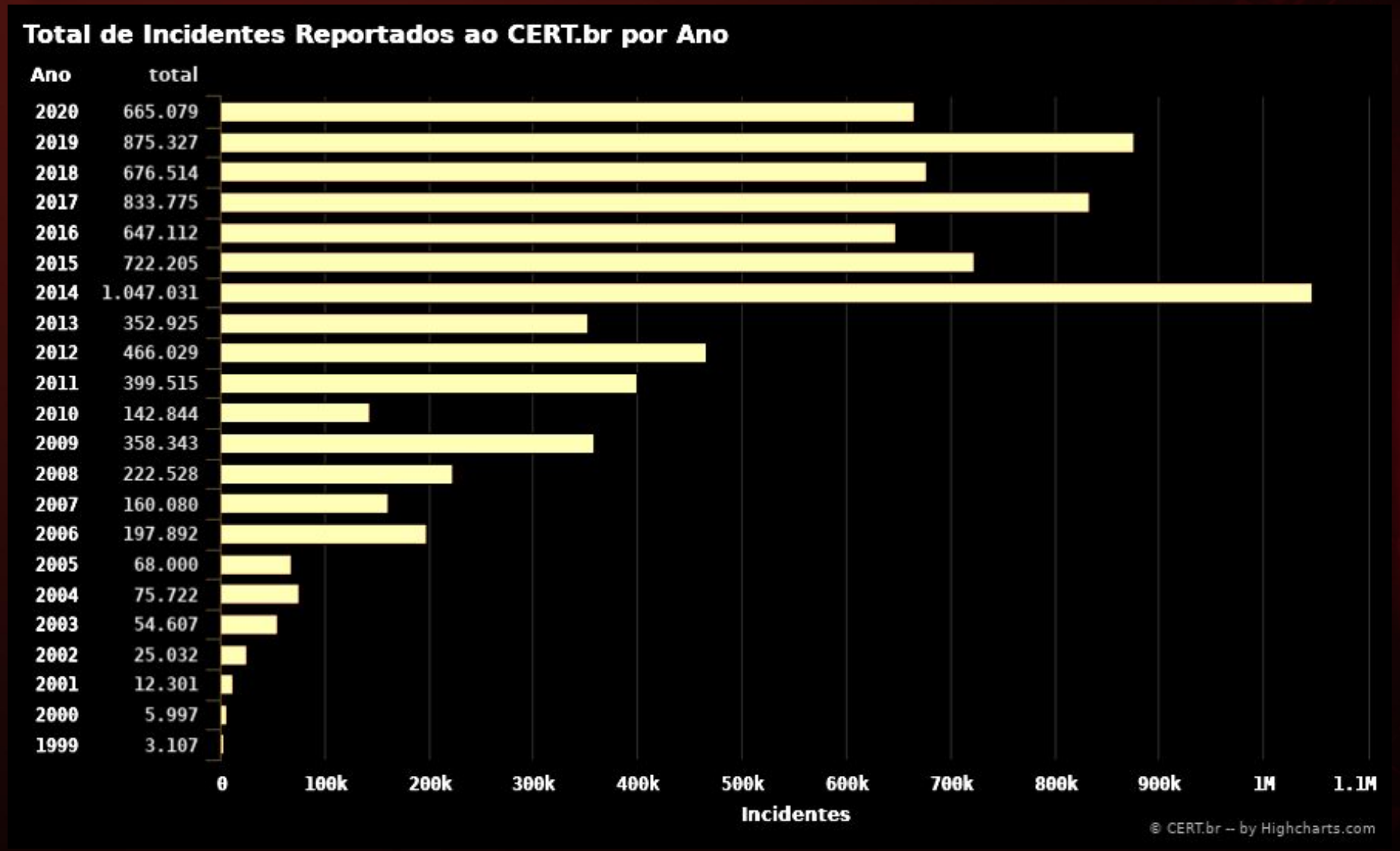
- **Contramedidas:** Métodos ou técnicas utilizadas para mitigar ataques ou para fechar as vulnerabilidades encontradas.

INCIDENTES

- Um incidente de segurança é um evento adverso confirmado, ou sob suspeita, e que está relacionado à segurança da informação

- Ele leva a perda ou abalo de um dos pilares da segurança
- Integridade, disponibilidade, confidencialidade

INCIDENTES FREQUENTES

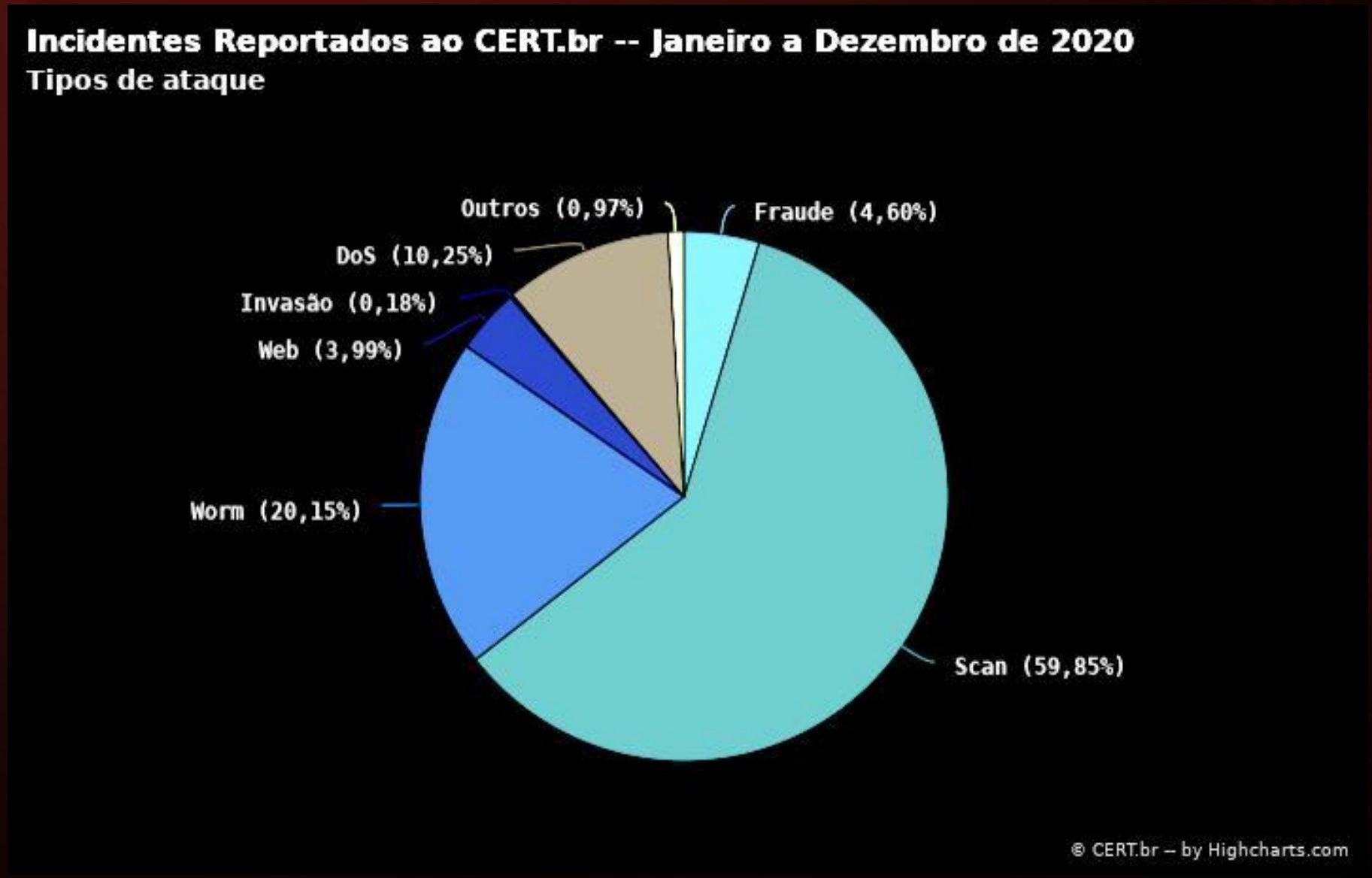


Fonte: 2

INCIDENTES FREQUENTES

Fonte: 2

INCIDENTES FREQUENTES



Fonte: 2

REFERÊNCIAS

1. https://www.security.ufrj.br/geral/o-que-e-um-incidente-de-seguranca-da-informacao/
2. https://www.cert.br/stats/incidentes/
3. https://www.security.ufrj.br/denuncie-um-incidente/
4. https://revistapesquisa.fapesp.br/vulnerabilidades-na-internet