UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# Segurança da Informação

## Aula 1 – Princípios da SegInfo, SegInfo x Segredes, Ciclo de Vida da Info

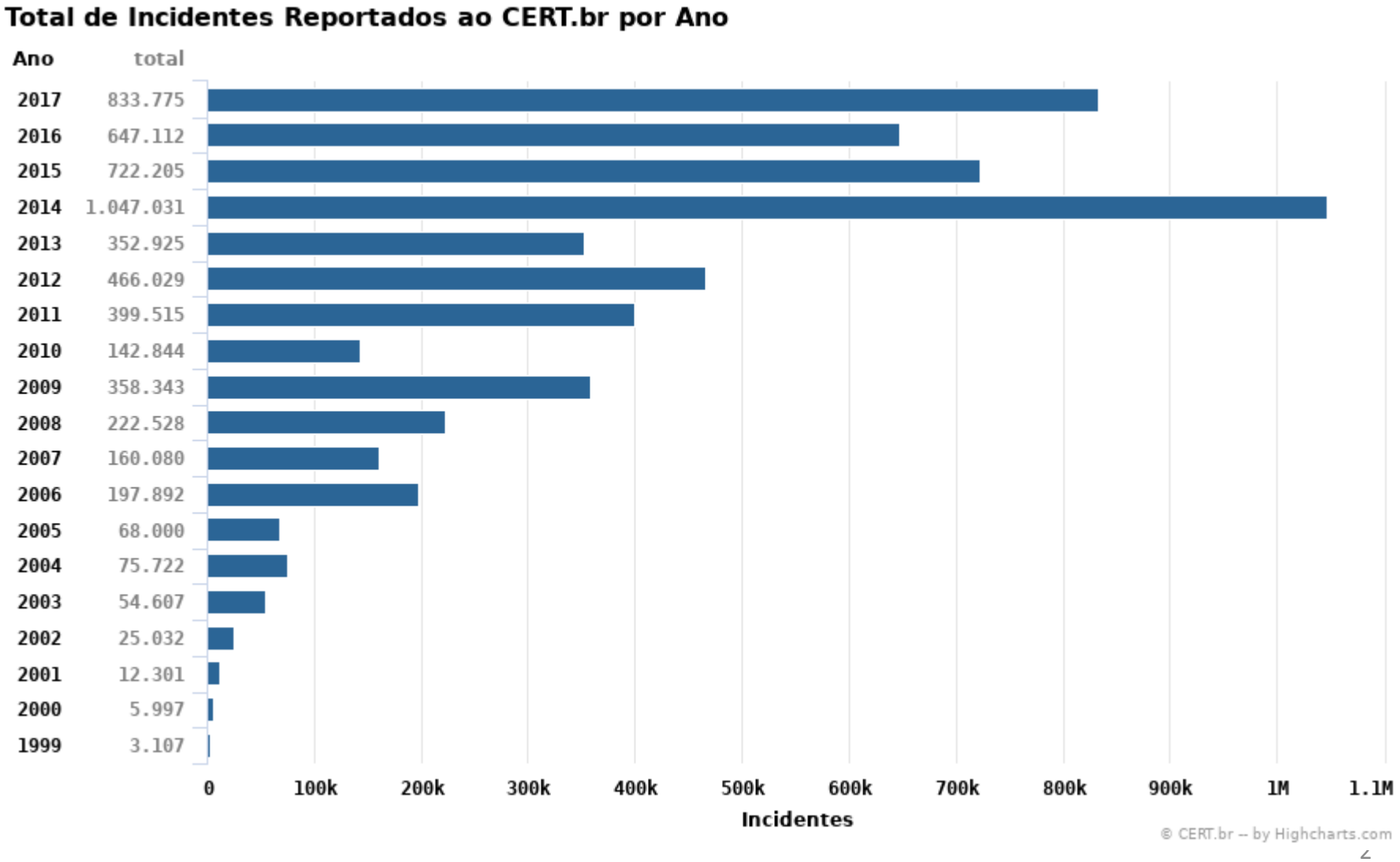
Prof. Dr. Eng. Fred Sauer

fsauer@gmail.com

http://www.fredsauer.com.br

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

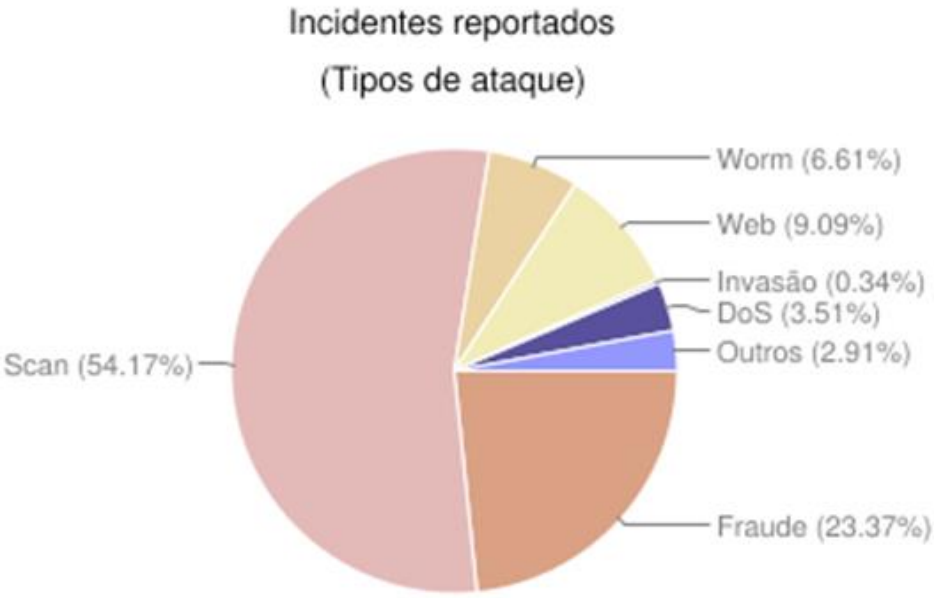
# Motivação

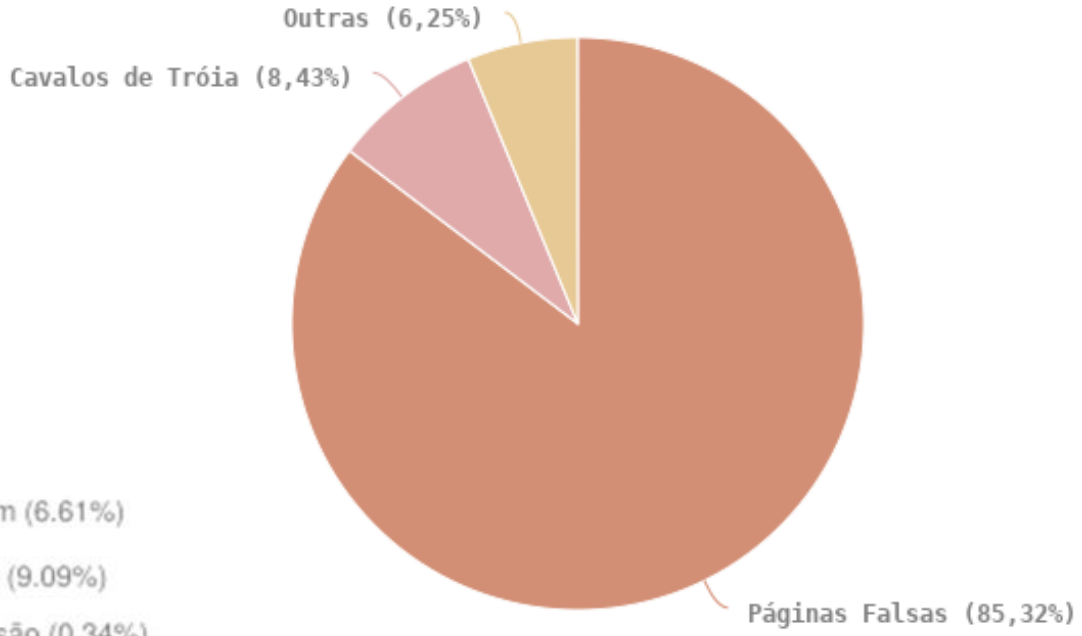



FONTE: http://www.cert.br, acessado em agosto/2018

# Motivação

**Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2015**




**Incidentes Reportados ao CERT.br -- Janeiro a Dezembro de 2017**

FONTE: http://www.cert.br, acessado em fevereiro/2017

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# VPNFilter

GESTÃO

## No Brasil, ataque afeta roteadores para minerar criptomoedas

*Segundo a ESET, uma campanha de criptojacking que afeta os roteadores MikroTik e modifica a configuração dos dispositivos*

12 de agosto de 2018 3 minutos de leitura

Por Redação

Comentar

Compartilhar!


Pesquisadores da ESET, empresa de detecção proativa de ameaças, descobriram uma campanha de criptojacking que afeta os roteadores MikroTik e modifica a configuração dos dispositivos para injetar uma cópia do script de mineração no navegador do Coinhive em algumas partes do tráfego web do usuário.

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# Ransomware

August 09, 2018

## Ransomware attack at Blue Springs Family Care in Missouri affects 45,000 patients

Blue Springs Family Care in Missouri was hit by a ransomware attack that compromised the information of nearly 45,000 patients.

The hospital's computer vendor discovered the attack on May 12.

The hospital's computer vendor discovered the attack on May 12 and promptly notified the FBI and Blue Springs Police Department. It also hired a forensic IT company to help quarantine the affected systems and install software to monitor whether any unauthorized person was accessing the system, according to *KCUR 89.3*.

Fortunately, the medical center was able to avoid paying the ransom and regained access to its systems by using backups, and has essentially been able to rebuild its systems from scratch.

Officials said they have no evidence of patient information been used by unauthorized individuals, adding that the number of affected patients was so large because it included medical records going back 10 years -- a requirement in the medical practice.

# SEGURANÇA DA INFORMAÇÃO

# SEGURANÇA DA INFORMAÇÃO

# Você sabe o que é

# INFORMAÇÃO ?

# INFORMAÇÃO É UM ATIVO

Ativo é qualquer coisa que tenha valor para a organização.

# INFORMAÇÃO É UM ATIVO

## Ativo é qualquer coisa que tenha valor para a organização.

Exemplos de ativos:

- **Ativos de informação**: base de dados e arquivos, contratos e acordos, ...
- **Ativos de software**: aplicativos, sistemas, etc...
- **Ativos físicos**: equipamentos computacionais, de comunicação
- **Serviços**: Eletricidade, refrigeração, etc.
- **Pessoas e suas qualificações, habilidades e experiências.**
- **Intangíveis, tais como a reputação e a imagem da organização.**

**SEGURANÇA DA INFORMAÇÃO** é definida como a "Preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas."

(ABNT NBR ISO/IEC 27000:2014)

## Segurança em Redes

Implementação **dos controles de segurança** para garantir o nível de segurança adequado **para o ambiente de rede**

## Segurança da Informação

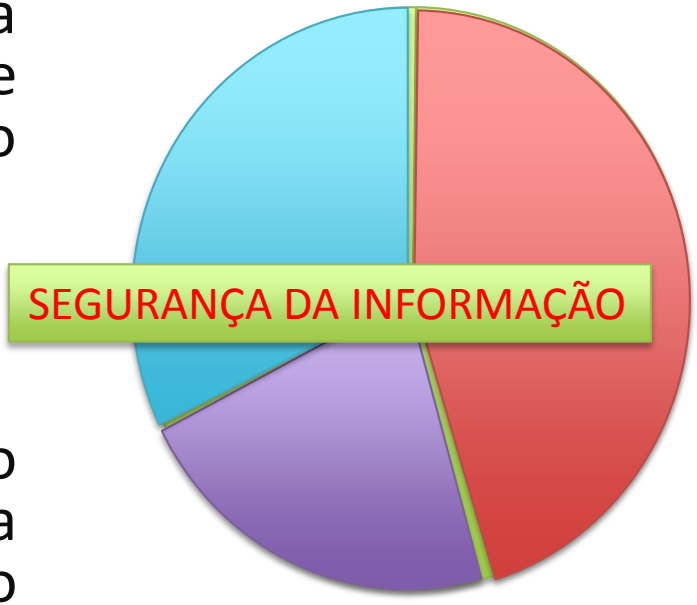
Visão mais ampla, como foco maior na garantia da segurança do negócio da empresa

## Segurança em Redes

Implementação dos controles de segurança para garantir o nível de segurança adequado para o ambiente de rede

## Segurança da Informação

Visão mais ampla, como foco maior na garantia da segurança do negócio da empresa



## Segurança em Redes

Implementação dos controles de segurança para garantir o nível de segurança adequado para o ambiente de rede

## Segurança da Informação

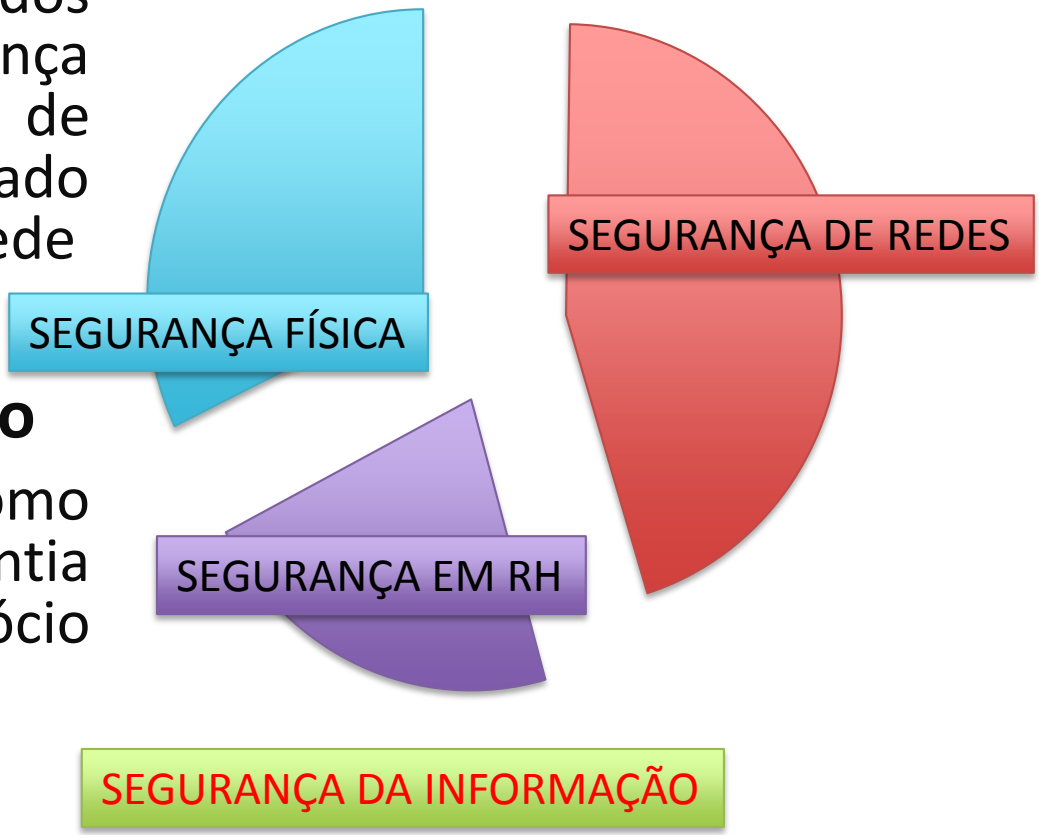
Visão mais ampla, como foco maior na garantia da segurança do negócio da empresa

## Segurança em Redes

Implementação dos controles de segurança para garantir o nível de segurança adequado para o ambiente de rede

## Segurança da Informação

Visão mais ampla, como foco maior na garantia da segurança do negócio da empresa



## Segurança em Redes

Implementação dos controles de segurança para garantir o nível de segurança adequado para o ambiente de rede

## Segurança da Informação

Visão mais ampla, como foco maior na garantia da segurança do negócio da empresa


SEGURANÇA DA INFORMAÇÃO

- Ciclo de vida da informação


**GARANTIR CID**

- **Criação e manipulação (ex. Alteração)**
  - Digitação de dados
  - Sites Web
  - Importação de outros sistemas
  - Importação de mídias

  - Classificação da informação
  - Credenciais de acesso futuro

- **Armazenamento**
  - Segurança de mídias removíveis
  - Impressões
  - Proteção contra furto e extravio
  - Cópias não autorizadas

- **Transporte**
  - Transmissão de dados
    - Segurança do canal
  - Transporte de mídia
    - Serviço de transporte/mensageiro
    - Lacres
    - Divisão de conteúdo

- **Descarte**
  - **É quando uma informação não se faz mais necessária e é excluída.**
    - **Critérios**
    - **Prazos**
  - **Há descarte de mídia?**
    - Mídias fixas e removíveis
    - Impressos

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# Fixação

- Há MUITAS motivações para a preocupação com segurança. Hoje, qualquer um de nós pode sofrer um ataque de _____RANSOMWARE_____ e ser compelido a pagar um resgate para voltar a ter acesso aos dados.
- O acrônimo para as principais propriedades da informação é _____CID_____. Aquele que busca garantir o acesso apenas de quem tem a NECESSIDADE de conhecer a informação é _____CONFIDENCIALIDADE_____

UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

# Fixação

- Segurança da informação é uma ciência ampla, que envolve as áreas de segurança de _____, que lida com o comportamento humano, a de _____, que lida com as ferramentas tecnológicas e a _____, que visa proteger os ativos.
- No ciclo de vida da informação, a etapa que deve ser tratada para evitar concentração de conhecimento estratégico com um único funcionário é _____.

RH
REDES
FÍSICA
ARMAZENAMENTO