

**UNI  
METRO  
CAMP**

**wyden**

Introdução à Segurança da Informação - ARA0064

Prof. José Luiz Alonso Silva, MsC

E-mail: [jose.lsilva@unimetrocamp.edu.br](mailto:jose.lsilva@unimetrocamp.edu.br)

## 1.1 Segurança da Informação

**UNI  
METRO  
CAMP**  
*wyden*

# Temas da Aula

- Segurança
- Informação e Dado
- Informação e o Negócio
- Aspectos Históricos
- Políticas e Segurança
- Pilares da Segurança
- Riscos
- Pontos de Atenção

# Lembre-se

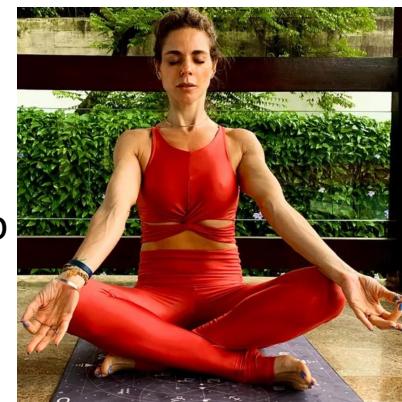
Participe da Aula

Quer parecer inteligente? **Nunca pergunte nada.**

**Leve sua dúvida para casa,** nunca faça perguntas

Aprender a expressar-se adequadamente exige prática

*Gyan Mudra*  
Mudra do conhecimento



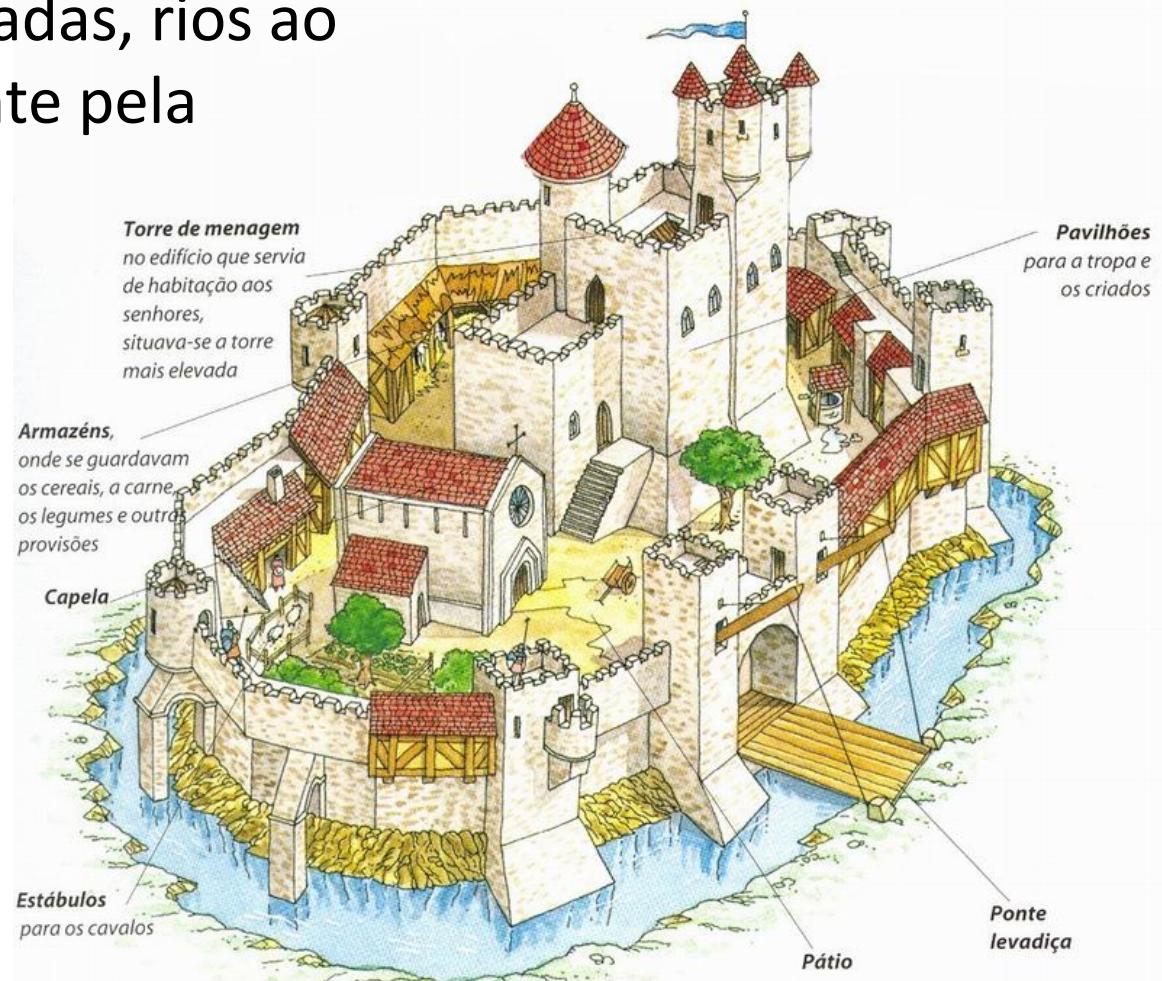
# Objetivo da Aula

- Empregar os conceitos básicos da área de segurança e informação, assim como seu valor, sua propriedade e seu ciclo de vida



# Segurança

Baseado no conceito de proteção por muralhas reforçadas, rios ao redor e principalmente pela localização



# Definição

- “A cibersegurança é um conjunto de ações e técnicas para proteger sistemas, programas, redes e equipamentos contra invasões.”

CYBERSECURITY &  
INFRASTRUCTURE  
SECURITY AGENCY

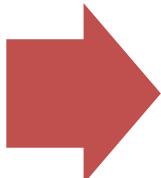


AMERICA'S CYBER DEFENSE AGENCY

# Segurança

- “A segurança da informação é um **conjunto de medidas** que se constituem basicamente de controles e política de segurança, tendo como **objetivo a proteção das informações** dos clientes e da empresa (ativos/bens), controlando o risco de revelação ou alteração por pessoas não autorizadas

Políticas,  
Práticas,  
Processos



Proteger  
informações

# Tipos de cibersegurança

## Segurança Operacional

A empresa protege seus dados definindo quem acessa e os níveis de acesso

## Segurança de Rede

Encarregada de proteger a rede contra acessos indevidos e ataques como DoS (*Denial of Service*)

## Segurança de Aplicativos

É a resposta contra as ameaças aos softwares instalados nos computadores e dispositivos móveis em geral, implementando protocolos de segurança durante seu desenvolvimento

## Recuperação de desastres

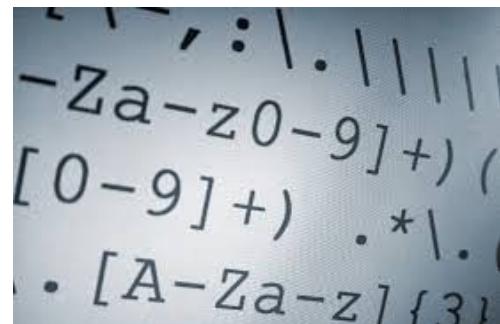
Define as práticas que uma organização utiliza em caso de desastres, para recuperar da forma mais rápida possível e com o menor dano possível

## Educação do Usuário Final

Encontrar e corrigir comportamentos de riscos dos usuários que podem expor dados sensíveis ou colocar uma organização em risco

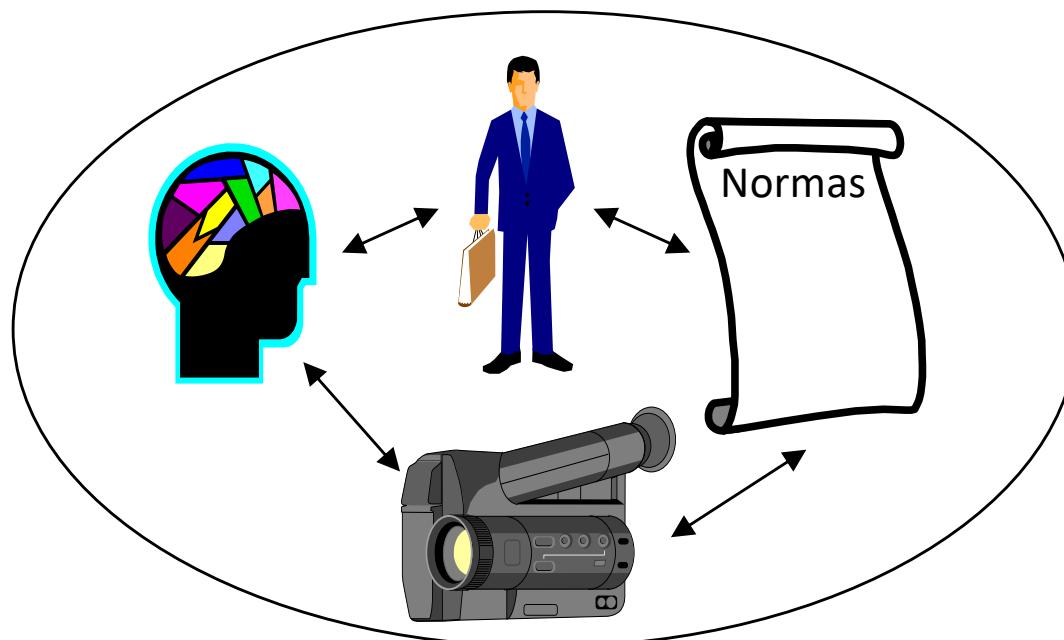
# Dado

- Conceito Tradicional de Dados:
  - Número e textos que estão baseados em registros, são “frios e pobres” no máximo com algum nível primário de correlação;
- Informação:
  - São os dados coletados, organizados, ordenados, aos quais são **atribuídos significados associados a um determinado contexto**, são “quentes e ricos”



# Informação

É produto de um longo processo de crescimento e aquisição de experiência



# Dado X Informação

- Para que os dados se tornem úteis como informação é necessário que **estejam disponíveis e sejam apresentados de tal forma que possa relacionar e atuar sobre eles**, com entendimento



# Informação e Negócios

- Hoje em dia a informação é o **bem mais valioso** de uma empresa/Cliente.



Será?

# Situação Problema

- O quanto estamos seguros hoje?

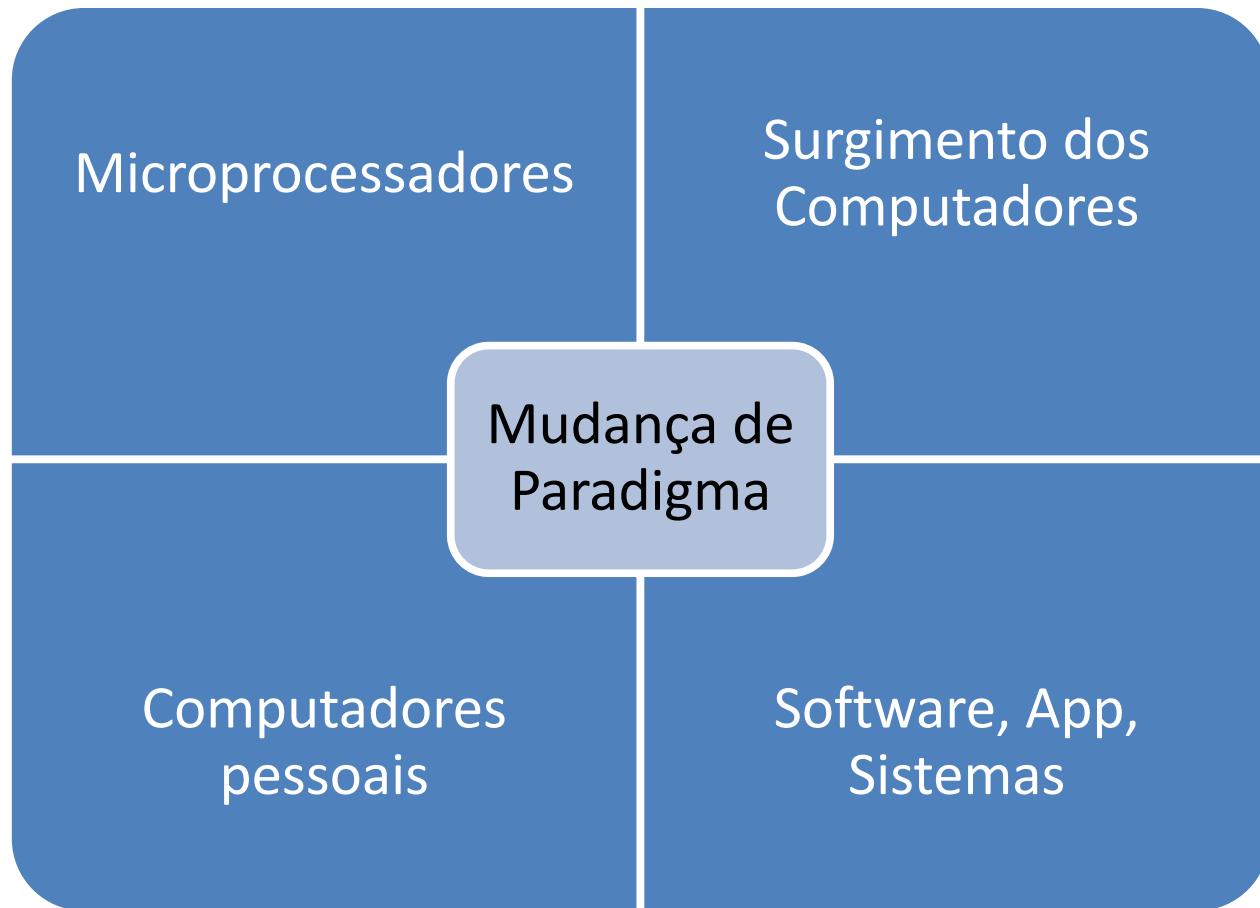


# Aspectos Históricos

- Era da informação
  - Década de 1970 fortalece-se o movimento onde o poder está nas mãos de quem detém a informação
  - Evolução para conhecimento



# Aspectos Históricos



# Visão contemporânea

## Importante

Cópia de  
segurança (*backup*)

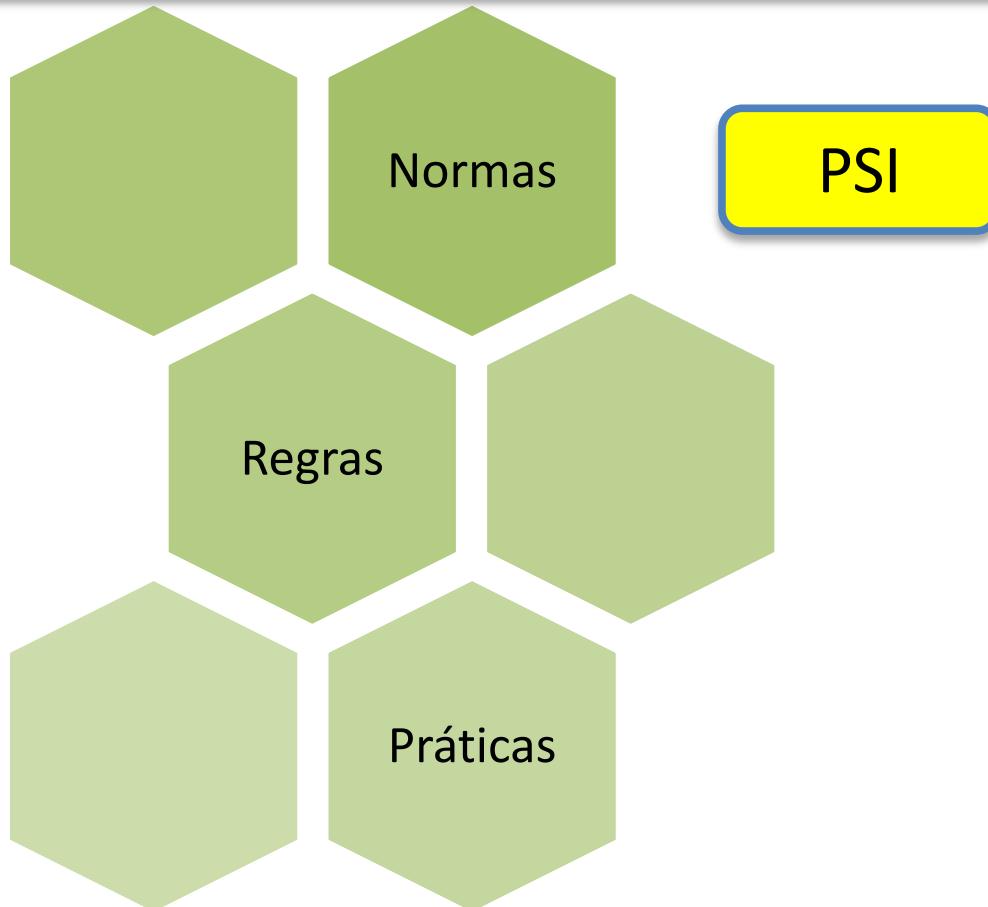
Governança de  
Dados

LGPD (Lei Geral de  
Proteção de Dados  
Pessoais)

Proteção dos dados  
(ativos da  
organização)

# Políticas de Segurança Informação

Conjunto de normas e diretrizes destinadas a os colaboradores que façam uso dessa infraestrutura



Proteção das informações

Proteção das informações

# Pilares da Segurança



Identificar



Proteger



Detectar



Responder



Recuperar



1 Identify

Understand your assets and the risks associated with them.



2 Protect

Establish safeguards to protect against cybersecurity events.



3 Detect

Identify and continuously monitor cybersecurity events.



4 Respond

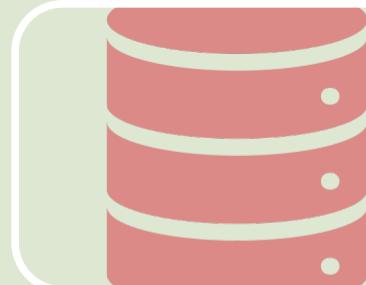
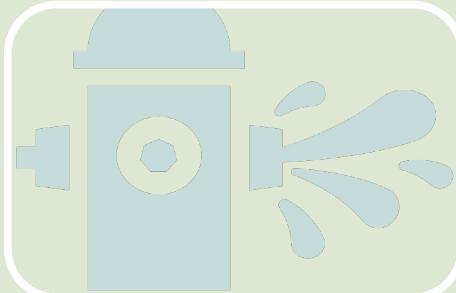
Respond quickly and appropriately to contain the impact of events.



5 Recover

Restore capabilities and services after a cybersecurity attack.

# Segurança Informação – “Garantir”



**Confidencialidade**

- Garantia de que uma informação só poderá ser conhecida por aqueles que tiverem tal direito

**Integridade**

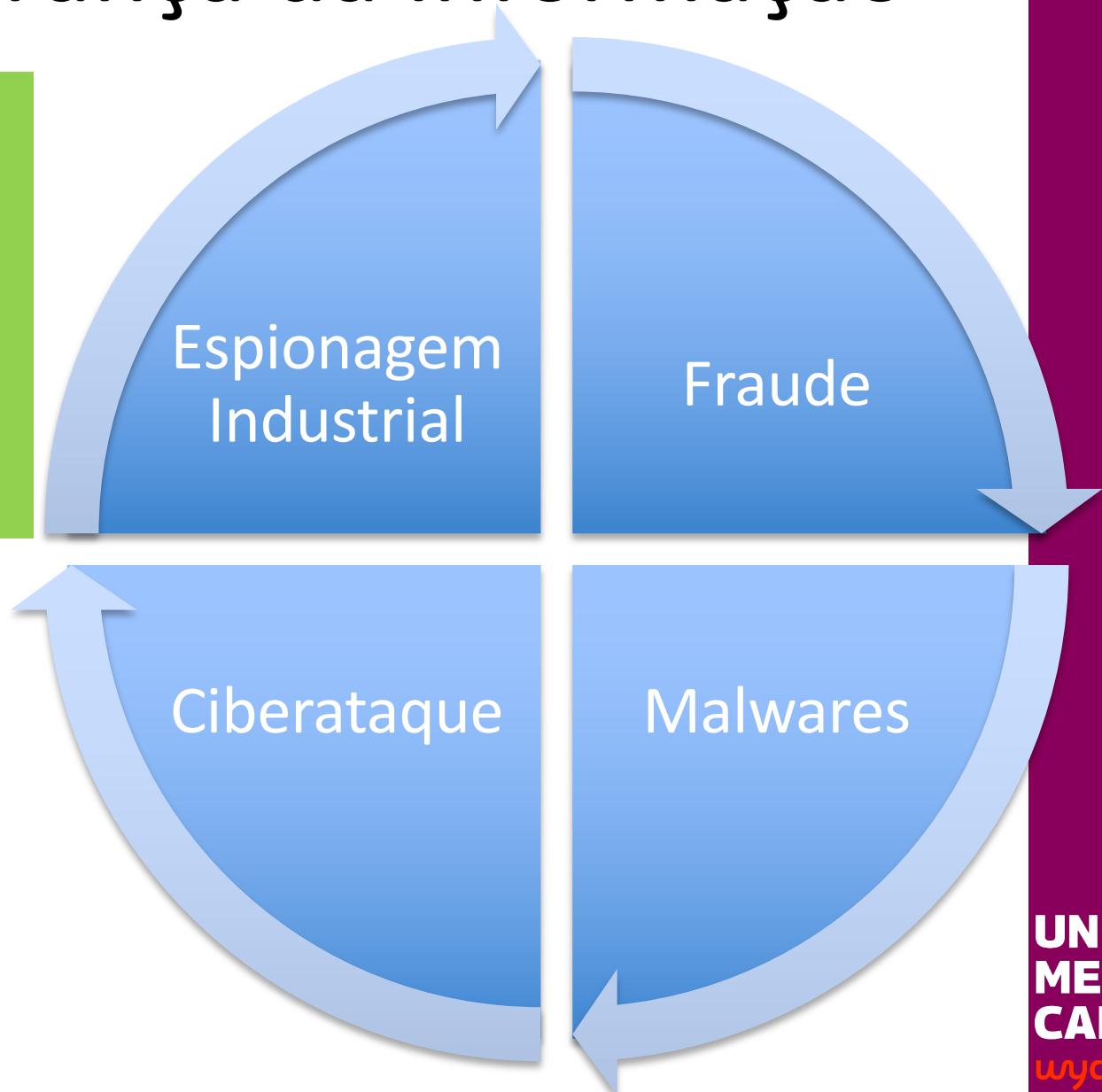
- Proteger a informação, processo ou sistema de alterações não autorizadas

**Disponibilidade**

- Informação, processos ou sistemas acessíveis quando solicitados

# Riscos Segurança da Informação

Probabilidade de uma ameaça explorar a vulnerabilidade de um bem de informação e, assim, prejudicar uma organização



# Exemplos Riscos Segurança da Informação

---

Exemplos

**Roubo de dados**

---

**Espionagem industrial**

---

**Hackers de senhas**

---

**Funcionários não especializados / erros humanos**

---

**Softwares vulneráveis**

---

**Ataques de ransomware**

---

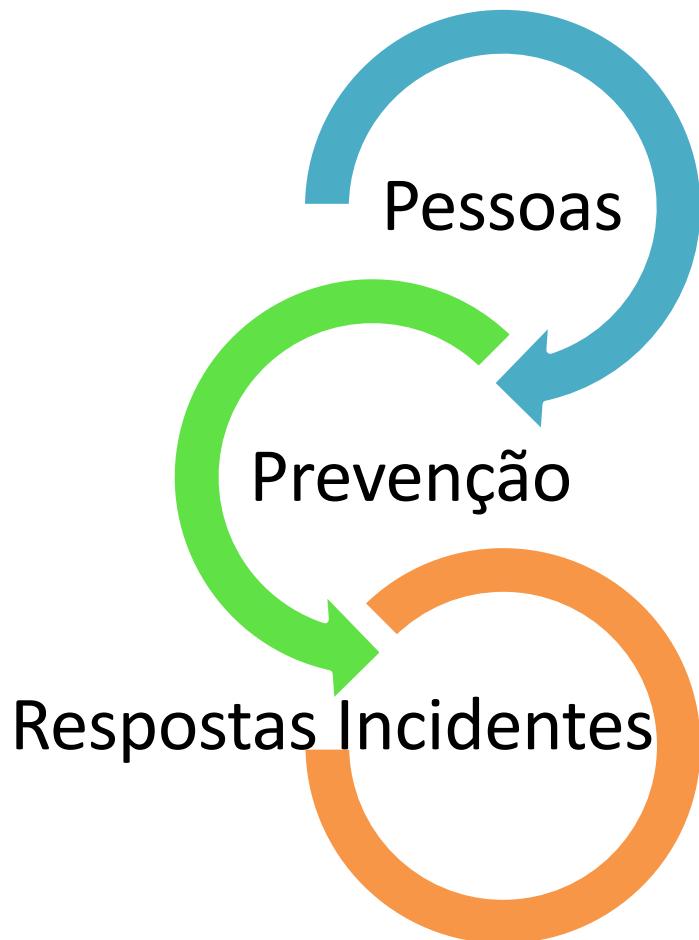
**Phishing**

---

**Adware**

---

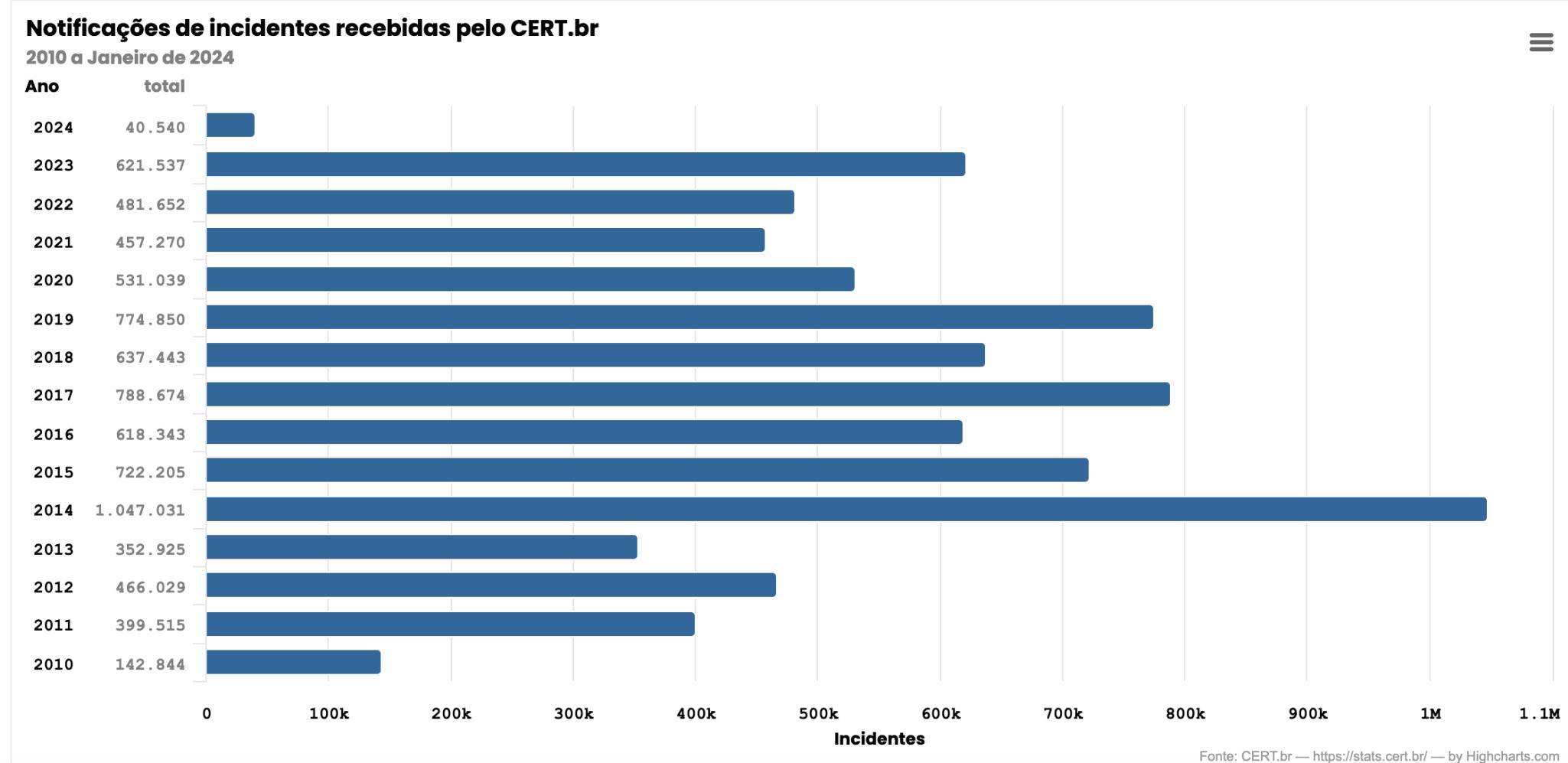
# Pontos de Atenção



# Situação Cibersegurança Brasil

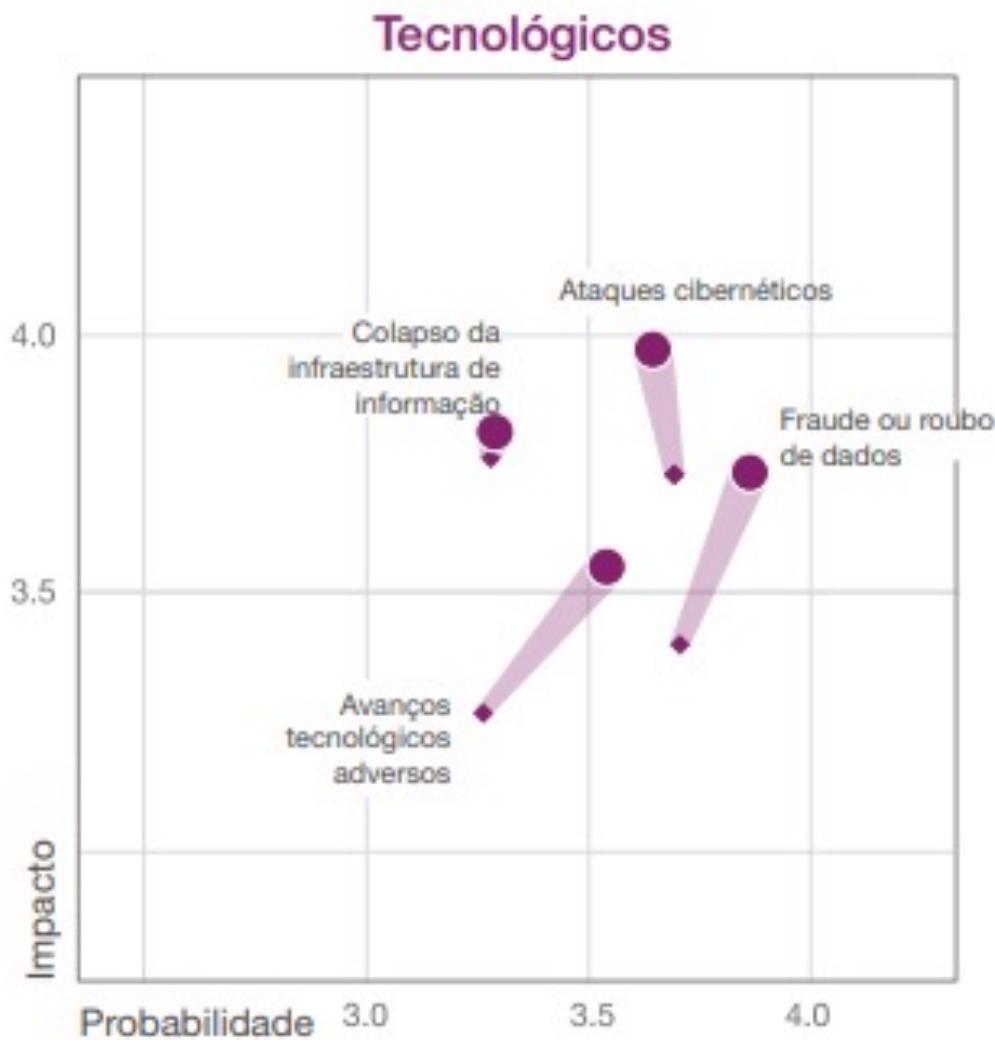
- De acordo com uma pesquisa da Netscout
  - O Brasil é o **2º país do mundo** em que mais ocorrem ciberataques
  - Mais de **439 mil** tentativas de invasões e de ataques de negação de serviço distribuído (**DDoS**) registrados, atrás apenas dos EUA

# Informações sobre Incidentes



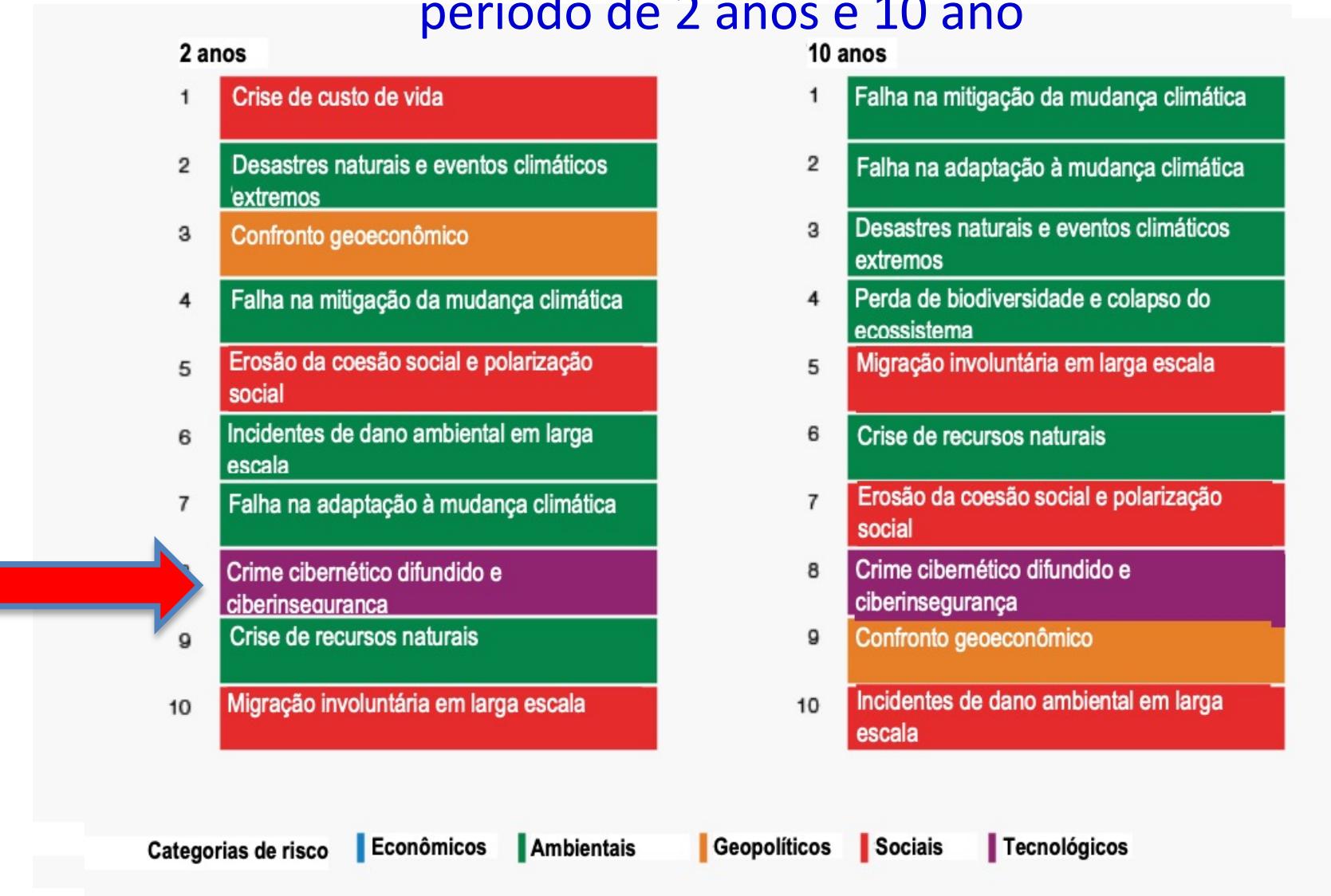
# Riscos Fórum Mundial Economia

## Relatório de 2020



# Riscos Fórum Mundial Economia

período de 2 anos e 10 ano

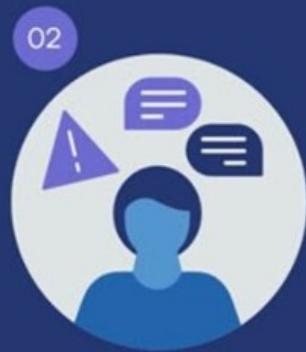


# Expectativas Riscos

Expectativas para 2024. Riscos manifestados atualmente por impacto



Clima extremo



Informações incorretas e desinformação



Polarização social e política



Crise do custo de vida



Ataques cibernéticos

Econômico

Ambiental

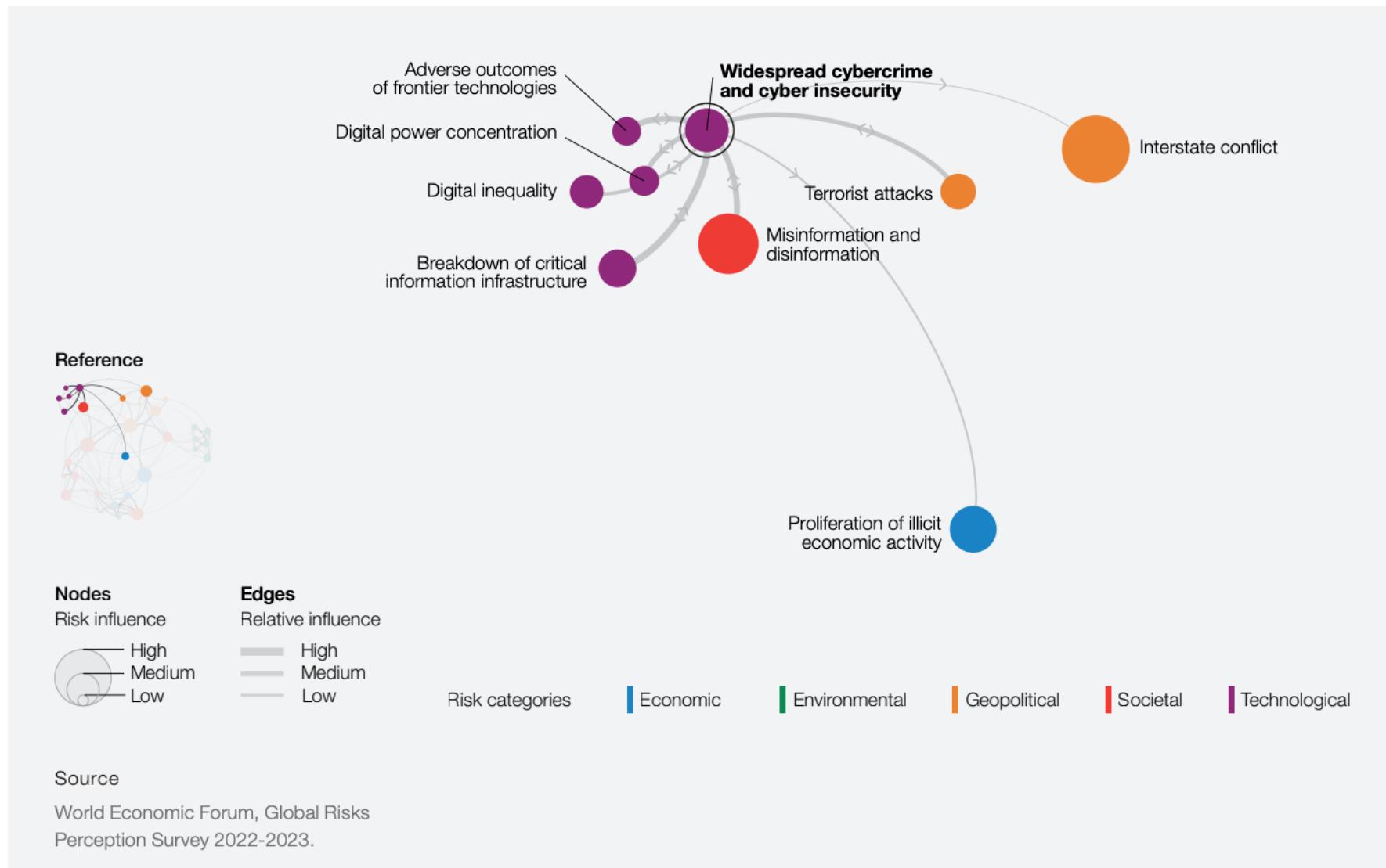
Geopolítico

Social

Tecnológico

Fonte: Relatórios de Riscos Globais 2024, Fórum Econômico Mundial

# Interconexão Riscos



# Alguns Situações

**Sony** (40 Gigabytes) informações extremamente sigilosas, como conteúdo de e-mails, filmes, projetos engavetados, roteiros e entre outros

**Ashley Madison** (40 milhões de clientes e o arquivo liberado tem cerca de 8,6GB)  
“Rede Social”

**Target** (70 milhões de registros com informações bancárias, números de telefone, e-mails e outros dados foram roubados)  
“Loja de vejo”

**Sally Beauty** (25.000 registros foram roubados)  
“Produtos de Beleza”

Violação de dados no **Uber** expõe documentos de quase mil motoristas dos EUA

**Coreia do Sul** acusa norte-coreanos por ciberataques contra usinas nucleares  
(2015 - [exame.com/tecnologia/](http://exame.com/tecnologia/))

# Desafios

## Segurança

- Deve ser tratada como questão de risco aos negócios e não somente como problema da área de TI

## Impunidade

- Os cyber criminosos acostumaram-se a agir com certo grau de impunidade

## Informação

- Empresas preferem simplesmente reconhecer os danos decorrentes de ataques cibernéticos como perda, a fim de proteger a confiança em seus sistemas e em suas marcas

## Conscientização

- Resolução das ameaças cibernéticas não cabe somente ao CIO. Esse é um problema que deve ser atacado de forma sistêmica, sob a liderança de CEO's



# E a carreira?



- **Blue Team**

- Manter e melhorar a postura de segurança de informação, ao identificar falhas de segurança e corrigindo as possíveis brechas. *Confira na lista abaixo algumas atribuições dessa equipe de hackers.*

- Monitoramento nos sistemas de segurança
    - Detecção de possíveis sistemas corrompidos
    - Ações de resposta e neutralização de ataques cibernéticos

# E a carreira?

- Forense
  - Evidências e provas de crimes cibernéticos
  - No campo da investigação criminal, um analista forense é um profissional responsável por aplicar metodologias para encontrar pistas deixadas na cena de um crime
  - Analise "digitais" e "pegadas" deixadas por criminosos que invadiram um sistema de segurança ou base de dados
  - Aplica métodos específicos para identificar fraudes, invasões, sabotagens, entre outros crimes digitais

# E a carreira?

- **GRG - governança, Risco e Conformidade**
  - normas que servem como requisitos regulatórios
  - Riscos e conformidade
  - Métodos estruturados para alinhar TI e Segurança da Informação

# E a carreira?

- **DevSecOps**
  - DEvSecOps é a abreviação do termo em inglês "***Development, Security e Operations***", que significa "Desenvolvimento, Segurança e Operações"
  - Esta área desenvolve softwares com segurança
  - Padrões
- Garantir a operação do software
  - Ambiente de produção sempre disponível e confiável

# Certificações

Certified Secure Computer User | CSCU

Certified SOC Analyst (CSA)

Certified Threat Intelligence Analyst (CTIA)

Certified Network Defender (CND)

Certified Incident Handler (ECIH)

Certified Penetration Tester (CPENT)

Certified Ethical Hacker (CEH)

Network Security Fundamentals (NSF)

Computer Hacking Forensic Investigator (CHFI)

Certified Application Security Engineer (CASE JAVA)

## Certifications

### ETHICAL HACKING

- > Certified Ethical Hacker (C|EH)
- > C|EH (MASTER)

### EXECUTIVE MANAGEMENT

- > Certified Chief Information Security Officer (C|CISO)
- > Associate C|CISO

### COMPUTER FORENSICS

- > Computer Hacking Forensic Investigator (C|HFI)

### NETWORK SECURITY

- > Certified Network Defender (C|ND)
- > ICS/SCADA Cybersecurity

### ENCRYPTION

- > Certified Encryption Specialist (E|CES)

### PEN TESTING

- > Certified Penetration Testing Professional (C|PENT)

### INCIDENT HANDLING

- > Certified Incident Handler (E|CIH)
- > Certified Threat Intelligence Analyst (C|TIA)

### CLOUD SECURITY

- > Certified Cloud Security Engineer (C|CSE)

### DEVSECOPS

- > Certified DevSecOps Engineer (E|CDE)

### CYBER TECHNICIAN

- > Certified Cybersecurity Technician (C|CT)

### BLOCKCHAIN

- > Blockchain Developer Certification (B|DC)
- > Blockchain Fintech Certification (B|FC)
- > Blockchain Business Leader Certification (B|BLC)

### BUSINESS CONTINUITY AND DISASTER RECOVERY

- > Disaster Recovery Professional (E|DRP)

### FUNDAMENTALS

- > Certified Secure Computer User (C|SCU)
- > EC-Council Certified Security Specialist (E|CSS)

### ESSENTIALS SERIES

- > Network Defense Essentials (N|DE)
  - > Ethical Hacking Essentials (E|HE)
  - > Digital Forensics Essentials (D|FE)
- ### APPLICATION SECURITY
- > Certified Application Security Engineer (C|ASE .NET)
  - > Certified Application Security Engineer (C|ASE Java)
  - > Web Application Hacking and Security (W|AHS)

# Duvidas, considerações ...



Imagen ícones MS-Power Point

# Referência Bibliográfica

- BAARS, Hans. **Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002?** Rio de Janeiro ? RJ ? Editora Brasport, 2018. Capítulo3. Disponível em:  
<https://plataforma.bvirtual.com.br/Acervo/Publicacao/160044>
- GALVÃO, Michele da Costa, Agnaldo Aragon. **Fundamentos em Segurança da Informação?** Rio de Janeiro ? RJ: Editora Pearson, 2015. Capítulo 1. Disponível em:  
<https://plataforma.bvirtual.com.br/Acervo/Publicacao/26525>

# Referências

- PWC. ***Global Digital Trust Insights Survey 2021.*** Disponível em: <<https://www.pwc.com.br/pt/estudos/servicos/consultoria-negocios/2020/global-digital-trust-insights.html#modules>>. Acesso em 26/02/2024
- PWC. **Prepare sua equipe de segurança para o futuro.** Disponível em: <<https://www.pwc.com.br/pt/estudos/servicos/consultoria-negocios/2020/global-digital-trust-insights/equipe-de-seguranca-para-o-futuro.html>>. Acesso em 26/02/2024

# Referências

- *World Economic Forum. Relatório Global de Riscos 2020.* Disponível em: <<https://www.zurich.com.br/-/media/project/zwp/brazil/docs/grr/relatorio-global-de-riscos-2020--sumario-executivo.pdf>>. Acesso em 26/02/2024
- Biblioteca de Segurança. **Análise do Relatório do Fórum Econômico Mundial.** Disponível em: <<https://www.bibliotecadeseguranca.com.br/videos/analise-do-relatorio-do-forum-economico-mundial/>>. Acesso em 26/02/2024 (Vídeo)

# Referências

- Gabriel Osório de Barros. **A Economia da Cibersegurança.** Disponível em: <<https://www.gee.gov.pt/pt/documentos/estudos-e-seminarios/temas-economicos/7237-te54-a-economia-da-ciberseguranca/file>>. Acesso em 26/02/2024
- Andre Gargaro. **Cyber Survey - Tendências em gestão de riscos cibernéticos e segurança da informação na América Latina e Caribe.** Disponível em: <<https://www2.deloitte.com/br/pt/pages/risk/articles/cyber-survey-2019.html>>. Acesso em 26/02/2024

# Referências

- Gov. UK Department for Digital, Culture, Media and Sport. **Cyber Security Breaches Survey 2021: Statistical Release.** Disponível em: <<https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021>>. Acesso em 02/03/2023
- Presidência da República. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em 26/02/2024

# Referências

- Gov. UK Department for Digital, Culture, Media and Sport. **Cyber Security Breaches Survey 2021: Statistical Release.** Disponível em: <<https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021>>. Acesso em 26/02/2024
- Presidência da República. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/l13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm)>. Acesso em 26/02/2024

# Referências

- *World Economic Forum. Cybersecurity Learning Hub.* Disponível em: <<https://www.weforum.org/projects/cybersecurity-learning-hub>>. Acesso em 26/02/2024
- Deloitte. *Cyber Survey.* Disponível em: <<https://www2.deloitte.com/br/pt/pages/risk/articles/cyber-survey-2019.html>>. Acesso em 26/02/2024

# Referências

- ***Forum Economic Global Risks - 2023.***  
Disponível em:  
[<https://www3.weforum.org/docs/WEF\\_Global\\_Risks\\_Report\\_2023.pdf>](https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf). Pag. 43  
Acesso em 26/02/2024
- DoS vs. DDoS Disponível em:  
[<https://www.fortinet.com/br/resources/cyberglossary/dos-vs-ddos>](https://www.fortinet.com/br/resources/cyberglossary/dos-vs-ddos). Acesso em 26/02/2024

# Referências

- Cert. **Cartilha de Segurança para Internet.** Disponível em:  
[<https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>](https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf). Acesso em 26/02/2024
- Governo Federal, GSI. **Livro Verde Segurança da Cibernética no Brasil.** Disponível em: [<https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2015/10/Livro\\_Verde\\_SEG\\_CIBER.pdf>](https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2015/10/Livro_Verde_SEG_CIBER.pdf). Acesso em 26/02/2024

# Referências

- FGV. **Política de Segurança da Informação.** Disponível em <[https://tic.fgv.br/sites/tic.fgv.br/files/arquivos/politica\\_de\\_seguranca\\_da\\_informacao.pdf](https://tic.fgv.br/sites/tic.fgv.br/files/arquivos/politica_de_seguranca_da_informacao.pdf)>. Acesso em 26/02/2024
- B<sup>3</sup> Brasil Bolsa Balcão. **Política de Segurança da Informação.** Disponível em <[https://s3.amazonaws.com/mz-filemanager/5fd7b7d8-54a1-472d-8426-eb896ad8a3c4/0b5bc320-709e-4f36-9526-f82630f66649\\_PoliticaSegurancalInformacao.pdf](https://s3.amazonaws.com/mz-filemanager/5fd7b7d8-54a1-472d-8426-eb896ad8a3c4/0b5bc320-709e-4f36-9526-f82630f66649_PoliticaSegurancalInformacao.pdf)> Acesso em 26/02/2024

**UNI  
METRO  
CAMP**  
*wyden*

# Atividade

- Acessar o [cert.br/](https://cert.br/)
  1. O que é o cert.br?
  2. Quais tipos de informações ele oferece?
  3. O que o time aprendeu?

Equipe até 5 pessoas 1 responde

Respostas no Forms

<https://forms.office.com/r/3g5AVEgH1g>



# Para Próxima Aula

## Assista aos vídeos

- Segurança da Informação: Controles Físicos e Lógicos:  
[https://www.youtube.com/watch?v= MAIYDTfcU](https://www.youtube.com/watch?v=MAIYDTfcU) – 8 minutos
- Explicando segurança física e logica, JOGANDO:  
<https://www.youtube.com/watch?v=d3GUEhI2F8E> – 13 minutos