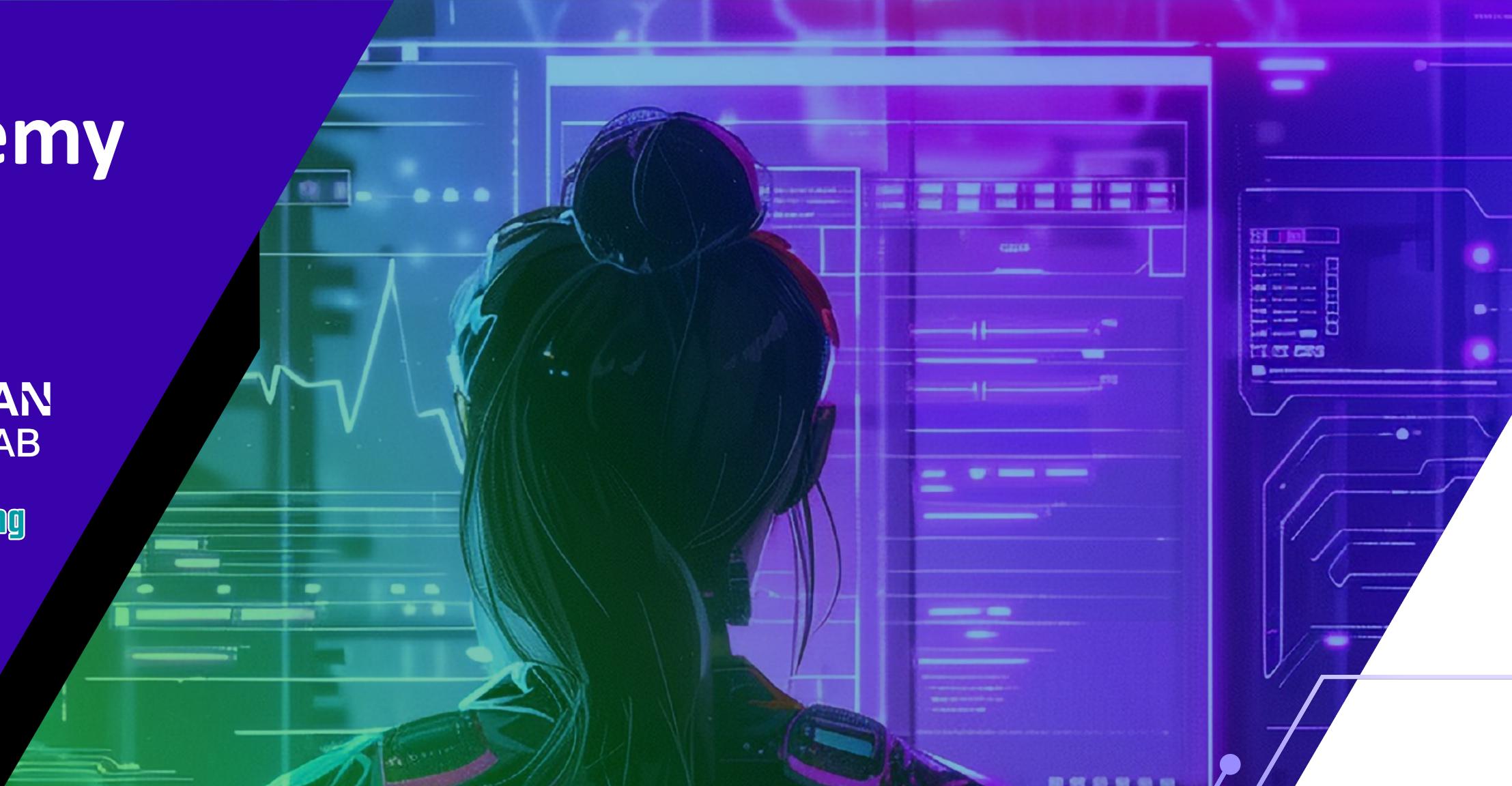


# Cyber Academy

FEBRABAN  
/CYBER LAB



Laboratório de Segurança Cibernética - 02/07/2025

# Os Pilares 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. Introdução
3. Pilares da Segurança da Informação
4. Pessoas, Processos e Tecnologias
5. Terminologia
6. Gestão de Riscos

# Objetivo

FEBRABAN  
/ CYBER LAB



# Objetivo

Entender os pilares fundamentais da Segurança da Informação, os seus conceitos principais e terminologias.

# Introdução

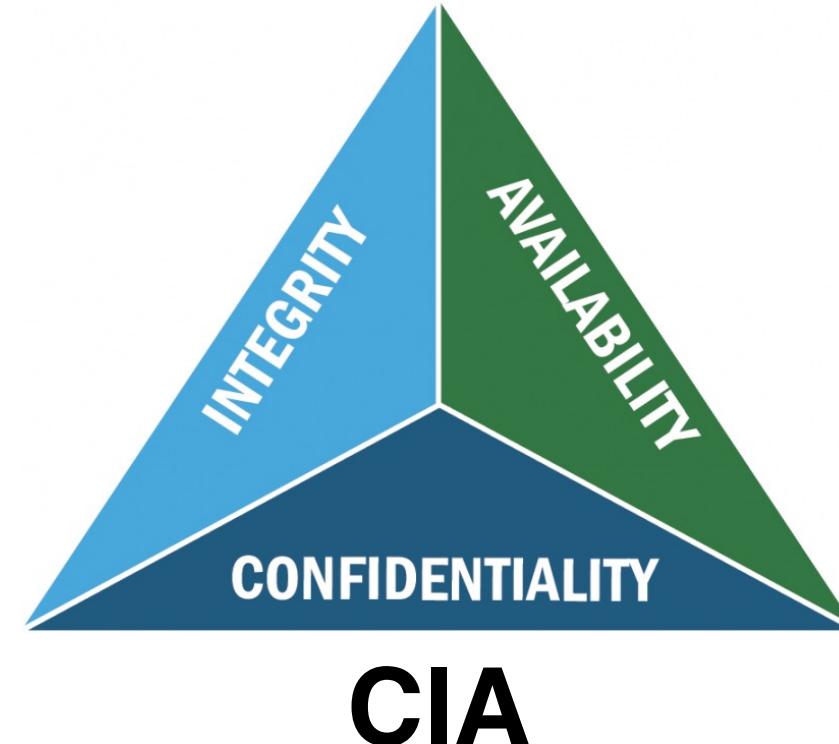
FEBRABAN  
/ CYBER LAB



- No módulo anterior, falamos sobre a **importância da Segurança da Informação (SI)** para as pessoas, empresas e para a sociedade.
- Verificamos que num mundo altamente conectado, existem ameaças que podem **causar sérios danos** às pessoas e aos negócios.
- É preciso fortalecer “cada elo” dessa corrente para termos **pessoas e sistemas mais protegidos e resilientes**.



- A Segurança da Informação é fundamentada em 3 (três) importantes pilares:
  - ✓ **Confidencialidade (Confidentiality)**
  - ✓ **Integridade (Integrity)**
  - ✓ **Disponibilidade (Availability)**



# Pilares da Segurança da Informação



# Pilares da 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

# Pilares da 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 page with a header containing the gov.br logo and links to the Presidency of the Republic, Government Organs, Access to Information, and Legislation. Below the header, there is a breadcrumb navigation: Home > Security of Information and Cybernetics > Glossary of Security Information. The main title is "Glossário de Segurança da Informação". At the bottom, there is a note indicating the document was published on November 26, 2021, at 14:21 and last updated on February 28, 2025, at 08:46.

# Pilares da Segurança da Informação

FEBRABAN  
/ CYBER LAB



# 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 ou disponível 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.



# Pilares da Segurança da Informação

- Utilizando a analogia de acesso ao cofre:
  - ✓ **Confidencialidade:** só você tem a chave do cofre.
  - ✓ **Integridade:** o conteúdo do cofre está intacto.
  - ✓ **Disponibilidade:** você consegue abrir o cofre sempre que precisa.



- Deve-se buscar proteger a informação em seus 3 (três) estados básicos, ou seja, em diferentes momentos do seu ciclo de vida:
  - ✓ **Em trânsito (trafegando)**
  - ✓ **Em uso (sendo processada)**
  - ✓ **Em repouso (armazenada)**



# Informação em Trânsito (trafegada)

- Dados que estão sendo transmitidos entre dois pontos, ou seja, pela rede.
- Quando você envia um e-mail, os dados trafegam da sua máquina até o servidor de e-mail e depois até o destinatário.
- Ao acessar um site com HTTPS, os dados do formulário que você preenche (como usuário e senha) estão em trânsito até o servidor.
- **Proteção típica:** Criptografia de comunicação, utilizando os protocolos de rede TLS/SSL (*Transport Layer Security/Secure Sockets Layer*), entre outros.



## Informação em Uso (processada)

- Dados que estão sendo ativamente processados por um sistema, por exemplo, na memória RAM ou CPU (Unidade Central de Processamento) de um computador.
- Quando você digita sua senha para se autenticar (fazer login) em um sistema, ela é processada para verificar se está correta.
- Ao abrir um arquivo no Word, ele é carregado na memória e manipulado pelo software.
- **Proteção típica:** Controle de acesso à memória, execução segura, DLP (*Data Loss Prevention*).



# Informação em Repouso (armazenada)

- Dados guardados em algum meio físico ou digital, como os discos rígidos dos computadores (HD, SSD, outros).
- Um arquivo salvo no seu computador (como um PDF ou planilha).
- Um banco de dados com informações de clientes armazenados em um servidor.
- **Proteção típica:** Criptografia em disco ou em banco de dados, controle de acesso físico e lógico.



# Cubo da Segurança de McCumber

Em 1991, John McCumber, especialista e pesquisador em Segurança da Informação, da Universidade de Washington, criou um modelo chamado de **Cubo de McCumber**.



# Cubo da Segurança de McCumber

## Propriedades da Segurança da Informação

Confidencialidade  
Integridade  
Disponibilidade



# Cubo da Segurança de McCumber

## Propriedades da Segurança da Informação

Confidencialidade  
Integridade  
Disponibilidade



# Pessoas, Processos e Tecnologias

FEBRABAN  
/CYBER LAB



# Segurança da Informação



A Segurança da Informação é como proteger uma casa. Você precisa de **pessoas** conscientes (quem moram na casa), **processos** bem definidos (rotinas seguras) e **tecnologia** adequada (fechaduras, alarmes).



- Mesmo com sistemas modernos, quem usa os equipamentos ainda são pessoas.
- Se um indivíduo cai em um golpe, compartilha senha ou deixa o computador desbloqueado, **toda a segurança pode ir por água abaixo**.
- Clicar em um e-mail falso com vírus.
- Usar uma senha fraca como 123456.
- Treinar, **conscientizar** e envolver as pessoas é essencial. **A segurança começa no comportamento**.



# Tecnologias – As ferramentas de proteção

- São os **sistemas e equipamentos usados para proteger os dados**. É como a fechadura da porta ou o alarme da casa.
- Antivírus, *firewalls*, autenticação em dois fatores.
- *Backup* automático dos arquivos.
- **A tecnologia ajuda, mas não resolve sozinha**. Ela precisa ser bem configurada, atualizada e usada corretamente.



# Processos – As regras do jogo

- São as **rotinas e políticas** que dizem como devemos agir para manter tudo seguro. **Não adianta cada um fazer do seu jeito.**
- Regras para definir e utilizar senhas fortes.
- Política que exige que computadores sejam bloqueados ao se afastar da mesa.
- **Processos claros** ajudam as pessoas a agir corretamente e evitam erros ou esquecimentos.



# Políticas e Normas

NORMA  
BRASILEIRA

ABNT NBR  
ISO/IEC  
27001

Terceira edição  
23.11.2022

Versão corrigida  
31.03.2023

---

Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos

*Information security, cybersecurity and privacy protection — Information security management systems — Requirements*

O sistema de gestão da segurança da informação preserva a **confidencialidade, integridade e disponibilidade** da informação pela aplicação de um processo de **gestão de riscos**, e fornece confiança para as partes interessadas de que os riscos são adequadamente gerenciados.

# Políticas e Normas

NORMA  
BRASILEIRA

ABNT NBR  
ISO/IEC  
27002

Terceira edição  
05.10.2022

---

Segurança da informação, segurança cibernética  
e proteção à privacidade — Controles de segurança  
da informação

*Information security, cybersecurity and privacy protection — Information  
security controls*



*Organizações de todos os tipos e tamanhos (incluindo setor público e privado, comercial e sem fins lucrativos) criam, coletam, tratam, armazenam, transmitem e descartam informações de diversas formas, incluindo eletrônica, física e verbal (por exemplo, conversas e apresentações).*

# Políticas e Normas

NORMA  
BRASILEIRA

ABNT NBR  
ISO/IEC  
27002

Terceira edição  
05.10.2022

---

Segurança da informação, segurança cibernética  
e proteção à privacidade — Controles de segurança  
da informação

Information security, cybersecurity and privacy protection — Information  
security controls



A segurança da informação é alcançada por meio da implementação de um conjunto adequado de controles, incluindo políticas, regras, processos, procedimentos, estruturas organizacionais e funções de software e hardware.

# Terminologia

FEBRABAN  
/ CYBER LAB



## Terminologia

SEGURANÇA DA INFORMAÇÃO

VS

SEGURANÇA CIBERNÉTICA

[☰](#)  WIKIPEDIA  
The Free Encyclopedia

Search Wikipedia  Search

Do

## *Cybernetics: Or Control and Communication in the Animal and the Machine*

4 languages ▾

**Contents** hide

(Top)

Reception

Table of contents

Supplementary chapters in the second edition

Synopsis

Introduction

Newtonian and Bergsonian Time

Groups and Statistical Mechanics

Time Series, Information, and Communication

Feedback and Oscillation

Article Talk

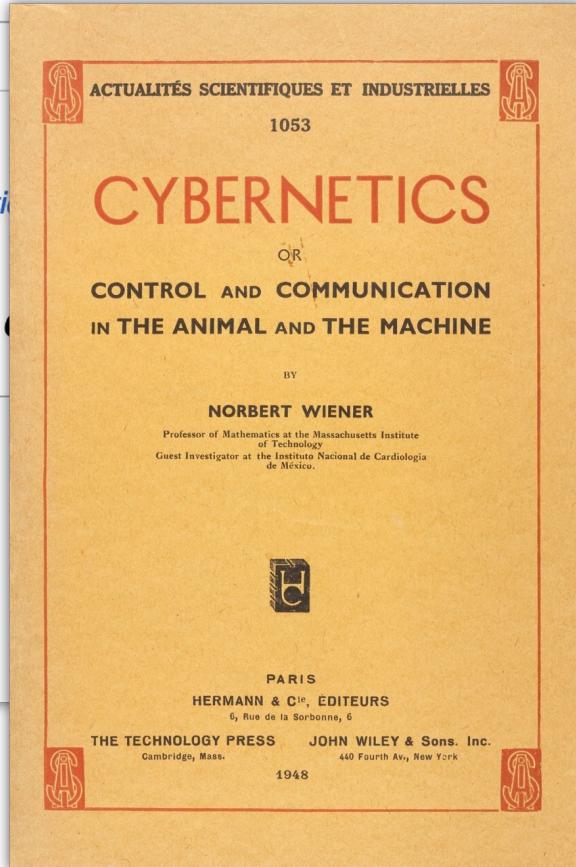
From Wikipedia, the free encyclopedia

"Cybernetics (book)" redirects here. For other topics, see [Cybernetics \(disambiguation\)](#)

**Cybernetics: Or Control and Communication in the Animal and the Machine**

is a book written by [Norbert Wiener](#) and published in 1948.<sup>[1]</sup> It is the first public usage of the term "cybernetics" to refer to self-regulating mechanisms. The book laid the theoretical foundation for [servomechanisms](#) (whether electrical, mechanical or hydraulic), automatic [navigation](#), [analog computing](#), [artificial intelligence](#), [neuroscience](#), and reliable [communications](#).

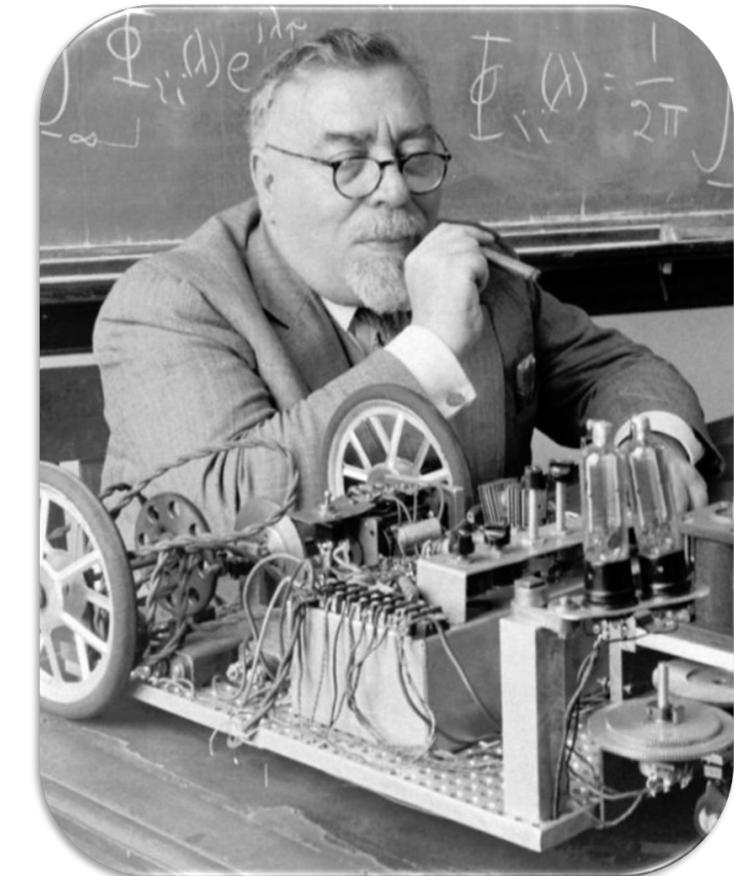
A second edition with minor changes and two additional chapters was published in 1961.



[https://en.wikipedia.org/wiki/Cybernetics:\\_Or\\_Control\\_and\\_Communication\\_in\\_the\\_Animal\\_and\\_the\\_Machine](https://en.wikipedia.org/wiki/Cybernetics:_Or_Control_and_Communication_in_the_Animal_and_the_Machine)

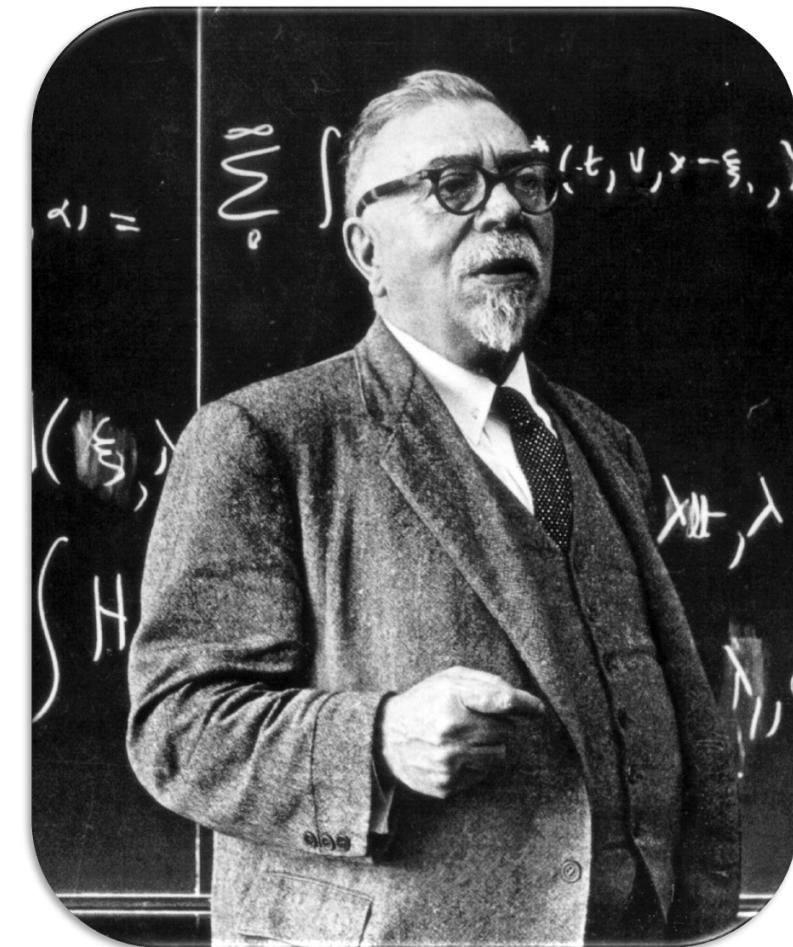
# Cibernética

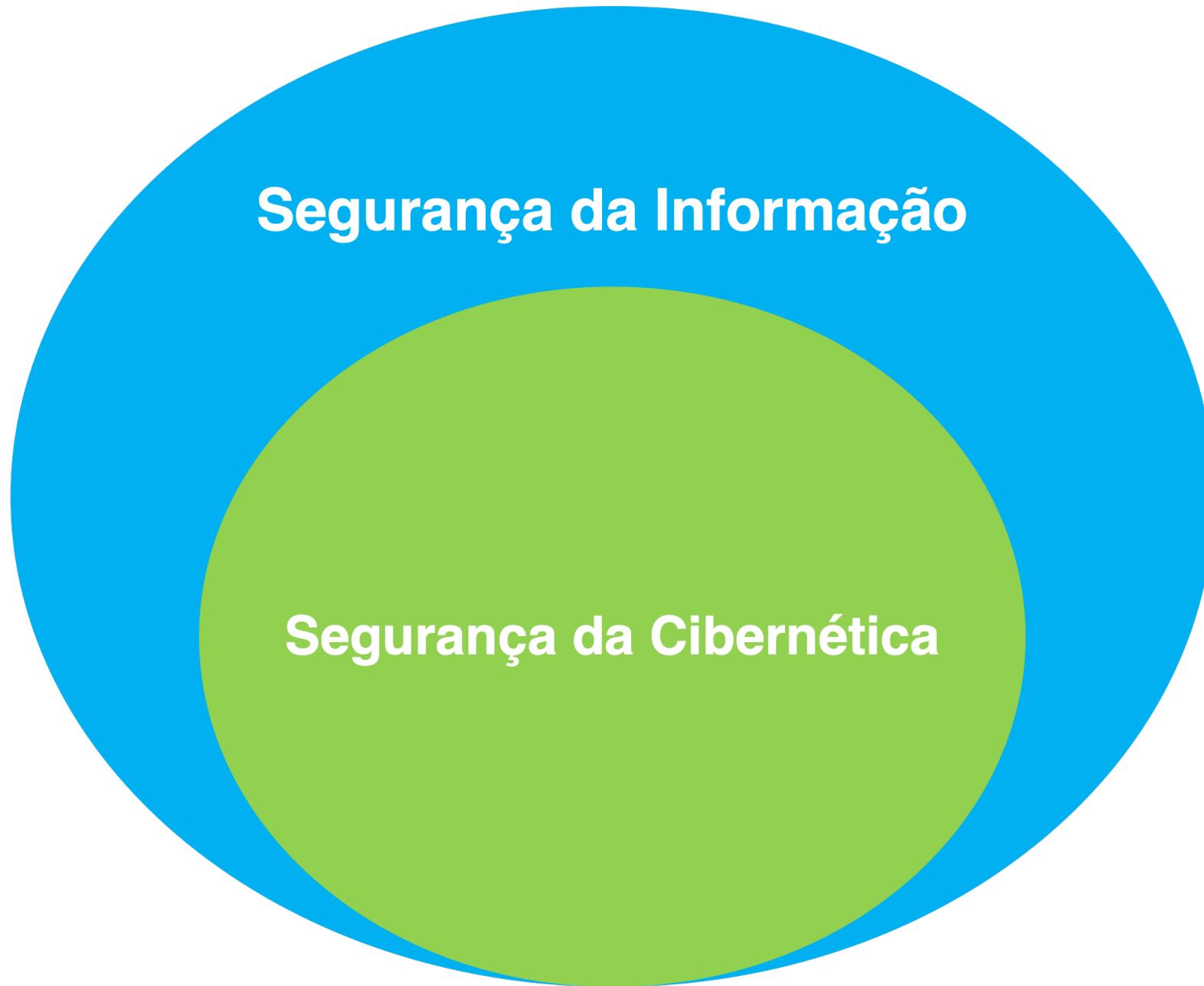
- O termo cibernética tem sua origem na palavra grega "kybernetes" (κυβερνήτης), que significa "timoneiro" ou "governador". Ele foi adaptado para designar o **estudo do controle e da comunicação nos sistemas biológicos e mecânicos**.
- O termo foi popularizado pelo matemático e filósofo **Norbert Wiener** em seu livro **"Cybernetics: Or Control and Communication in the Animal and the Machine"**, publicado em 1948. Ele usou o termo para descrever o campo interdisciplinar que estuda como sistemas – sejam vivos ou artificiais – controlam e comunicam informações.



# Cibernética

- Durante a Segunda Guerra Mundial, Wiener trabalhou no desenvolvimento de sistemas de controle para artilharia antiaérea. Ele percebeu que a interação entre os sistemas humanos e mecânicos poderia ser compreendida usando conceitos matemáticos, como feedback e comunicação. Esses estudos deram origem ao campo da cibernética.
- A cibernética, no contexto de Wiener, explorava a aplicação de princípios de controle, retroalimentação (*feedback*) e comunicação para entender e projetar sistemas complexos. Isso incluía tanto máquinas (como computadores) quanto sistemas biológicos (como organismos vivos ou ecossistemas).





# Terminologia

- **SEGURANÇA DA INFORMAÇÃO** - ações que objetivam viabilizar e assegurar a **disponibilidade**, a **integridade**, a **confidencialidade** e a **autenticidade** das informações.
- **SEGURANÇA CIBERNÉTICA** - ações voltadas para a **segurança de operações**, visando garantir que os **sistemas de informação** sejam capazes de resistir a eventos no **espaço cibernetico**, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados **armazenados, processados ou transmitidos** e dos serviços que esses sistemas ofereçam ou tornem acessíveis.

# Terminologia

- **Segurança da Informação**
  - ✓ Refere-se à proteção de dados e informações, independentemente do formato ou meio (digital, físico, verbal, outros).
  - ✓ Abrange políticas, processos, controle de acesso, gestão de riscos, e pode incluir informações armazenadas em papel, verbalizadas ou digitais.
- **Segurança Cibernética**
  - ✓ É um subconjunto da segurança da informação que se concentra exclusivamente na proteção de sistemas, redes e dados contra ameaças que surgem no espaço digital ou cibernetico.
  - ✓ Inclui práticas como gerenciamento de redes, proteção de estações de trabalho e resposta a incidentes de rede.

# Terminologia

- **Segurança da Informação**

- ✓ E mais ampla e inclui qualquer forma de proteção de informações.
- ✓ Pode incluir medidas físicas (como trancas em arquivos ou cofres).
- ✓ Protege dados e informações, independentemente de como são armazenados.

- **Segurança Cibernética**

- ✓ Foca no ambiente digital e cibernético.
- ✓ Utiliza ferramentas digitais (firewalls, antivírus, criptografia de dados).
- ✓ Protege ativos e informações no espaço cibernético.

# Vulnerabilidade

**Vulnerability:** A characteristic or specific **weakness** that renders an organization or asset (such as information or an information system) open to **exploitation** by a given **threat** or susceptible to a given hazard.



# Exploit

**Exploit:** A technique to *breach the security* of a network or information system in violation of security policy.



## Ameaça

**Threat:** A *circumstance or event that has or indicates the potential to exploit vulnerabilities and to adversely impact* (create adverse consequences for) organizational operations, organizational assets (including information and information systems), individuals, other organizations, or society. Includes an *individual or group of individuals*, entity such as an organization or a nation, action, or occurrence.



## Ameaça

*"Qualquer circunstância ou evento com potencial para **impactar negativamente** as operações organizacionais (incluindo missão, funções, imagem ou reputação), ativos organizacionais, indivíduos, outras organizações ou a Nação através de um sistema de informação por meio de acesso não autorizado, destruição, divulgação, modificação de informações e/ou negação de serviço."*

# Ameaça



## Risco

**Risk:** *The potential for an unwanted or adverse outcome resulting from an incident, event, or occurrence, as determined by the likelihood that a particular threat will exploit a particular vulnerability, with the associated consequences.*



## Ameaças

- *Hackers*
- *Insiders*
- Funcionário insatisfeito
- Crime organizado
- Competidores
- Governos/Estados
- APT

## Vulnerabilidades

- Rede
- Sistema Operacional
- Aplicação web
- Banco de Dados
- Equipamentos de rede e de segurança
- CVE

## Riscos

- Perda de vida
- Fraude
- Vazamento de dados
- Extorsão
- Roubo de informações valiosas
- Descrédito (imagem)
- Perda de confiança

# Hacker

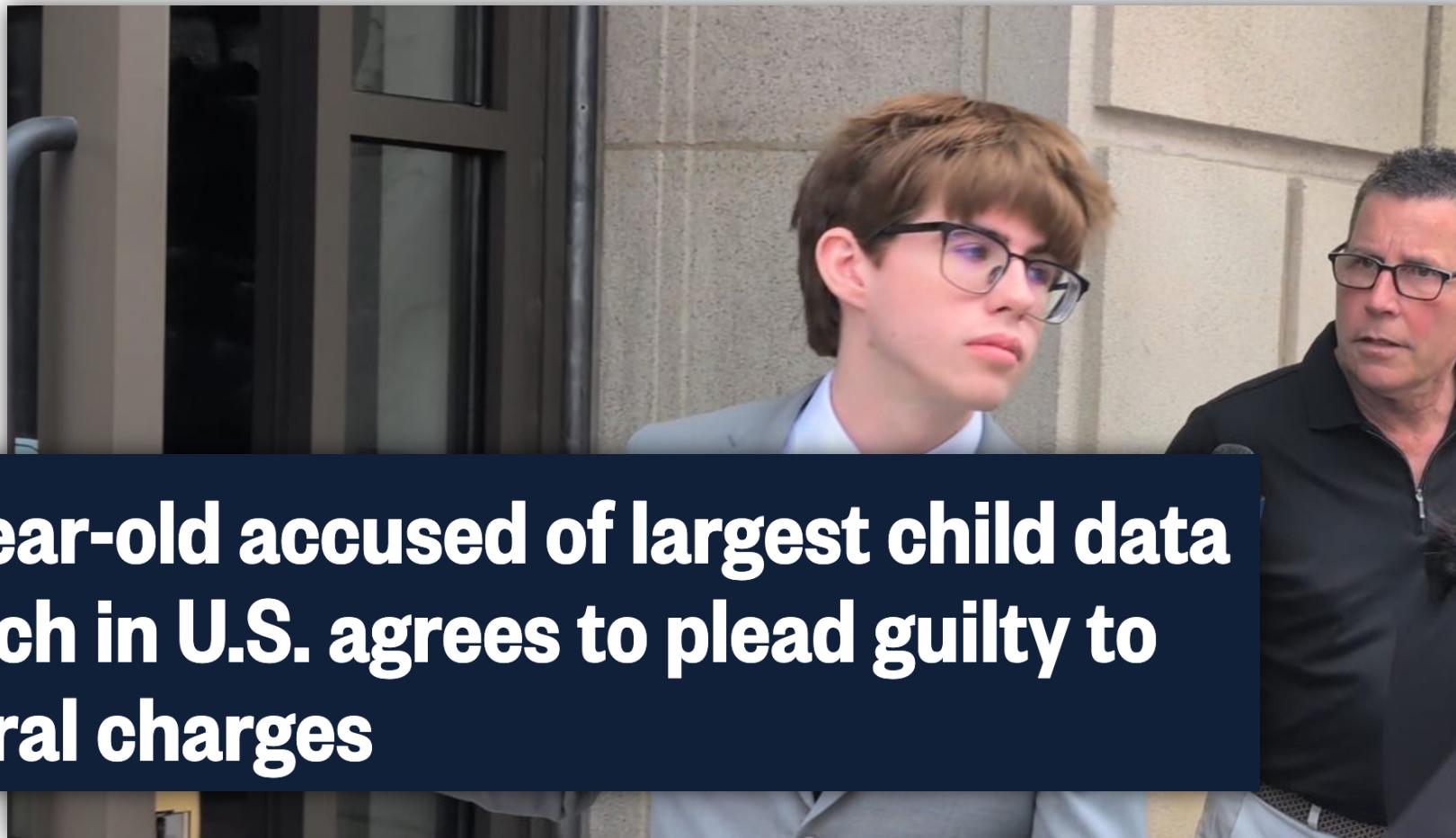
- Hacker é uma pessoa que entende muito de computadores, redes e sistemas, utilizando esse conhecimento para explorar como as coisas funcionam ou para encontrar falhas.
- *A person who has knowledge and skill in analyzing program code or a computer system, modifying its functions or operations and altering its abilities and capabilities.*
- *A hacker may be ethical and authorized (the original definition) or may be malicious and unauthorized (the altered but current use of the term).*



# Unethical Hacker

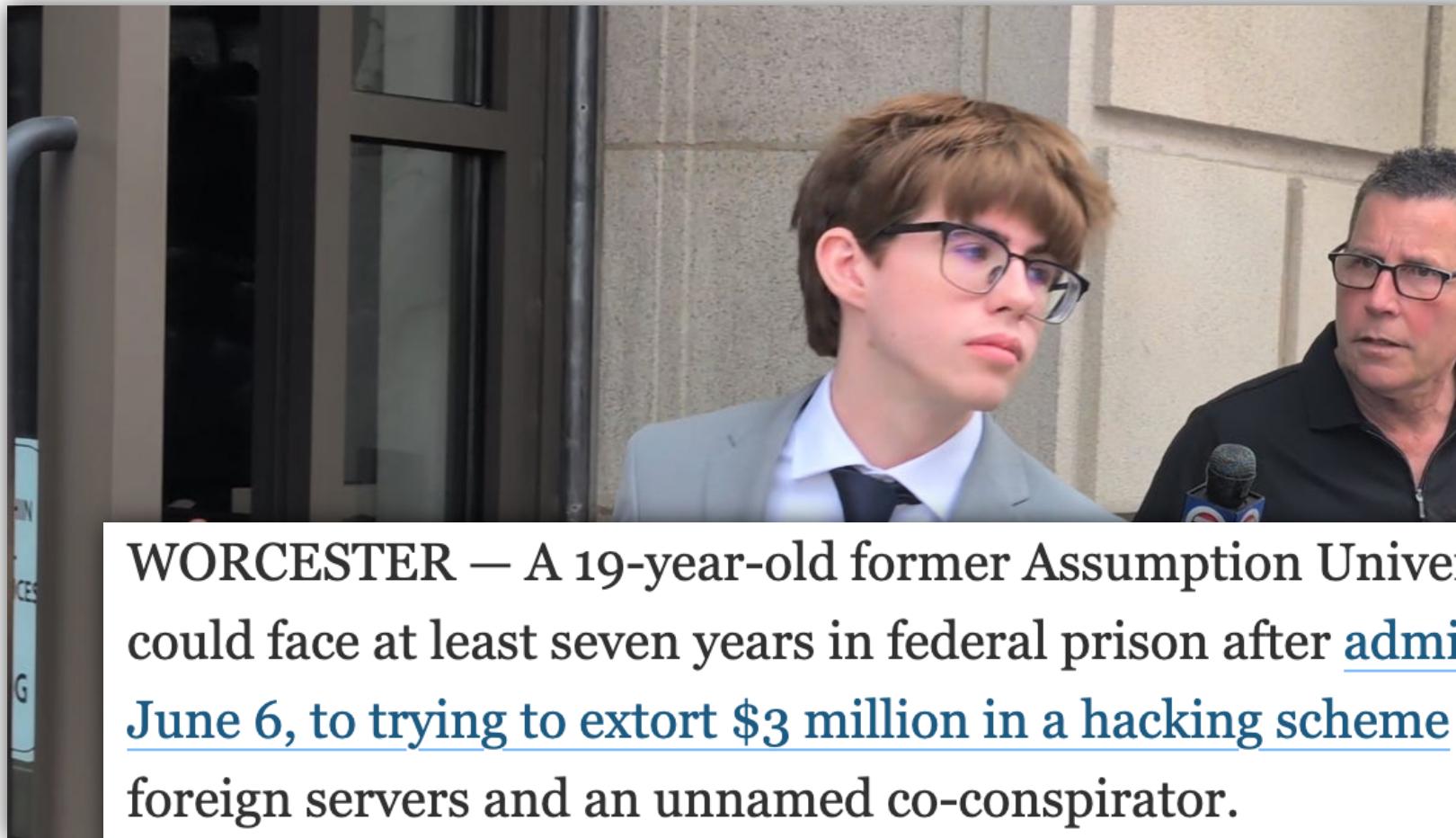


# Unethical Hacker



**19-year-old accused of largest child data breach in U.S. agrees to plead guilty to federal charges**

# Unethical Hacker



WORCESTER — A 19-year-old former Assumption University student could face at least seven years in federal prison after admitting Friday, June 6, to trying to extort \$3 million in a hacking scheme that involved foreign servers and an unnamed co-conspirator.

# Threat Agent/Actor (*adversary*) – Agente/Ator de Ameaça

*“An individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.”*

- Estados-nações
- Grupos Terroristas
- Ativistas
- Facções Políticas
- Organizações Criminosas
- Criminosos digitais
- Outros

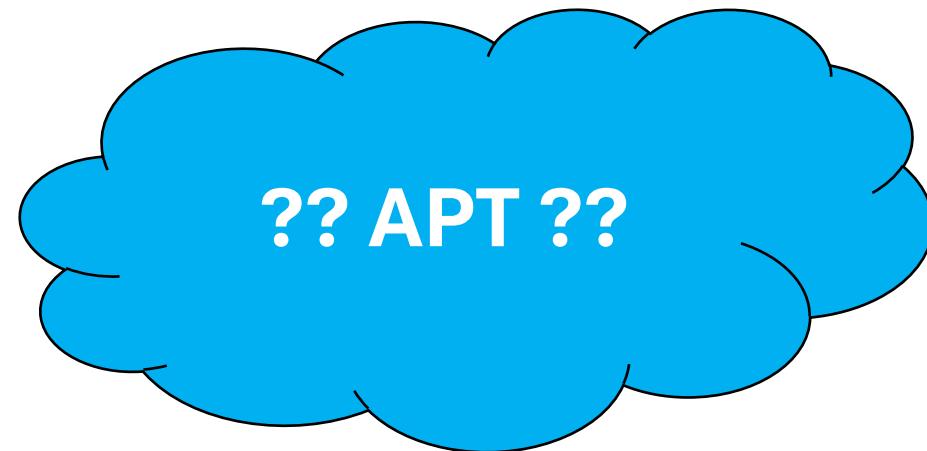
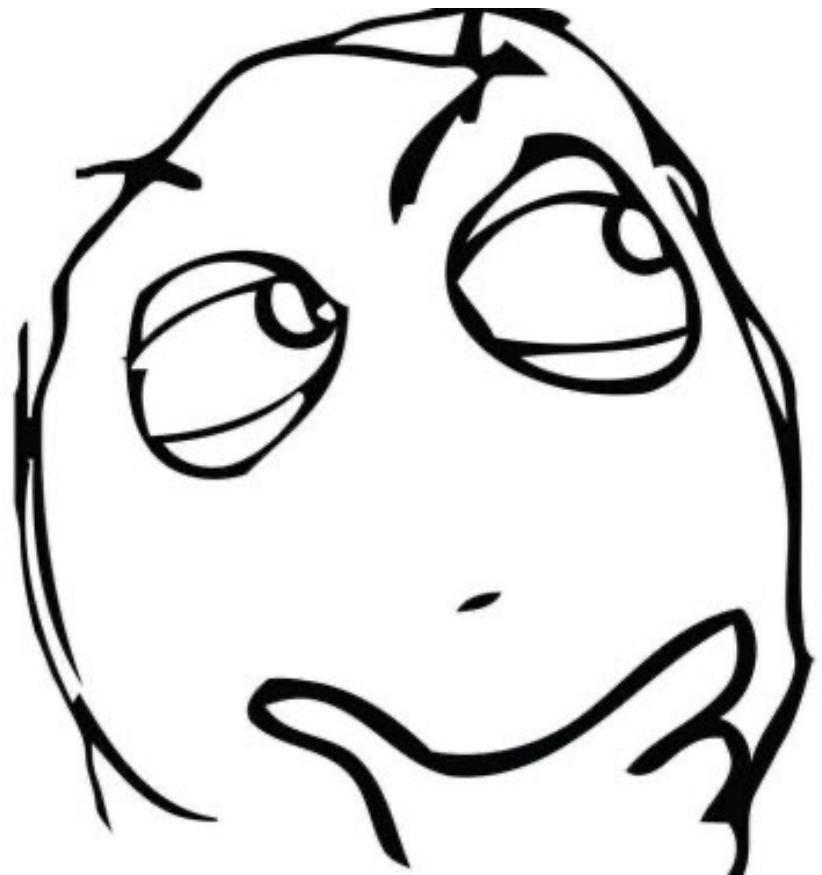


## Motivos

Os motivos que levam os atacantes a desferir ataques na Internet e nas organizações são diversos, variando da simples diversão até a realização de ações criminosas:

- ✓ Motivações Financeiras
- ✓ Motivações Comerciais
- ✓ Motivações Ideológicas
- ✓ Motivações Políticas
- ✓ Demonstração de Poder
- ✓ Prestígio
- ✓ Espionagem





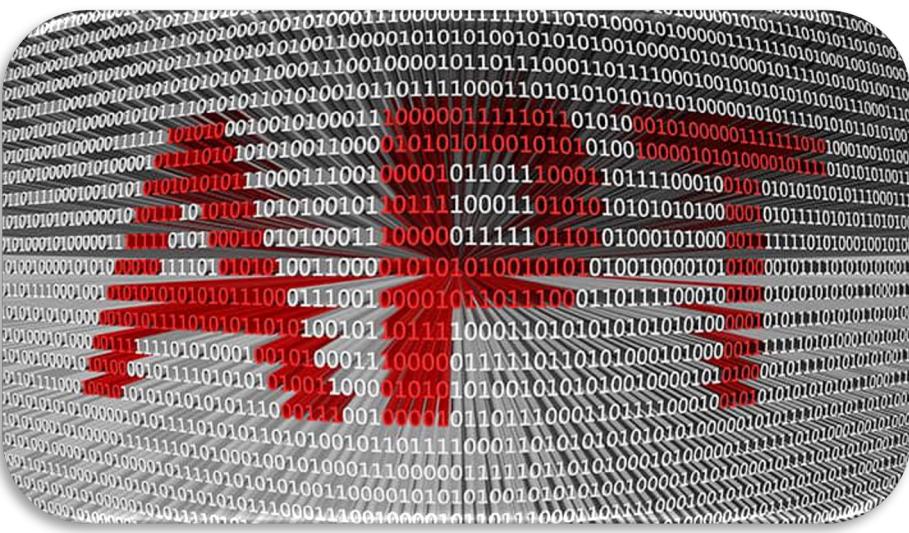
# APT (CISA)



## ***Advanced Persistent Threat*** **(Ameaça Persistente Avançada)**

“A **sophisticated** threat actor, often associated with a **nation-state**, that has the **resources and capabilities to conduct a sustained cyber campaign** against a target individual or organization. The APT often spends a lot of time learning about their target before conducting an **intrusion to establish an undetected presence** in the target’s network. This ultimately enables the APT to surveil the target, steal sensitive data, or conduct other malicious activity over a **prolonged period of time**.”

# APT (NIST)



## *Advanced Persistent Threat*

“An adversary that possesses **sophisticated levels of expertise and significant resources** which allow it to create opportunities to achieve its objectives by using **multiple attack vectors** (e.g., cyber, physical, and deception). These objectives typically include **establishing and extending footholds** within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, **undermining or impeding critical aspects of a mission, program, or organization**; or positioning itself to carry out these objectives in the future.”

# APT (NIST)



*The advanced persistent threat:*

- (i) *pursues its objectives repeatedly over an **extended period of time**;*
- (ii) ***adapts** to defenders' efforts to resist it; and*
- (iii) *is **determined** to maintain the level of interaction needed to execute its objectives.*

## Advanced

- Adversários altamente **motivados**
- **Patrocinados** por estados ou grandes organizações
- Bem **organizados** e estruturados
- Utilizam diversas técnicas de invasão, das **básicas** às **avançadas**
- Podem explorar **vulnerabilidades 0-day**



## Persistent

- **Permanecem** por muito tempo na rede ou infraestrutura do alvo/vítima
- Conseguem ficar “**invisíveis**” (*stealthy*) na rede
- Se **espalham** fundo nas redes e sistemas
- Configuram diversos mecanismos de persistência (**backdoors**)
- Utilizam diversas técnicas de **evasão**



# Threat

- Existem diversas **motivações**
  - ✓ Financeira
  - ✓ Espionagem (industrial ou governo)
  - ✓ Ideológica/Política
- Infraestruturas Críticas
- Mapear a organização
- Descobrir e extrair informações valiosas



# Evento

- **Evento** pode ser entendido como qualquer atividade dentro de sua organização.
- **Eventos de segurança** de computadores são ocorrências em um sistema ou rede que são relevantes para a sua segurança.
- Eventos de segurança de computadores, geralmente, são atividades suspeitas no sistemas e redes.
- **Glossário GSI**
  - **EVENTO** - qualquer mudança de estado que tem importância para a gestão de um item de configuração ou serviço de tecnologia da informação. Em outras palavras, qualquer ocorrência dentro do escopo de tecnologia da informação que tenha relevância para a gestão dos serviços entregues ao cliente.
  - **EVENTO DE SEGURANÇA** - qualquer ocorrência identificada em um sistema, serviço ou rede, que **indique uma possível falha** da política de segurança, falha das salvaguardas ou mesmo uma situação até então desconhecida, que possa se tornar relevante em termos de segurança.

# Incidente

- **ITIL v4**
  - ✓ Um incidente é definido como um **evento não planejado que causa uma interrupção ou redução na qualidade de um serviço de TI**. Qualquer situação que compromete ou potencialmente compromete a operação normal de um serviço de TI, impactando os usuários ou o negócio.
- **ISO/IEC 27035:1 – Information technology – Information security incident management (Principles and Process)**
  - ✓ “*single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security*”
- **NIST SP 800-61 Rev. 2, Computer Security Incident Handling Guide**
  - ✓ “*A computer security incident is a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices*.”

# Incidente

## NIST SP 800-61 Rev.3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management

An occurrence that *actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies.*

- ***ENISA (European Union Agency for Cybersecurity)***
  - ✓ “*Security Incident: An occurrence that harms integrity, accessibility, confidentiality or authenticity of a computer (or other device) or a network.*”
- ***SANS Computer Security Incident Handling Step-by-Step Guide***
  - ✓ “*an adverse event in an information system and/or network, or the threat of the occurrence of such an event*”
- ***Glossário GSI***
  - ✓ ***INCIDENTE DE SEGURANÇA*** - qualquer *evento adverso, confirmado ou sob suspeita*, relacionado à segurança dos sistemas de computação ou das redes de computadores.

## Incidente

# Glossário de Segurança da Informação (GSI)

**Incidente Cibernético:** ocorrência que **pode comprometer, real ou potencialmente**, a **disponibilidade, a integridade, a confidencialidade** ou a **autenticidade** de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema.



## Incidente

- Estação de trabalho infectada por um malware que coleta dados sensíveis do usuário e do sistema (*infostealer*).
- Um atacante obtém dados médicos de pacientes, de uma base de dados de um hospital, e ameaça liberar na Internet, caso a organização não pague um valor em bitcoin.
- Usuário recebe um *phishing* e clica num link suspeito, fornecendo usuário e senha de um sistema corporativo.
- Uma *botnet* (Mirai) envia uma grande quantidade de requisições para um site de um empresa, inviabilizando o acesso aos serviços web (DDoS).
- O *malware* Stuxnet alterou os dados dos sistemas de controle (SCADA), usados em instalações nucleares do Irã, fazendo com que centrífugas operassem em velocidades perigosas, enquanto reportavam dados normais aos operadores.
- O site de uma empresa foi invadido e os atacantes modificaram o conteúdo da página, desfigurando o site (*defacement*).

# Incidente

- Estação de trabalho infectada por um malware que coleta dados sensíveis do usuário e do sistema (*infostealer*). **Afeta a confidencialidade.**
- Um atacante obtém dados médicos de pacientes, de uma base de dados de um hospital, e ameaça liberar na Internet, caso a organização não pague um valor em bitcoin. **Afeta a confidencialidade.**
- Usuário recebe um *phishing* e clica num link suspeito, fornecendo usuário e senha de um sistema corporativo. **Afeta a confidencialidade.**
- Uma *botnet* (Mirai) envia uma grande quantidade de requisições para um site de um empresa, inviabilizando o acesso aos serviços web (DDoS). **Afeta a disponibilidade.**
- O *malware* Stuxnet alterou os dados dos sistemas de controle (SCADA), usados em instalações nucleares do Irã, fazendo com que centrífugas operassem em velocidades perigosas, enquanto reportavam dados normais aos operadores. **Afeta a integridade.**
- O site de uma empresa foi invadido e os atacantes modificaram o conteúdo da página, desfigurando o site (*defacement*). **Afeta a integridade.**

# Gestão de Riscos

FEBRABAN  
/ CYBER LAB



**Nenhum sistema é 100% seguro!**

# Gestão de Riscos

- Risco é a chance de algo ruim acontecer (incerteza). Gestão de Riscos é **identificar** esses perigos antes que eles aconteçam, e **tomar decisões** para **evitar ou reduzir os danos**.
- Gestão de Riscos em Segurança da Informação é o **processo de descobrir** o que pode ameaçar os dados e sistemas de uma empresa (ou pessoa), **avaliar** o impacto disso e **escolher** a melhor forma de proteger.



# Gestão de Riscos

- Vamos utilizar a analogia de **proteção de uma casa**.
- Você tranca as portas, fecha as janelas, coloca um alarme.
- **Por quê?** Porque existe o **risco de um roubo**.
- Se mora em um **bairro perigoso**, o **risco é maior**. Se tem uma **porta frágil**, o **risco também aumenta**.
- Você faz uma **gestão de riscos** quando decide:
  - ✓ “Vou investir em um portão mais forte.”
  - ✓ “Vou instalar câmeras.”
  - ✓ “Vou contratar seguranças.”



# Gestão de Riscos

- No contexto de uma empresa, temos:
  - ✓ Dados de clientes
  - ✓ Informações financeiras
  - ✓ Sistemas que mantêm tudo funcionando
- Esses dados podem ser:
  - ✓ Vazados (por um ataque cibernético)
  - ✓ Apagados (por um erro ou falha do sistema)
  - ✓ Roubados (em um golpe de *phishing*)



NORMA  
BRASILEIRA

ABNT NBR  
ISO/IEC  
27005

Quarta edição  
30.05.2023

**Segurança da informação, segurança cibernética e proteção à privacidade — Orientações para gestão de riscos de segurança da informação**

*Information security, cybersecurity and privacy protection — Guidance on managing information security risks*

- Atividades coordenadas para direcionar e controlar uma organização com relação aos riscos de segurança da informação:
  - ✓ Estabelecimento do contexto
  - ✓ Identificação de riscos
  - ✓ Análise de riscos
  - ✓ Avaliação de riscos
  - ✓ Tratamento de riscos
  - ✓ Aceitação de riscos
  - ✓ Comunicação e consulta
  - ✓ Monitoramento e análise crítica

# Gestão de Riscos

- Estratégias para proteção das informações da empresa.
- **Minimizar os impactos** no caso de um incidente cibernético.
- **Defesa em profundidade.**
- Várias camadas de proteção.



Gestão de riscos é como usar o cinto de segurança: você espera nunca precisar, mas se algo der errado, ele pode salvar sua vida. Em Segurança da Informação, é isso que fazemos: **prevenimos antes de remediar.**

**FIM**  
**Muito obrigado**

**FEBRABAN**  
/ CYBER LAB

