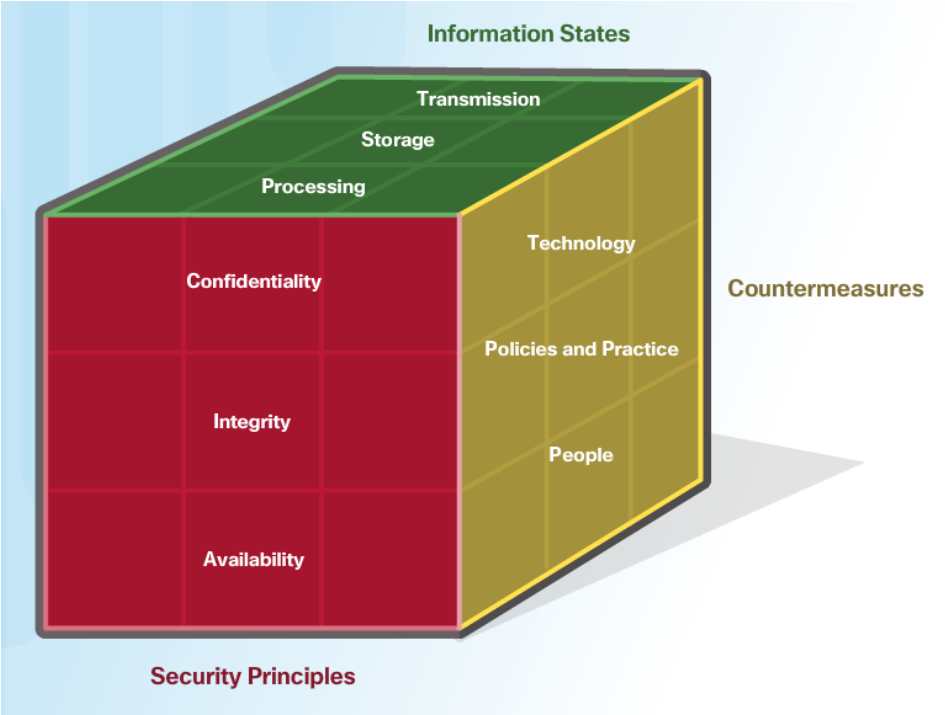
OBJETIVOS

- Necessidade de Segurança
- Ameaças, criminosos, especialistas, certificações;
- Princípios de Segurança da Informação;
- Incidentes Reportados.

PRINCÍPIOS: AS 3 DIMENSÕES

Primeira dimensão (Princípios da Segurança da Informação).

- ✓ Esses três princípios do CID são a **confidencialidade (privacidade), integridade (precisão, consistência e confiabilidade da informação) e disponibilidade (informação está acessível).**



CONFIDENCIALIDADE

Princípio da Confidencialidade

- A confidencialidade impede a divulgação de informações a pessoas, recursos e processos não autorizados. Outro termo para confidencialidade é a privacidade.
- As organizações precisam formar funcionários sobre as melhores práticas para proteger informações confidenciais para se protegerem e a organização contra ataques.
- **Os métodos utilizados para garantir a confidencialidade incluem criptografia de dados, autenticação e controle de acesso.**

CONFIDENCIALIDADE

Protegendo a Privacidade dos Dados

- As organizações coletam uma grande quantidade de dados e grande parte desses dados não é sensível porque está disponível publicamente, como nomes e números de telefone.
- Outros dados coletados, porém, são sensíveis. Informações sensíveis são protegidas contra o acesso não autorizado para salvaguardar um indivíduo ou uma organização.

CONFIDENCIALIDADE

Controlando o Acesso

- O controle de acesso define uma série de esquemas de proteção que impedem o acesso não autorizado a um computador, rede, banco de dados ou outros recursos de dados. Os conceitos de AAA envolvem três serviços de segurança: Autenticação, Autorização e Auditoria.
- **Autenticação:** verifica a identidade de um usuário para impedir o acesso não autorizado. Os usuários provam sua identidade com um nome de usuário ou I.D.
- **Autorização:** determina quais recursos os usuários podem acessar, juntamente com as operações que os usuários podem executar. A autorização também pode controlar quando um usuário tem acesso a um recurso específico.
- **Auditoria:** acompanha o que os usuários fazem, incluindo o que eles acessam, a quantidade de tempo que eles acessam, e as mudanças feitas.

INTEGRIDADE

Princípio da integridade dos dados

- ✓ A integridade é a precisão, consistência e confiabilidade dos dados durante todo o seu ciclo de vida.
- ✓ **Os métodos utilizados para garantir a integridade dos dados incluem hash, verificações de validação de dados e verificações de consistência de dados.**

Necessidade de Integridade de Dados

- ✓ A necessidade de integridade de dados varia de acordo com a forma como uma organização usa dados. Por exemplo, o Facebook não verifica os dados que um usuário publica em um perfil. Um banco ou organização financeira atribui maior importância à integridade, pois as transações e contas de clientes devem ser mantidas integras.
- ✓ Proteger a integridade dos dados é um desafio constante para a maioria das organizações. A perda de integridade dos dados pode tornar os recursos de dados inteiros não confiáveis ou inutilizáveis

INTEGRIDADE

Verificações de integridade

- ✓ Uma verificação de integridade é uma maneira de medir a consistência de uma coleção de dados (um arquivo, uma imagem ou um registro). A verificação de integridade executa um processo chamado de função hash para tirar instantâneo dos dados em um instante.

DISPONIBILIDADE

- A disponibilidade de dados é o princípio usado para descrever a necessidade de manter a disponibilidade de sistemas e serviços de informação em todos os momentos. Ataques provocam falhas do sistema e podem impedir o acesso a sistemas e serviços de informação.
- **Os métodos utilizados para garantir a disponibilidade incluem redundância do sistema, backups do sistema, maior resiliência do sistema, manutenção de equipamentos, sistemas operacionais atualizados e software e planos para recuperar rapidamente de desastres imprevistos.**

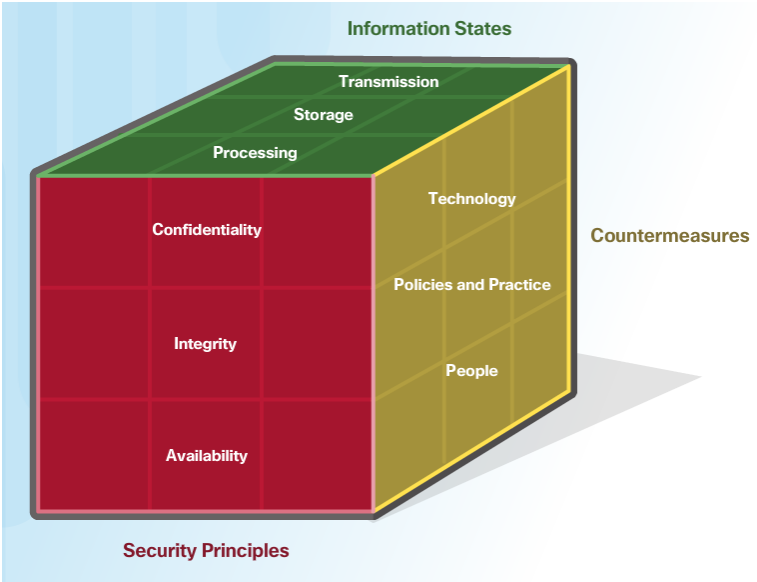
DISPONIBILIDADE

- Os sistemas de alta disponibilidade geralmente incluem três princípios de projeto: eliminar pontos únicos de falha, fornecer links confiáveis e detectar falhas à medida que ocorrem.
- As organizações podem garantir disponibilidade implementando o seguinte:
  - ✓ Manutenção de Equipamento
  - ✓ Atualizações nos sistemas
  - ✓ Testar backups
  - ✓ Planejar desastres
  - ✓ Implementar novas tecnologias
  - ✓ Monitorar atividade incomuns
  - ✓ Teste para verificar a disponibilidade

PRINCÍPIOS: AS 3 DIMENSÕES

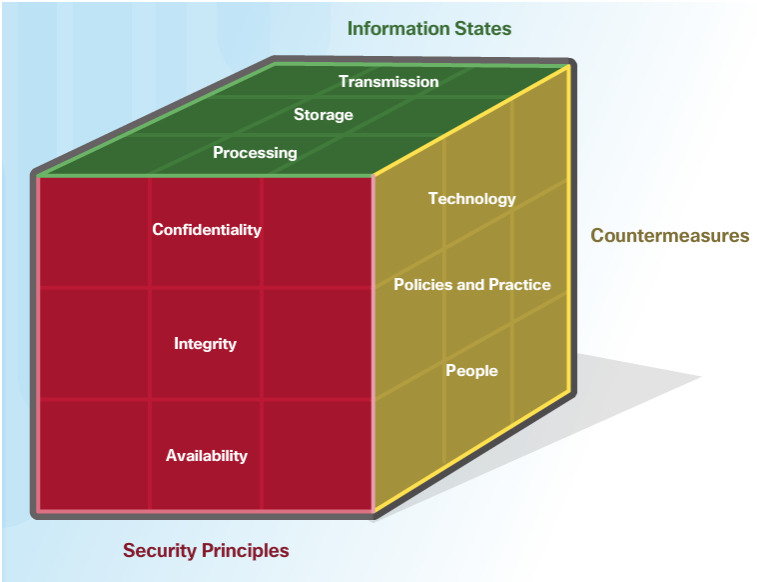
Segunda Dimensão (Dados possíveis).

- ✓ Dados em armazenados ou em repouso: informações armazenadas na memória ou no disco.
- ✓ Dados em trânsito: transferindo dados entre sistemas de informação.
- ✓ Dados em processamento: executa operações nos dados para alcançar um objetivo desejado.



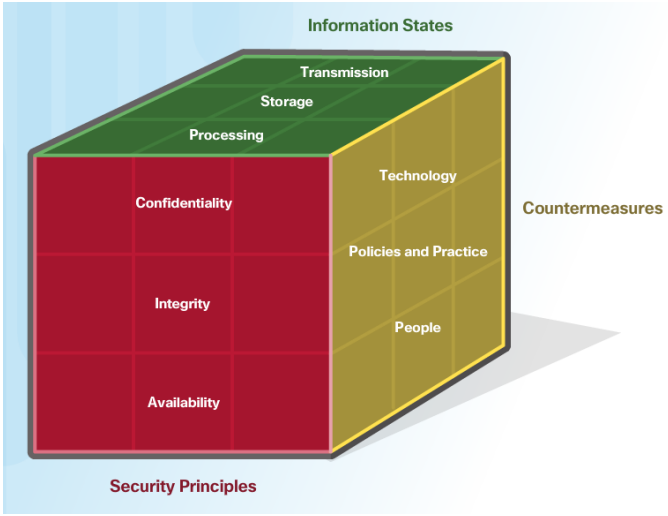
DADOS EM REPOUSO

- Os dados armazenados referem-se a dados em repouso. Os dados em repouso significam que um tipo de dispositivo de armazenamento retém os dados quando nenhum usuário ou processo está usando.
- Um dispositivo de armazenamento pode ser local (em um dispositivo de computação) ou centralizado (na rede). Existem várias opções para armazenar dados.



DADOS EM REPOUSO

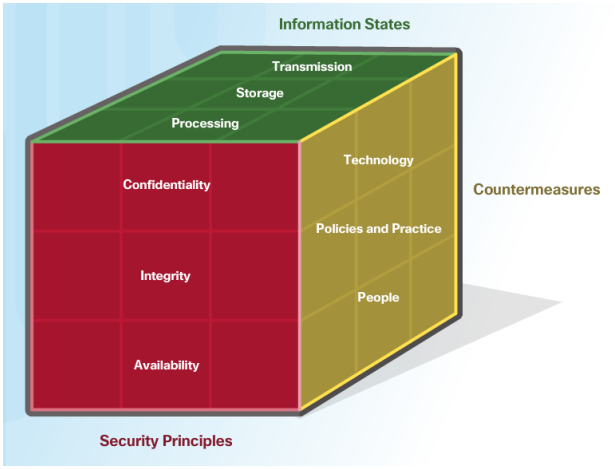
- A matriz redundante de discos independentes (RAID) usa vários discos rígidos em uma matriz, que é um método de combinação de vários discos para que o sistema operacional os veja como um único disco. O RAID oferece melhor desempenho e tolerância a falhas.
- Um dispositivo de armazenamento em rede (NAS) é um dispositivo de armazenamento conectado a uma rede que permite o armazenamento e a recuperação de dados de uma localização centralizada por usuários autorizados da rede. Os dispositivos NAS são flexíveis e escaláveis, o que significa que os administradores podem aumentar a capacidade conforme necessário.



DADOS EM TRÂNSITO

A transmissão de dados envolve o envio de informações de um dispositivo para outro. Métodos para transmitir informações entre dispositivos:

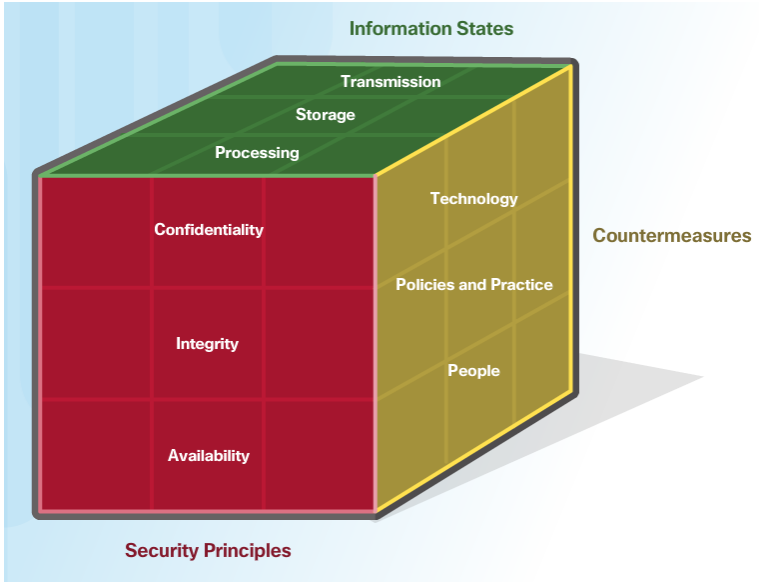
- Usa mídia removível para mover fisicamente dados de um computador para outro
- Redes cabeadas, redes sem fio
- Os maiores desafios para um profissional de segurança são:
  - ✓ **Protegendo a confidencialidade dos dados** - os atacantes podem capturar, salvar e roubar dados em trânsito.
  - ✓ **Protegendo a integridade dos dados** - os atacantes podem interceptar e alterar os dados em trânsito.
  - ✓ **Proteção da disponibilidade de dados** - os atacantes podem usar dispositivo não autorizados para interromper a disponibilidade de dados.



PRINCÍPIOS: AS 3 DIMENSÕES

Terceira Dimensão (Formas de Proteção).

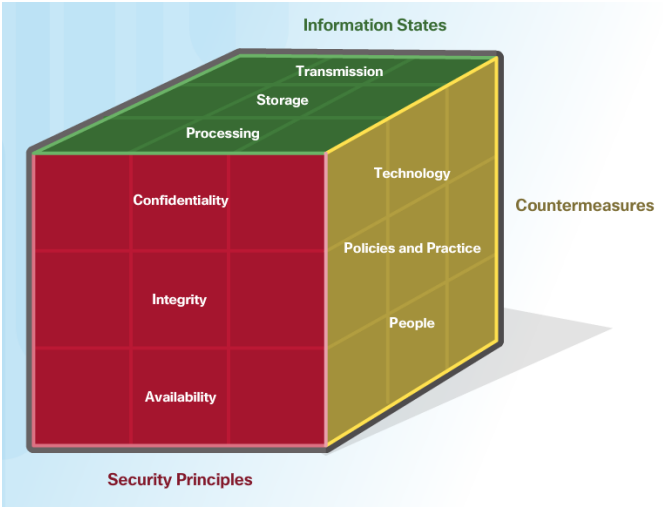
- ✓ **Tecnologias:** dispositivos e produtos disponíveis para proteção dos sistema de informação.
- ✓ **Políticas e Práticas:** procedimentos e diretrizes de boas práticas de segurança.
- ✓ **Pessoas:** conscientização dos perigos que ameaçam o seu dia-a-dia.



TECNOLOGIAS

Proteções baseadas em rede:

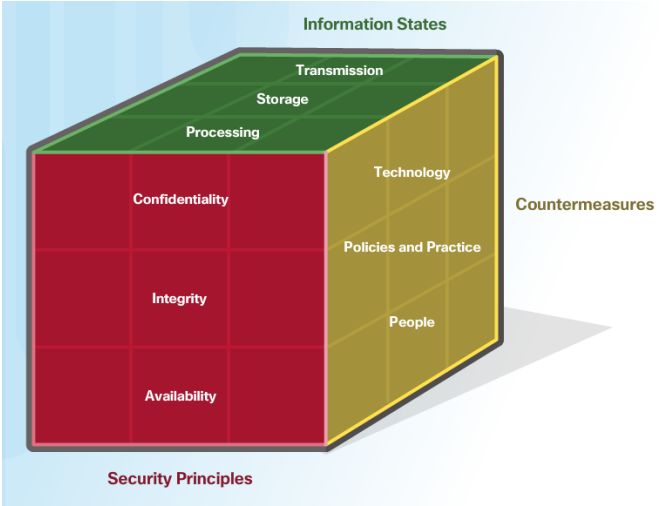
- **Virtual Private Network (VPN)** é uma rede virtual segura que usa a rede pública (ou seja, a Internet). A segurança de uma VPN reside na criptografia do conteúdo de pacotes entre os pontos finais que definem a VPN.
- **Controle de acesso à rede** requer um conjunto de verificações antes de permitir que um dispositivo se conecte a uma rede. Algumas verificações comuns incluem **software antivírus atualizado ou atualizações do sistema operacional instaladas.**
- **A segurança do ponto de acesso sem fio** inclui a implementação de **autenticação e criptografia.**



TECNOLOGIAS

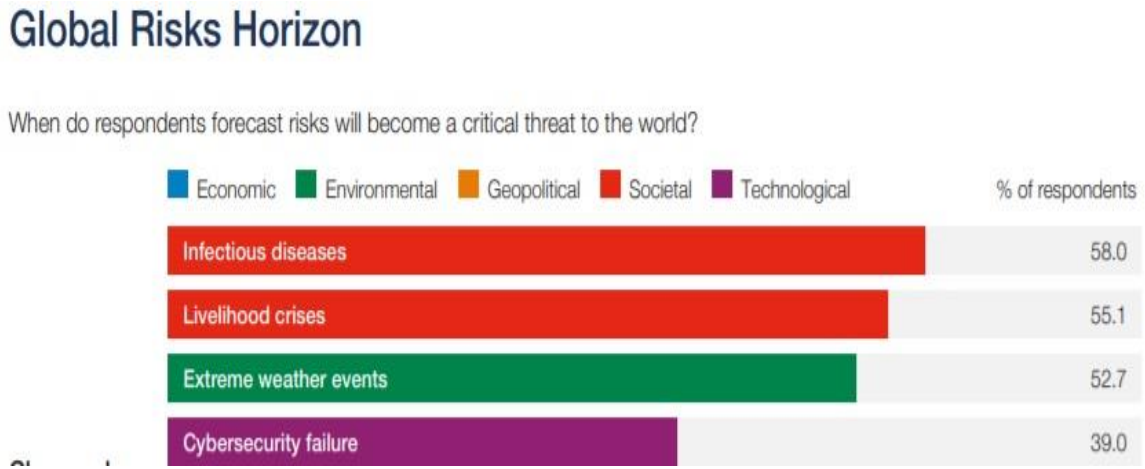
Proteções baseadas em nuvem:

- ✓ **Software como Serviço (SaaS)** permite que os usuários tenham acesso ao software aplicativo e aos bancos de dados. Os provedores de nuvem gerenciam a infraestrutura. Os usuários armazenam dados nos servidores do provedor da nuvem.
- ✓ **Infra-estrutura como Serviço (IaaS)** fornece recursos de computação virtualizados pela Internet. O provedor hospeda o hardware, o software, os servidores e os componentes de armazenamento.



RISCOS NA INTERNET

- A transformação digital e o incremento nos processos de segurança cibernética são elementos que devem caminhar lado a lado. Um estudo do Fórum Econômico Mundial de 2021 [1] revelou que falhas em cybersegurança foram indicadas como o quarto maior risco para o curto prazo e que agentes privados e governamentais tendem a se envolver em ataques cibernéticos mais perigosos e sofisticados em um futuro próximo. Portanto, é imprescindível que as organizações olhem para o futuro de uma maneira pragmática, entendendo a importância de ter processos seguros que acompanhem a evolução das tecnologias utilizadas.



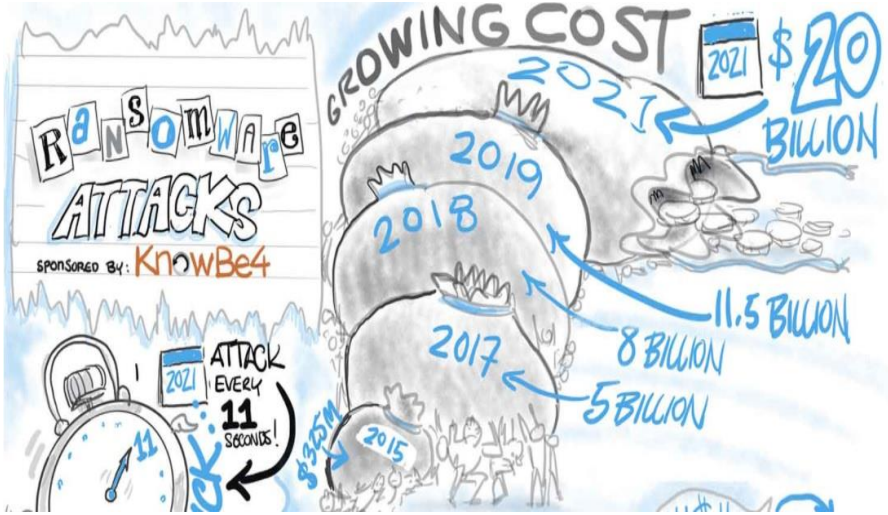
Fonte: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

RISCOS NA INTERNET

- **Mapas de ataques**: apresentam mapas de ataques cibernéticos em tempo real.
  - https://threatmap.checkpoint.com/ThreatPortal/livemap.html
  - https://threatmap.fortiguard.com/
  - https://cybermap.kaspersky.com/

RISCOS NA INTERNET

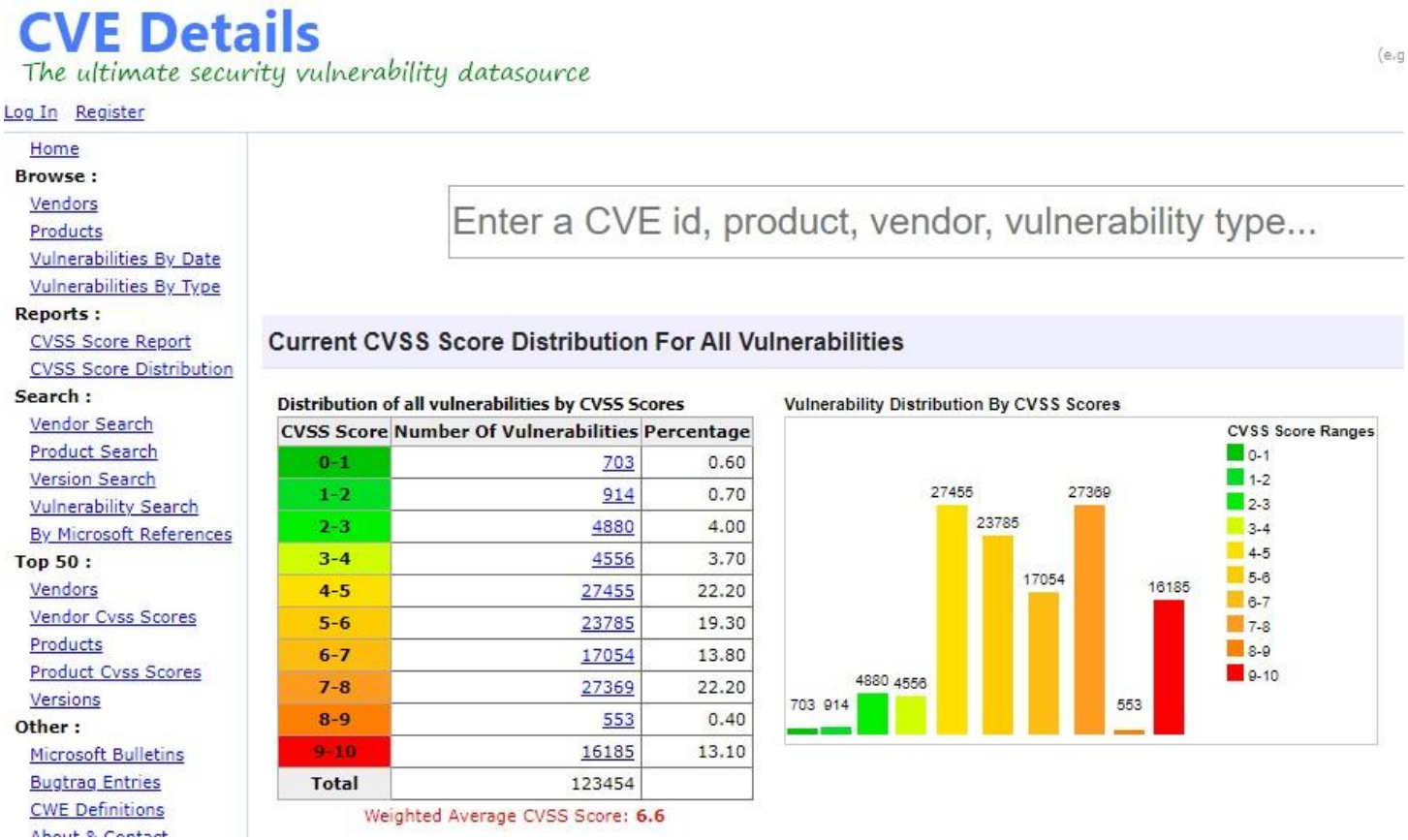
- Ransomware – um malware que infecta computadores (e dispositivos móveis) e restringe seu acesso a arquivos, muitas vezes ameaçando a destruição permanente de dados, a menos que um resgate seja pago – atingiu proporções epidêmicas globalmente e é o “ método de ataque ” para os cibercriminosos.
- A previsão mais recente é que os custos globais de danos de ransomware atingirão US$ 20 bilhões até 2021 – o que é 57 vezes mais do que em 2015. Isso torna o ransomware o tipo de crime cibernético que mais cresce.



Fonte: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

RISCOS NA INTERNET

- **Banco de dados de vulnerabilidades**: foi desenvolvido para fornecer um banco de dados publicamente disponível de todas as vulnerabilidades conhecidas. http://www.cvedetails.com/



CVE Details

The ultimate security vulnerability datasource

Log In Register

Home
Browse :
Vendors
Products
Vulnerabilities By Date
Vulnerabilities By Type
Reports :
CVSS Score Report
CVSS Score Distribution
Search :
Vendor Search
Product Search
Version Search
Vulnerability Search
By Microsoft References
Top 50 :
Vendors
Vendor Cvss Scores
Products
Product Cvss Scores
Versions
Other :
Microsoft Bulletins
Bugtraq Entries
CWE Definitions

Enter a CVE id, product, vendor, vulnerability type...

Current CVSS Score Distribution For All Vulnerabilities

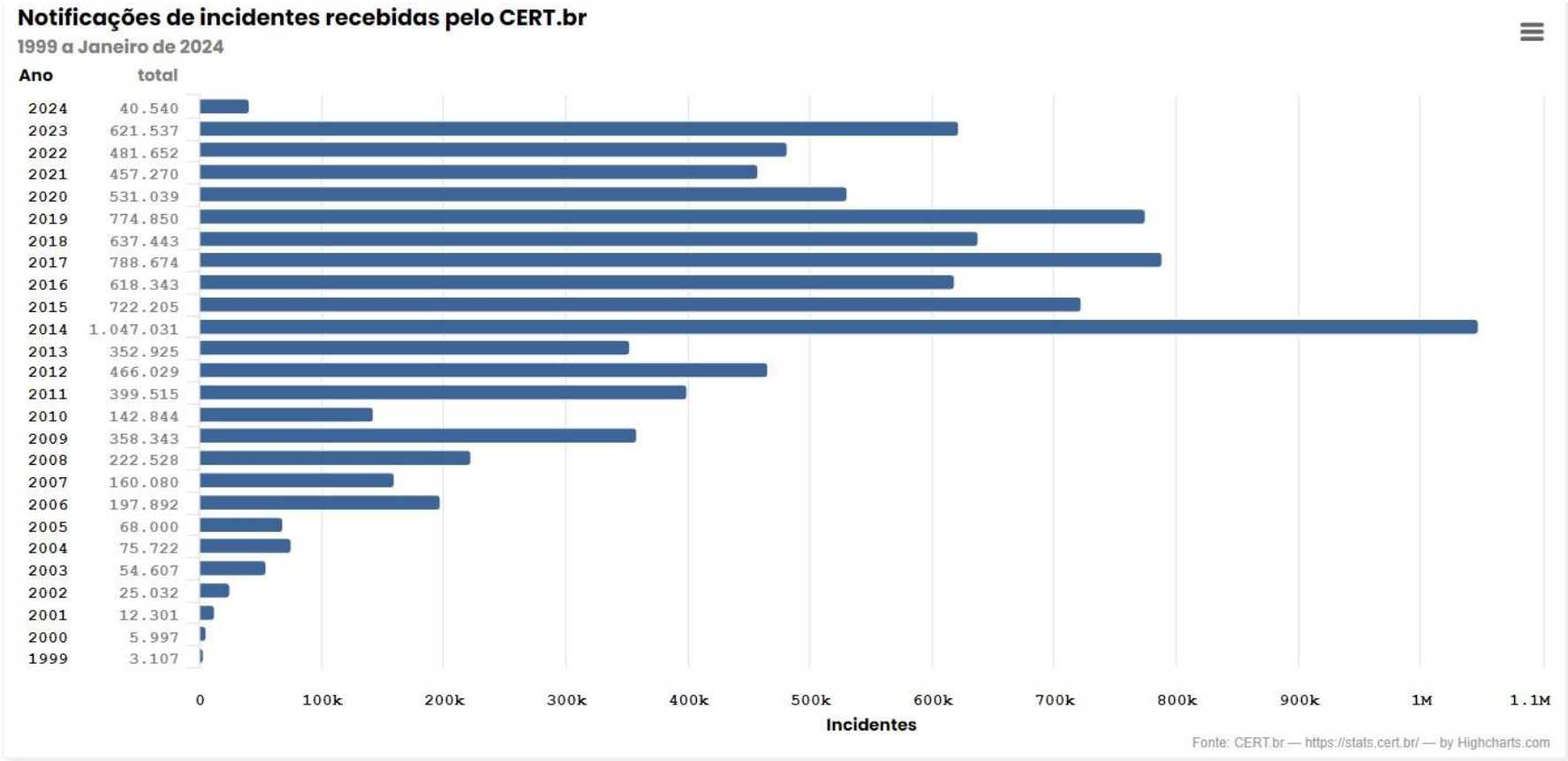
Distribution of all vulnerabilities by CVSS Scores

CVSS Score	Number Of Vulnerabilities	Percentage
0-1	703	0.60
1-2	914	0.70
2-3	4880	4.00
3-4	4556	3.70
4-5	27455	22.20
5-6	23785	19.30
6-7	17054	13.80
7-8	27369	22.20
8-9	553	0.40
9-10	16185	13.10
Total	123454	

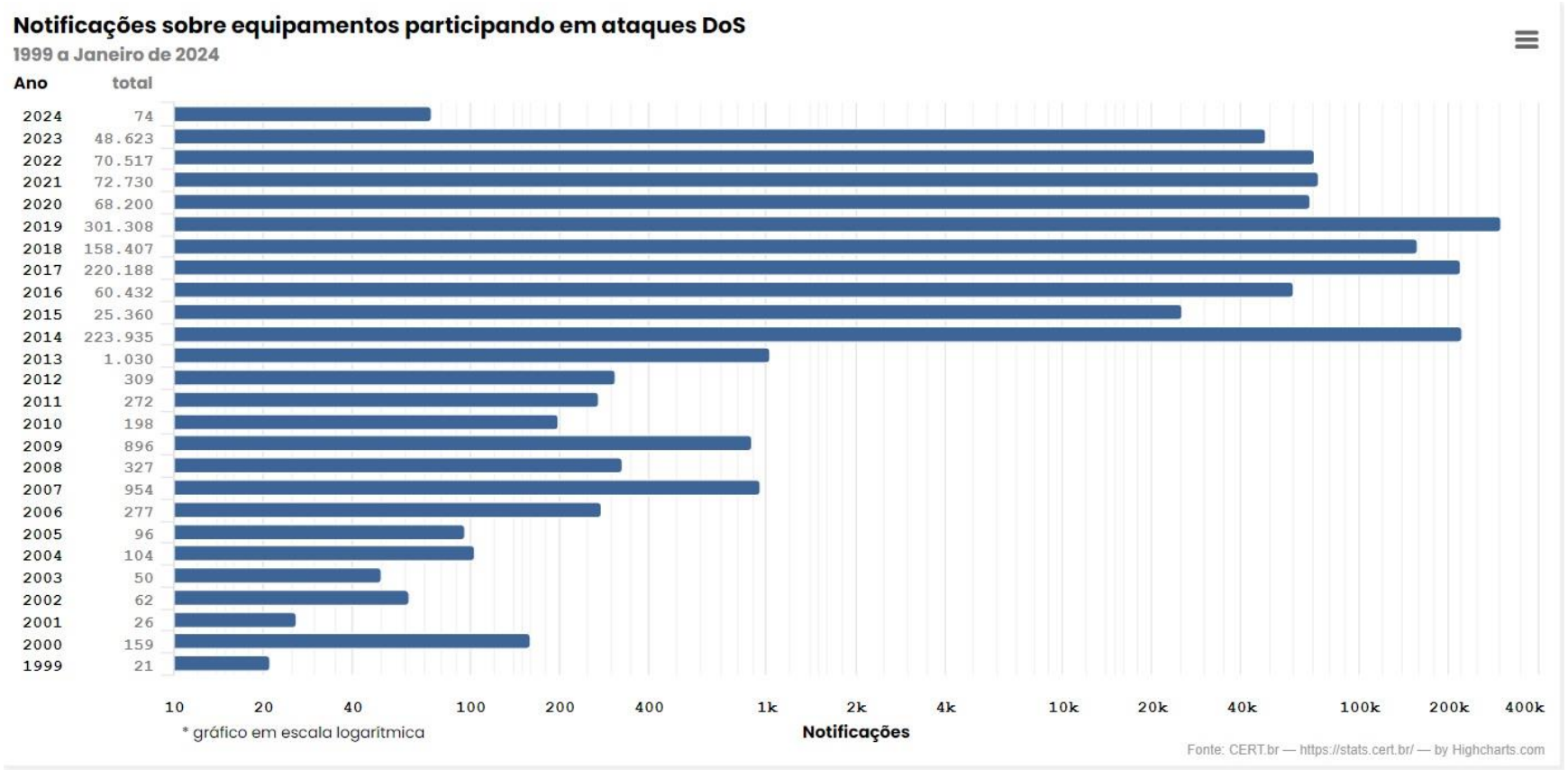
Weighted Average CVSS Score: **6.6**

Vulnerability Distribution By CVSS Scores

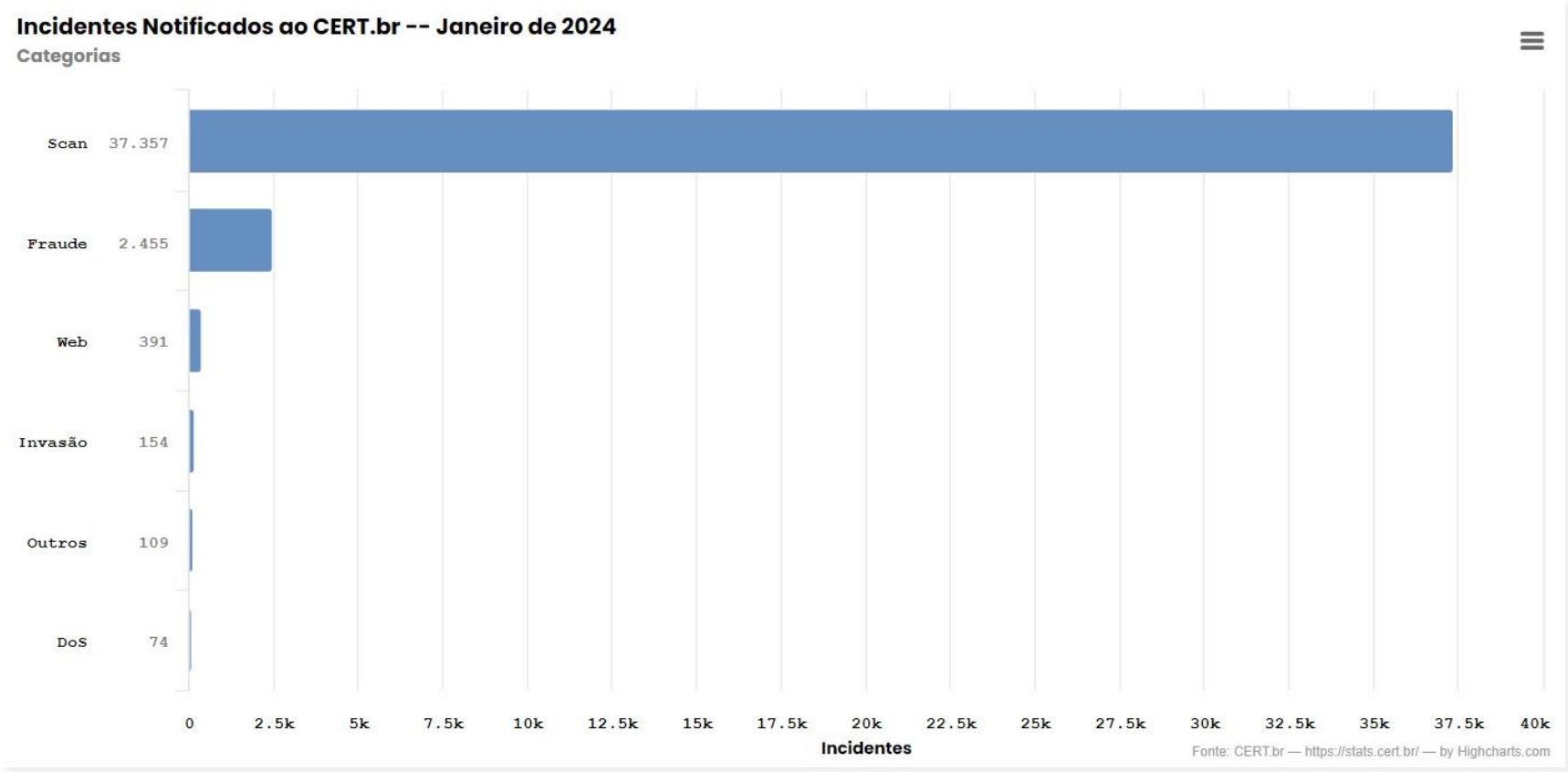
RISCOS NA INTERNET



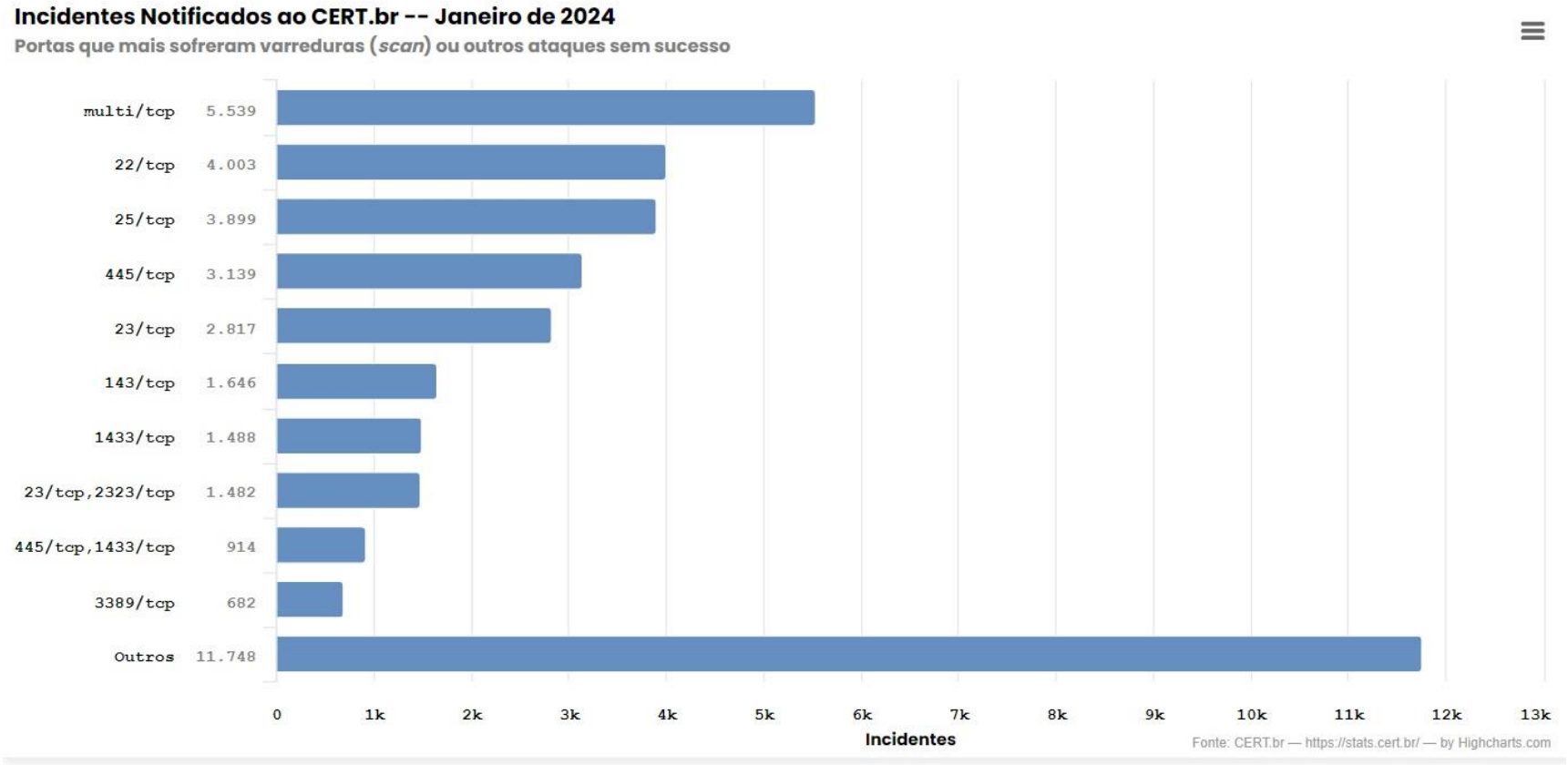
RISCOS NA INTERNET



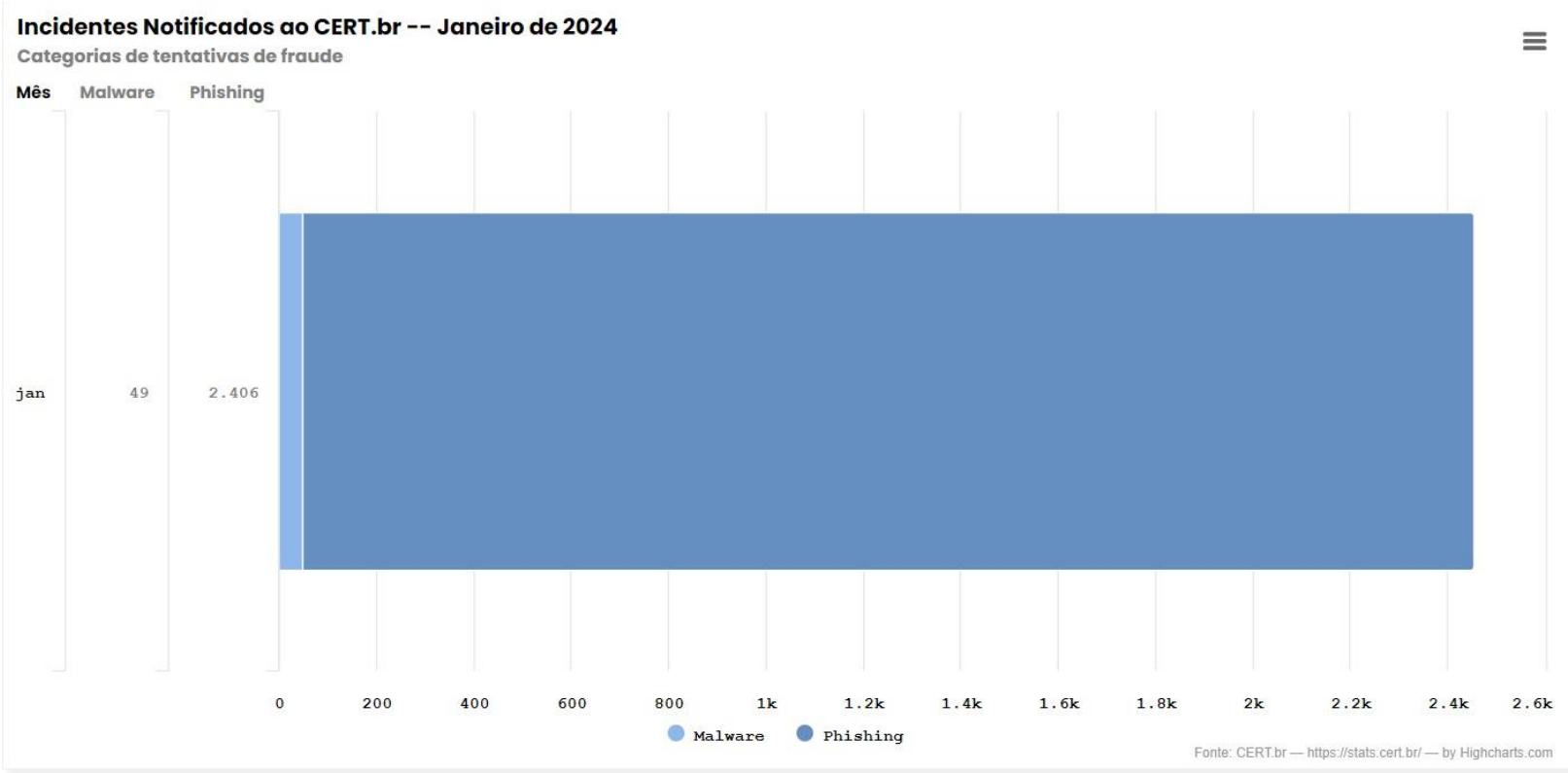
RISCOS NA INTERNET



RISCOS NA INTERNET

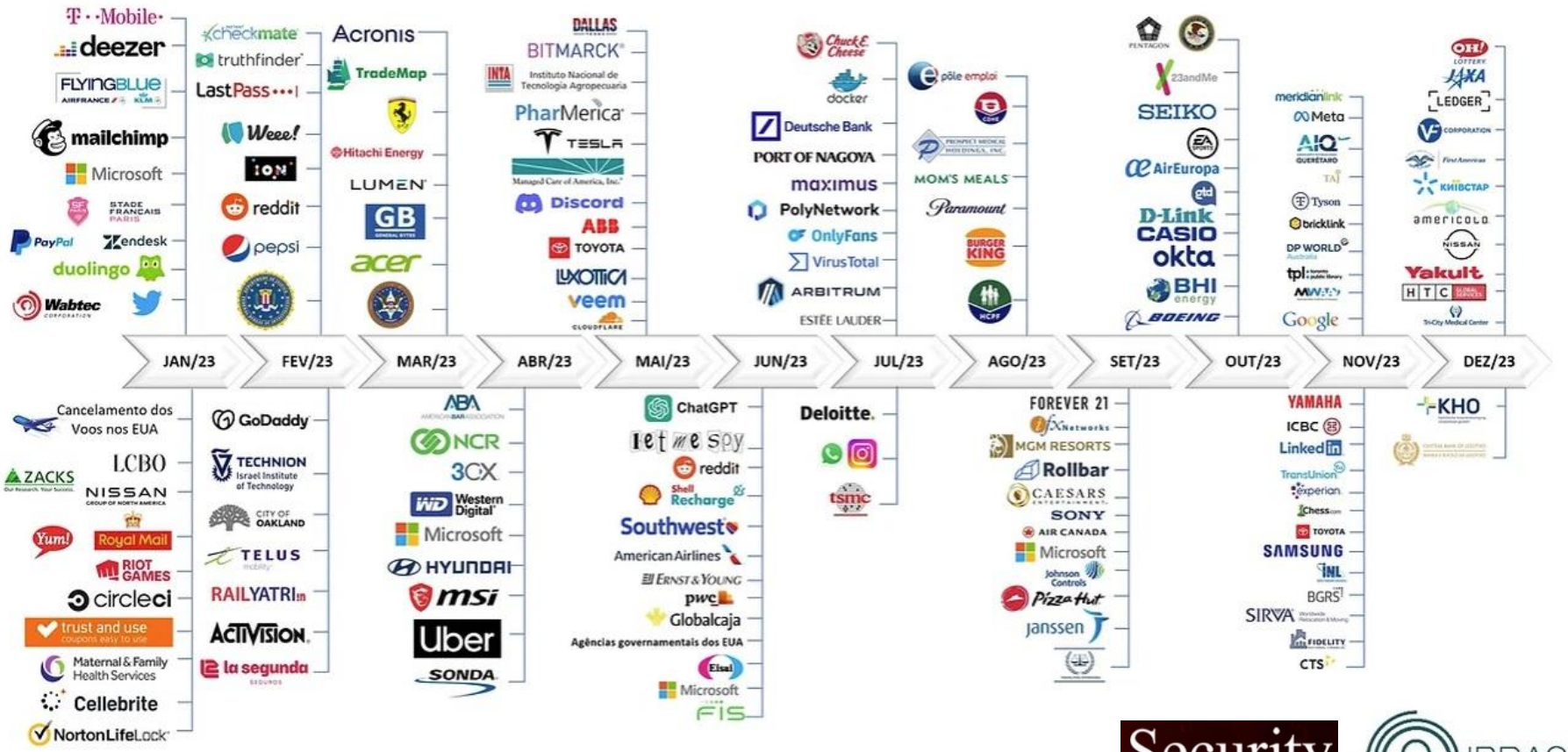


RISCOS NA INTERNET



INCIDENTES COM REPERCUSSÃO NA MÍDIA - MUNDIAL (2023)

Contexto Atual – Incidentes de segurança com repercussão na mídia (Mundial)*



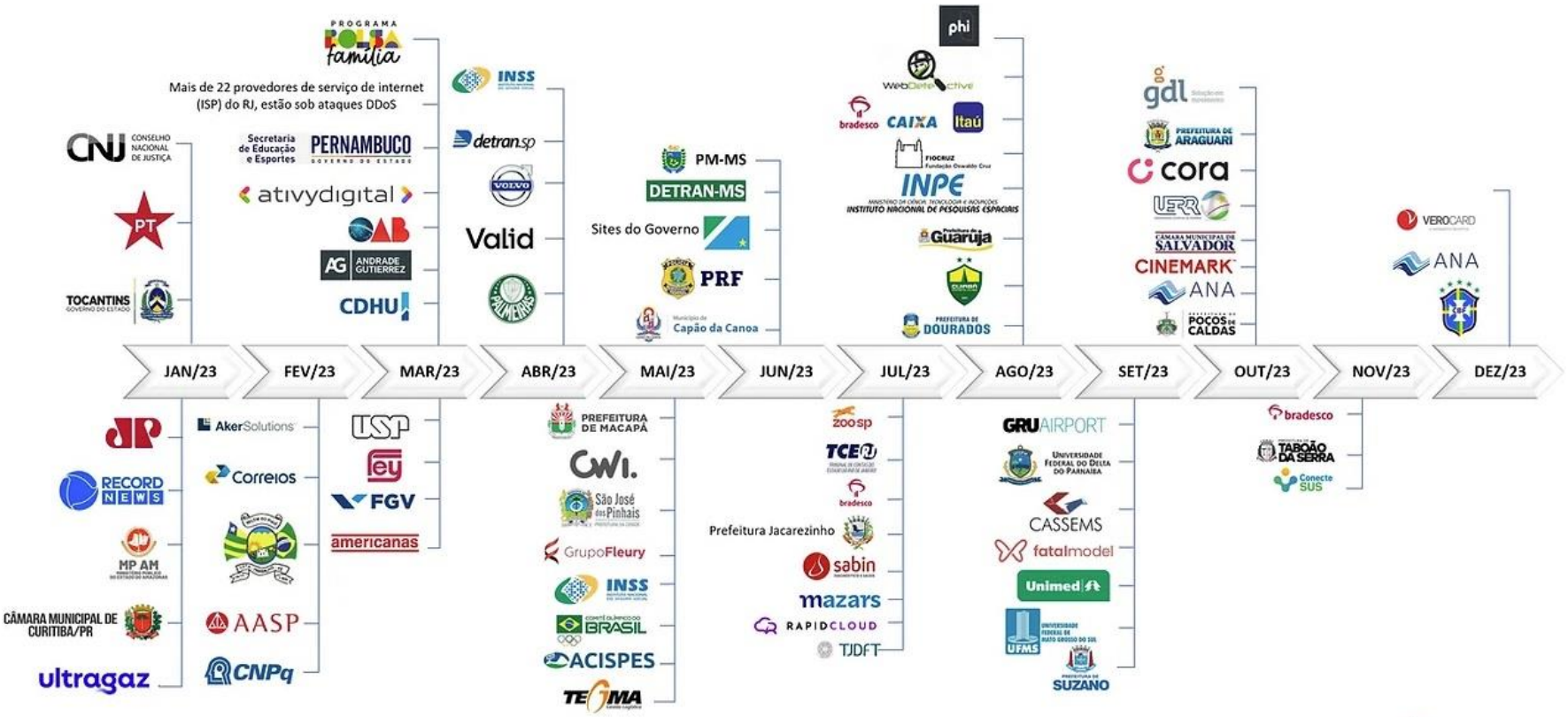
- Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade

Security REPORT

IBRASPD

INCIDENTES COM REPERCUSSÃO NA MÍDIA - BRASIL (2023)

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



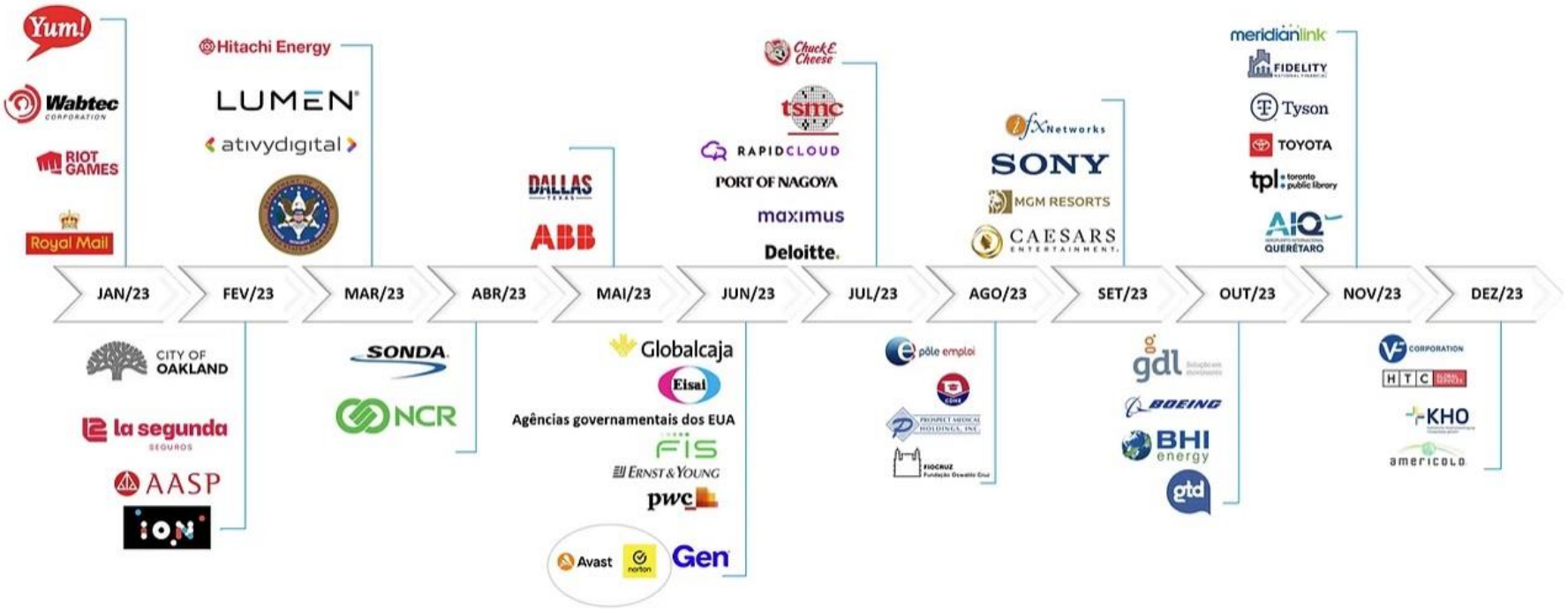
- Casos Divulgados pela mídia, onde houve o comprometimento de um dos pilares da CID: Confidencialidade, Integridade ou Disponibilidade

Security REPORT

IBRASPD

RANSOMWARE COM REPERCUSSÃO NA MÍDIA (2023)

Contexto Atual – RANSOMWARE com repercussão na mídia*



- Casos Divulgados

Security REPORT

IBRASPD

RANSOMWARE COM REPERCUSSÃO NA MÍDIA (2023)

Vazamentos de dados pessoais com repercussão na mídia*

- Casos Divulgados

Security REPORT

IBRASPD

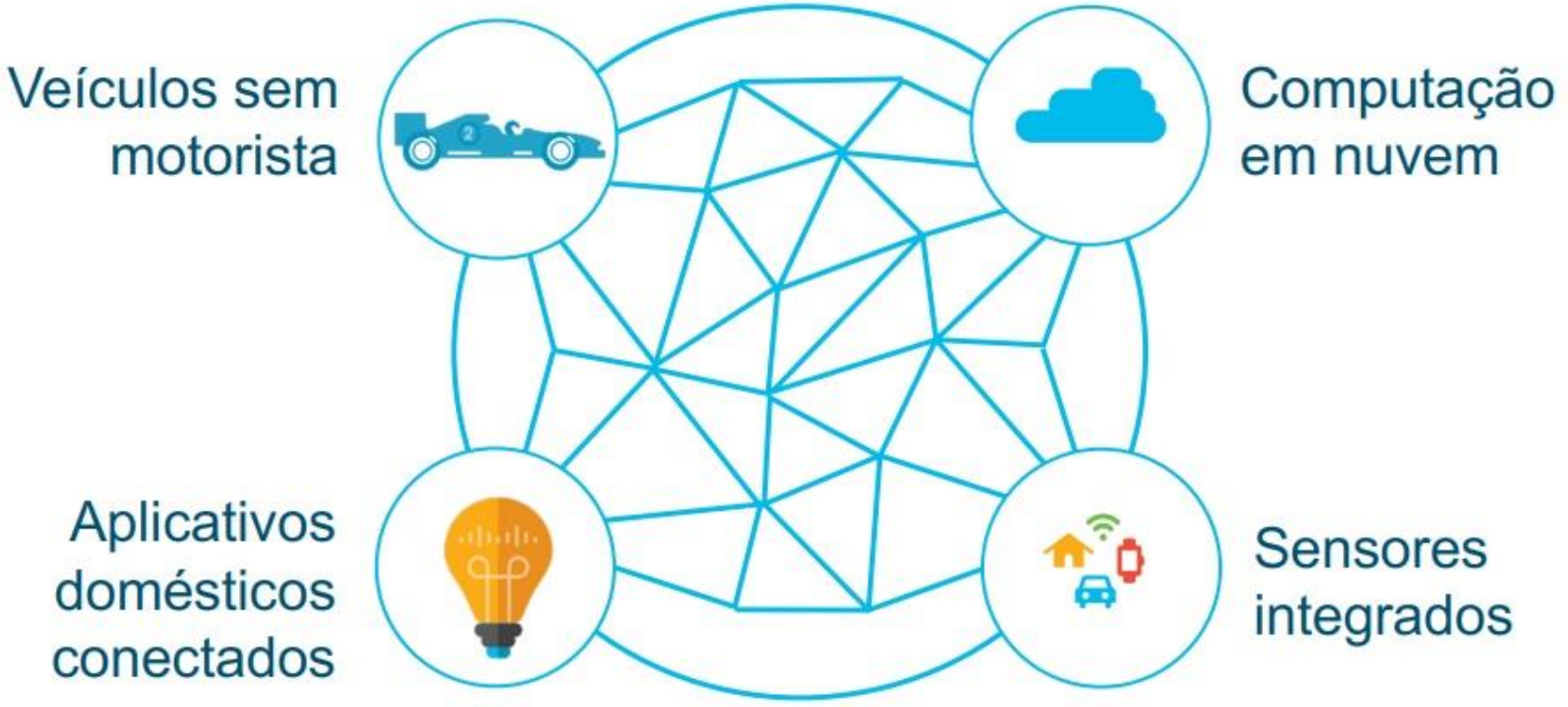
AMEAÇA, VULNERABILIDADE E RISCOS

- **Ameaça**
  - Perigo potencial para um ativo, como dados ou a rede.
- **Vulnerabilidade**
  - Fraqueza em um sistema que pode ser explorado por uma ameaça.
- **Exploit**
  - Código malicioso que explora uma vulnerabilidade.
- **Risco**
  - Probabilidade de uma ameaça explorar uma vulnerabilidade de um ativo e resultar em uma conseqüência indesejável.
- **Termos**
  - Payload/shell code: é parte de um exploit que realiza uma ação maliciosa (adduser, shell)
  - Zero day: falha descoberta antes de existir um patch para a vulnerabilidade (bugbounty)
  - Backdoor: método que permite o acesso não autorizado
  - DoS (Denial of Service): ataque de negação de serviço.

ONDE ESTÃO AS VULNERABILIDADES

- Sistemas Operacionais
- Softwares/programas
- Servidores/hosts
- Insfraestrutura
- Redes de Computadores
- Redes Wireless
- Aplicações WEB
- Aplicativos Mobile
- Internet of Things (IoT)
- Hardware
- Local físico
- Pessoas

ONDE ESTÃO AS VULNERABILIDADES



VISÃO GERAL DE MERCADO

- O mercado latino-americano de **segurança cibernética** foi avaliado em **US$ 5,26 bilhões em 2020**, e espera crescer registrando um CAGR de 10,8% durante o período de previsão (2021-2026). Com o recente surto da pandemia de COVID-19, as organizações em todo o mundo devem responder proativamente às ameaças cibernéticas que testemunharam um aumento durante a pandemia. Por conta disso, a resiliência cibernética, que se refere à capacidade de um setor ou organização de responder, se preparar e se recuperar de ataques cibernéticos, tornou-se uma necessidade absoluta e não uma opção no cenário atual.

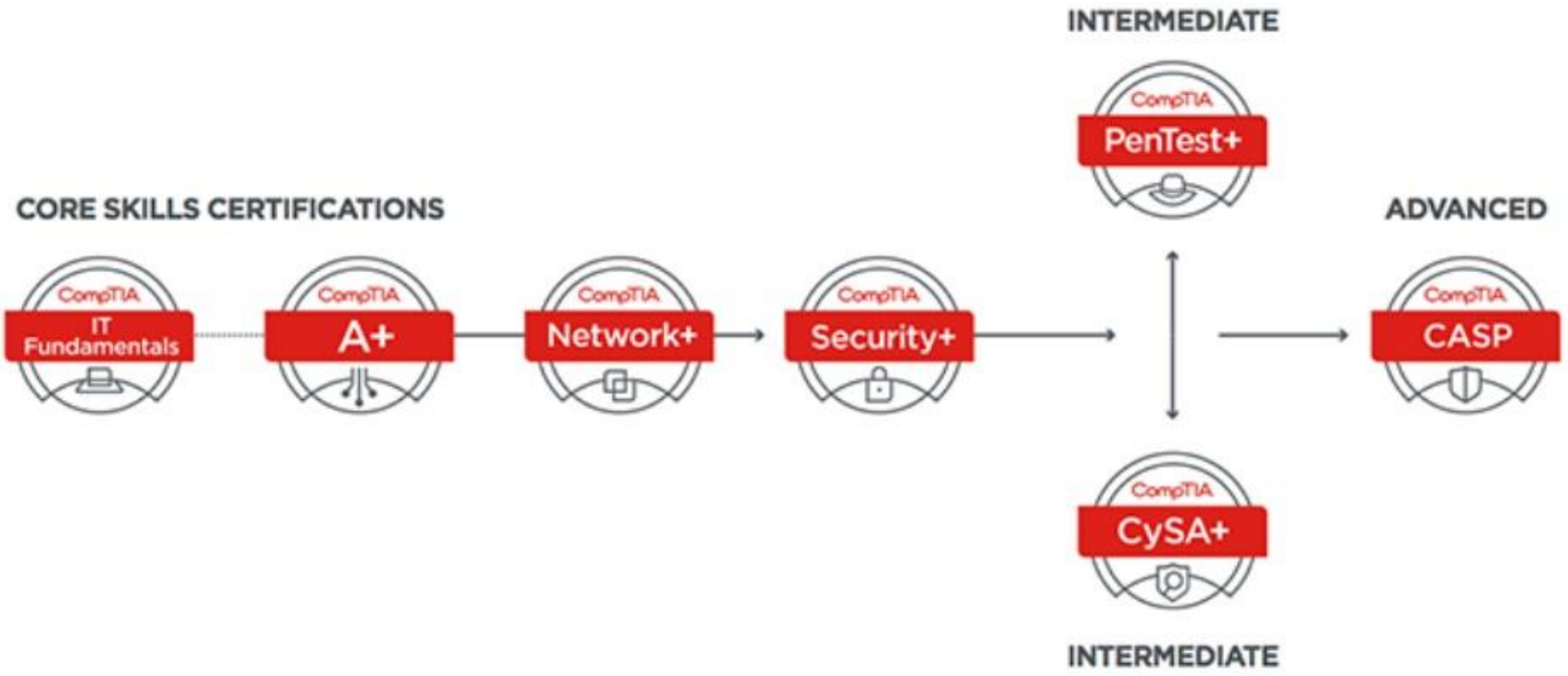
Fonte: https://www.mordorintelligence.com/industry-reports/latin-america-cyber-security-market

VISÃO GERAL DE MERCADO

- A adoção de soluções de segurança cibernética deverá crescer com a crescente penetração da internet entre os países da **América Latina**. Além disso, a **expansão da rede sem fio para dispositivos móveis** aumentou a vulnerabilidade dos dados, tornando a segurança cibernética uma parte integrante de todas as organizações da América Latina. Os incidentes crescentes de ataques cibernéticos e as regulamentações que exigem relatórios estão impulsionando o crescimento do mercado de segurança cibernética na América Latina.
- O **Brasil** é uma das economias emergentes com **crescente investimento em infraestrutura de TI e crescente penetração de smartphones e internet**. Embora o país esteja se movendo em direção às TIC avançadas, faltam medidas adequadas de segurança cibernética, devido às quais os hackers estão encontrando vulnerabilidades para explorar. Portanto, as crescentes conexões IoT estão fortalecendo a demanda por soluções de segurança cibernética.
- No entanto, a **falta de profissão de segurança cibernética** tem sido um fator preocupante, limitando o crescimento do mercado de segurança cibernética na América Latina.

Fonte: https://www.mordorintelligence.com/industry-reports/latin-america-cyber-security-market

CAMINHOS DE CERTIFICAÇÃO

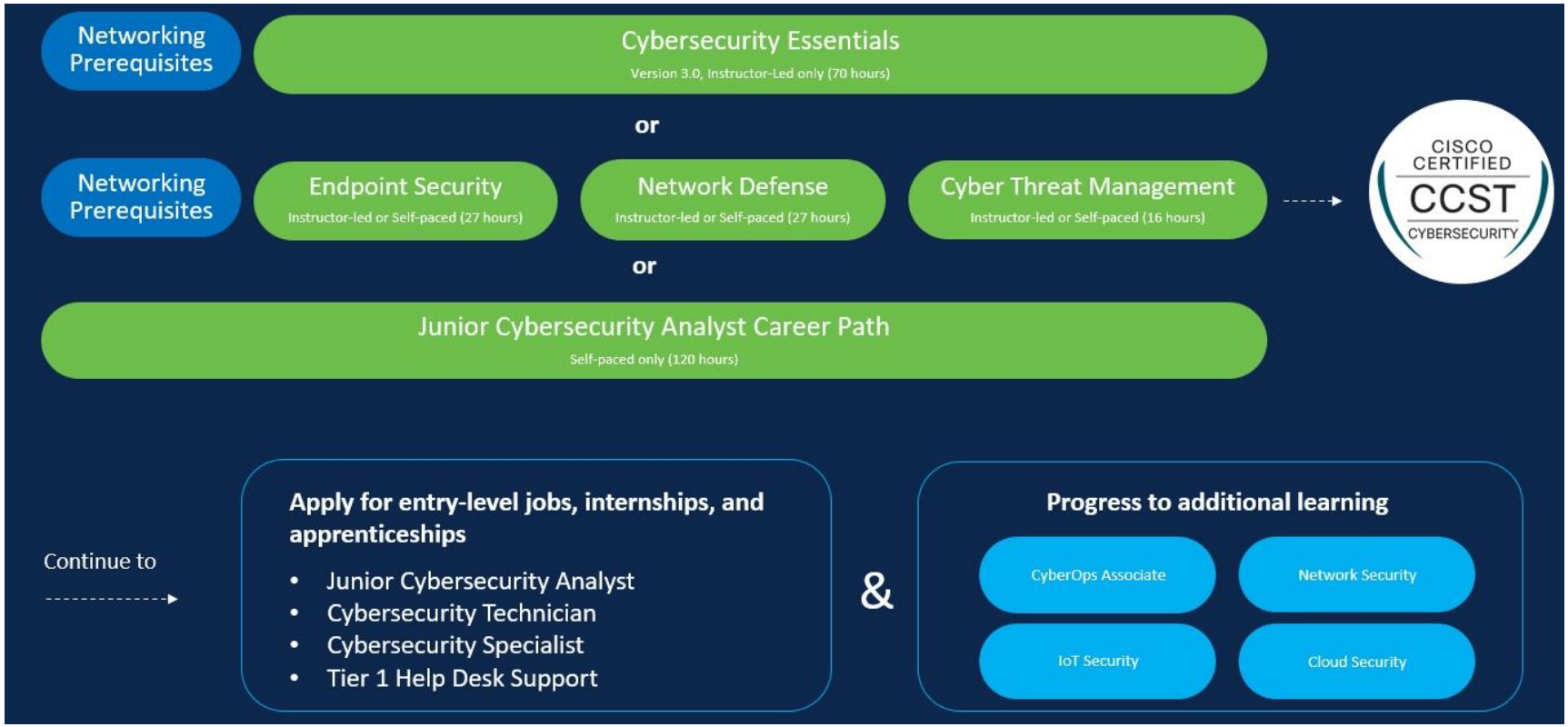


Fonte: https://www.comptia.org/pt/certificacoes

CAMINHOS DE CERTIFICAÇÃO

Fonte: https://www.cisco.com/c/dam/en_us/training-events/certifications/career-path.pdf

CAMINHOS DE CERTIFICAÇÃO



Fonte: https://www.cisco.com/c/dam/en_us/training-events/certifications/career-path.pdf

CAMINHOS DE CERTIFICAÇÃO

Fonte: https://certiport.pearsonvue.com/Certifications/Cisco/Certified-Support-Technician/Overview.aspx

PROFISSIONAIS X CRIMINOSOS

- **Profissional de Segurança da Informação:** ajuda a proteger as informações garantindo confidencialidade, integridade e disponibilidade, assim como reduzir os riscos.
- **Áreas de atuação:**
  - Segurança defensiva
  - Segurança ofensiva
  - Investigação
  - Monitoramento
  - Pesquisa
  - Gestão da Segurança da Informação
  - Análise de Malware

PROFISSIONAIS X CRIMINOSOS

- **White Hat**
  - Excelentes conhecimentos
  - Ético
  - Não viola leis
  - Definições (White Hat, Hacker, Ethical Hacker, Pentester)

- **Black Hat**
  - Excelentes conhecimentos
  - Não é Ético
  - Viola leis e comete crimes
  - Definições (Black Hat, Cracker, Hacker Malicioso, Criminoso)

ÉTICA EM SEGURANÇA CIBERNÉTICA

- **Ética de um especialista em segurança cibernética**
  - A ética é um "sussurro" que orienta um especialista em segurança cibernética sobre o que ele deve ou não fazer, independentemente de ser lícito. A empresa confia ao especialista em segurança os dados e recursos mais confidenciais. O especialista em segurança cibernética precisa compreender como a lei e os interesses da empresa ajudam a orientar as decisões éticas.
- **Computer Ethics Institute**
  - O Computer Ethics Institute é um recurso para identificar, avaliar e responder aos problemas éticos em todo o setor de tecnologia da informação. O CEI foi uma das primeiras empresas a reconhecer os problemas de políticas éticas e públicas provenientes do crescimento rápido da área de tecnologia da informação.
    - http://cpsr.org/issues/ethics/cei/

ÉTICA EM SEGURANÇA CIBERNÉTICA

- Honra e dever. Eles são partes fundamentais de uma carreira em segurança da informação. E são partes fundamentais de ser membro de um (ISC) ².
- **Critérios do Código de Ética (ISC2):**
  - Proteger a sociedade, o bem comum, a confiança pública necessária e a infraestrutura.
  - Agir de forma honrosa, honesta, justa, responsável e legal.
  - Fornecer serviço diligente e competente aos diretores.
  - Avançar e proteger a profissão.
  - https://www.isc2.org/Ethics#

LEGISLAÇÃO BRASILEIRA DE CRIMES CIBERNÉTICOS

- **Lei Carolina Dieckmann – 12737**
  - **“Invasão de dispositivo informático: Art. 154-A”**. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
  - Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
  - http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12737.htm

LEGISLAÇÃO BRASILEIRA DE CRIMES CIBERNÉTICOS

- **Lei Marco Civil da Internet – 12965**
  - Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.
  - Regula o uso da Internet (Provedores devem manter o histórico de acesso dos usuários por pelo menos 6 meses).
  - http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm
- **Lei Geral de Proteção de Dados (LGPD) – 13709**
  - Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
  - Transparência no uso e armazenamento dos dados.
  - http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

APLICAÇÕES USANDO CRIPTOGRAFIA

- Comunicações seguras:
  - Tráfego Web: https;
  - Tráfego wireless;
- Criptografia em disco, Servidores, Banco de Dados;
- Criptografia no TCP/IP:
  - Camada de rede (IPSec);
  - Camada de transporte (SSL, TLS);
  - Camada de aplicação (PGP, ssh, https).

BIBLIOGRAFIA

- PTES – Penetration Testing Execution Standard. Disponível em: <http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines>. Acesso em: 03.08.2024.
- CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes. Disponível em: <https://www.cert.br/stats/incidentes>. Acesso em: 03.08.2024.
- ISC. Ethics Committee Members. Disponível em: <https://www.isc2.org/Ethics#> Acesso em: Acesso em: 03.08.2024.
- LGPD. Lei Geral de Proteção de Dados. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: Acesso em: 03.08.2024.
- IBRASPD – Instituto Brasileiro de Segurança, Proteção e Privacidade de Dados. <https://www.ibraspd.org/incidentes>. Acesso em: 03.08.2024.

BIBLIOGRAFIA

- SECURITYREPORT – Painel de Incidentes Cibernéticos. <https://www.securityreport.com.br/email/InfoSR2023.html>. Acesso em: 03.08.2024.
- CISCO. Segurança Cibernética. Disponível em: <https://skillsforall.com>. Acesso em: 03.08.2024.
- CERTIPORT. Caminho de Certificação CCST. Disponível em: <https://certiport.pearsonvue.com/Certifications/Cisco/Certified-Support-Technician/Overview.aspx> . Acesso em: 03.08.2024.
- Notas de aula.