



Crimes Digitais

Pedro Lucas Damasceno
Robson Novato

Tabela de conteúdos

01

Contexto

Mundo interconectado e dependente da tecnologia

02

Impactos

Comprometimento da confiança, privacidade e segurança

03

Exemplos

Phishing, ransomware, DDoS, hacking

04

Conclusão


Adaptação jurídica e métodos preventivos



01

Contexto

Em um mundo digital
interconectado, os crimes
cibernéticos infiltram-se
sorrateiramente, corroendo a
confiança, roubando privacidade e
ameaçando a essência da sociedade
moderna



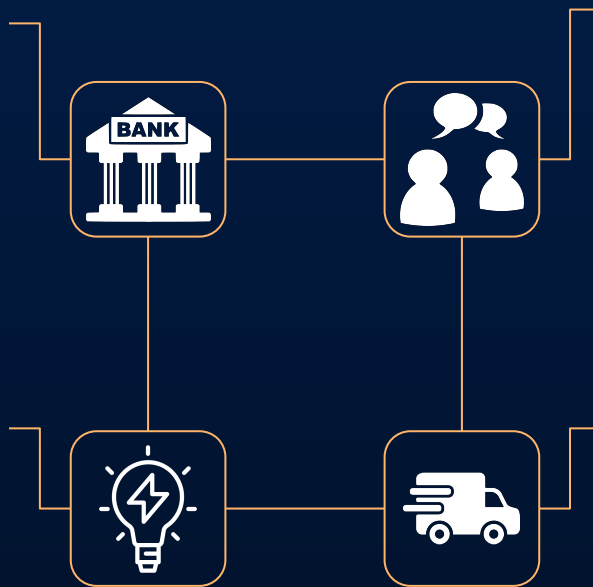
Dependência tecnológica

Financeiro

Transações, processar pagamentos, monitorar riscos e garantir a segurança das operações financeiras

Energia

Monitorar, controlar e otimizar a produção, distribuição e consumo de energia



Comunicações

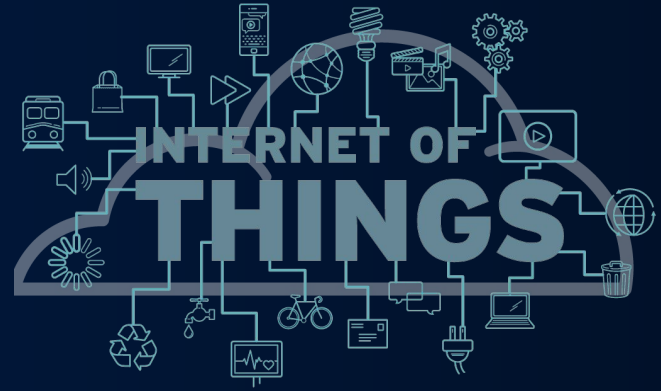
Redes de telefonia, internet, serviços de streaming e mídias sociais interligando pessoas e empresas

Transporte

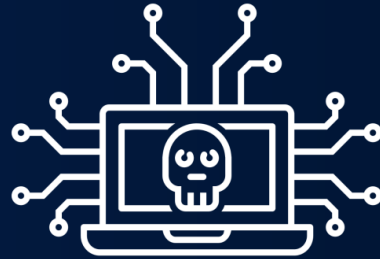
Rastreamento, gerenciamento de frota, sistemas de navegação GPS

IoT

- Conectividade
- Escalabilidade constante
- Coleta de dados em tempo real e automação



O que são crimes digitais?



Uso ilegal de tecnologia da informação e comunicação para realizar atividades ilícitas, como roubo de informações, fraude, invasões, difamação, entre outros.

Contexto tecnológico e social



Anonimato

Identities falsas,
VPNs



Jurisdição

Cruzamento de
fronteiras geográficas



Complexidade

Malwares sofisticados
e criptografia



Avanço tecnológico



Novos desafios, uma vez
que os criminosos digitais
podem explorar novas
vulnerabilidades e utilizar
técnicas avançadas

Ocorrência de crimes digitais

2021 - Brasil chega ao 2º lugar dos países mais que mais sofreram ataques virtuais criminosos na América Latina e Caribe, de acordo com levantamento feito pela Fortinet Threat Intelligence Insider Latin America.

88,5 bilhões de tentativas de ataques cibernéticos em 2021, um aumento de mais de 950% com relação a 2020.

Somente nos primeiros três meses de 2022, a procura por seguros cibernéticos cresceu 41,5% quando comparado com o mesmo período do ano passado

 **BRAZIL** 


2 MOST-ATTACKED COUNTRY

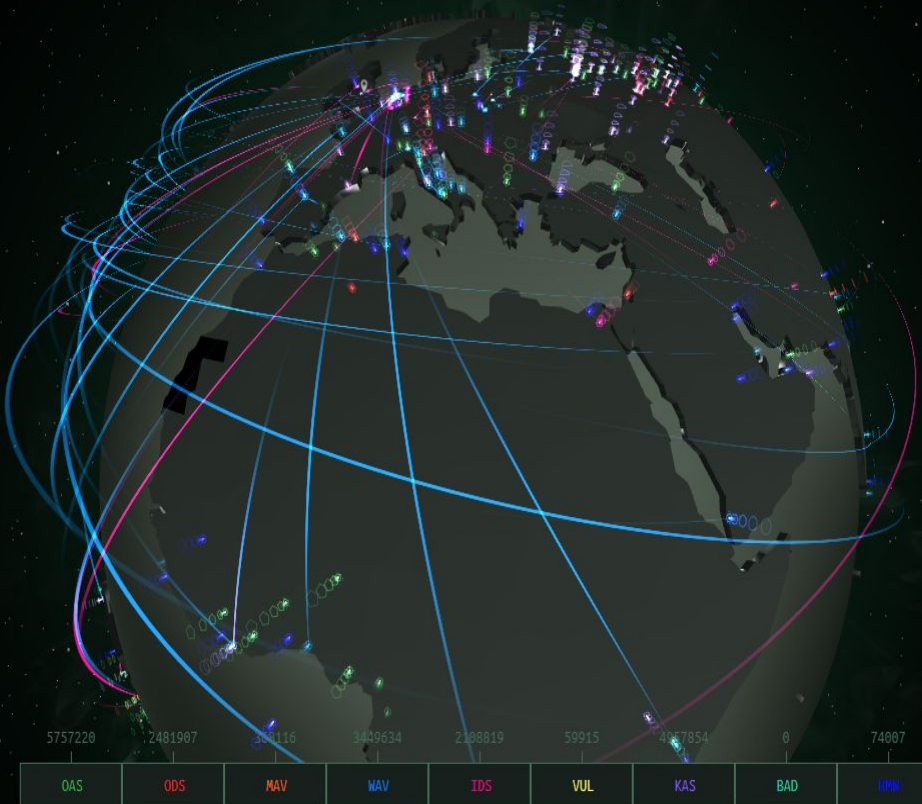
OAS	825864
ODS	129672
NAV	7895
NAV	141419
IDS	221274
VUL	2698
KAS	75328
BAD	0
BWV	3457

Detections discovered since 00:00 GMT

[More details](#)

Share data



Jurisdição brasileira

Lei	Descrição
Marco Civil da Internet (Lei nº 12.965/2014)	Estabeleceu princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Ela aborda questões como neutralidade de rede, privacidade, proteção de dados pessoais e responsabilidade dos provedores de Internet.
Lei Geral de Proteção de Dados (Lei nº 13.709/2018)	Estabeleceu regras para o tratamento de dados pessoais por empresas e organizações. Ela garante aos indivíduos o direito à privacidade e ao controle sobre suas informações pessoais.
Lei Carolina Dieckmann (Lei nº 12.737/2012)	Tipifica como crime a invasão de dispositivos eletrônicos e a divulgação não autorizada de conteúdo íntimo na Internet

Jurisdição brasileira

- **Estrutura e capacidade de investigação:** O Estado brasileiro ainda enfrenta desafios em termos de estrutura e capacidade para lidar com investigações de crimes digitais. A falta de especialização e treinamento adequado dos agentes responsáveis pelas investigações pode dificultar a identificação e a responsabilização dos criminosos.
- **Cooperação internacional:** Muitos crimes digitais têm alcance transnacional, o que exige uma cooperação eficiente com outros países para investigação e responsabilização dos infratores. No entanto, a cooperação internacional nesse contexto nem sempre é fácil de ser alcançada, devido a barreiras jurídicas, burocráticas e culturais. Essa falta de cooperação pode dificultar o combate efetivo aos crimes digitais.
- **Conscientização e educação:** A falta de conscientização e educação adequada sobre segurança digital e crimes cibernéticos também é uma falha significativa. Muitas pessoas não possuem conhecimento suficiente sobre as ameaças online e as melhores práticas de segurança, o que pode torná-las mais vulneráveis a ataques. Investir em programas de conscientização e educação é fundamental para mitigar essas vulnerabilidades.
- **Dificuldades na obtenção de provas:** A coleta de evidências digitais muitas vezes é complexa e requer expertise técnica. A obtenção de provas digitalmente armazenadas, como registros de comunicação, logs de servidores e dados em nuvem, pode ser um desafio, especialmente quando envolve provedores de serviços estrangeiros. A falta de mecanismos eficientes para obtenção e preservação de provas digitais pode dificultar a investigação e o processo judicial.



02

Impactos

Impactos na sociedade

Perda financeira

Roubos de informações pessoais, fraudes bancárias, ataques a sistemas de pagamento e extorsões online

Violência e intimidação

Bullying virtual, assédio online e ameaças, causando danos psicológicos e emocionais às vítimas

Danos à reputação

Ataques cibernéticos, como vazamentos de dados, podem expor informações confidenciais e sensíveis, causando danos irreparáveis



Desconfiança na internet

Aumento da desconfiança das pessoas em relação à internet.

Desafios legais e jurídicos

Dificuldade da aplicação da lei, uma vez que os criminosos podem operar em jurisdições diferentes.

Necessidade de segurança digital aprimorada

Exigindo investimentos significativos em tecnologia e treinamento

Perda *financeira*

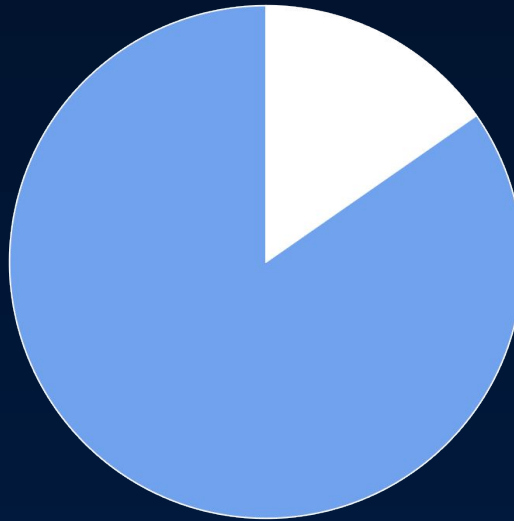
- Roubo de informações financeiras: Um dos principais objetivos dos cibercriminosos é obter informações financeiras confidenciais, como números de cartões de crédito, senhas de contas bancárias e detalhes de contas online.
- Fraude bancária: Os criminosos digitais frequentemente criam esquemas sofisticados de phishing, que são e-mails falsos e sites que imitam instituições financeiras legítimas.
- Custos de recuperação e prevenção: Além das perdas financeiras diretas causadas pelo crime digital, as vítimas também precisam investir recursos financeiros para recuperar dados perdidos.

Desconfiança na internet

15,32%
Fraudulentas



Transações no
e-commerce mundial
foram potencialmente
fraudulentas



84,68%
Reais



Transações reais

Fonte: TransUnion

Violência e *intimidação*

- Bullying virtual: O cyberbullying envolve a prática de assediar, ameaçar, humilhar ou ridicularizar outras pessoas através da internet ou de dispositivos eletrônicos.
- Assédio online: O assédio online pode assumir várias formas, incluindo mensagens ameaçadoras, comentários ofensivos e disseminação de informações privadas para difamar ou envergonhar uma pessoa.
- Grooming: O grooming é um método utilizado por predadores online para ganhar a confiança de crianças e adolescentes com o objetivo de explorá-los sexualmente, coletar informações pessoais ou envolvê-los em atividades ilegais.

Desafios legais e jurídicos

1996



Lei dos Crimes Informáticos
(Lei nº 9.296/1996)

Disposições relacionadas à interceptação de comunicações telefônicas como meio de obtenção de prova em investigações criminais.

2012



Marco Civil da Internet (Lei nº 12.965/2014)

Legislação abrangente que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil.

2012



Lei Carolina Dieckmann (Lei nº 12.737/2012)

Tipificou o crime de invasão de dispositivos eletrônicos para obtenção, adulteração ou destruição de dados sem autorização do titular.

2018



Lei de Proteção de Dados Pessoais (Lei nº 13.709/2018)

Estabelece regras sobre o tratamento de dados pessoais, responsabilidades das empresas e penalidades por violações.

Necessidade de segurança digital

aprimorada

- Preservação da reputação: Para empresas e organizações, uma violação de segurança cibernética pode resultar em danos significativos à reputação. A perda de confiança dos clientes e parceiros de negócios pode ter efeitos devastadores e duradouros.
- Defesa contra ciberspionagem e ciberataques governamentais: Governos e organizações estão em risco de ciberspionagem e ciberataques promovidos por outros países. Reforçar a segurança digital é fundamental para proteger informações sensíveis, segredos comerciais e interesses nacionais.
- Conformidade com regulamentações: Muitos setores estão sujeitos a regulamentações rigorosas de segurança cibernética. O aprimoramento da segurança digital é essencial para garantir a conformidade com essas leis e padrões.

Danos a reputação

China

Ciberspionagem e roubo de propriedade intelectual.

Estados Unidos

Stuxnet, um worm de computador descoberto em 2010, que foi aparentemente projetado para atacar o programa nuclear do Irã



Rússia

Interferência em eleições estrangeiras e ciberataques a infraestruturas críticas de outros países.

Coreia do Norte

Vinculada a ataques cibernéticos em larga escala, como o ataque ao estúdio de cinema Sony Pictures em 2014.

03

Exemplos

Phishing

A fatura falhou - conta bloqueada

NETFLIX

Oi [REDACTED]


Estamos tendo problemas com suas informações de faturamento atuais. Tentaremos novamente, mas por enquanto você pode atualizar seu MASTERCARD em seus detalhes de pagamento.

ATUALIZAR CONTA AGORA

Estamos aqui para ajudar quando você precisar. Visite a Central de Ajuda para mais informações ou entre em contato conosco .

Seus amigos no Netflix

Phishing

From: GlobalPay <VT@globalpay.com> 
Subject: Restore your account
Date: February 7, 2014 3:47:02 AM MST
To: David

[Hide](#)

1 Attachment, 7 KB

Save ▼

Quick Look

Dear customer,

We regret to inform you that your account has been restricted.

To continue using our services please download the file attached to this e-mail and update your login information.

© GlobalPaymentsInc



[update2816.html \(7 KB\)](#)

Ransomware

Renner sofre ataque de ransomware

A Renner sofreu um ataque de ransomware nesta quinta-feira, 19, que tirou do ar o seu sistema de e-commerce. A empresa confirmou o ataque em um fato relevante divulgado ao mercado.

Informações não oficiais dizem que a empresa acordou um pagamento de 20 milhões de dólares em criptomoedas, após uma negociação para reduzir a quantia de 1 bilhão de reais. Contudo, a Renner, em comunicado, negou a informação de que teria pago US\$20 milhões aos hackers.

Fonte:

<https://exame.com/tecnologia/renner-sofre-ataque-de-ransomware-e-sistemas-da-empresa-ficam-fora-do-ar/>

Ransomware

“Prisão” de hóspedes no hotel Romantik Seehotel Jägerwirt

Entre 2016 e 2017, o hotel de luxo Romantik Seehotel Jägerwirt, na Áustria, sofreu três ataques de ransomware. Dentre eles, o último entrou para a história: na ocasião, foi atingido o sistema de fechaduras inteligentes das portas dos quartos dos hóspedes, assim como o acesso à seção administrativa do hotel.

Para liberar os dados necessários, os hackers demandaram o resgate de 1500 euros em bitcoins . Diante da urgência e dos clientes “presos”, o hotel arcou com o pagamento, buscando reduzir os prejuízos.

Fonte: <https://backupgarantido.com.br/blog/exemplos-de-ransomware/>

Propriedade intelectual

SCI-HUB

...to remove all barriers in the way of science

Acesso gratuito a milhões de artigos de pesquisa,
sem levar em consideração os direitos autorais,
contornando as barreiras das editoras de diversas
maneiras

Propriedade intelectual



Compartilhamento de mídia através de torrent

Propriedade intelectual

DE/NUVO
X

EMPRESS

Violação de DRM em jogos eletrônicos

Outros exemplos

- Disseminação de vírus, malware, keylogger
- *Cryptojacking* (invasão de computadores para mineração de criptomoedas)
- Interrupção ou perturbação em sites ou perfis para disseminar mensagens difamatórias ou insultos dirigidos a empresas ou pessoas
- Golpes e fraudes realizados por meios de redes sociais, anúncios falsos, Whatsapp, entre outros

E as *fake news*?

- “Criar e compartilhar fake news, desinformação, não é um crime em si no Brasil. Se você postar uma mentira na internet, você não está cometendo um crime naquele momento, mas, dependendo da mentira, do dano que ela causa, do contexto, ele pode ser enquadrado em outros crimes” - Francisco Brito Cruz, diretor do InternetLab, centro de pesquisa em direito e tecnologia.



Conclusão

04

Normas ISO

Documentos estabelecidos por consenso e aprovado por um organismo reconhecido, que fornece, para uso comum e repetitivo, regras, diretrizes ou características para atividades ou seus resultados, visando a obtenção de alto grau de ordenação em um dado contexto.



Normas ISO

ISO 27001 - Especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão

da segurança da informação dentro do contexto da organização;

ISO 27002 - A norma ISO/IEC 27002:2022 fornece um conjunto abrangente de controles de segurança da informação comumente utilizados, incluindo orientação para implementação desses controles em uma organização, é complementar à 27001 e totalmente indispensável à sua aplicação;

ISO 27005 - Fornece diretrizes para o estabelecimento de uma abordagem sistemática para o gerenciamento de riscos da Segurança da Informação;

ISO 27035 - Fornece diretrizes para gestão e operação de resposta a incidentes de TI;

ISO 27701 - A norma ISO 27701 especifica quais são os requisitos e fornece diretrizes para o estabelecimento, implementação, manutenção e melhoria contínua de um sistema de Gestão de Privacidade da Informação;

ISO 22301 - É uma norma para GCN (Gestão de Continuidade de Negócios) que permite identificar possíveis ameaças e quais as funções críticas de negócio poderão ser afetadas causando interrupções para o negócio;

CIS Controls

Desenvolvido pelo Center for Internet Security® (CIS), publicado oficialmente em 2013, os CIS Controls são um conjunto prioritário e prescritivo de práticas recomendadas de segurança cibernética, e ações defensivas que podem ajudar a prevenir os principais ataques cibernéticos conhecidos.

O CIS Controls foi criado para estabelecer um padrão mínimo dentro da gestão de Segurança da Informação para empresas privadas nos EUA, especificamente aquelas com a intenção de fornecer seus produtos e serviços ao governo americano. Com o tempo, passou a ser um dos padrões mais aceitos no mercado mundial em termos de padronização de procedimentos em SI.

De forma estrutural, os CIS Controls são compostos por 18 (V8) recomendações divididas em três categorias diferentes de subcontroles:

- **Básico**: controles que garantem a prontidão da defesa virtual, como inventários, manutenção, monitoramento e privilégios administrativos;
- **Essencial**: combatem ameaças técnicas mais específicas e que precisam de atenção especial, sejam dados, perímetro, acesso wi-fi e contas;
- **Organizacional**: ao contrário dos anteriores, seu foco não é em questões técnicas, mas nas pessoas e processos da organização. Essas práticas garantem a maturidade da segurança a longo prazo.

Processo de *hardening*

Processo de tornar seus sistemas, redes, softwares, hardwares e firmwares, bem como infraestruturas de TI mais resistentes a ataques.

Consiste em fazer a implementação de senhas seguras, remoção de serviços desnecessários, protocolos inseguros e aplicação de pacotes atualizados.

Ferramentas de teste

NMAP

Com essa poderosa ferramenta conseguimos identificar serviços executando em um ativo e até mesmo atacá-los.



Metasploit

O Metasploit é um dos frameworks de teste de penetração mais populares do mundo. Nele é possível executar exploits contra um server vulnerável e explorá-lo.



Ferramentas de teste

Hydra

Basicamente o Hydra descobre senha através de Brute Force (tentativa e erro), ele busca em wordlists possíveis usuários/senhas e vai testando as combinações, uma a uma. O Hydra tem suporte aos serviços Telnet, Formulário HTTP/HTTPS, SSH, MySQL, PostgreSQL, MSSQL, SMB, LDAP, FTP, SNMP, CVS, VNC, entre outros.



Educação digital dos *usuários*

- Reconhecer domínios falsos e/ou possíveis fraudes
- Manutenção de senhas seguras
- Manter sistema operacional e softwares constantemente atualizados
- Uso responsável das redes sociais
- Realizar backup de dados regularmente
- Prudência ao baixar e abrir arquivos

Obrigado!

Perguntas?



- GOUVÊA, Sandra. O direito na era digital: crimes praticados por meio da informática. Mauad Editora Ltda, 1997.
- GOGOLIN, Greg. The digital crime tsunami. Digital investigation, v. 7, n. 1-2, p. 3-8, 2010.
- BARRETT, Neil. Digital crime: Policing the cybernation. London: Kogan Page, 1997
- TransUnion