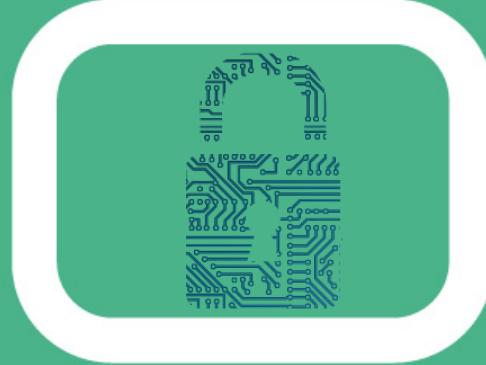


“Tudo o que entra na Internet, jamais sai da internet”



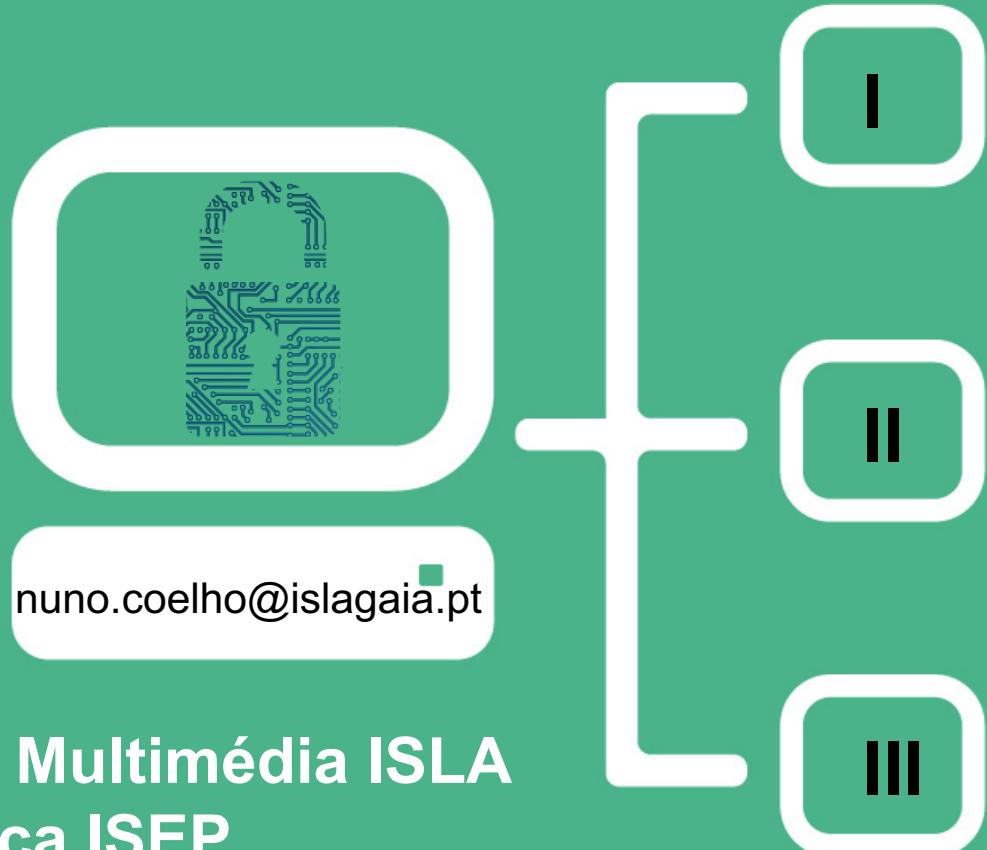
nuno.coelho@islagaia.pt



Direito da Comunicação



isla
instituto politécnico de gestão e tecnologia



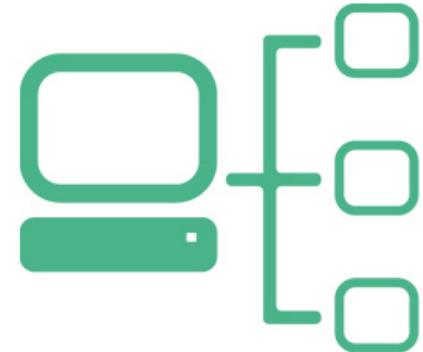
Nuno Mateus Coelho
BEng. Engenharia Sistemas Multimédia ISLA
MEng. Engenharia Informática ISEP
PhD. Informatics Researcher UTAD - UMIST

Módulo I - Constituição



isla
instituto politécnico de gestão e tecnologia

Artigo 35º Constituição



VII REVISÃO CONSTITUCIONAL [2005]

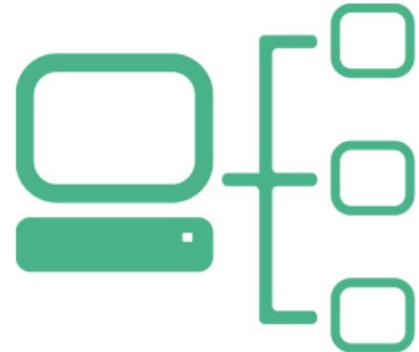
TÍTULO II

Direitos, liberdades e garantias

CAPÍTULO I

Direitos, liberdades e garantias pessoais

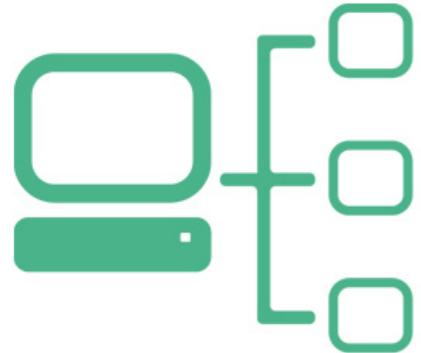
Artigo 35º Constituição



Artigo 35.º nº. 1

Utilização da informática

Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.

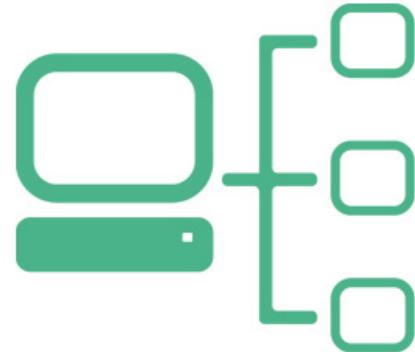


Artigo 35º Constituição

Artigo 35.º nº. 2

A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente.

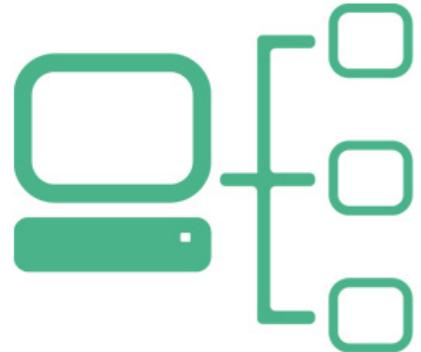
Artigo 35º Constituição



Artigo 35.º nº. 3

A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.

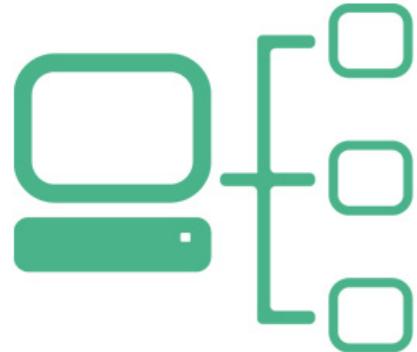
Artigo 35º Constituição



Artigo 35.º nº. 4

É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei.

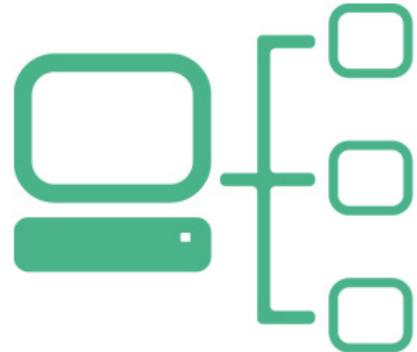
Artigo 35º Constituição



Artigo 35.º nº. 5

É proibida a atribuição de um número nacional único aos cidadãos.

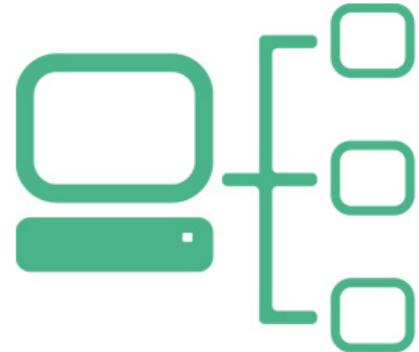
Artigo 35º Constituição



Artigo 35.º nº. 6

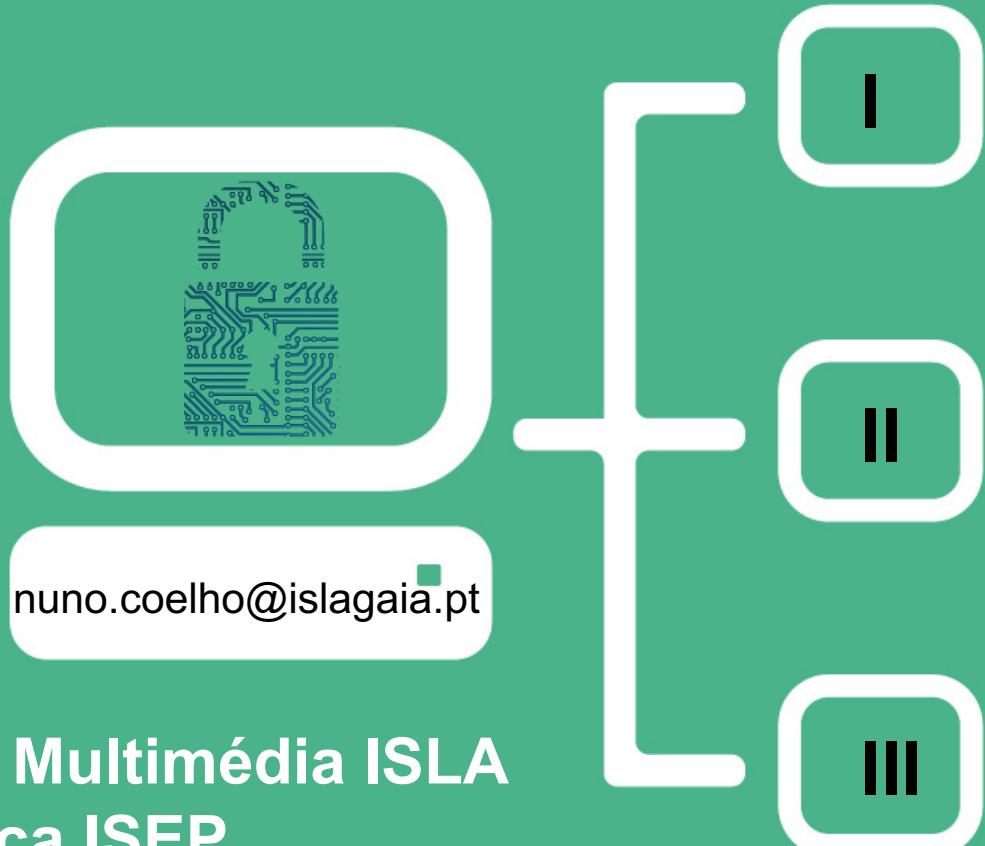
A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de proteção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.

Artigo 35º Constituição



Artigo 35.º nº. 7

Os dados pessoais constantes de ficheiros manuais gozam de proteção idêntica à prevista nos números anteriores, nos termos da lei.



Nuno Mateus Coelho

BEng. Engenharia Sistemas Multimédia ISLA

MEng. Engenharia Informática ISEP

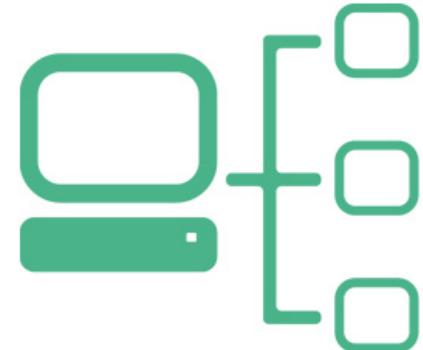
PhD. Informatics Researcher UTAD - UMIST

Módulo II - Cibercrime

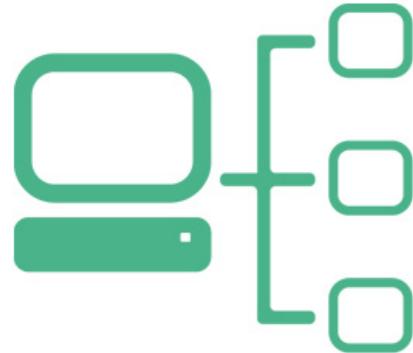


isla
instituto politécnico de gestão e tecnologia

Criminalidade Informática

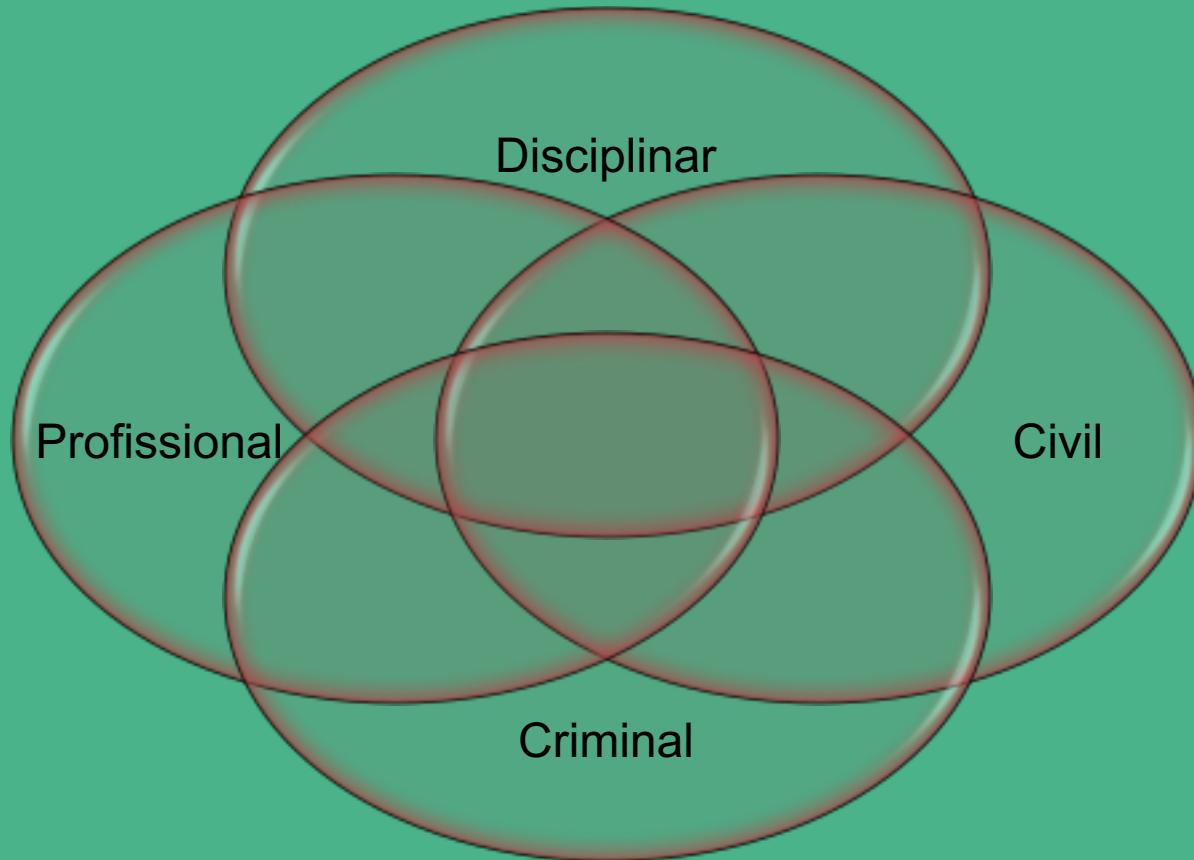


Direito Criminal

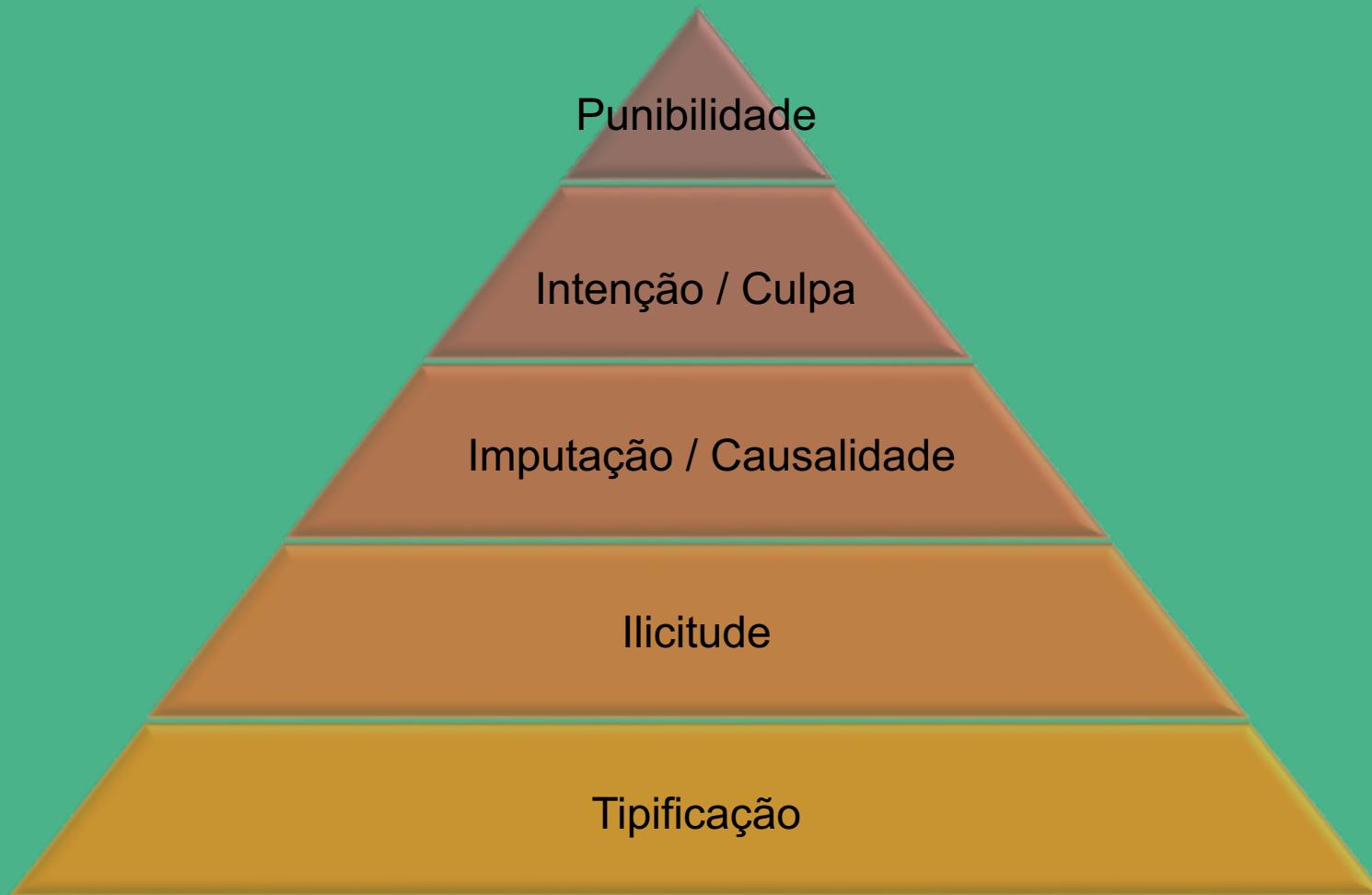
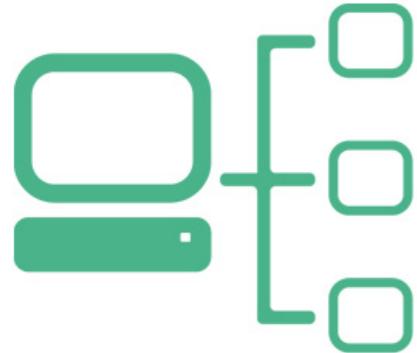


Criminalidade Informática

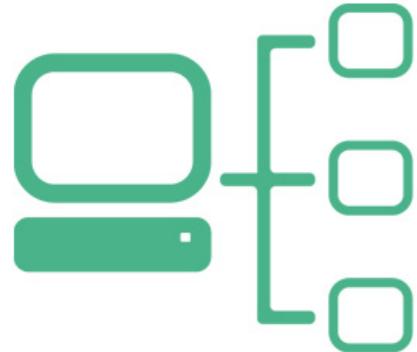
Responsabilidade



Responsabilidade criminal



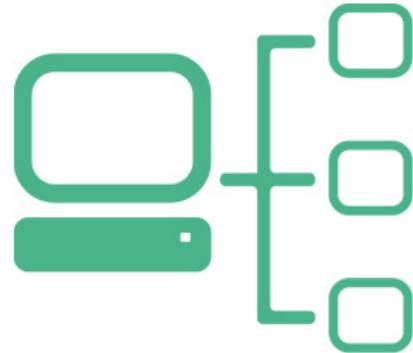
Responsabilidade criminal



Cibercrime Definição:

- Recorre a tecnologias de informação e comunicação
- Dirigido contra tecnologias de informação e comunicação
- E ainda pode usar tecnologias de informação e comunicação para a prática de outros crimes
- Todos os crimes praticados com recurso a meios informáticos

Cibercrime



Tipificação:

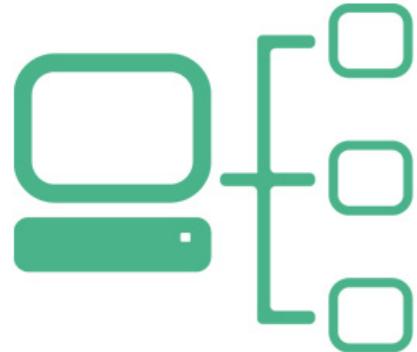
•Crimes contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos

- Acesso ilegítimo
- Interceção ilegítima
- Sabotagem informática
- Devassa por meio de Informática

•Crimes relacionados com sistemas informáticos

- Falsidade informática
- Burla informática
- Burla nas telecomunicações

Cibercrime



Tipificação:

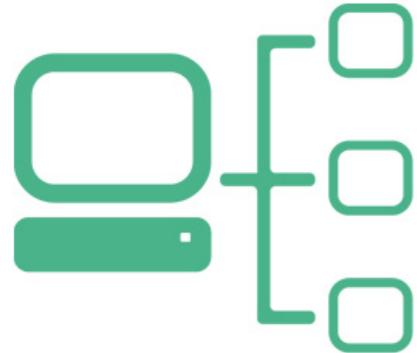
- **Crimes relacionados com o conteúdo**

- Difusão de pornografia infantil
- Falsidade informática

- **Crimes praticados contra os direitos de autor e direitos conexos**

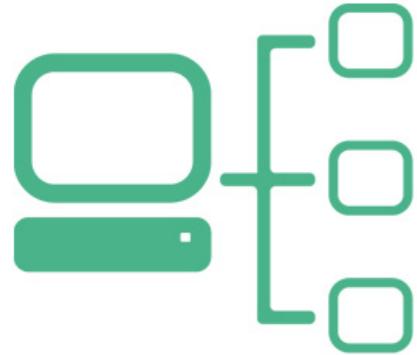
- Cópia/Reprodução ilícita/Pirata de Programas/filmes/música/obras literárias

Cibercrime



Características:

- Afetam gravemente a economia nacional
- Facilitam direta ou indiretamente outras atividades criminosas
- Apresentam dificuldades de recolha de prova -**Princípio da Territorialidade**
- Relevância da localização: onde os dados estão armazenados e como acedemos?

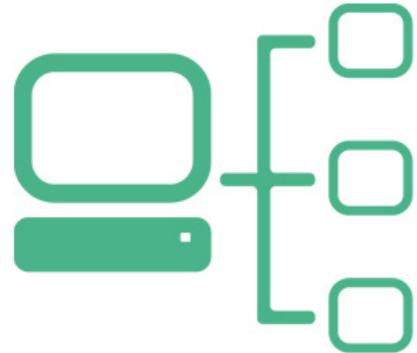


Cibercrime

Legislação Nacional:

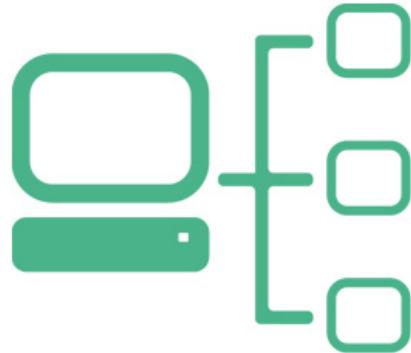
- Lei 109/09, 15/09 –Lei do Cibercrime
- Código Penal
- Lei 67/98, 26/10 –Proteção dos Dados Pessoais
- Lei 12/05, 26/01 –Dados pessoais na Saúde
- DLei252/94, 20/10 –Proteção de Software
- Dlei63/85, 14/03 (L82/13, 6/12) –Cód. Direitos Autor e Direitos Conexos
- Lei 41/04, 18/08 –Lei Proteção Dados Pessoais nas Telecomunicações
- Lei 32/08, 17/07 –Dados de Tráfego
- Dlei7/04, 7/01 –at.º 22 “Comunicações não solicitadas”
- Dlei63/09, 10/03 (Lei 177/99, 21/05), -Audiotexto
- Dlei290-D/99, 02/08 (Dlei88/09, 9/04)–Assinatura Digital
- Dlei143/01, 06/04, (Dlei57/08, Dlei82/08, Dlei317/09 e Dlei24/14, 14/02) –Fraude com cartão de crédito
- Lei 5/04, 10/02 (Lei 35/08, 28/07), Lei das Comunicações Eletrónicas

Cibercrime



- Crimes clássicos
 - Burlas, ameaças, injúrias e difamações
- Novos crimes específicos
 - Obtenção fraudulenta da identidade digital
 - Ataques contra a segurança, confidencialidade e fiabilidade dos sistemas

Cibercrime



2

THEME 1: SHOCKING SCALE: NUMBER OF VICTIMS

“**1 MILLION+** **VICTIMS A DAY**

EVERY DAY THERE ARE TWICE AS MANY CYBERCRIME VICTIMS AS NEW BORN BABIES ^{iv}



50,000

VICTIMS EVERY HOUR

hr

820

VICTIMS EVERY MINUTE

min

14

VICTIMS EVERY SECOND

sec

7 /10



69% of adults have experienced cybercrime in their lifetime. Compared to the 2010 survey, there has been a 3% rise in overall cybercrime ^v

589 MILLION

Cybercrime has affected 589m people in just 24 countries - equivalent to 9% of the entire population of the world ^{vi}



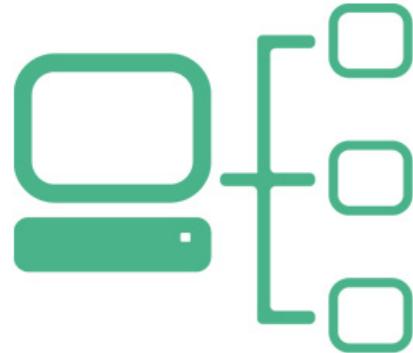
65%

Among all cybercrime victims surveyed, nearly two thirds have fallen prey in the past 12 months alone - a total of 431m adults in 24 countries

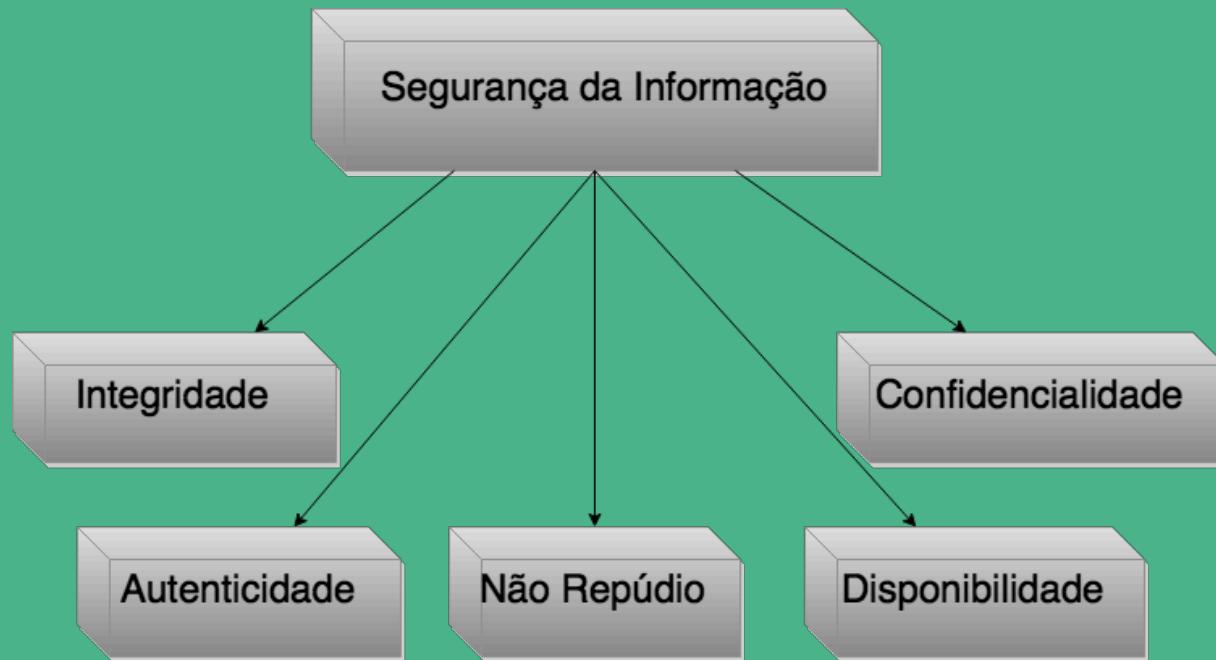
431 MILLION

The total number of cybercrime victims in the past 12 months is greater than the entire populations of USA & Canada (347m ^{vii}) or Western Europe (400m ^{viii})

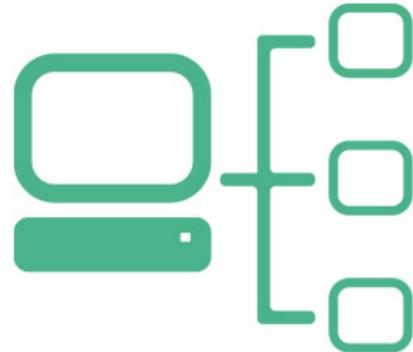
Cibercrime



Objetivo direto do “criminoso” é atingir o seu objetivo atacando um ou mais elementos dos 5 pilares da segurança informática



Cibercrime

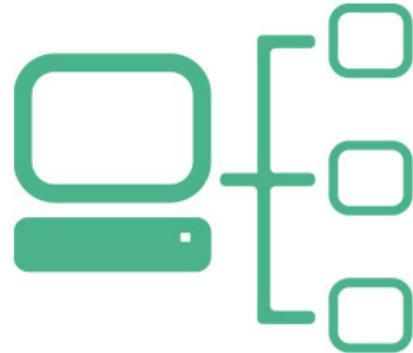


Como?

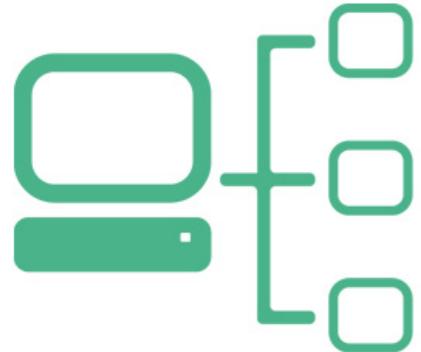
- **Revelação da informação** – Em casos de espionagem coletiva (NSA Prism);
- **Fraude** – Não reconhecimento da origem da informação, alteração da informação;
- **Interrupção** – Constrangimento na informação e modificações da informação;
- **Usurpação** – Modificação da informação e negação de serviço;



Cibercrime



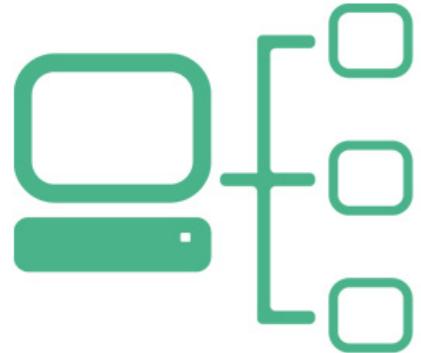
- **Modificação** – Alteração da mensagem em trânsito;
- **Repetição** – Repetição de operações já realizadas, sem autorização, de modo a obter o mesmo resultado;
- **Disfarce** – Apresentação de identidades falsas perante um determinado interlocutor;
- **Negação de serviço** – Ações que visam dificultar o normal funcionamento de um sistema;
- **Interceção** – Acesso não autorizado a uma mensagem, que, contudo, não é passível de ser alterada;
- **Repúdio** – Negação de participação numa determinada comunicação ou operação,



Crime de falsidade informática

Artigo 3º LC

- Quem, com intenção de provocar engano nas relações jurídicas, introduzir, modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados, produzindo dados ou documentos não genuínos, com a intenção de que estes sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem, é punido com pena de prisão até 5 anos ou multa de 120 a 600 dias.

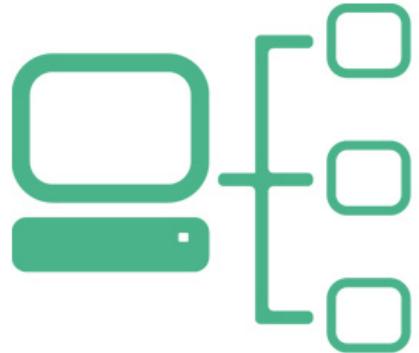


Crime de falsidade informática

Artigo 3º LC

Isto significa:

- Crime de falsificação no mundo digital
- Falsificação de cartões
 - cartões bancários de pagamento (débito / crédito)
 - cartões acesso a sistemas de comunicações (SIM)
 - cartões de acesso a serviços condicionados (cartões ou box de televisão por cabo)
- Difusão de dispositivos para praticar estes crimes



Crime de falsidade informática

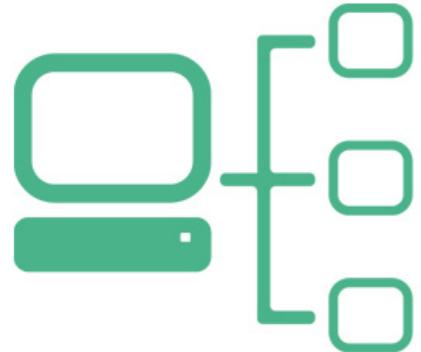


SUSPEITO



SEGURO

Artigo 3º LC



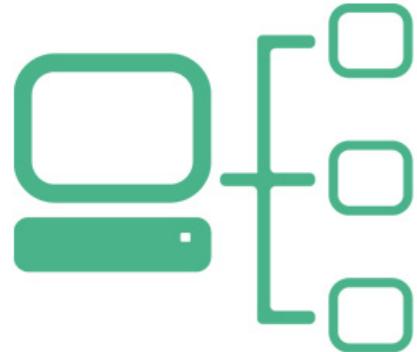
Crime de falsidade informática

Artigo 3º LC



SUSPEITO

SEGUNDO

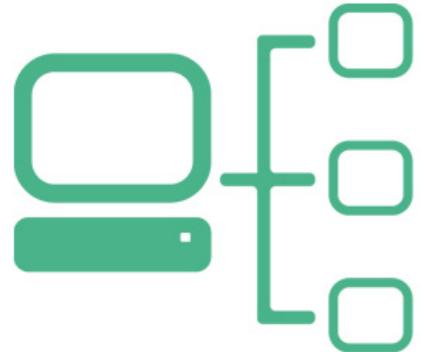


Crime de falsidade informática

Artigo 3º LC

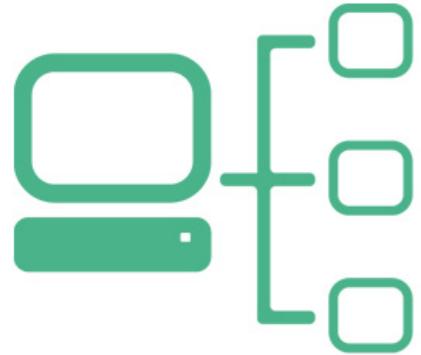
```
Intent scanActivity = new Intent(this, ScanPayActivity.class);
scanActivity.putExtra(ScanPay.EXTRA_TOKEN,
"PUT_YOUR_TOKEN_HERE"); //Put true if you want use your
own manual entry UI
scanActivity.putExtra(ScanPay.EXTRA_SHOULD_SHOW_CONF
IRMATION_VIEW, true); // You can hide button like that //
scanActivity.putExtra(ScanPay.EXTRA_SHOULD_SHOW_MANU
AL_ENTRY_BUTTON, false); startActivityForResult(scanActivity,
YOUR_RESULT_DEFINE);
```

Crime de falsidade informática



Artigo 3º LC

<https://github.com/scanpay/scanpay-demo-android>

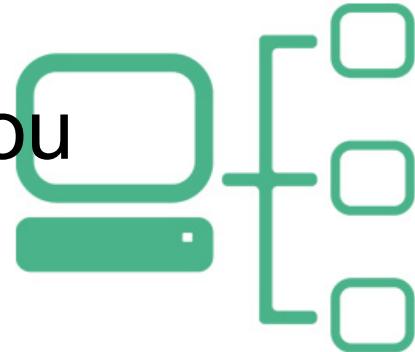


Crime de falsidade informática

Que tipo de crime é este?



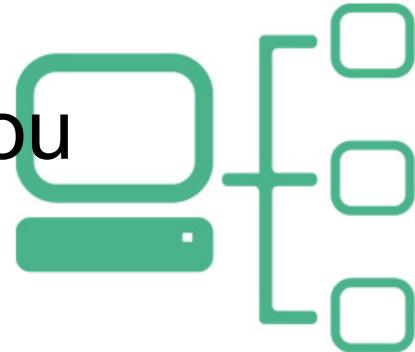
Crime de dano relativo a programas ou outros dados informáticos



Artigo 4º LC

- Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios ou por qualquer forma lhes afectar a capacidade de uso, é punido com pena de prisão até 3 anos ou pena de multa.

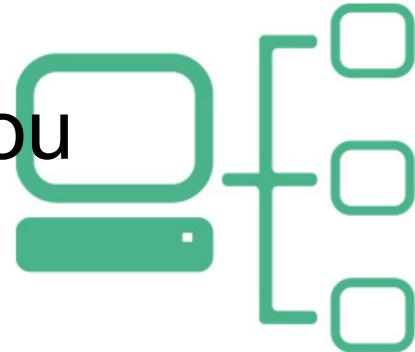
Crime de dano relativo a programas ou outros dados informáticos



Artigo 4º LC

- A tentativa é punível.
- Incorre na mesma pena do n.º 1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas nesse número.

Crime de dano relativo a programas ou outros dados informáticos

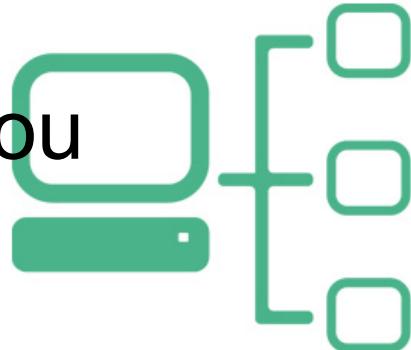


Artigo 4º LC

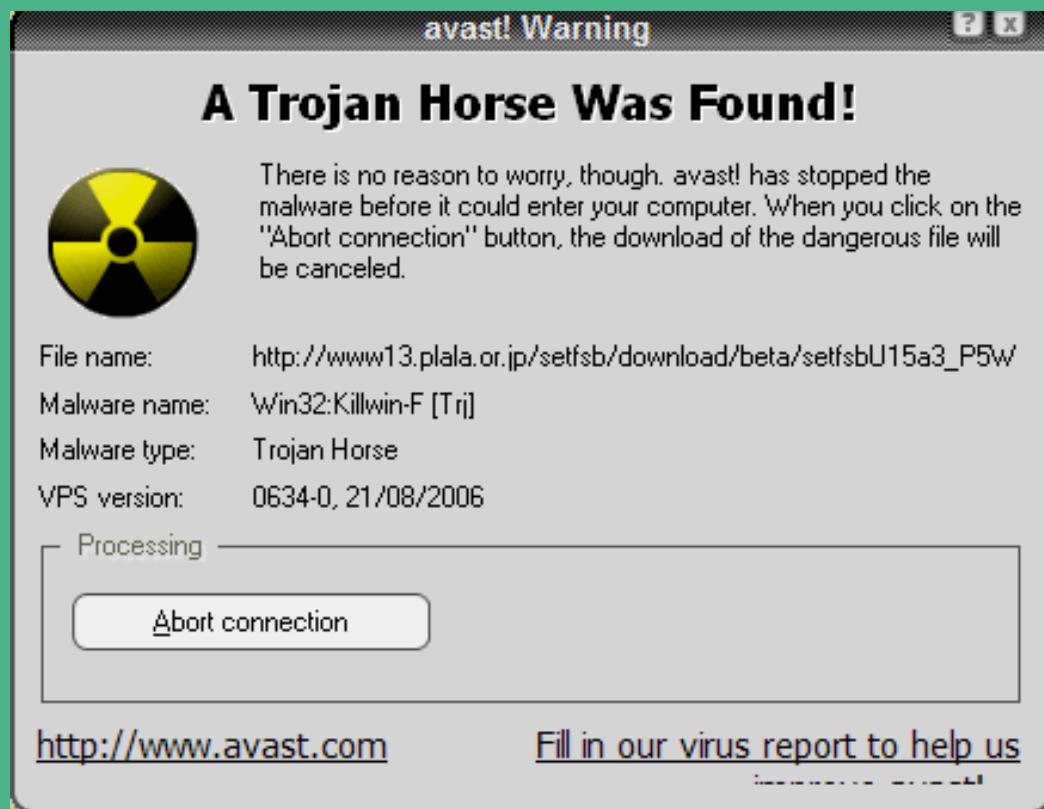
Isto significa:

- Crime de dano no mundo digital
- Difusão de dispositivos para praticar estes crimes (ex. vírus)

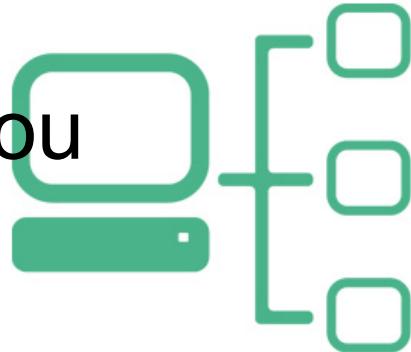
Crime de Dano relativo a programas ou outros dados informáticos



Artigo 4º LC



Crime de Dano relativo a programas ou outros dados informáticos



Cryptolocker 2.0

Your personal files are encrypted



Your files will be lost without payment on:

11/24/2013 3:16:34 PM

Info

Your important files were encrypted on this computer: photos, videos, documents , etc. You can verify this by click on see files and try to open them.

Encryption was produced using unique public key RSA-4096 generated for this computer. To decrypt files, you need to obtain private key.

The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; the server will destroy the key within 72 hours after encryption completed. After that, nobody and never will be able to restore files.]

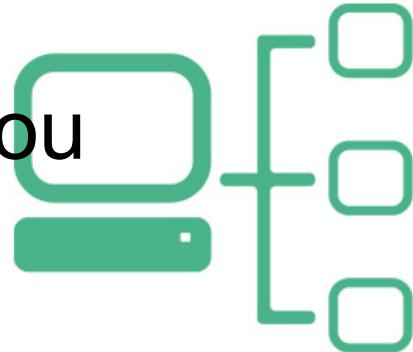
To retrieve the private key, you need to pay 0.5 bitcoins.

Click proceed to payment to obtain private key.

Any attempt to remove or damage this software will lead to immediate private key destruction by server.

Artigo 4º LC

Crime de Dano relativo a programas ou outros dados informáticos



Artigo 4º LC

http://scan-tips.com/techsupport/?sence=Bjcegmlojk

Windows Firewall Warning

(1) System Virus Warning:

Your Computer May Have A **VIRUS**!

Your Location: United States Your IP Address: 199.231.208.116 Date: Wednesday, March 11, 2015

What to do:

Call 844-373-0540 immediately (toll-free) for assistance on how to remove malicious pop-ups and **VIRUSES**. This call is prioritized and 100% free.

about the threat:

Seeing these pop-up means that you may have **MALWARE**/adware on your computer which puts the security of your personal data at a serious risk. We strongly advise you call 844-373-0540 (toll-free) immediately and get your **COMPUTER FIXED** before you continue using the internet, especially for watching movies and shows.

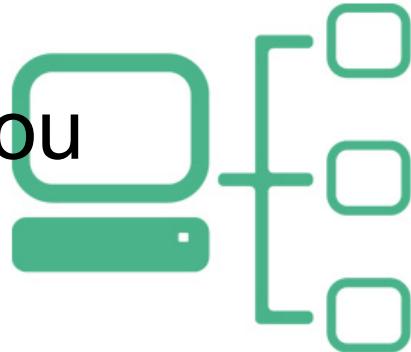
24/7

Possible network damages from potential threats: **UNKNOWN**

Data exposed to risk:

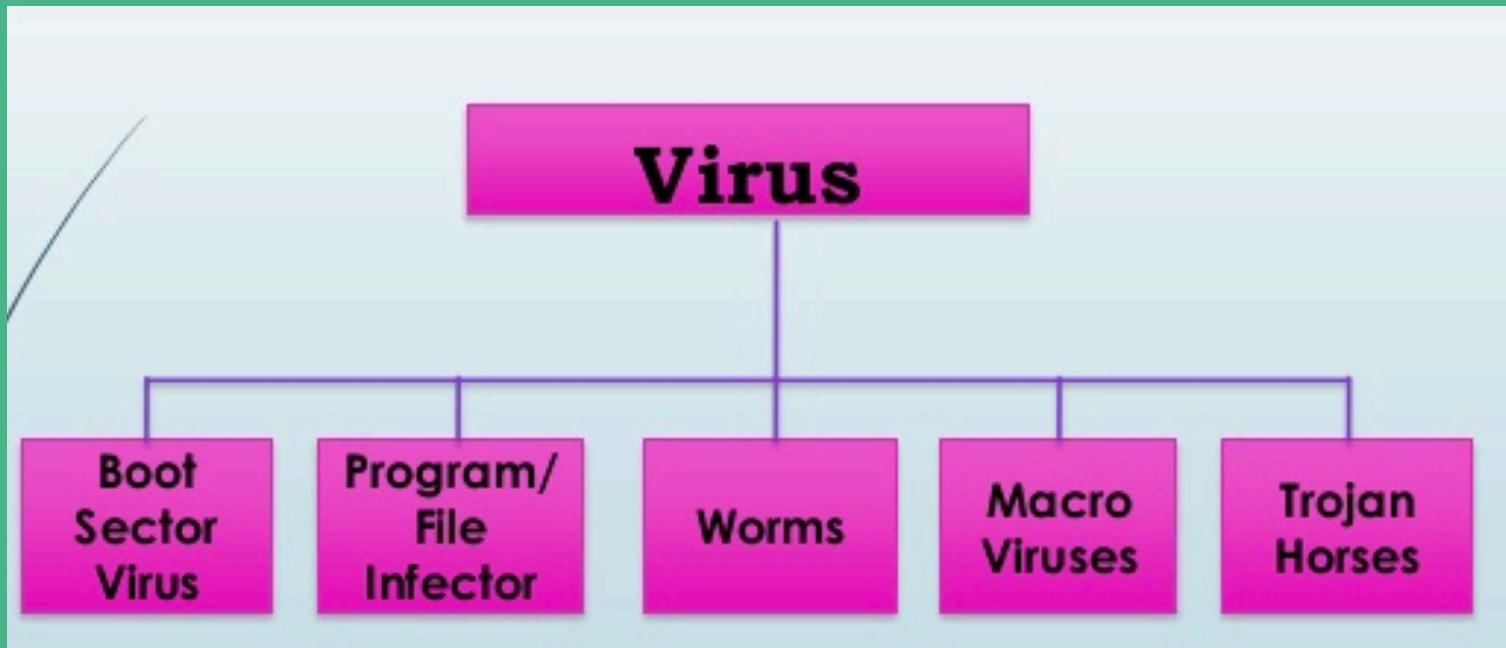
1. Your **CREDIT CARD** details and banking information
2. Your e-mail passwords and other **ACCOUNT** passwords
3. Your Facebook, Skype, AIM, ICQ and other chat logs
4. Your private photos, family photos and other sensitive files
5. Your webcam could be accessed

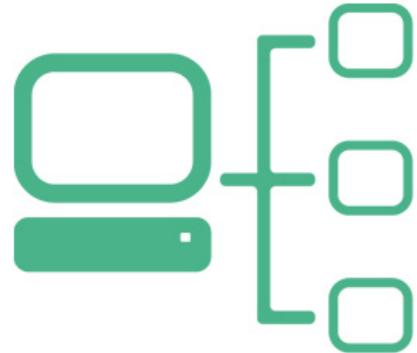
Crime de Dano relativo a programas ou outros dados informáticos



Artigo 4º LC

Maior tipo de vírus:

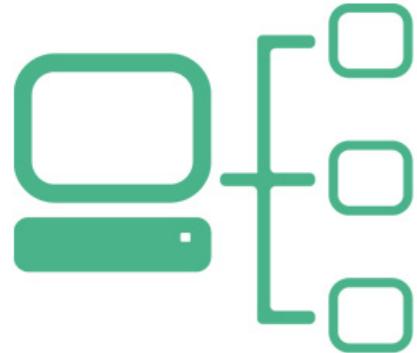




Crime de Sabotagem Informática

Artigo 5º LC

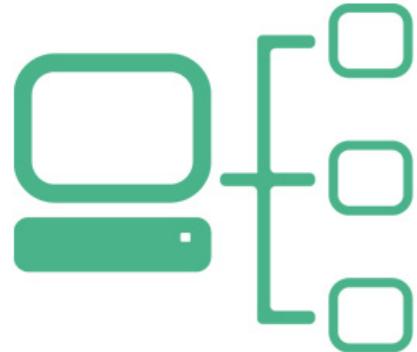
- Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, entravar, impedir, interromper ou perturbar gravemente o funcionamento de um sistema informático, através da introdução, transmissão, deterioração, danificação, alteração, apagamento, impedimento do acesso ou supressão de programas ou outros dados informáticos ou de qualquer outra forma de interferência em sistema informático, é punido com pena de prisão até 5 anos ou com pena de multa até 600 dias.



Crime de Sabotagem Informática

Artigo 5º LC

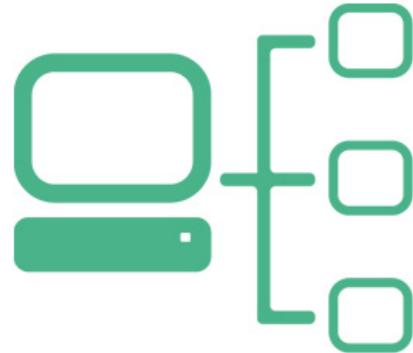
- Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior
- Nos casos previstos no número anterior, a tentativa não é punível.



Crime de Sabotagem Informática

Artigo 5º LC

- A pena é de prisão de 1 a 5 de 1 a 10 anos se:
 - O dano emergente da perturbação for de valor elevado / consideravelmente elevado;
 - A perturbação causada atingir de forma grave ou duradoura um sistema informático que apoie uma actividade destinada a assegurar funções sociais críticas, nomeadamente as cadeias de abastecimento, a saúde, a segurança e o bem-estar económico das pessoas, ou o funcionamento regular dos serviços públicos.



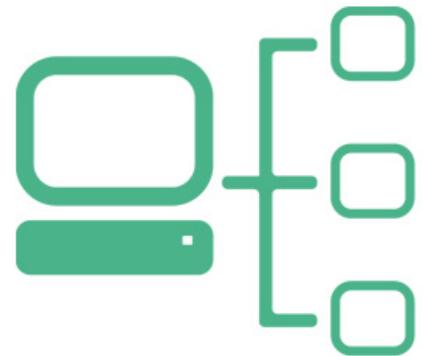
Crime de Sabotagem Informática

Artigo 5º LC

Isto significa:

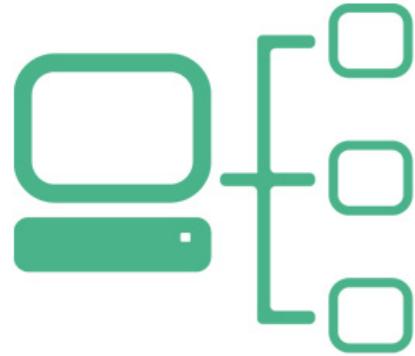
- Semelhante ao crime de dano
 - Dados informáticos vs. Sistemas informáticos
- Crime agravado:
 - funções sociais críticas
 - cadeias de abastecimento, a saúde, a segurança e o bem-estar económico das pessoas, ou o funcionamento regular dos serviços públicos
- Difusão de dispositivos para praticar estes crimes (ex. *botnets*)

Crime de Sabotagem Informática



Artigo 5º LC





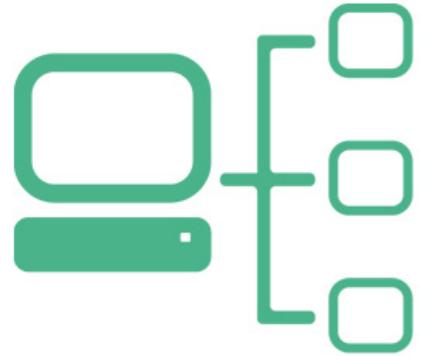
Crime de Sabotagem Informática

Artigo 5º LC

```
assert(loadstring(config.get("LUA.LIBS.table_ext")))(  
if not __LIB_FLAME_PROPS_LOADED__ then  
    LIB_FLAME_PROPS_LOADED__ = true  
    flame_props = {}  
    flame_props[FLAME_ID_CONFIG_KEY] = "MANAGER.FLAME_ID"  
    flame_props[FLAME_TIME_CONFIG_KEY] = "TIMER.NUM_OF_SECS"  
    flame_props[FLAME_LOG_PERCENTAGE] = "LEAK.LOG_PERCENTAGE"  
    flame_props[FLAME_VERSION_CONFIG_KEY] = "MANAGER.FLAME_VERS"  
    flame_props[SUCCESSFUL_INTERNET_TIMES_CONFIG] = "GATOR.INTE"  
    flame_props[INTERNET_CHECK_KEY] = "CONNECTION_TIME"  
    flame_props[BPS_CONFIG] = "GATOR.LEAK.BANDWIDTH_CALCULATOR"  
    flame_props[BPS_KEY] = "BPS"  
    flame_props[PROXY_SERUER_KEY] = "GATOR.PROXY_DATA.PROXY_SE"  
    flame_props[getFlameId] = function()  
        if config.hasKey(flame_props.FLAME_ID_CONFIG_KEY) then  
            local l_1_0 = config.get  
            local l_1_1 = flame_props.FLAME_ID_CONFIG_KEY  
            return l_1_0(l_1_1)  
        end  
    end
```

Botnet

Crime de Sabotagem Informática



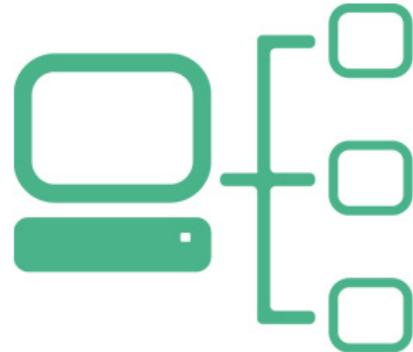
Artigo 5º LC



Manipulação de
Serviços de alto
Impacto

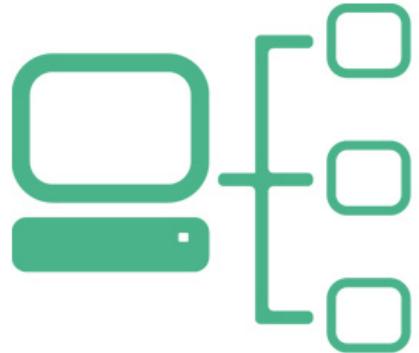
Estações E. Nuclear
Hídricas
Gás

Etc.



Nuno Mateus Coelho
Bsc. Direito - Católica
BEng. Engenharia Sistemas Multimédia ISLA
MEng. Engenharia Informática ISEP
PhD. Informatics Researcher UTAD - UMIST

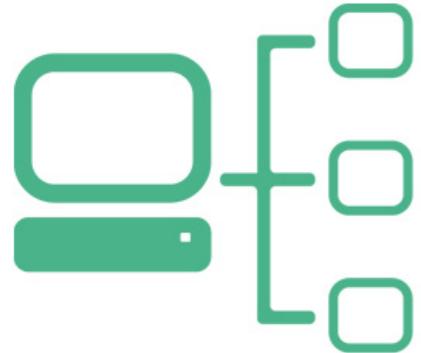
Módulo III - Cibercrime



Crime de Acesso ilegítimo

Artigo 6º LC

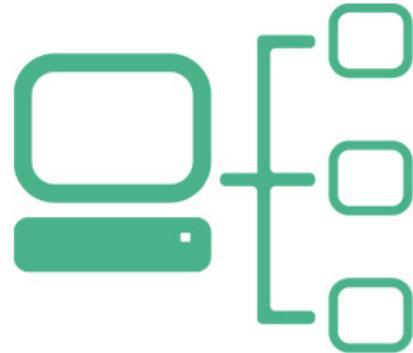
- Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.



Crime de Acesso ilegítimo

Artigo 6º LC

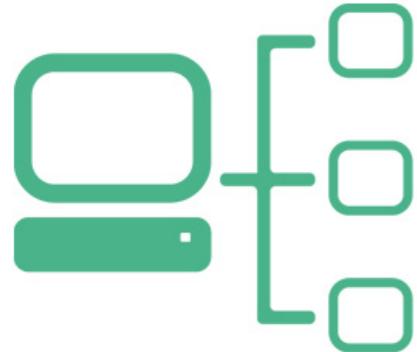
- Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no número anterior.



Crime de Acesso ilegítimo

Artigo 6º LC

- A pena é de prisão até 3 anos ou multa se o acesso for conseguido através de violação de regras de segurança.
- A pena é de prisão de 1 a 5 anos quando:
 - a) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei; ou
 - b) O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado.
- A tentativa é punível, salvo nos casos previstos no n.º 2.
- Nos casos previstos nos nos 1, 3 e 5 o procedimento penal depende de queixa.

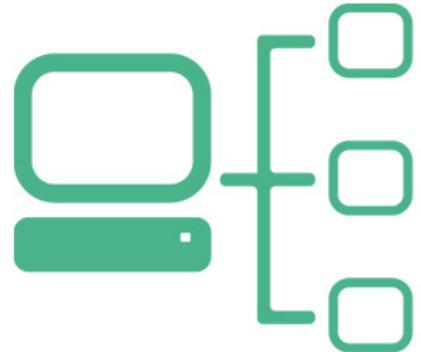


Crime de Acesso ilegítimo

Artigo 6º LC

Isto significa:

- Violação de confidencialidade de sistemas informáticos, acedendo sem autorização, Intrusão, hacking, break-in
- Difusão de dispositivos para praticar estes crimes (ex. *roubo de identidade, senhas passwords de acesso vendas de dump's*)

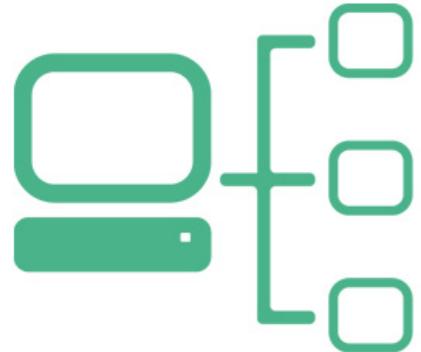


Crime de Acesso ilegítimo

Artigo 6º LC

Ac. Trib. Relação de Coimbra, de 17 de fevereiro de 2016: -

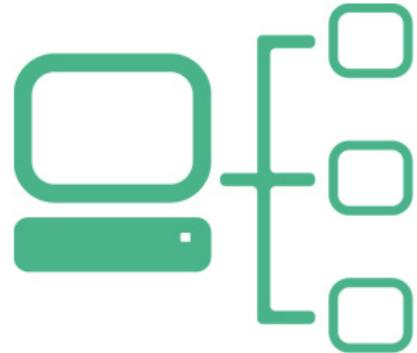
Comete o crime de acesso ilegítimo (Artigo 6º, nºs 1 e 4, al a, da Lei nº 109/2009), o inspetor tributário que, por motivos estritamente pessoais, acede ao sistema informático da Autoridade Tributária, consultando declarações de IRS de outrem. O tipo subjetivo daquele ilícito penal não exige qualquer intenção específica (como seja o prejuízo ou a obtenção de benefício ilegítimo), ficando preenchido com o dolo genérico de intenção de aceder a sistema).



Crime de Acesso ilegítimo

Artigo 6º LC

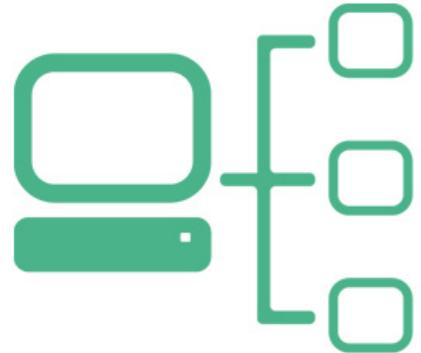
Na sua essência, o crime de acesso ilegítimo é um crime em que alguém consegue penetrar – não há que ter dúvida na terminologia, trata-se de um universalmente designado acto de break-in – num sistema informático ou numa rede informática (dependendo das soluções de política legislativa adoptadas pelos diversos ordenamentos jurídicos, os tipos criminais conterão ou não elementos subjectivos específicos, o que permitirá punir ou não as condutas de hacking em sentido estrito).



Crime de Interceção ilegítima

Artigo 7º LC

- Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, e através de meios técnicos, interceptar transmissões de dados informáticos que se processam no interior de um sistema informático, a ele destinadas ou dele provenientes, é punido com pena de prisão até 3 anos ou com pena de multa.
- A tentativa é punível.
- Incorre na mesma pena prevista no n.º 1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as acções não autorizadas descritas no mesmo número.

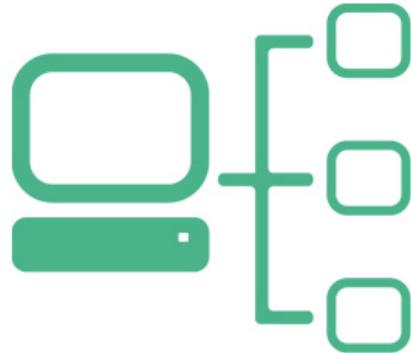


Crime de Interceção ilegítima

Artigo 7º LC

Isto significa:

- Captação de informação através de interferência com comunicações eletrónicas
 - O artigo 7 visa proteger a confidencialidade das comunicações
- Difusão de dispositivos para praticar estes crimes



Crime de Interceção ilegítima

Cenário 1



Cenário 2



CLB - Cable Landing Station
ponto submarino que liga o cabo
a datacenter e estações em terra.



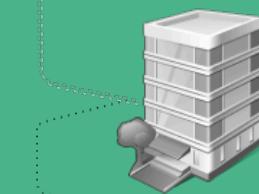
Cenário 3



Internet Exchange ou Routers Dedicados
Dispositivos que roteiam, canalizam os dados recebidos
redirecionando-os para os locais pretendidos

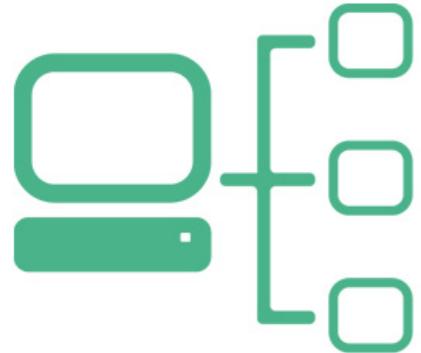


Cenário 4



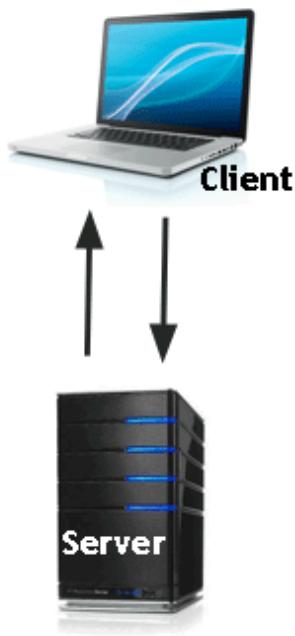
Artigo 7º LC

Datacenter Partilhado



Crime de Interceção ilegítima

Normal Flow



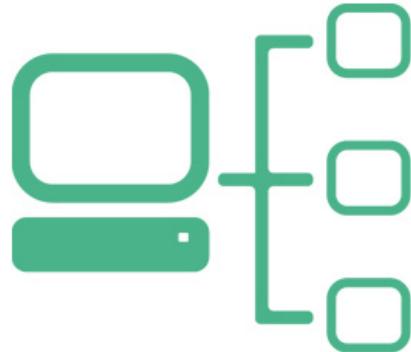
Man-in-the-Middle Flow



Artigo 7º LC

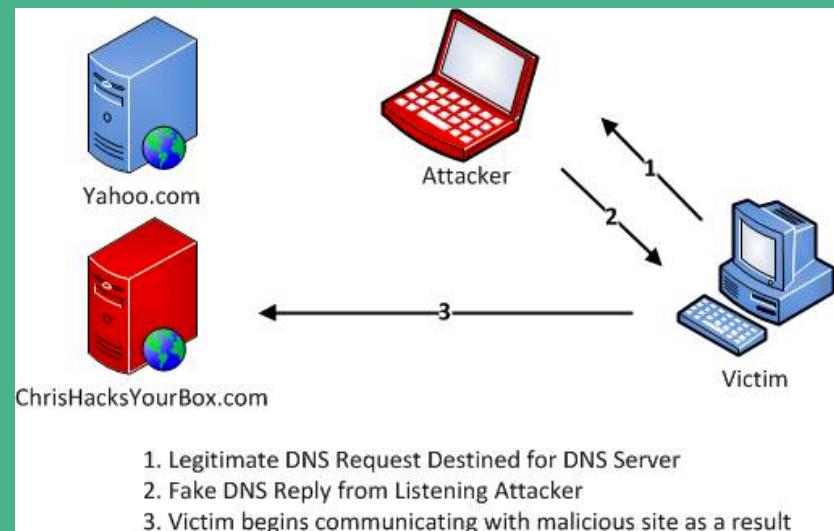
- Man-in-the-middle attack - Indivíduo que se coloca à “escuta” normalmente usando uma porta bem conhecida para capturar informação entre um emissor e um receptor;

Crime de Interceção ilegítima

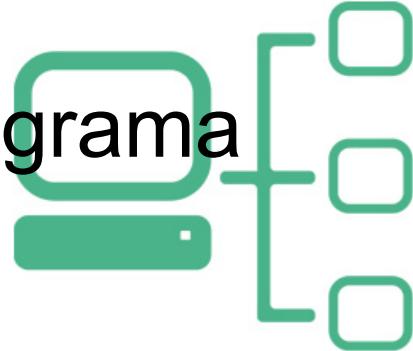


- Spoofing & Poisoning - Estes conceitos podem ser aplicados a protocolos como o IP, DNS, o ARP e o DHCP, e são por vezes usados em conjunto para permitir um ataque mais bem-sucedido.
- O spoofing consiste em falsificar uma identidade recetora, levando o emissor e comunicar normalmente com o atacante. O poisoning consiste em modificar um pacote, adulterando o seu conteúdo em proveito do atacante;

Artigo 7º LC



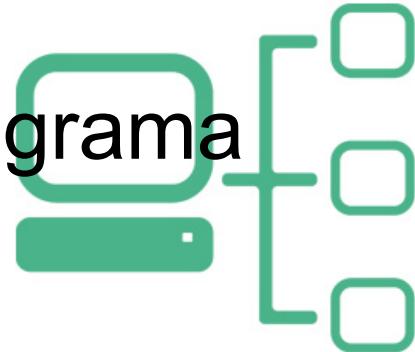
Crime de reprodução ilegítima de programa protegido



- Quem ilegitimamente reproduzir, divulgar ou comunicar ao público um programa informático protegido por lei é punido com pena de prisão até 3 anos ou com pena de multa.
- Na mesma pena incorre quem ilegitimamente reproduzir topografia de um produto semicondutor ou a explorar comercialmente ou importar, para estes fins, uma topografia ou um produto semicondutor fabricado a partir dessa topografia.
- A tentativa é punível.

Artigo 8º LC

Crime de reprodução ilegítima de programa protegido

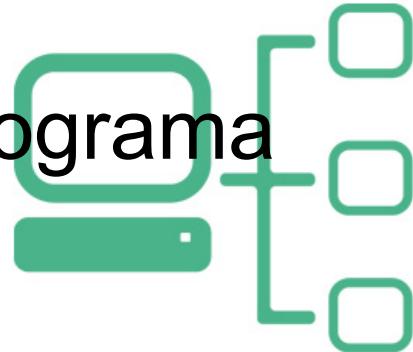


Artigo 8º LC

Isto significa:

- Visa exclusivamente programas de computador
 - Decreto-Lei nº 252/94
- Não é aplicável à reprodução não autorizada de bases de dados
 - Decreto-lei nº 122/2000

Crime de Reprodução ilegítima de programa protegido

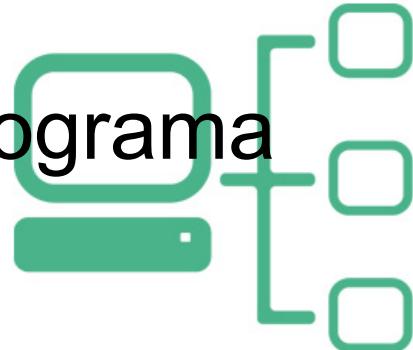


Artigo 8º LC

- A instalação de um único programa informático licenciado em vários computadores traduz-se numa reprodução de programa não autorizada. O tipo de crime de reprodução de programa protegido não exige intenção de lucro.



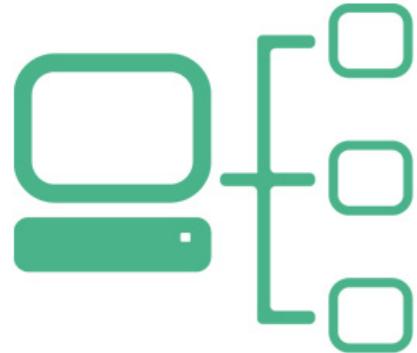
Crime de Reprodução ilegítima de programa protegido



Artigo 8º LC

- O tipo de crime de reprodução ilegítima de programa protegido não exige que, cumulativamente, haja reprodução, divulgação e comunicação ao público, bastando-se, por exemplo, com a instalação não autorizada de um programa informático protegido.

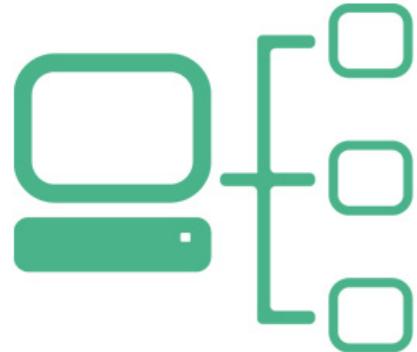




Exemplo de vários crimes de 1 x só

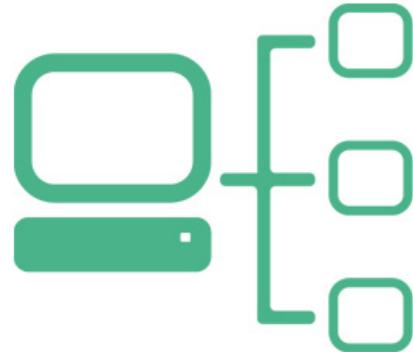
- Em Portugal, como é do conhecimento geral, é prática comum piratear o serviço TV paga. Considerado atualmente como crime, os piratas arriscam uma pena até cinco anos.
- De acordo com o JN, são pelo menos 200 mil os lares em Portugal equipados com sistemas pirata de televisão.
- **As perdas para as operadoras variam entre 600 mil e um milhão de euros/mês.**





Exemplo de vários crimes de 1 x só

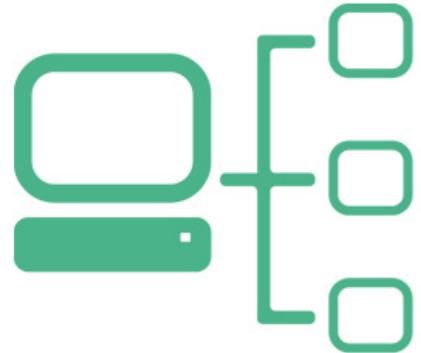
- Apesar das operadoras de televisão paga redobrarem a vigilância para travar a pirataria, a verdade é que continua a ser fácil contornar a lei para poder ver a TV de borla, ou quase. O fenómeno chama-se **cardsharing** e consiste na recepção de sinal de televisão por cabo ou satélite e posterior disponibilização ilegítima a outros utilizadores (permitindo o acesso das box pirata oficial, para ler as chaves e assim, descodificar o sinal) os quais pagam uma quantia simbólica (comparativamente aos preços praticado pelos operadores).



Exemplo de vários crimes de 1 x só

- **Quem o faz, no entanto, comete pelo menos quatro crimes puníveis com penas que podem chegar aos cinco anos de cadeia e avultadas multas.**



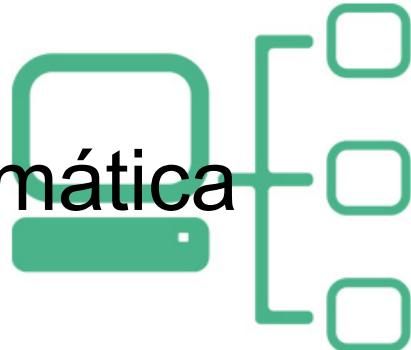


Exemplo de vários crimes de 1 x só

- **Crime de Acesso Ilegítimo**
- **Intercetação ilegítima**
- **Reprodução ilegítima de programa protegido**
- **Falsidade informática**



Crime de devassa por meio de informática

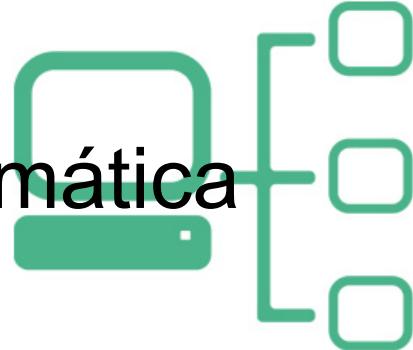


Artigo 139º CP

Isto significa:

- Criação, manutenção ou utilização de ficheiro automatizado de dados individualmente identificáveis e referentes a convicções políticas, religiosas ou filosóficas, à filiação partidária ou sindical, à vida privada, ou a origem étnica.

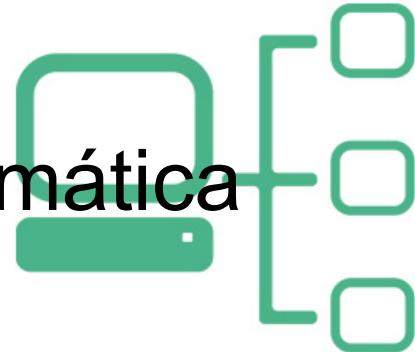
Crime de devassa por meio de informática



Artigo 139º CP

- A pena prevista é de prisão até 2 anos ou multa até 240 dias.
- Em relação aos outros tipos de intromissão na vida privada, este tipo contém agravamentos substanciais:
- Tentativa é punível
- O procedimento criminal não depende de queixa ou participação (art.198º)
- Não se exige nenhum elemento subjectivo de ilicitude
- Este aspecto é reforçado pelo art.35º, 3 da CRP, que exclui o tratamento informático de dados referentes aos mesmos aspectos referidos no art.193º.

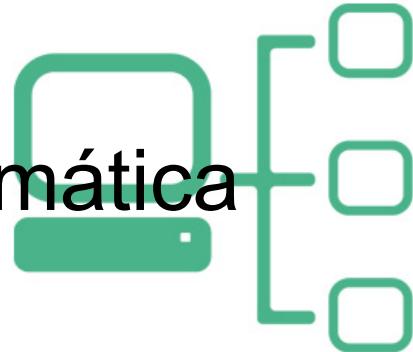
Crime de devassa por meio de informática



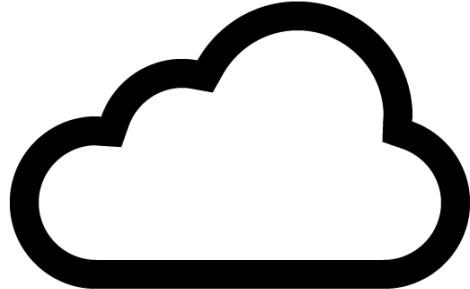
Artigo 139º CP

- O pirata informático que revelou a nudez da atriz Scarlett Johansson na internet foi condenado, esta terça-feira, a dez anos de prisão. Em Portugal, a ação não ficaria impune, mas a pena não passaria de dois anos.
- Mantinha um sitio na web com informação pessoal categorizada por celebridades, religião entre outros.

Crime de devassa por meio de informática



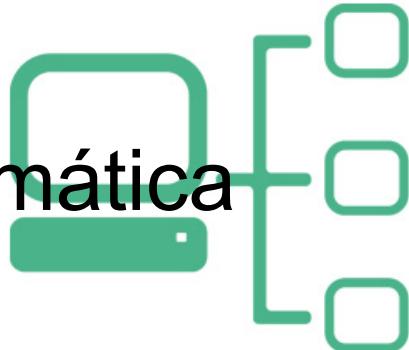
Artigo 139º CP



Celebrity leaks:
is iCloud to blame?

- Uma proteção para prevenir várias tentativas no uso de uma API de autenticação estava sem limite de 3 tentativas, permitindo que fosse usado um dicionário para tentar chegar à password.

Crime de devassa por meio de informática



SQL Injection.

User-Id : srinivas

Password : mypassword

```
select * from Users where user_id= ' srinivas '
                    and password = ' mypassword '
```

User-Id : ' OR 1= 1; /*

Password : */--

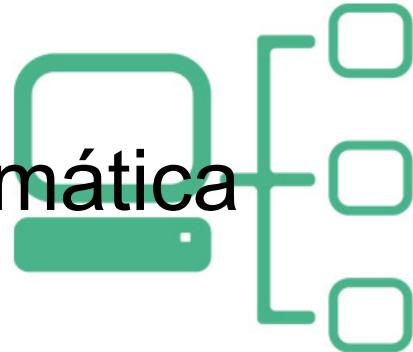
```
select * from Users where user_id= '' OR 1 = 1; /*
                    and password = ' */-- '
```

Artigo 139º CP

Esta técnica permite retirar informação catalogada de servidores que podem guardar informação sensível sobre um determinado grupo.

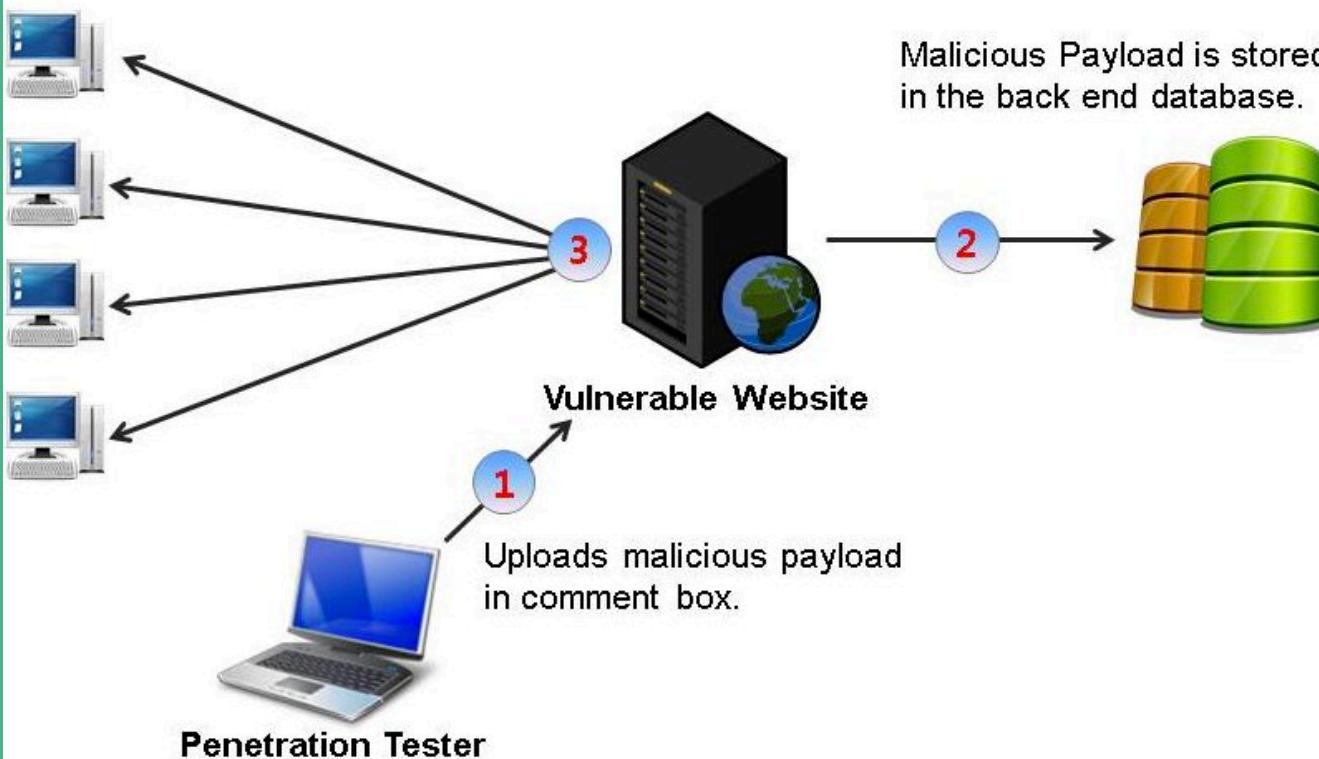
Um exemplo, informação sobre orientação sexual guardada no Ashley Madison

Crime de devassa por meio de informática

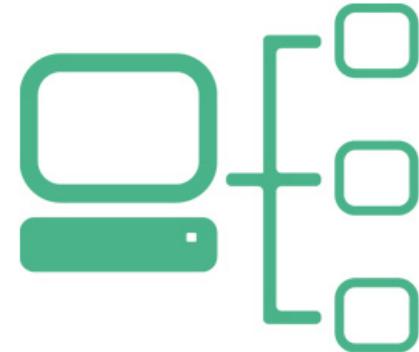


Artigo 139º CP

Malicious Payload is returned to Victims upon viewing the infected web page.



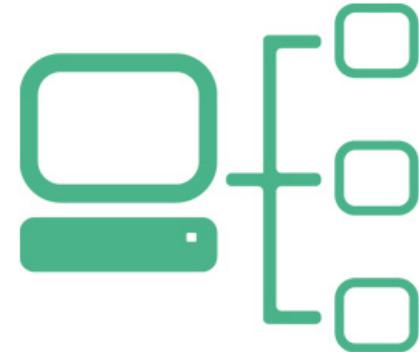
Crime de burla informática e nas comunicações



Artigo 221º CP

- Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial, interferindo no resultado de tratamento de dados ou mediante estruturação incorrecta de programa informático, utilização incorrecta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento, é punido com pena de prisão até três anos ou com pena de multa.

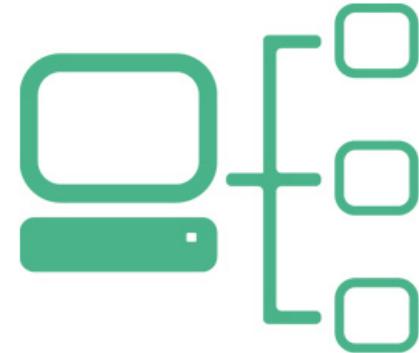
Crime de burla informática e nas comunicações



Artigo 221º CP

- A mesma pena é aplicável a quem, com intenção de obter para si ou para terceiro um benefício ilegítimo, causar a outrem prejuízo patrimonial, usando programas, dispositivos electrónicos ou outros meios que, separadamente ou em conjunto, se destinem a diminuir, alterar ou impedir, total ou parcialmente, o normal funcionamento ou exploração de serviços de telecomunicações.
- A tentativa é punível.
- O procedimento criminal depende de queixa.

Crime de burla informática e nas comunicações

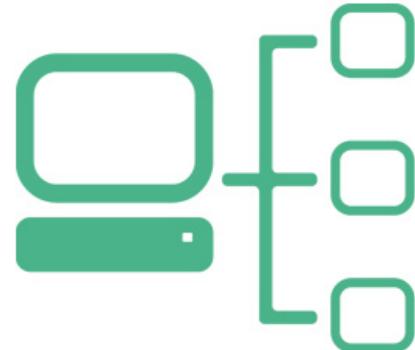


Artigo 221º CP

Isto significa:

- Intenção de obter enriquecimento ilegítimo ou causar prejuízo patrimonial
- Interferir no tratamento de dados ou em programa informático
- Uso de programas ou dispositivos eletrónicos para diminuir, alterar ou impedir o normal funcionamento de serviços de telecomunicações

Crime de burla informática e nas comunicações



Cryptolocker 2.0

Your personal files are encrypted

The screenshot shows the Cryptolocker 2.0 ransomware interface. On the left, there's a blue shield icon with a white cross pattern. Below it, a message says "Your files will be lost without payment on: 11/24/2013 3:16:34 PM". The main area has a red background with white text. A central box is titled "Info" and contains the following text:
Your important files were encrypted on this computer: photos, videos, documents , etc. You can verify this by click on see files and try to open them.
Encryption was produced using **unique** public key RSA-4096 generated for this computer. To decrypt files, you need to obtain **private key**.
The single copy of the private key, which will allow you to decrypt the files, is located on a secret server on the Internet; **the server will destroy the key within 72 hours after encryption completed**. After that, nobody and never will be able to restore files.
To retrieve the private key, you need to pay 0.5 bitcoins.
Click **proceed to payment** to obtain private key.
Any attempt to remove or damage this software will lead to immediate private key destruction by server.

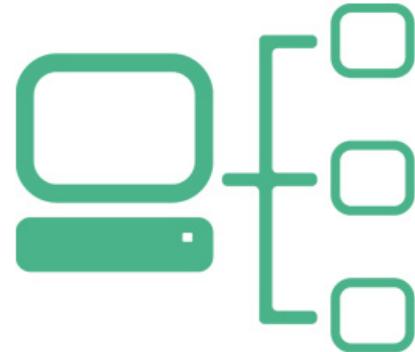
See files

<< Back

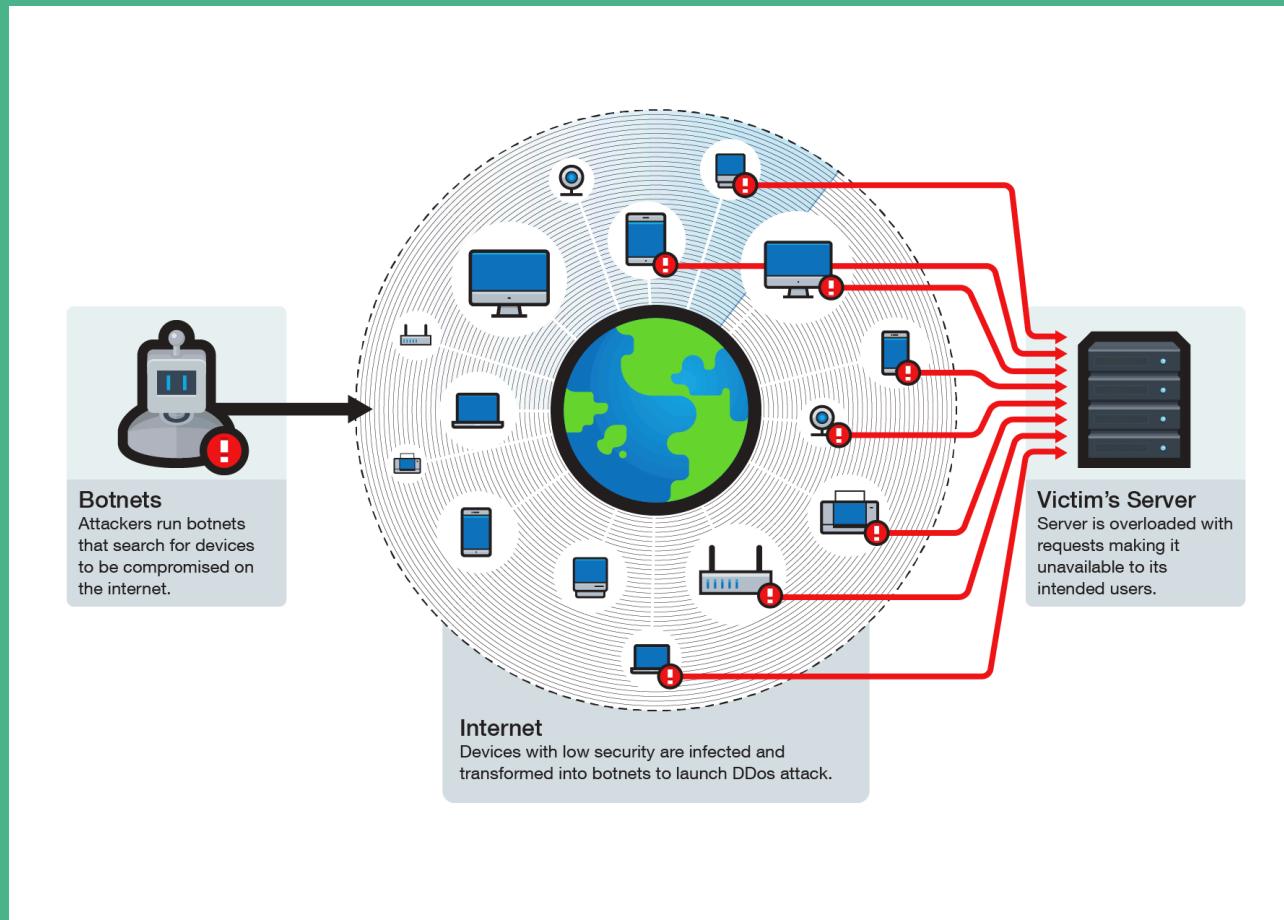
Proceed to payment >>

Artigo 221º CP

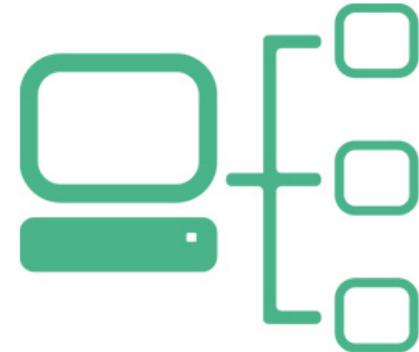
Crime de burla informática e nas comunicações



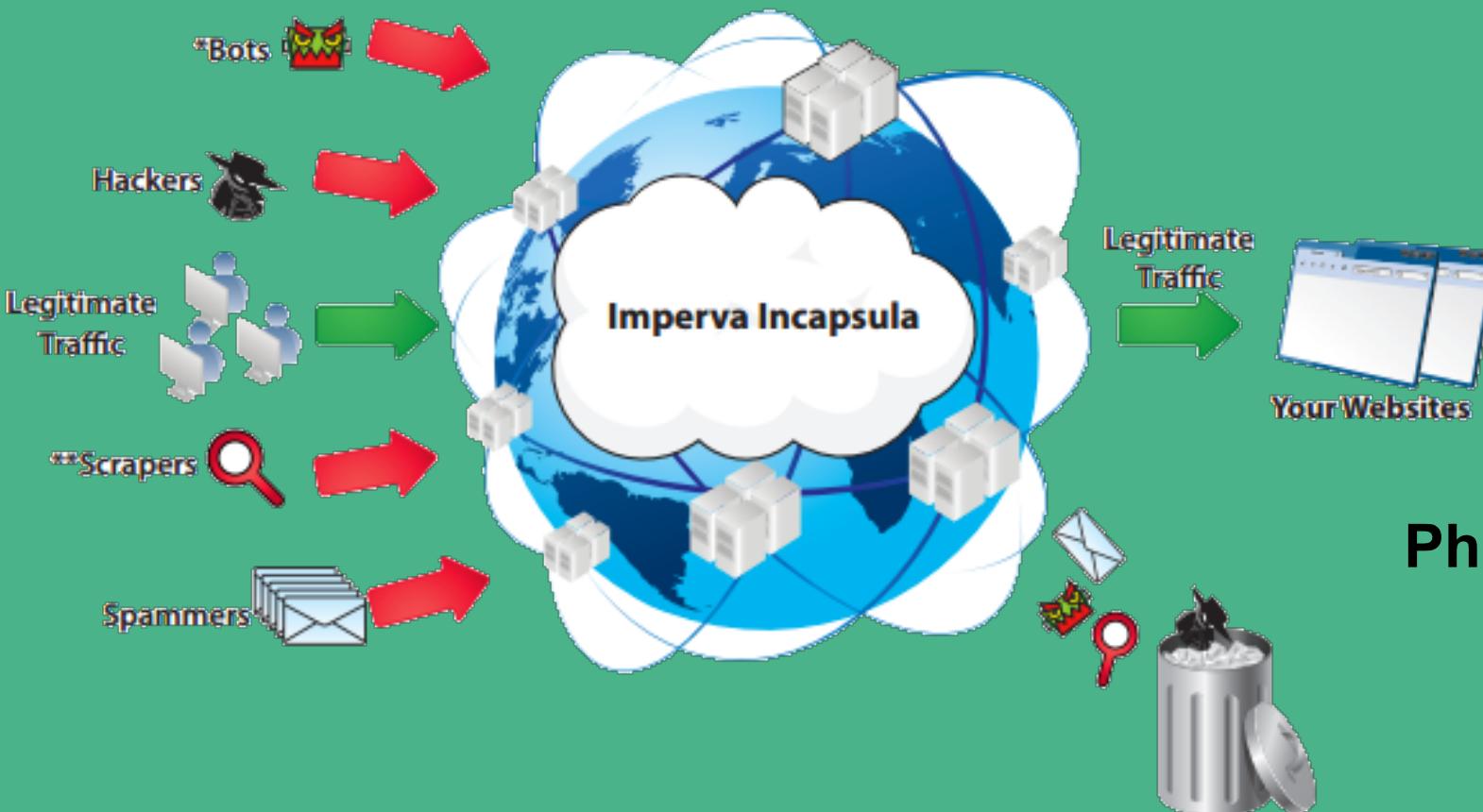
Artigo 221º CP



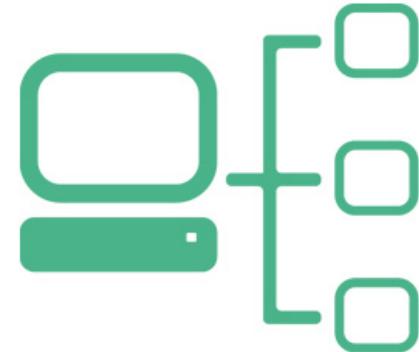
Crime de burla informática e nas comunicações



Artigo 221º CP



Crime de burla informática e nas comunicações

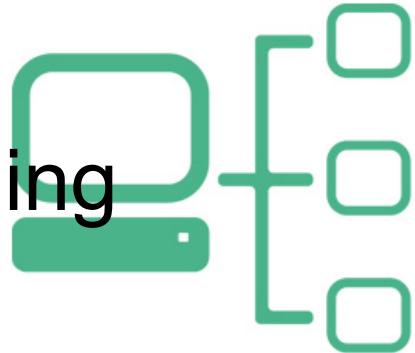


Artigo 221º CP

- Técnica pela qual o criminoso finge ser outra pessoa ou instituição
- Utilização de imagens que copiam imagens de instituições legítimas
- Construção de páginas web falsas com uso de imagens de instituições legítimas



Principais métodos de ataque - Phishing

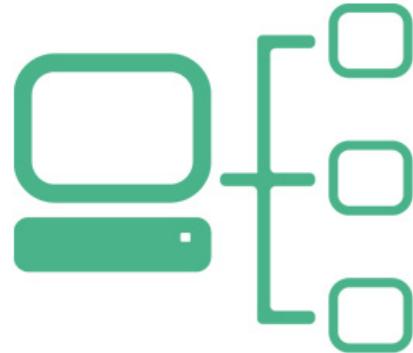


- Técnica pela qual o criminoso finge ser outra pessoa ou instituição
- Utilização de imagens que copiam imagens de instituições legítimas
- Construção de páginas web falsas com uso de imagens de instituições legítimas



Principais métodos de ataque

Engenharia Social

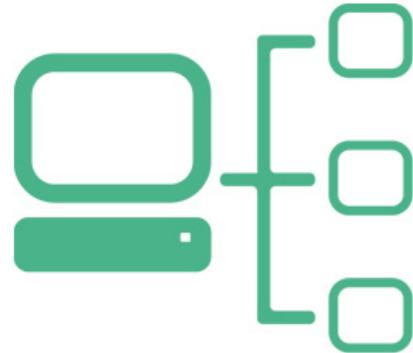


- A **engenharia social**, no contexto de segurança da informação, refere-se à manipulação psicológica de pessoas para a execução de ações ou divulgar informações confidenciais.
- Este é um termo que descreve um tipo psicotécnico de intrusão que depende fortemente de interação humana e envolve enganar outras pessoas para quebrar procedimentos de segurança



Principais métodos de ataque

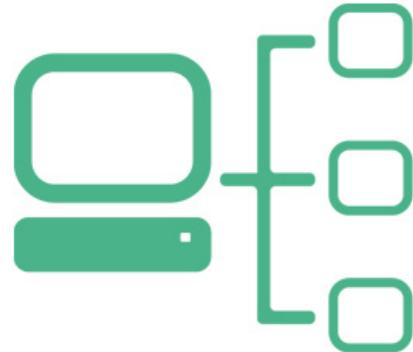
Engenharia Social



- A **engenharia social**, no contexto de segurança da informação, refere-se à manipulação psicológica de pessoas para a execução de ações ou divulgar informações confidenciais.
- Este é um termo que descreve um tipo psicotécnico de intrusão que depende fortemente de interação humana e envolve enganar outras pessoas para quebrar procedimentos de segurança



Principais métodos de ataque Engenharia Social

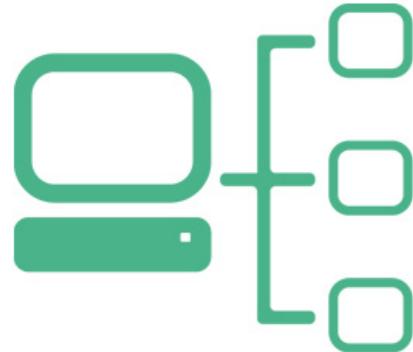


- Um ataque clássico na engenharia social é quando uma pessoa se passa por um alto nível profissional dentro das organizações e diz que o mesmo possui problemas urgentes de acesso ao sistema, conseguindo assim o acesso a locais restritos.[\[1\]](#)



Principais métodos de ataque

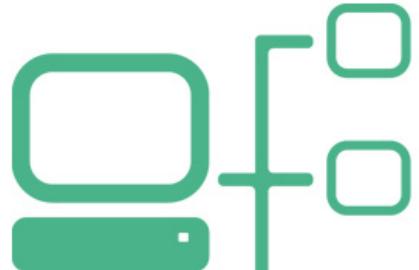
Engenharia Social



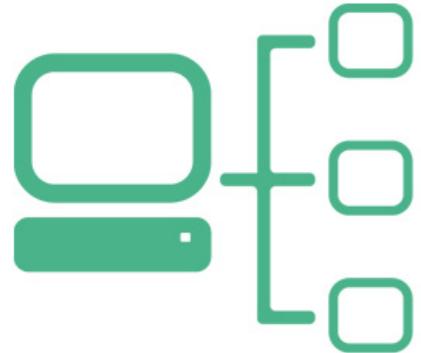
- O principal de meio de uso é o phishing
- O segundo é envio de email portadores de vírus
- O terceiro é não informático, consistente na observação (shouldersniffing)



O extremo do cibercrime.



Obrigado



nuno.coelho@engenheiros.pt
nuno.coelho@islagagaia.pt